

KATEDRA ZA OPERACIJSKE SUSTAVE

Administracija operacijskih sustava

Lab 06 – DNS i GPO

REV 3.3

Sadržaj

Uvod	2
Implementacija DNS infrastrukture	4
Zadaci	4

Uvod

DNS servis od presudne je važnosti za Active Directory – AD bez njega ne može funkcionirati. U prethodnim smo ga vježbama uzimali zdravo za gotovo. Podsjetimo se, instalacijski čarobnjak Active Directoryja ponudio nam je opciju instalacije DNS poslužitelja, mi smo je prihvatili te naposljetku uz domenski kontroler „dobili“ i DNS poslužitelj. Upravo s tom pretpostavkom i započinjemo današnju vježbu – imamo funkcionalnu DNS infrastrukturu koju želimo proširiti i konfigurirati prema svojim potrebama.

Prije nego što opišemo strukturu koju želimo postići, ponovimo ukratko ključne pojmove DNS-a s praktičnoga gledišta.

- **Primarna zona** (engl. *Primary zone*): DNS poslužitelj koji sadržava primarnu zonu jest glavni izvor informacija o toj zoni. Takav se poslužitelj zove **glavni poslužitelj** (engl. *Master server*) i on pohranjuje **glavnu kopiju** (engl. *Master copy*) zone u AD-u ili u datoteci. Predefinirano ime datoteke s DNS zonom jest *ime_zone.dns*, a datoteka se nalazi u mapi **%windir%\System32\Dns** na DNS poslužitelju. Svakako prednost dajemo pohrani zone u ADu radi bolje sigurnosti, učinkovitijeg upravljanja i bolje (fleksibilnije) replikacije. Napomenimo da za pojedinu zonu može postojati samo jedan glavni poslužitelj. Primarna zona neke DNS zone može se modificirati, a promjene se repliciraju na ostale DNS servere.
- **Sekundarna zona** (engl. *Secondary zone*): DNS poslužitelj koji sadržava sekundarnu zonu neke primarne DNS zone upotrebljava se, najčešće, za ravnomjerno raspoređivanje opterećenja na mreži (engl. *Load balancing*). U sekundarnoj zoni nisu moguće izmjene. Ona je, drugim riječima, dostupna samo za čitanje informacija (engl. *Read only*). Predefinirano ova zona nije instalirana.
- **Krnja zona** (engl. *Stub zone*): Krnja je zona preslika zone koja sadržava samo one resurse koji su potrebni za identifikaciju autoritativnih DNS poslužitelja za tu zonu. Krnja se zona rabi za održavanje ili unapređenje učinkovitosti DNS rezolucije. Predefinirano ova zona nije instalirana.
- **Reverzna zona** (engl. *Reverse lookup zone*): Standardna DNS rezolucija na osnovi imena dobavlja IP adresu računala. Obrnuta DNS rezolucija funkcionira uz pomoć reverzne zone. Reverzna je zona imena **in-addr.arpa** i omogućuje rezoluciju IP adrese na osnovi imena. Predefinirano ova zona nije instalirana.
- **Prijenos zone** (engl. *Zone transfer*): Prijenos podataka među zonama potpuni je ili djelomični prijenos svih podataka zone s primarnog DNS poslužitelja koji sadržava određenu zonu na sekundarni DNS poslužitelj koji sadržava presliku zone. Prijenos zone predefinirano nije uključen i mora se uključiti za sve zone posebno.
- **Prosljeđivanje** (engl. *Forwarding*): Poslužitelj za prosljeđivanje (engl. *Forwarder*) jest DNS poslužitelj u mreži koji se rabi za prosljeđivanje DNS upita za vanjska DNS imena DNS poslužiteljima izvan lokalne mreže. DNS poslužitelj konfiguriran kao prosljednik znatno će smanjiti količinu DNS prometa prema Internetu i ubrzati DNS rezoluciju. Njegov lokalni DNS *cache* vrlo će brzo obuhvaćati većinu zahtjeva koji dolaze iz lokalne mreže.
- **Uvjetno prosljeđivanje** (engl. *Conditional forwarding*): Poslužitelj za uvjetovano prosljeđivanje (engl. *Conditional forwarder*) na osnovi imena domene u DNS upitu prosljeđuje upit specificiranom DNS poslužitelju.

