POGLAVLJE 5

Integracija DNS-a i servisa Active Directory

Lekcija 1: Osnove razrešavanja DNS imena 110

Lekcija 2: Objašnjenje zona i načina njihovog konfigurisanja 114

Lekcija 3: Replikacija i transfer zona 124

Lekcija 4: Nadgledanje i rešavanje problema DNS-a za servis Active Directory 129

O ovom poglavlju

U Microsoft Windows 2000 Serveru, servis sistema imena domena (engl. *Domain Name System*, DNS) integrisan je u servis Active Directory i u njegovu implementaciju. U slučaju da Active Directory i Windows 2000 Server instalirate zajedno:

- DNS razrešavanje imena je neophodno da bi se mogli locirati Windows 2000 kontroleri domena. Servis Netlogon koristi podršku DNS servera za zapis resursa za servise (SRV) da bi omogućio registraciju kontrolera domena u DNS prostoru imena domena.
- Servis Active Directory može da se koristi za smeštaj, integrisanje i replikaciju zona.

Ovo poglavlje upoznaje vas sa zonama i postupkom razrešavanja DNS imena. U njemu se takođe razmatraju prednosti korišćenja zona integrisanih u servis Active Directory, a obavićete i praktični rad koji se odnosi na postupak konfigurisanja zona. Na kraju, u ovom poglavlju razmatraju se replikacija i transfer zona, a saznaćete i kako se rešavaju problemi vezani za konfigurisanje DNS-a u servisu Active Directory.

Pre nego što počnete

Da biste uradili lekcije iz ovog poglavlja, morate da:

- Obavite instalaciju opisanu u odeljku „Uvodne napomene o knjizi”.
- Instalirate servis Active Directory prema uputstvima iz poglavlja 4.
- Imate iskustvo u korišćenju Microsoftovih upravljačkih konzola (MMC).

Lekcija 1: Osnove razrešavanja DNS imena

Servis DNS omogućava razrešavanje imena klijentima koji imaju sistem Windows 2000. Postupkom razrešavanja imena korisnici mogu da pristupe serverima na osnovu njihovih imena, umesto da koriste IP adrese koje se po pravilu teško pamte. Ova lekcija upoznaje vas sa postupkom razrešavanja imena.

Kada pređete ovu lekciju, moći ćete da:

- Objasnite postupak razrešavanja imena.

Predviđeno vreme za ovu lekciju je 10 minuta.

Razrešavanje imena

Razrešavanje imena (engl. *name resolution*) je postupak kojim se DNS imena prevode u IP adrese. To je slično traženju imena u telefonskom imeniku, u kome je ime pretplatnika povezano sa telefonskim brojem. Na primer, kada se povežete na sajt Microsofta, koristite ime *www.microsoft.com*. DNS razrešava *www.microsoft.com* u njegovu IP adresu: 207.46.130.149. Korelacija imena i IP adresa čuva se u DNS distribuiranoj bazi podataka.

Način IP adresiranja

IP adresa je identifikator svakog host računara koji komunicira koristeći TCP/IP protokol. Svaka 32-bitna IP adresa interno se deli na dva dela – mrežni identifikator i matični identifikator.

- Mrežni identifikator, poznat i kao mrežna adresa, definiše jedinstveni segment mreže u okviru šire TCP/IP Internet-mreže (mreže sastavljene od više mreža). Svi sistemi koji se priključe na mrežu i dele pristup toj istoj mreži, u svojoj kompletnoj IP adresi imaju zajednički mrežni identifikator. Njega svaka mreža takođe koristi kao svoj jedinstveni identifikator unutar šireg Internet umreženja.
- Matičnim identifikatorom, koji je poznat i kao host adresa, definisan je TCP/IP čvor (radna stanica, server, usmerivač, ili neki drugi TCP/IP uređaj). Matični identifikator svakog uređaja jedinstveno definiše pojedine sisteme unutar njihove mreže.

Primer 32-bitne IP adrese:

```
10000011 01101011 00010000 11001000
```

Da bi se IP adresiranje uprostilo, IP adrese se iskazuju u decimalnim brojevima razdvojenim tačkama. 32-bitna IP adresa je izdeljena na četiri 1-bitna okteta od po osam elemenata. Ovi okteti se prevode u decimalne brojeve (brojčani sistem sa bazom 10) koji su razdvojeni tačkama. U skladu sa tim, prethodni primer IP adrese preveden u decimalne brojeve razdvojene tačkama izgleda ovako: 131.107.16.200.

U primeru ove IP adrese (131.107.16.200), ukoliko prva dva broja (131.107) IP adrese označavaju onaj deo adrese koji je mrežni identifikator, onda zadnja dva broja (16.200) IP adrese označavaju onaj deo adrese koji je matični identifikator.

Upiti za traženje

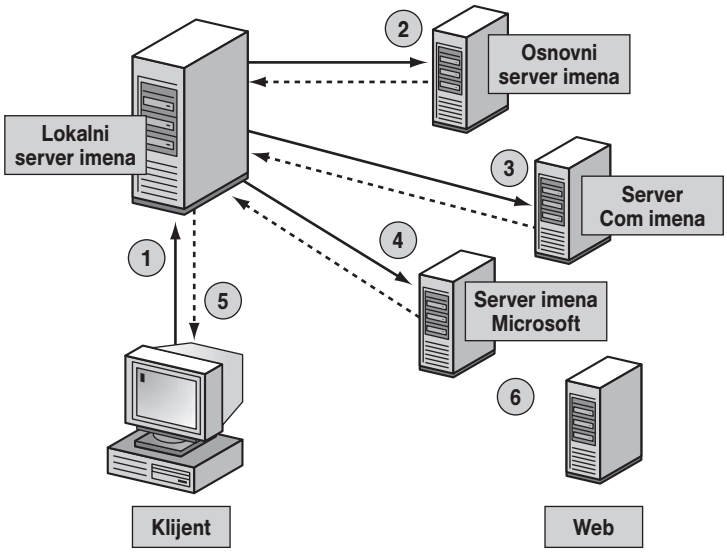
Serveri DNS imena rešavaju upite za traženje unapred i upite za traženje unazad. Upit za *traženje unapred* (engl. *forward lookup*) razrešava ime u IP adresu. Upit za *traženje unazad* (engl. *backward lookup*) prevodi IP adresu u ime. Server imena može da raz-

rešava upite u zoni za koju ima ovlašćenje. Ukoliko server imena ne može da razreši upit, prosleđuje ga ostalim serverima imena koji mogu da ga razreše. Server imena kešira rezultate upita da bi smanjio DNS saobraćaj na mreži.

Traženje unapred

Pri razrešavanju imena, DNS servis radi na principu klijent/server. Da bi razrešio upit za traženje unapred, klijent dostavlja upit lokalnom serveru imena. On rešava upit ili ga prosleđuje drugom serveru imena na rešavanje.

Na slici 5.1 predstavljen je klijent izvan zone microsoft.com, koji zadaje upit serveru imena za IP adresu *www.microsoft.com*.



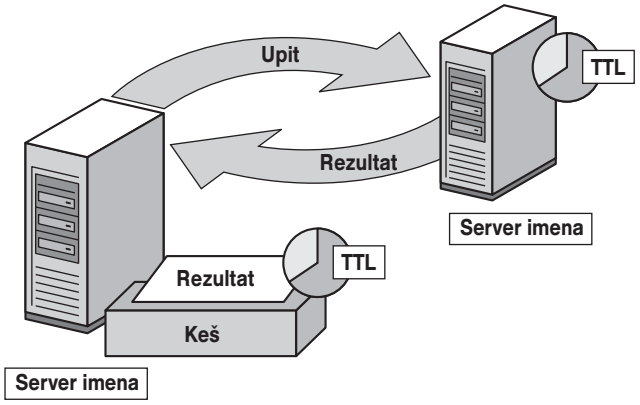
Slika 5.1 Razrešavanje upita za traženje unapred

Brojevi na slici označavaju sledeće aktivnosti:

1. Klijent zadaje svom lokalnom serveru imena upit za traženje unapred za ime *www.microsoft.com*.
2. Na osnovu tog upita, lokalni server imena proverava bazu podataka svoje zone da bi utvrdio da li sadrži korelaciju ime – IP adresa. Lokalni server imena nema ovlašćenje za domen microsoft.com, tako da on upit prosleđuje jednom od osnovnih DNS servera zahtevajući razrešavanje host imena. Osnovni server imena odgovara upućivanjem imena com na server.
3. Lokalni server imena šalje zahtev serveru imena com, koji odgovara upućivanjem imena Microsoft na servere.
4. Lokalni server imena upućuje zahtev serveru imena Microsoft. Server imena Microsoft prima zahtev. Pošto server imena Microsoft ima ovlašćenje za taj deo prostora imena domena, on vraća IP adresu za *www.microsoft.com* lokalnom serveru imena.
5. Server imena upućuje klijentu IP adresu za *www.microsoft.com.*
6. Razrešavanje imena je završeno i klijent može da pristupi *www.microsoft.com.*

Keširanje servera imena

Kada server imena obrađuje upit, ponekad je potrebno da zada nekoliko upita dok ne dobije odgovor. Sa svakim upitom, server imena otkriva druge servere imena koji imaju ovlašćenje za neki deo prostora imena domena. Server imena kešira te rezultate upita da bi smanjio mrežni saobraćaj (slika 5.2).



Slika 5.2 Keširanje rezultata upita

Kada server imena dobije rezultat upita, dolazi do sledećih postupaka:

1. Server imena kešira rezultat upita za određeni period vremena, koji se naziva rok trajanja (engl. *Time to Live*, TTL).

Napomena Zona koja šalje rezultat upita definiše TTL, koji možete da konfigurišete koristeći DNS konzolu. Podrazumevana vrednost za TTL je 60 minuta.

---

2. Kada je server imena keširao rezultat upita, počinje odbrojavanje TTL-a.
3. Kada istekne TTL, server imena briše rezultat upita iz svoje keš memorije.

Keširanje rezultata omogućava serveru imena da brzo reši druge upite upućene istom delu prostora imena domena.

Napomena Manje vrednosti TTL-a koristite ukoliko želite da podaci o prostoru imena domena na mreži budu što aktuelniji. Kraći TTL, međutim, *povećava* opterećenje servera imena. Duži TTL smanjuje vreme razrešavanja. Međutim, ukoliko dođe do promene (na primer, promena u podmreži), klijent neće dobiti ažurirane podatke sve dok ne istekne TTL i novi upit bude upućen tom delu prostora imena domena.

Upit za traženje unazad

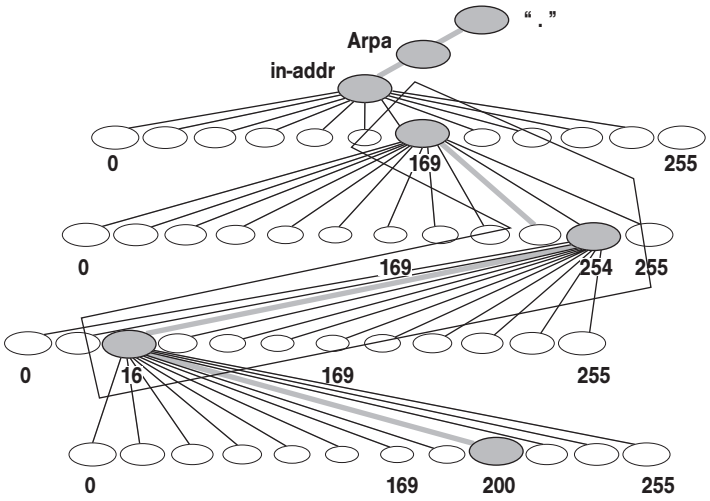
Upitom za traženje unazad za datu IP adresu pronalazite odgovarajuće ime. Alatke za rešavanje problema, na primer, program NSLOOKUP koji se aktivira sa komandne linije, koriste upite za traženje unazad da bi kao rezultat vratile imena glavnih računara. Pored toga, u nekim aplikacijama primenjuju se takve mere bezbednost koje se baziraju na mogućnosti povezivanja na imena, a ne na IP adrese.

Pošto je distribuirana DNS baza podataka indeksirana na osnovu imena a ne na osnovu IP adresa, upit za traženje unazad zahtevao bi iscrpno pretraživanje svakog imena domena. Da bi se ovaj problem prevazišao, kreiran je specijalni domen drugog nivoa nazvan *in-addr.arpa*.

Domen in-addr.arpa drži se istog hijerarhijskog principa imenovanja kao i ostali prostori imena domena; međutim, on se zasniva na IP adresama, a ne na imenima domena:

- Poddomeni dobijaju imena po brojevima iz IP adrese iskazane decimalnim brojevima koji su razdvojeni tačkama.
- Redosled okteta IP adrese je obrnut.
- Kompanije administriraju poddomene domena in-addr.arpa na osnovu dodeljene IP adrese i maske podmreže.

Na primeru na slici 5.3 vidi se kako je u domenu in-addr.arpa prikazana IP adresa 169.254.16.200. Kompanija kojoj je dodeljen adresni opseg od 169.254.16.0 do 169.254.16.255 sa maskom podmreže 255.255.255.0 imaće ovlašćenje za 16.254.169 in-addr.arpa domen.



Slika 5.3 Domen in-addr.arpa

Rezime lekcije

U ovoj lekciji naučili ste da je razrešavanje imena postupak kojim se imena prevode u IP adrese i da su podaci o vezivanju imena za odgovarajuće IP adrese smešteni u distribuiranoj DNS bazi podataka. Saznalii ste da DNS serveri imena rešavaju upite za traženje unapred, kao i šta se dešava kada klijent zada upit serveru imena za neku IP adresu. Naučili ste, takođe, o keširanju servera imena, kao i to da server imena kešira rezultate upita da bi se smanjio saobraćaj na mreži.

Pored upita za traženje unapred, DNS serveri imena rešavaju i upite za traženje unazad. Ova vrsta upita razrešava IP adresu i kao rezultat daje ime. Pošto je distribuirana DNS baza podataka indeksirana na osnovu imena a ne na osnovu IP adrese, kreiran je specijalni domen drugog nivoa pod nazivom in-addr.arpa. Ovaj domen se pridržava iste šeme hijerarhijskog imenovanja kao ostali prostor imena domena; on se, međutim, zasniva na IP adresama umesto na imenima domena.

Lekcija 2: Objašnjenje zona i načina njihovog konfigurisanja

DNS servis omogućava da DNS prostor imena bude podeljen u zone koje čuvaju podatke o imenima za jedan ili više DNS domena. Zona postaje ovlašćeni izvor podataka o svakom DNS imenu domena koji je obuhvaćen zonom. Ova lekcija upoznaje vas sa DNS zonama i načinom njihovog konfigurisanja.

Kada pređete ovu lekciju, moći ćete da:

- Prepoznate tipove zona.
- Navedete prednosti zona integrisanih sa servisom Active Directory.
- Objasnite delegiranje zona.
- Konfigurišete zone.
- Konfigurišete dinamički DNS (DDNS) za zonu.

Predviđeno vreme za ovu lekciju je 30 minuta.

Zone

U DNS servisu postoji opcija kojom prostor imena možete podeliti u jednu ili više zona, koje se onda mogu smeštati, distribuirati i replicirati na druge DNS servere. DNS prostor imena predstavlja logičku strukturu vaših mrežnih resursa, a DNS zone omogućavaju fizičko smeštanje tih resursa.

Planiranje zona

Prilikom odlučivanja o tome da li da DNS prostor imena podelite u dodatne zone ili ne, uzmite u obzir sledeće razloge za korišćenje dodatnih zona:

- Da li je potrebno da upravljanje delom vašeg DNS prostora imena delegirate na drugu lokaciju ili na drugo odeljenje unutar vaše organizacije?
- Da li je potrebno da jednu veću zonu podelite na manje zone, kako biste time opterećenje raspodelili na više servera, poboljšali efikasnost razrešavanja DNS imena, ili kreirali DNS okruženje koje je otpornije na greške?
- Da li je potrebno da prostor imena proširite jednovremenim dodavanjem brojnih poddomena, kao u slučaju otvaranja nove filijale firme ili sajta?

Ukoliko na jedno od ovih pitanja odgovorite potvrdno, verovatno bi trebalo da prostoru imena dodate novu zonu ili da prestruktuirate postojeće. Strukturu zona planirajte u skladu sa potrebama vaše firme.

Postoje dve vrste zona u pogledu načina pretraživanja: zone za traženje unapred i zone za traženje unazad.

Zone za traženje unapred

Zona za traženje unapred (engl. *forward lookup zone*) omogućava izvršavanje upita za traženje unapred. Na serverima imena morate da konfigurišete bar jednu zonu za traženje unapred, da bi DNS servis funkcionisao. Kada instalirate servis Active

Directory koristeći Active Directory Installation Wizard i dopustite da čarobnjak instalira i konfiguriše vaš DNS server, automatski se kreira zona za traženje unapred na bazi DNS imena koje ste dali serveru.

➤ **Da biste napravili novu zonu za traženje unapred:**

1. Pritisnite dugme Start, pokažite najpre na Programs, zatim na Administrative Tools, a nakon toga izaberite DNS.
2. Proširite prikaz DNS servera.
3. Pritiskom na desni taster miša najpre izaberite omotnicu Forward Lookup Zone, a zatim New Zone. Otvoriće se čarobnjak New Zone Wizard koji vas vodi kroz postupke kreiranja zone za traženje unapred. Čarobnjak vam omogućava sledeće opcije konfigurisanja: Zone Type (tip zone), Zone Name (ime zone), Zone File (datoteka zone) i Master DNS Server (glavni DNS server).