Nakon kratkog ponavljanja opišimo okruženje koje želimo postići:

- **SERVERDC:** domenski kontroler i glavni DNS poslužitelj za racunarstvo.edu DNS zonu. Na njemu ćemo izraditi zonu za reverznu pretragu, konfigurirati prijenos zona i prosljeđivanje upita na drugu zonu.
- **SERVER1:** server član domene racunarstvo.edu na kojem ćemo instalirati DNS servis. Zatim ćemo izraditi sekundarnu zonu DNS zone racunarstvo.edu. Jednako ćemo tako izraditi jednu potpuno novu DNS zonu imena aos.edu u koju ćemo ručno dodati A zapis.
- **CLI1:** klijentsko računalo, član domene racunarstvo.edu, kojima ćemo se ćemo koristiti za testiranje funkcionalnosti DNS infrastrukture.

Implementacija DNS infrastrukture

Zadaci

1. Postaviti **racunarstvo.edu** na **SERVERDC**.
2. Instalirajte na oba poslužitelja DNS uloge.
3. Na **SERVERDC** podesite primarnu DNS zonu **vspr.edu**, te reverznu zonu za **10.10.10.0** mrežu.
4. Na **SERVER1** podesite sekundarnu zonu **vspr.edu**, te primarnu **algebra.edu**.
5. Na svakoj zoni kreirati host zapis za **www** tako da pokazuje na adresu poslužitelja 10.10.10.80.
6. Prigodno podesite i reverznu **10.10.10.x** zonu.
7. Uvjetnim proljeđivanjem podesite DNS servis na **SERVERDC**-u dostupnost **algebra.edu** zone.
8. Testirajte iz klijenta i napravite screenshot rezultata za:
 - a. Korištenjem **SERVERDC**-a kao DNS-a za upite:
 - i. www.vspr.edu
 - ii. www.algebra.edu
 - iii. 10.10.10.1 iv. 10.10.10.80
 - b. Korištenjem **SERVER1** kao DNS-a za upite:
 - i. www.vspr.edu
 - ii. www.algebra.edu iii. 10.10.10.1
9. Dodajte **Imstudenta-S1** i **CLI1** kao **članove** domene
10. Kreirajte **OU Serveri** i dodajte **SERVER1** unutra.
11. Kreirajte **OU Zaposlenici** i dodajte **CLI1** unutra.
12. Unutar **OU Zaposlenici** kreirajte korisnika **Zaposlenik01** i **Zaposlenik02**.

Podešavanje GPO-a

1. Promjeniti **Default Domain Policy** tako da zahtjeva minimalnu dužinu lozine od 10 znakova, te skratiti maksimalno trajanje na 30 dana.
2. Kreirati novi **GPO DisableSpooler** koji na **OU Serveri** onemogućuje servis za printanje – **Print Spooler**.
3. Kreirati **GPO MapPdrive** koji svim zaposlenicima mapira dijeljeni folder [\\Imstudenta-S1\Podaci](#) (potrebno ga je kreirati) kao disk **P**: Napraviti screenshot uspješno postavljenog diska i GPO postavki.
4. Kreirati novi GPO koji isključuje “General” stranicu u Internet Options dijelu Internet explorera.
5. Kreirati novi GPO koji svim korisnicima preumjerava mapu s dokuemntima na zajedničku dijeljenu mapu na serveru Imstudenta-S1. Mapu kreirajte sami I osigurajte da samo korisnik čiji su dokumenti u mapi ima u nju pristup
6. Kreirajte GPO koji će na svim računalima prebaciti RDP pristup sa porta 3389 na port 33389.
7. Onemogućiti svim zaposlenicima pristup do **ControlPanela** na korisničkim računalima korištenjem GPO-a. Napraviti screenshot zabrane pristupa na **CLI1**.
8. Nakon ponovnog pokretanja klijenta I servera ispišite popis svih politika koje se odnose na korisnika Zaposlenik02