Zone Type

Možete da konfigurišete tri tipa zona:

- **Active Directory-integrated.** Zona integrisana u servis Active Directory je glavna kopija nove zone. Ta zona koristi servis Active Directory za skladištenje i repliciranje datoteka zone.
- **Standard primary.** Standardna primarna zona je glavna kopija nove zone koja se čuva u obliku tekstualne datoteke. Primarnu zonu administrirate i održavate na računaru na kome ste zonu kreirali.
- **Standard secondary.** Standardna sekundarna zona je duplikat postojeće zone. Sekundarne zone služe samo za čitanje i čuvaju se u obliku standardnih tekstualnih datoteka. Primarna zona mora biti konfigurisana tako da sama kreira sekundarnu zonu. Kada stvarate sekundarnu zonu, morate da odredite DNS server, koji se naziva glavni server (engl. *master server*), koji će podatke zone preneti serveru imena na kome se nalazi sekundarna zona. Sekundarnu zonu pravite da biste obezbedili redundantnost i da biste smanjili opterećenje servera imena na kome se nalazi datoteka baze podataka primarne zone.

Prednosti zona integrisanih u servis Active Directory

Zone integrisane u servis Active Directory preporučuju se za mreže koje koriste DNS za podršku servisa Active Directory, jer vam pružaju sledeće prednosti:

- Ažuriranje sa više glavnih primeraka (engl. *multimaster update*) i povećana bezbednost na bazi mogućnosti koje poseduje servis Active Directory.

U standardnom modelu zonskog skladištenja, DNS ažuriranja se obavljaju na bazi modela sa jednim glavnim primerkom (engl. *single master update model*). U takvom modelu, samo jedan ovlašćeni DNS server u zoni je određen da bude primarni izvor za tu zonu. Taj server održava glavni primerak zone u obliku lokalne datoteke. Kod ovog modela, primarni server zone predstavlja fiksnu tačku mogućeg kvara. Ako taj server postane nedostupan, zahtevi DNS klijenata za ažuriranjem u toj zoni ne mogu se izvršiti.

Kod načina skladištenja koji je integrisan sa direktorijumom, DNS se dinamički ažurira na bazi modela sa više glavnih primeraka. Kod tog modela, svaki ovlašćeni DNS server (na primer, kontroler domena sa DNS servisom) može da bude primarni izvor za tu zonu. Pošto se glavni primerak zone održava u bazi podataka servisa Active Directory, koja se u potpunosti replicira na sve kontrolere domena, zonu može da ažurira DNS ser-

vis na bilo kom kontroleru domena u domenu. Kod modela ažuriranja sa više glavnih primeraka, svaki primarni server u zoni koja je integrisana sa direktorijumom može da izvršava zahteve DNS klijenata za ažuriranjem zone, sve dok je kontroler domena na raspolaganju i pristupačan na mreži.

Takođe, u slučaju zone koja je integrisana sa direktorijumom, možete da koristite mogućnost uređivanja liste za kontrolu pristupa (ACL), da biste kontrolisali pristup zoni ili određenim zapisima resursa u zoni. Na primer, ACL za određeno ime domena u zoni može da se ograniči tako da je dinamičko ažuriranje dozvoljeno određenim DNS klijentima, ili da se ovlasti neka bezbedna grupa, kao što su administratori domena, koji imaju dozvole da ažuriraju zonu ili da zapisuju svojstva. Ova bezbednosna opcija nije vam na raspolaganju u slučaju standardnih primarnih zona.

- Zone se automatski repliciraju i sinhronizuju na nove kontrolere domena, kada se nova zona doda u Active Directory domen.

Iako je DNS servis moguće selektivno uklanjati sa kontrolera domena, zone koje su integrisane sa direktorijumom već su smeštene na sve kontrolere domena, tako da skladištenje zone i upravljanje njome ne predstavlja dodatno opterećenje za resurse. Pored toga, metodi sinhronizovanja informacija koje su smeštene u direktorijumu omogućavaju bolje performanse od onih koje se dobijaju standardnim metodama ažuriranja zone koji u nekim slučajevima zahtevaju transfer celokupne zone.

- Integrisanjem smeštaja DNS prostora imena u servis Active Directory, pojednostavljujete planiranje i administriranje DNS-a i servisa Active Directory.

Kada su prostori imena smešteni odvojeno i repliciraju se takođe odvojeno (na primer, DNS smeštaj i replikacija zasebno, a Active Directory zasebno), uvodi se dodatna administrativna složenost u planiranje mreže i osmišljavanje njenog eventualnog daljeg širenja. Integrisanjem DNS smeštaja, u jednu administrativnu celinu možete da objedinite upravljanje smeštajem i replikacijom podatka DNS-a i servisa Active Directory.

- Replikacija direktorijuma brža je i efikasnija od standardne DNS replikacije.

Pošto se postupak replikacije servisa Active Directory odvija na bazi svojstava, obrađuju se samo relevantne promene. Zbog toga se pri ažuriranju zona koje su smeštene u direktorijumu manipuliše manjom količinom podataka.

Ime zone

U tipičnom slučaju, zona dobija ime po domenu koji je na vrhu hijerarhije obuhvaćene tom zonom. Na primer, ime zone koja obuhvata microsoft.com i sales.microsoft.com bilo bi microsoft.com. O imenovanju zona detaljnije se možete informisati u poglavlju 2, „Upoznavanje servisa Active Directory”.

Datoteka zone

U slučaju standardne primarne zone za traženje unapred, morate da odredite datoteku zone. To je ime datoteke baze podataka za zonu, koje je formirano od imena zone i nastavka .dns. Na primer, ukoliko je ime zone microsoft.com, podrazumevano ime datoteke baze podataka za zonu je MICROSOFT.COM.DNS.

Kada zonu premeštate sa drugog servera, možete da uvezete i postojeću datoteku zone. Pre nego što kreirate novu zonu, postojeću datoteku morate da smestite u direktorijum *systemroot*\sytem32\DNS na ciljnom računaru, pri čemu „systemroot” označava omotnicu u koju je instaliran Windows 2000, što u tipičnom slučaju predstavlja omotnicu C:\Winnt.

Glavni DNS serveri

U slučaju standardne sekundarne zone za traženje unapred, morate da odredite DNS servere sa kojih želite da kopirate zonu. Morate da unesete IP adresu jednog ili više DNS servera.

Zona za traženje unazad

Zona za traženje unazad (engl. *reverse lookup zone*) omogućava upite za traženje unazad. Postojanje ove vrste zone nije obavezno. Međutim, zona za traženje unazad je neophodna za finkcionisanje nekih alatki za rešavanje problema, na primer NSLOOKUP, i da bi se u dnevničkim datotekama Internet Information Services (IIS) zapisivalo ime, a ne IP adresa.

➤ **Da biste kreirali zonu za traženje unazad:**

1. Pritisnite dugme Start, pokažite najpre na Programs, zatim na Administrative Tools, a nakon toga izaberite DNS.
2. Proširite prikaz DNS servera.
3. Pritiskom na desni taster miša najpre izaberite omotnicu Reverse Lookup Zone, a zatim New Zone. Otvoriće se čarobnjak New Zone Wizard koji vas vodi kroz postupke kreiranja zone za traženje unazad. Čarobnjak vam omogućava sledeće opcije konfigurisanja: Zone Type, Zone Name, Zone File i Master DNS Servers.

Tip zone

Kao što smo objasnili ranije, za tip zone odaberite jednu od opcija: zona integrisana u servis Active Directory, standardna primarna zona ili standardna sekundarna zona.

Zona za traženje unazad

Da biste identifikovali zonu za traženje unazad, upišite mrežni identifikator ili ime zone. Na primer, mrežni identifakor sa IP adresom 169.254.16.200 daće kao rezultat mrežni identifikator 169.254. Svi upiti za traženje unazad unutar umreženja 169.254 biće rešavani u novoj zoni.

Datoteka zone

Za standardnu primarnu zonu za traženje unazad morate da odredite datoteku zone. Podrazumevano ime datoteke zone određeno je mrežnim identifikatorom i maskom podmreže. DNS okreće redosled IP okteta i dodaje sufiks in-addr.arpa. na primer, zona za traženje unazad za umreženje 169.254 je 254.169.in-addr.arpa.dns.

Kada zonu premeštate sa drugog servera, možete da uvezete i postojeću datoteku zone. Pre nego što kreirate novu zonu, postojeću datoteku morate da smestite u direktorijum *systemroot*\sytem32\DNS na ciljnom računaru.

Glavni DNS serveri

Za standardnu primarnu zonu za traženje unazad, morate da odredite DNS servere sa kojih želite da kopirate zonu. Treba da unesete IP adresu jednog ili više DNS servera.

Zapisi resursa

Zapisi resursa su zapisi u datoteci baze podataka za zonu koji povezuju imena DNS domena sa relevantnim podacima određenih mrežnih resursa, na primer nekom IP adresom. Postoji mnogo raznih tipova zapisa resursa. Kada se kreira zona, DNS automatski dodaje dva zapisa resursa. To su zapisi Start of Authority (SOA) i Name Server (NS). U tabeli 5.1 opisani su ovi tipovi zapisa, kao i ostali često korišćeni zapisi resursa.

Tabela 5.1 Često korišćeni tipovi zapisa resursa

Vrsta zapisa resursa	Opis
Host (A)	Daje listu korelacija: ime matičnog računara – IP adresa, za zonu za traženje unapred.
Alias (CNAME)	Kreira alijas, ili alternativno ime, za određeno ime matičnog računara. Zapis Canonical Name (CNAME) možete koristiti da biste postigli da više imena ukazuju na istu IP adresu. Isti računar može biti matični za FTP server, na primer za *ftp.microsift.com* i za Web server, na primer za *www.microsoft.com.*
Host Information (HINFO)	Prepoznaje CPU i operativni sistem na matičnom računaru. Ovaj zapis možete da koristite kao jednostavnu alatku za praćenje resursa.
Mail Exchanger (MX)	Određuje server koji će služiti za razmenu elektronske pošte za određeni domen, kao i redosled korišćenja servera ukoliko ih ima više.
Name Server (NS)	Prikazuje listu servera imena koji su dodeljeni određenom domenu.
Pointer (PTR)	Ukazuje na drugi deo prostora imena domena. Na primer, u zoni za traženje unazad, daje listu korelacija IP adresa – ime.
Service (SRV)	Pokazuje na kom serveru se nalaze određeni servisi. Na primer, ako klijent želi da pronađe server koji ocenjuje validnost zahteva za prijavljivanje, on može da zada upit DNS serveru kako bi dobio spisak kontrolera domena i njihovih IP adresa.
Start of Authority (SOA)	Ukazuje na server imena koji predstavlja ovlašćeni izvor podataka unutar domena. Prvi zapis u datoteci baze podataka za zonu mora biti SOA zapis.

Napomena Da biste se detaljnije informisali o zapisima resursa, potražite **RFC 1035, RFC 1183, RFC 1886, RFC 2052** pomoću vašeg Web pretraživača, kako biste preuzeli sadržaj ovih Request for Comment (RFC).

➤ **Da biste pregledali zapis resursa:**

1. U stablu DNS konzole, izaberite zonu za koju želite da pregledate zapise resursa.
2. U oknu sa detaljima, izaberite zapis koji želite da pregledate.
3. Sa menija Action izaberite Properties.
4. U okviru za dijalog Properties pregledajte osobine koje se odnose na izabrani zapis.
5. Kada završite pregledanje zapisa, pritisnite dugme OK.

➤ **Da biste dodali zapis resursa:**

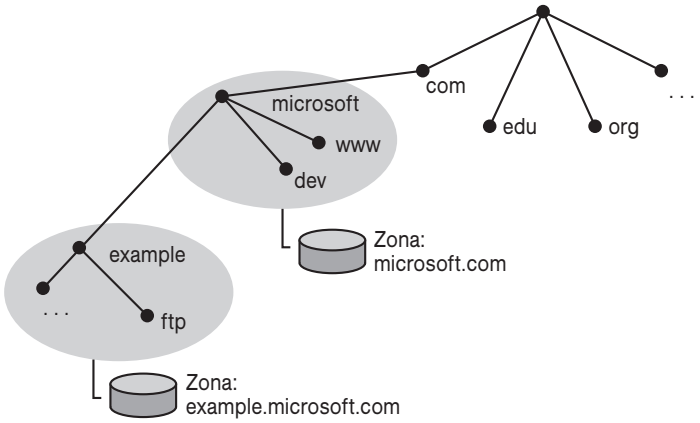
1. Pritiskom na desni taster miša najpre izaberite zonu kojoj želite da dodate zapis, a zatim tip zapisa koji želite da dodate, na primer New Host ili New Mail Exchanger.

Delegiranje zona

Zona započinje kao baza za skladištenje podataka za jedno DNS ime domena. Ukoliko dodajete druge domene koji se nalaze ispod domena na osnovu kojeg je zona kreirana, ti domeni mogu biti deo iste zone ili deo druge zone. Kada dodate poddomen, možete da:

- Upravljate njime i uključite ga da bude deo originalnih zapisa zone.
- Delegirate ga u drugu zonu koja je kreirana da podrži poddomen.

Na primeru sa slike 5.4 prikazan je domen microsoft.com koji sadrži imena domena za kompaniju Microsoft. Kada je domen microsoft.com prvi put kreiran na samostalnom serveru, bio je konfigurisan kao jedna zona za ceo Microsoft DNS prostor imena. Međutim, ukoliko se u domenu microsoft.com ukaže potreba za poddomenima, oni se moraju uključiti u zonu ili se moraju delegirati u drugu zonu. U primeru na slici 5.4, poddomen *example* dodat je domenu microsoft.com. Zona example.microsoft.com kreirana je da bi podržala poddomen example.microsoft.com.



Slika 5.4 Delegiranje novog poddomena u novu zonu

Kada zone delegirate unutar prostora imena, morate takođe da kreirate SOA zapise resursa da biste ukazali na ovlašćeni DNS server nove zone. To je neophodno da bi se nadležnost prenela i da bi se drugim DNS serverima i klijentima preneli tačni podaci o tome koji su novi serveri dobili ovlašćenje za novu zonu. U postupku delegiranja zona može vam pomoći čarobnjak New Delegation Wizard.

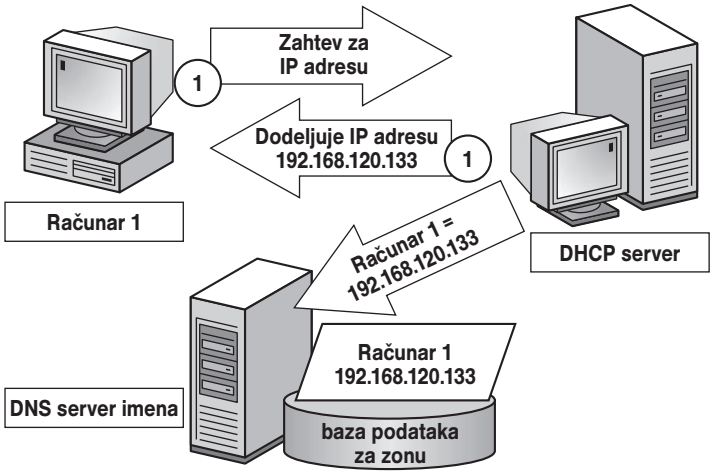
➤ **Da biste delegirali zonu:**

1. Na stablu DNS konzole izaberite poddomen za koji želite da kreirate delegiranje zone.
2. Sa menija Action izaberite New Delegation.
3. Na pozdravnoj stranici čarobnjaka New Delegation Wizard pritisnite dugme Next.
4. Na stranici Delegated Domain Name definišite ime domena kojeg želite da kreirate, a zatim pritisnite dugme Next.
5. Na stranici Name Servers definišite servere koji će biti matični za delegiranu zonu, a zatim pritisnite dugme Next.
6. Na stranici Completing The New Delegation Wizard pregledajte definisane stavke, a zatim pritisnite dugme Finish.

Napomena Svi domeni (ili poddomeni) koji se prikazuju kao podobni za delegiranje zone, moraju biti kreirani u tekućoj zoni pre nego što izvršite delegiranje.

Konfigurisanje dinamičkog DNS-a

DNS servis poseduje mogućnost dinamičkog ažuriranja koja se naziva dinamički DNS (*Dynamic DNS,* DDNS). Kad je DNS servis u pitanju, ukoliko dođe do promena u domenu za koji ovlašćenje ima server imena, na primarnom serveru imena morate ručno da ažurirate datoteku baze podataka za zonu. U slučaju DDNS-a, serveri imena i klijenti unutar mreže automatski ažuriraju datoteku baze podataka za zonu (slika 5.5).



Slika 5.5 DDNS ažurira datoteku baze podataka za zonu kada dođe do promene IP adrese

Dinamičko ažuriranje

Možete da konfigurišete listu servera ovlašćenih da iniciraju dinamičko ažuriranje. Lista može da obuhvati sekundarne servere imena, kontrolere domena i druge servere koji obavljaju mrežnu registraciju za klijente kao što su serveri sa servisima Dynamic Host Configuration Protocol (DHCP) ili Windows Internet Naming Service (WINS).

DDNS i DHCP

DDNS je u interakciji sa DHCP-om da bi za matične računare u mreži održao sinhronizovanost preslikavanja imena u IP adrese. Podrazumevano je da DHCP servis dopušta klijentima da zoni dodaju svoje zapise tipa A (Host), a DHCP servis dodaje zoni zapise resursa tipa PTR. Kada zakup istekne, DHCP servis briše zapise tipa A i PTR.

Važno Da bi dinamička ažuriranja mogla da se vrše, DHCP server morate da konfigurišete tako da ukazuje na odgovarajuće DNS servere. Konfigurisanje DHCP-a prevazilazi opseg ovog kursa, pa vas radi detaljnijeg informisanja na ovu temu upućujemo na *MCSE Training Kit - Microsoft Windows 2000 Network Infrastructure Administration.*

➤ **Da biste konfigurisali zonu za DDNS:**

1. Na DNS konzoli pritiskom na desni taster miša izaberite zonu za traženje unapred, odnosno unazad, koju želite da konfigurišete, a zatim izaberite Properties.
2. Na kartici General, izaberite jednu od sledećih opcija u listi Allow Dynamic Updates?:
   - **No.** Za ovu zonu nisu dozvoljena dinamička ažuriranja.
   - **Yes.** Dozvoljeni su svi zahtevi za dinamička ažuriranja DNS-a za ovu zonu.
   - **Only Secure Updates.** Dozvoljena su samo ona dinamička ažuriranja DNS-a koja koriste bezbedni DNS za tu zonu. Ovo je opcija koja se preporučuje.

Opcija Only Secure Updates je na raspolaganju samo kod tipa zone integrisane u servis Active Directory. Ukoliko izaberete opciju Only Secure Updates, dozvola molioca da može ažurirati zapise u bazi podataka za zonu testira se korišćenjem mehanizama koji se navode u protokolu bezbednog ažuriranja DNS koji sledi.

Napomena Da biste se detaljnije informisali o DDNS-u, pomoću svog Web pretraživača potražite **RFC 2136** i **RFC 2137**.

Praktični rad: Konfigurisanje zona

U ovoj vežbi kreiraćete zonu za traženje unapred i zonu za traženje unazad.

➤ **Da biste kreirali zonu za traženje unapred:**

1. Pritisnite dugme Start, pokažite najpre na Programs, zatim na Administrative Tools, a nakon toga izaberite DNS.
   Prikazaće se prozor DNS konzole.
2. Dvostrukim pritiskom na taster miša izaberite SERVER1 (ili ime vašeg računara).
   Prikazaće se omotnica Forward Lookup Zones and Reverse Lookup Zones.
3. Pritiskom na desni taster miša najpre izaberite SERVER1, a zatim New Zone.
   Pojavljuje se čarobnjak New Zone Wizard.
4. Da biste nastavili, pritisnite dugme Next.
   Prikazuje se stranica Zone Type.
5. Uverite se da je izabrana opcija Standard Primary, a zatim pritisnite dugme Next.
   Prikazuje se strana Forward or Reverse Lookup Zone.
6. Uverite se da je izabrana opcija Forward Lookup Zone, a zatim pritisnite dugme Next.
   Prikazaće se stranica Zone Name.
7. Upišite **training.microsoft.com**, a zatim pritisnite dugme Next. (Ukoliko ste umreženi, posavetujte se sa administratorom mreže da li je u redu da ovo ime koristite kao DNS ime domena.)
   Prikazaće se stranica Zone File.
8. Uverite se da je izabrana opcija Create a New File With this File Name i da je TRAINING.MICROSOFT.COM.DNS ime datoteke koja će biti kreirana. (Ukoliko niste koristili training.microsoft.com kao ime domena u koraku 7, prikazaće se ime koje ste upisali u koraku 7, sa nastavkom .dns.)
9. Pritisnite dugme Next.
10. Pritisnite dugme Finish.

➤ **Da biste kreirali zonu za traženje unazad:**

1. Pritiskom na desni taster miša najpre izaberite SERVER1, a zatim New Zone.
   Pojavljuje se čarobnjak New Zone Wizard.
2. Da biste nastavili, pritisnite dugme Next.
   Prikazuje se stranica Zone Type.
3. Uverite se da je izabrana opcija Standard Primary, a zatim pritisnite dugme Next.
   Prikazuje se strana Forward or Reverse Lookup Zone.
4. Uverite se da je izabrana opcija Reverse Lookup Zone, a zatim pritisnite dugme Next.
   Prikazaće se stranica Reverse Lookup Zone.
5. Uverite se da je izabran Network ID, a zatim u polje Network ID upišite **10.10.1**. (Ukoliko ste umreženi i niste koristili 10.10.1.1 kao svoju statičku IP adresu, upišite oktete koji predstavljaju vaš mrežni identifikator).

Napomena Primetićete da je u polju Name na dnu prozora upisano in-addr.arpa ime i da ono glasi 1.10.10.in-addr.arpa. Ukoliko niste koristili 10.10.1.1, ime će odgovarati onoj IP adresi koju koristite.

---

6. Pritisnite dugme Next.
   Prikazuje se stranica Zone File.
7. Uverite se da je izabrana opcija Create a New File With this File Name i da je 1.10.10.in-addr.arpa.dns ime datoteke koja će biti kreirana. (Ukoliko niste koristili 10.10.1 kao mrežni identifikator u koraku 5, ime datoteke će odgovarati IP adresi koju ste koristili.)
8. Pritisnite dugme Next.
   Prikazuje se stranica Completing the New Zone Wizard.
9. Pregledajte podatke na stranici Completing the New Zone Wizard, a zatim pritisnite dugme Finish.

Vežba 2:Konfigurisanje DDNS servisa

U ovoj vežbi konfigurisaćete DDNS servis, da biste omogućili dinamičko ažuriranje zona za traženje unapred i zona za traženje unazad.

➤ **Da biste konfigurisali DDNS:**

1. Na stablu DNS konzole, dvostrukim pritiskom na taster miša izaberite SERVER1 (ili ime vašeg servera).
2. Dvostrukim pritiskom na taster miša izaberite Forward Lookup Zone, a zatim na isti način izaberite training.microsoft.com. (Ukoliko kao DNS ime domena niste upotrebili training.microsoft.com, dvostrukim pritiskom na taster miša izaberite ime koje ste dali DNS domenu.)
3. Pritiskom na desni taster miša izaberite training.microsoft.com (ili vaše DNS ime domena), a zatim izaberite Properties.
   Otvara se okvir za dijalog training.microsoft.com Propeties. (Ukoliko kao DNS ime domena niste upotrebili training.microsoft.com, ime u naslovu okvira za dijalog odraziće ime koje ste dali DNS domenu.)
4. Sa liste Allow Dynamic Updates? na kartici General, izaberite Yes, a zatim pritisnite dugme OK.
   Ovim konfigurišete DDNS za zonu za traženje unapred.

5. Dvostrukim pritiskom na taster miša izaberite Reverse Lookup Zones, a zatim izaberite 10.10.1.x Subnet, odnosno zonu za traženje unazad koju ste kreirali u vežbi broj 1.
6. Pritiskom na desni taster miša izaberite 10.10.1.x Subnet, a zatim izaberite Properties.
   Otvara se okvir za dijalog 10.10.1.x Subnet Properties.
7. Sa liste Allow Dynamic Updates? na kartici General, izaberite Yes, a zatim pritisnite dugme OK.
   Ovim ste konfigurisali DDNS za zonu za traženje unazad.

Vežba 3: Dodavanje zapisa resursa

U ovoj praktičnoj vežbi dodaćete zoni zapis tipa PTR.

➤ **Da biste zoni dodali PTR zapis resursa:**

1. Na stablu konzole dvostrukim pritiskom na taster miša izaberite Reverse Lookup Zones.
2. Izaberite 10.10.1.x Subnet. (Ukoliko za ime vašeg servera niste upotrebili statičku IP adresu 10.10.1.1, izaberite odgovarajuću podmrežu.)
   Koji tipovi zapisa resursa postoje u zoni za traženje unazad?
3. Na stablu konzole, pritiskom na desni taster miša izaberite 10.10.1.x Subnet (ukoliko za ime vašeg servera niste upotrebili statičku IP adresu 10.10.1.1, izaberite odgovarajuću podmrežu), a zatim izaberite New Pointer.
4. U polje Host IP Number, u oktet koji je istaknut u vašoj IP adresi upišite **1**.
   U polje Host Name najpre upišite potpuno kvalifikovano ime domena vašeg računara, a zatim tačku. Možete takođe da „pretražujete" kroz postojeće DNS zapise koristeći opciju Browse. Na primer, ako je ime vašeg računara SERVER1, upišite **server.microsoft.com.** Nemojte zaboraviti da upišete tačku na kraju.
5. Pritisnite dugme OK.
   Zapis tipa Pointer pojaviće se u oknu sa detaljima.
6. Zatvorite DNS konzolu.

Rezime lekcije

U ovoj lekciji naučili ste da u DNS servisu postoji opcija za podelu prostora imena na jednu ili više zona, koje mogu biti smeštene, distribuirane i replicirane na druge DNS servere. DNS prostor imena predstavlja logičku strukturu mrežnih resursa, a DNS zone predstavljaju mesto za fizičko skladištenje tih resursa.

Naučili ste, takođe, da konfigurišete zone za traženje unapred odnosno unazad i saznali ste da se primarne zone integrisane u direktorijum preporučuju zbog toga što imaju sledeće prednosti: ažuriranje na principu više glavnih primeraka, povećanu bezbednost, automatsko repliciranje zone u slučaju dodavanja novih kontrolera domena, jednostavnije administranje sa integrisanim skladištenjem prostora imena i brže repliciranje.

Naučili ste da dodajete zapise resursa i da delegirate zone prilikom dodavanja novih poddomena. Saznali ste, takođe, da DNS servis obuhvata mogućnost dinamičkog ažuriranja pod nazivom DDNS, kojim serveri imena i klijenti na mreži automatski ažuriraju datoteke baze podataka za zonu.

U praktičnom delu ove lekcije, kreirali ste za DNS servis zone za traženje unapred, odnosno unazad, konfigurisali ste zone za DDNS i dodali ste PTR zapis resursa u zonu za traženje unazad.

Lekcija 3: Replikacija i transfer zona

Ova lekcija vas upoznaje sa replikacijom i transferom zona. *Transfer zone* (engl. *zone transfer)* je postupak u kome DNS serveri međusobno sarađuju u cilju održavanja i sinhronizacije pouzdanih podataka o imenima.

Kada pređete ovu lekciju, moći ćete da:

- Objasnite svrhu transfera zona.
- Konfigurišete transfer zona.

Predviđeno vreme za ovu lekciju je 10 minuta.

Replikacija i transfer zona

Zbog velikog značaja koji zone imaju u DNS-u, one treba da budu dostupne sa više DNS servera u mreži, čime se obezbeđuje pristupačnost i otpornost na kvarove pri razrešavanju upita imena. U suprotnom, ukoliko bismo koristili samo jedan server i on prestane da reaguje, upiti za traženje imena u toj zoni ne bi uspeli. Kada više servera održava zonu, transferi zone su potrebni da bi se replicirale i sinhronizovale sve kopije zone koje se koriste na svim serverima konfigurisanim da budu serveri zone.

Kada definišete strukturu zone, postoji nekoliko važnih razloga zbog kojih treba da koristite dodatne DNS servere za repliciranje zone:

- Dodatni DNS serveri obezbeđuju redundantnost zone, omogućavajući da se klijentima razrešavaju DNS imena u zoni iako je primarni server zone prestao da reaguje.
- Dodatni DNS serveri mogu se koristiti u svrhu smanjenja intenziteta DNS mrežnog saobraćaja. Na primer, dodavanje DNS servera na suprotnoj strani neke spore veze u regionalnoj mreži (WAN), može biti korisno za upravljanje mrežnim saobraćajem i smanjenje njegovog intenziteta.
- Dodatni sekundarni serveri mogu da se upotrebe u svrhu smanjenja opterećenja primarnog servera zone.

Kada se u mrežu doda novi DNS server konfigurisan kao novi sekundarni server u postojećoj zoni, on sprovodi *transfer cele zone* (engl. *full zone transfer, AXFR*) kako bi dobio i replicirao kompletnu kopiju zapisa resursa te zone. U starijim verzijama instalacije DNS servera, takođe se koristi isti metod transfera cele zone kada se zahteva njeno ažuriranje zbog nastalih izmena. DNS servis kod Windows 2000 Servera podržava *inkrementalni transfer zone* (engl. *incremental zone transfer, IXFR*), koji predstavlja obnavljanje postupka transfera onih promena DNS zone koje su u međuvremenu nastale.

Inkrementalni transferi zone

RFC 1995 opisuje IXFR kao dodatni DNS standard za replikaciju DNS zona. IXFR omogućava efikasniji način propagiranja promena u zoni i njenog ažuriranja.

U starijim verzijama DNS-a, uvek kada se zahtevalo ažuriranje zone, bio je neophodan transfer cele datoteke zonske baze podataka, primenom AXFR upita. Umesto te vrste upita, kod inkrementalnog transfera zone koristi se upit IXFR. On omogućava da sekundarni server preuzme samo one promene zone koje su mu potrebne da bi svoju kopiju zone sinhronizovao sa njenim izvorom, odnosno primarnom ili sekundarnom kopijom zone koju održava drugi DNS server.

Kod IXFR transfera zone, prvo se ustanovi razlika između izvorne i replicirane verzije zone. Ukoliko se ustanovi da su obe verzije identične – što je označeno u polju za serijski broj (engl. *serial number field*) u SOA zapisu resursa svake zone – do transfera ne dolazi.

Ukoliko je serijski broj zone na izvoru veći nego što je na sekundarnom serveru koji postavlja zahtev za ažuriranje, transfer se vrši za promene u zapisima resursa samo za svaku inkrementalnu verziju zone. Da bi jedan IXFR upit uspeo i da bi se promene prosledile, izvorni DNS server zone mora da održava podatke o istoriji inkrementalnih promena zone koje će da koristi pri odgovaranju na upite. Inkrementalni transfer zahteva manje mrežnog saobraćaja i obavlja se mnogo brže.

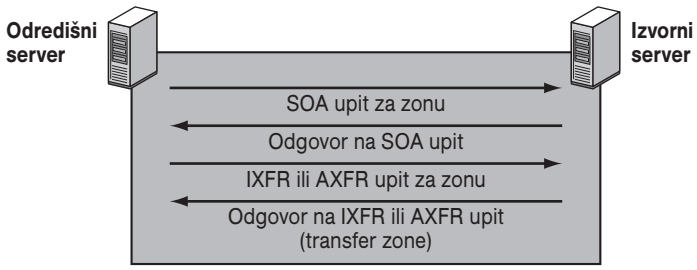
Primer: transfer zone

Pored toga što se može inicirati ručno, do transfera zone dolazi u sledećim situacijama:

- Kada pokrećete DNS servis na sekundarnom serveru zone.
- Po isteku vremenskog intervala za osvežavanje zone.
- Kada nastanu promene u primarnoj zoni a konfigurisana je lista za obaveštavanje.

Sekundarni server zone uvek inicira transfer zone i zahtev za transfer dostavlja DNS serveru koji je konfigurisan kao izvorni za tu zonu. Taj DNS server može biti bilo koji drugi DNS server, bilo primarni bilo sekundarni, na kome je učitana zona. Kada izvorni server primi zahtev za zonu, on može da odgovori delimičnim transferom ili transferom cele zone.

Kao što je prikazano na slici 5.6, transferi zone između servera odvijaju se po utvrđenom postupku. On se razlikuje u zavisnosti od toga da li je zona prethodno bila replicirana ili se vrši inicijalna replikacija nove zone.



Slika 5.6 Postupak transfera zone

U ovom primeru, dolazi do sledećeg redosleda postupaka između servera koji zahteva transfer zone – ciljnog servera – i izvornog servera, drugog DNS servera koji skladišti zonu.

1. Tokom novog konfigurisanja odredišni server šalje inicijalni (AXFR) zahtev za transfer zone DNS serveru koji je konfigurisan kao izvorni za zonu.
2. Izvorni server odgovara i vrši transfer cele zone na odredišni server.
3. Kada istekne interval osvežavanja, odredišni server upućuje izvornom serveru SOA upit, zahtevajući obnavljanje zone.
4. Izvorni server odgovara na upit svojim SOA zapisom.

   Taj odgovor sadrži serijski broj aktuelnog stanja zone na izvornom serveru.

5. Odredišni server proverava serijski broj u SOA zapisu odgovora i donosi odluku o načinu osvežavanja zone.

   Ukoliko je vrednost serijskog broja u odgovoru jednaka aktuelnom lokalnom serijski broju, zaključak je da su zone identične na oba servera i da transfer zone nije potreban. Odredišni server obnavlja zonu tako što interval osvežavanja vraća na početak, a veličinu intervala određuje vrednost u odgovarajućem polju SOA zapisa u odgovoru izvornog servera.

   Ukoliko je vrednost serijskog broja u odgovoru veća od aktuelnog lokalnog serijskog broja, zaključak je da postoji nova verzija zone i da je transfer neophodan.

6. Ukoliko odredišni server zaključi da je zona pretrpela promene, on izvornom serveru šalje IXFR upit koji u SOA zapisu zone sadrži vrednost lokalnog serijskog broja.
7. Izvorni server odgovara inkrementalnim ili kompletnim transferom zone.

   Ukoliko izvorni server podržava inkrementalni transfer i čuva podatke o istoriji inkrementalnih promena zone zbog modifikovanja zapisa resursa, on može odgovoriti inkrementalnim (IXFR) transferom zone.

   Ukoliko izvorni server ne podržava inkrementalni transfer ili ne čuva podatke o istoriji promena zone, on može, kao alternativno rešenje, da odgovori transferom cele zone (AXFR).

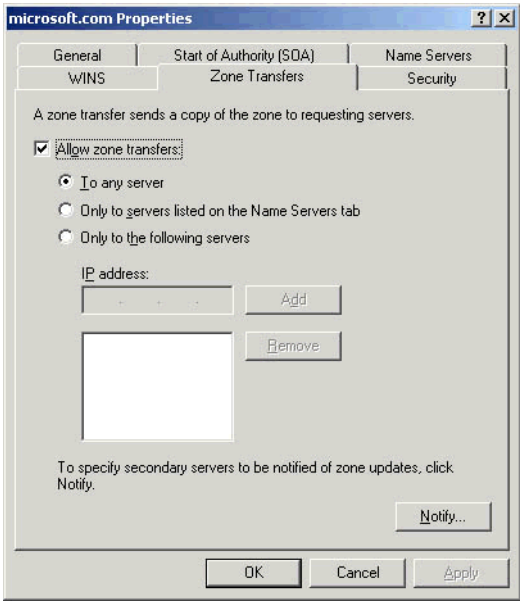
Napomena Windows 2000 Server podržava upite tipa IXFR i inkrementalni transfer zone. Starije verzije DNS servisa u sistemu Windows NT Server 4.0 i mnoge druge instalacije DNS servera ne podržavaju inkrementalni transfer zone, tako da se za replikaciju koriste samo upiti tipa AXFR i transferi cele zone.

Bezbednost transfera zone

DNS konzola vam omogućava da odredite servere kojima je dozvoljeno da učestvuju u transferu zone. Time možete da sprečite neželjene pokušaje nepoznatih ili neovlašćenih DNS servera da preuzmu podatke zone ili da zahtevaju njeno ažuriranje.

➤ **Da biste odredili servere kojima je dozvoljeno da učestvuju u transferima zone:**

1. Pritisnite dugme Start, pokažite najpre na Programs, zatim na Administrative Tools, a nakon toga izaberite DNS.
2. Na stablu DNS konzole pritiskom na desni taster miša izaberite zonu za koju želite da uređujete transfer zone, a zatim izaberite Properties.
3. Otvorite karticu Zone Transfer (slika 5.7).



Slika 5.7 Kartica Zone Transfer

4. Odredite servere kojima želite da dozvolite transfere zone, a zatim pritisnite dugme OK.

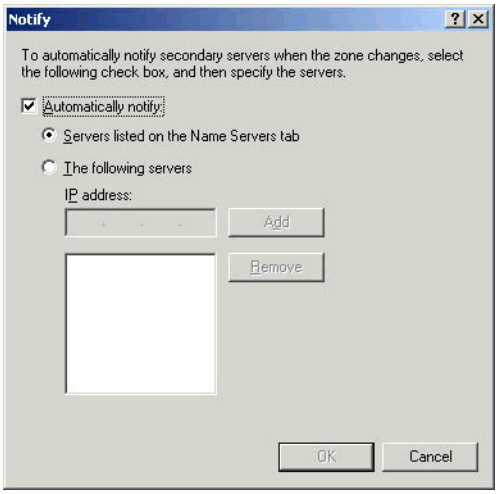
DNS obaveštavanje

DNS servis podržava DNS obaveštavanje (engl. *DNS notification*) koje predstavlja savremenu reviziju standardne DNS specifikacije (RFC 1996). DNS obaveštavanje je mehanizam kojim se izabranoj grupi servera u zoni dojavljuje čim dođe do promena u zoni. Obavešteni serveri mogu zatim inicirati postupak transfera zone i od servera koji ih obaveštava preuzeti nastale promene da bi zonu ažurirali.

DNS obaveštavanje koristite samo za dojavu DNS serverima koji rade kao sekundarni serveri zone. Za replikaciju zona integrisanih u direktorijum nije potrebno DNS obaveštavanje, jer svaki server koji učita zonu od servisa Active Directory automatski proziva direktorijum otprilike svakih 15 minuta (što zavisi od intervala osvežavanja zadatog u SOA zapisu) da bi ažurirao i osvežio zonu. U ovakvim slučajevima, konfigurisanje liste obaveštavanja može u praksi da oslabi performanse sistema, jer prouzrokuje nepotrebne dodatne zahteve za transfer ažurirane zone.

➤ **Da biste odredili servere koji će biti obaveštavani:**

1. Pritisnite dugme Start, pokažite najpre na Programs, zatim na Administrative Tools, a nakon toga izaberite DNS.
2. Na stablu DNS konzole pritiskom na desni taster miša najpre izaberite zonu za koju želite da uređujete transfer zone, a zatim Properties.
3. Otvorite karticu Zone Transfer, a zatim izaberite Notify.
4. U okviru za dijalog Notify (slika 5.8) odredite sekundarne servere koji će biti obaveštavani kada dođe do promene u zoni, a zatim pritisnite dugme OK.



Slika 5.8 Okvir za dijalog Notify

Postupak DNS obaveštavanja

Dajemo vam kratki pregled tipičnog postupka DNS obaveštavanja:

1. Na DNS serveru došlo je do promena u lokalnoj zoni koja za druge servere predstavlja izvor. Kada dođe do promena izvorne zone, takođe se promeni i vrednost u polju za serijski broj SOA zapisa, čime se označava postojanje nove verzije lokalne zone.
2. Izvorni server šalje obaveštenje ostalim serverima koji su navedeni u prozoru Notify.
3. Svi sekundarni serveri koji prime obaveštenje mogu serveru koji je uputio obaveštenje odgovoriti iniciranjem zahteva za transfer zone. Tada se može nastaviti normalan postupak transfera zone opisan u prethodnom odeljku.

Rezime lekcije

U ovoj lekciji naučili ste da su transferi zone neophodni da bi se replicirale i sinhronizovale sve kopije zone na svakom serveru koji je konfigurisan da održava zonu. Kada se novi DNS server doda u mrežu i konfiguriše kao novi sekundarni server u postojećoj zoni, u slučaju starijih verzija DNS servera obavlja se inicijalni transfer cele zone da bi se dobila i replicirala kompletna kopija zapisa resursa za zonu. U slučaju Windows 2000 Servera, DNS servis podržava inkrementalni transfer zone, koji predstavlja revidirani, efikasniji postupak transfera onih promena DNS zone koje nastanu u međuvremenu.

Naučili ste, takođe, da DNS konzola omogućava da definišete servere kojima je dozvoljeno da učestvuju u transferu zone. Na kraju, naučili ste da DNS obaveštavanje koristi mehanizam kojim obaveštava odabranu grupu sekundarnih servera u zoni da je u njoj došlo do promena. Obavešteni serveri zatim mogu da iniciraju postupak transfera zone kojim od servera koji ih je obavestio preuzimaju nastale promene da bi ažurirali zonu. DNS konzola omogućava vam da odredite sekundarne servere koji će biti obaveštavani, dok za replikaciju zona integrisanih sa direktorijumom, DNS obaveštavanje nije potrebno.

Lekcija 4: Nadgledanje i rešavanje problema DNS-a za servis Active Directory

U ovoj lekciji objasnićemo opcije nadgledanja koje postoje za DNS servere. Opisaćemo takođe probleme na koje možete naići pri konfigurisanju DNS-a za servis Active Directory, kao i njihova moguća rešenja.

Kada pređete ovu lekciju, moći ćete da:

- Nadgledate DNS server.
- Rešavate probleme konfigurisanja probleme vezane za konfigurisanje DNS-a u okviru servisa Active Directory.

Predviđeno vreme za ovu lekciju je 10 minuta.

Nadgledanje DNS servera

U Windows 2000 Server postoje dve opcije za nadgledanje DNS servera:

- Podrazumevana opcija zapisivanja poruka događaja DNS servera u dnevnik DNS servera.
- Opciono otkrivanje i otklanjanje grešaka u dnevniku praćenja koji se evidentira u obliku tekstualne datoteke na računaru DNS servera.

Dnevničko praćenje događaja na DNS serveru

U sistemu Windows 2000 Server, poruke događaja DNS servera čuvaju se u dnevniku DNS servera odvojeno od događaja izazvanih drugim aplikacijama i servisima. Dnevnik DNS servera možete pregledati korišćenjem alatke Event Viewer. Dnevnik sadrži osnovne, unapred određene događaje koje evidentira DNS servis servera, na primer pokretanje i zaustavljanje DNS servera.

Event Viewer takođe možete da koristite da biste pregledali i nadgledali DNS događaje koji se odnose na klijente. Ti događaji pojavljuju se u sistemskom dnevniku i upisuje ih DNS klijentski servis na svakom računaru sa sistemom Windows 2000 svih verzija.

Napomena Način korišćenja alatke Event Viewer možete detaljnije upoznati u poglavlju 14, „Upravljanje performansama servisa Active Directory”.

Opcije otkrivanja i otklanjanja grešaka

DNS konzola omogućava vam da podesite dodatne opcije evidentiranja, da biste napravili privremeni dnevnik praćenja u obliku tekstualne datoteke o aktivnostima DNS servera. Datoteka koja se formira i koristi u tu svrhu, DNS.LOG, smeštena je u omotnici *systemroot*\System32\Dns. Kod Windows 2000 DNS servera podržane su opcije za dnevničko evidentiranje otkrivanja i otklanjanja grešaka navedene u tabeli 5.2.

Tabela 5.2 Opcije za dnevničko evidentiranje otkrivanja i otklanjanja grešaka kod DNS servera

Opcija evidentiranja	Opis
Query	Evidentira upite klijenata koje DNS server prima.
Notify	Evidentira poruke obaveštenja koje od drugih servera prima servis DNS servera.

Tabela 5.2 Opcije za dnevničko evidentiranje otkrivanja i otklanjanja grešaka kod DNS servera

Opcija evidentiranja	Opis *(nastavak)*
Update	Evidentira dinamička ažuriranja koja od drugih računara prima servis DNS servera.
Questions	Evidentira sadržaj odeljka sa pitanjima svake poruke DNS upita koje obradi servis DNS servera.
Answers	Evidentira sadržaj odeljka sa odgovorima svake poruke DNS upita koje obradi servis DNS servera.
Send	Evidentira broj poruka DNS upita koje je poslao servis DNS servera.
Receive	Evidentira broj poruka DNS upita koje je primio servis DNS servera.
UDP	Evidentira broj DNS zahteva koje primi servis DNS servera preko UDP priključka.
TCP	Evidentira broj DNS zahteva koje primi servis DNS servera preko TCP priključka.
Full Packets	Evidentira broj celih paketa napisanih i upućenih od strane servisa DNS servera.
Write Through	Evidentira broj paketa upućenih servisu DNS servera i nazad u zonu.

Podrazumevano je da su sve opcije za dnevničko evidentiranje otkrivanja i otklanjanja grešaka (engl. *debug logging*) onemogućene. Kada ih selektivno omogućite, servis DNS servera može da vrši dodatno evidentiranje praćenja odabranih tipova događaja ili poruka u cilju rešavanja problema i otkrivanja i otklanjanja grešaka servera.

Dnevničko evidentiranje otkrivanja i otklanjanja grešaka može opteretiti resurse, zauzeti veliki prostor na disku i negativno uticati na ukupne performanse servera. Zbog toga ga treba koristiti samo privremeno, u slučajevima kada su vam potrebne detaljne informacije o radu servera.

➤ **Da biste podesili opcije za dnevničko evidentiranje otkrivanja i otklanjanja grešaka DNS servera:**

1. Na stablu DNS konzole, pritiskom na desni taster miša najpre izaberite server imena, a zatim Properties.
2. Na kartici Logging izaberite opcije otkrivanja i otklanjanja grešaka koje želite da evidentirate, a zatim pritisnite dugme OK.

Scenarija za rešavanje problema koji se odnose na DNS

U tabeli 5.3 dat je opis nekih problema na koje možete naići u vezi sa zonama, kao i njihovih mogućih rešenja.

Tabela 5.3 Scenarija za rešavanje problema koji se odnose na zonu

Simptom: problemi koji se odnose na transfer zone	
Uzrok	**Rešenje**
Prekid rada servisa DNS servera ili pauza u radu zone	Proverite da li su pokrenuta oba DNS servera koja učestvuju u transferu zone: glavni (izvor) i sekundarni (odredište), kao i da li je na jednom od servera zona stavljena u stanje pauze.

Tabela 5.3 Scenarija za rešavanje problema koji se odnose na zonu *(nastavak)*

DNS serveri koji učestvuju u transferu nemaju međusobnu mrežnu vezu	Eliminišite mogućnost baznih problema u povezivanju na mrežu ovih servera. Proverite da li svaki server ima vezu sa mrežom, tako što ćete korišćenjem komande PING sa udaljenog partnera tog servera dobiti njegovu IP adresu. Testiranje povezanosti treba da uspe u oba smera. Ukoliko ne uspe, ispitajte problem međusobne mrežne povezanosti i rešite ga.
Serijski broj je isti na izvornom i odredišnom serveru. Pošto je vrednost na oba servera ista, između njih neće doći do transfera zone.	Koristeći DNS konzolu uradite sledeće: na kartici Start of Authority (SOA), vrednost serijskog broja zone na glavnom serveru (izvoru) povećajte tako da bude veći od vrednosti na upotrebljivom sekundarnom serveru (odredištu). Inicirajte transfer zone na sekundarnom serveru.
Između glavnog servera (izvora) i ciljnog sekundarnog servera (odredišta) postoje problemi interoperabilnosti	Ispitajte moguće uzroke problema interoperabilnosti između Windows 2000 DNS servera i drugih DNS servera sa različitim softverom, na primer starijim verzijama programa Berkeley Internet Name Domain (BIND).
U zoni postoje zapisi resursa ili neki drugi podaci koje DNS server ne može da pročita	Proverite da li zona sadrži nekompatibilne podatke, na primer nepodržane vrste zapisa resursa ili neispravne podatke. Proverite takođe da li je server konfigurisan tako da sprečava učitavanje zone ukoliko otkrije neispravne podatke i proverite način na koji proverava imena. Ovi parametri se mogu konfigurisati pomoću DNS konzole.
Podaci od autoriteta u zoni su netačni	Ukoliko transfer zone i dalje ne uspeva, proverite da li zona sadrži nestandardne podatke. Da biste odredili da li su pogrešni podaci zone mogući uzrok njenog neuspelog transfera, pregledajte poruke u dnevniku događaja DNS servera.

Simptom: delegiranje zone ne funkcioniše

Uzrok	Rešenje
Delegiranje zone nije ispravno konfigurisano	Pregledajte kako se koriste delegiranja zone i ukoliko je potrebno revidirajte konfigurisanje zone.

U tabeli 5.4 opisano je nekoliko problema na koje možete naići pri dinamičkom ažuriranju i njihova moguća rešenja.

Tabela 5.4 Rešavanje problema scenarija dinamičkog ažuriranja

Simptom: klijent ne vrši dinamička ažuriranja

Uzrok	Rešenje
Klijent (ili njegov DHCP server) ne podržava korišćenje protokola za DNS dinamičko ažuriranje	Proverite da li klijent (ili server) podržava DNS dinamički protokol za ažuriranje koristeći opcije podrške dinamičkom ažuriranju u Windowsu 2000. Da bi DNS server registrovao računare klijenata i da bi ih dinamički ažurirao, instalirajte Windows 2000 na računare klijenata ili ih unapredite u taj sistem, ili na mrežu instalirajte i koristite Windows 2000 DHCP server da biste iznajmljivali klijentske računare.
Klijent nije mogao da se registruje i izvrši ažuriranje kod DNS servera zbog nedostajućeg ili pogrešnog DNS konfigurisanja	Proverite da li je klijent u potpunosti i tačno konfigurisan za DNS i ukoliko je potrebno, ažurirajte konfiguraciju. Da biste ažurirali DNS konfiguraciju klijenta, uradite sledeće: konfigurišite primarni DNS sufiks na računaru klijenta za statičke TCP/IP klijente, ili konfigurišite DNS sufiks za tačno određenu vezu za korišćenje na jednoj od instaliranih mrežnih veza na računaru klijenta.

Tabela 5.4 Rešavanje problema scenarija dinamičkog ažuriranja *(nastavak)*

DNS server ne podržava dinamičko ažuriranje	Proverite da li klijentov DNS server može da podržava protokol za dinamičko ažuriranje, kao što je opisano u RFC 2136. Za Windows DNS servere, samo Windows 2000 DNS serveri podržavaju dinamičko ažuriranje, dok ga DNS server iz sistema Windows NT Server 4.0 ne podržava.
DNS server podržava dinamičko ažuriranje, ali nije konfigurisan da ga prima	Proverite da li je primarna zona u kojoj klijenti zahtevaju ažuriranje konfigurisana tako da omogućava dinamičko ažuriranje. Kod Windows 2000 DNS servera podrazumevana opcija za novu primarnu zonu je da ne dozvoljava dinamičko ažuriranje. Na DNS serveru koji sadrži upotrebljivu primarnu zonu modifikujte osobine zone tako da omogućava ažuriranje.
Baza podataka za zonu nije dostupna	Proverite da li postoji zona, i da li je ona dostupna za ažuriranje. U slučaju standarne primarne zone, proverite da li na serveru postoji datoteka zone i da li je zona u stanju pauze. Sekundarne zone ne podržavaju dinamičko ažuriranje. U slučaju zone integrisane u servis Active Directory, proverite da li DNS server funkcioniše kao kontroler domena i da li ima pristup bazi podataka servisa Active Directory u kojoj su smešteni podaci o zoni.

Rezime lekcije

U ovoj lekciji učili ste o raspoloživim opcijama za nadgledanje DNS servera. Sagledali ste takođe i neke eventualne probleme vezane za konfigurisanje DNS-a i njihova moguća rešenja.

Pregled

Svrha sledećih pitanja je da utvrdite ključne informacije koje su iznete u ovom poglavlju. Ukoliko ne budete u stanju da odgovorite na neko od njih, pročitajte ponovo lekciju na koju se pitanje odnosi i pokušajte ponovo da odgovorite. Odgovore na ova pitanja možete naći u dodatku A, „Pitanja i odgovori”.

1. Koja je svrha upita za traženje unapred, a koja upita za traženje unazad?

2. Koje su prednosti korišćenja zone integrisane u servis Active Directory?

3. Čemu služi SOA zapis resursa?

4. Šta je potrebno da uradite kada delegirate zonu unutar prostora imena?

5. Zbog čega je upit tipa IXFR efikasniji od AXFR upita?