



## KATEDRA ZA OPERACIJSKE SUSTAVE

# Planiranje mrežne infrastrukture

---

## Lab 01 – Napredni mrežni servisi



REV 1.2

Vedran Dakić

## Sadržaj

Uvod .....	1
Prije vježbe .....	4
Konfiguracija naprednih DHCP opcija .....	4
Podjela raspona .....	4
DHCP super-raspon .....	5
DHCP failover .....	6
Konfiguracija naprednih DNS opcija .....	8
DNSSEC .....	8
Raspon DNS portova .....	9
Zaključavanje DNS keša .....	9
Izrada GlobalNames zone .....	9
Rezultat vježbe .....	10
Što treba znati nakon ove vježbe? .....	11
Dodatna literatura .....	11

## Uvod

U današnjoj vježbi ćemo upoznati opcije DHCP i DNS poslužitelja s kojima se u prijašnjim kolegijima nismo bavili, a koje mogu dobro doći u osiguravanju infrastrukture ovih kritičnih mrežnih servisa. Podsjetimo se s predavanja opcija DHCP poslužitelja koje ćemo danas konfigurirati:

- **DHCP raspon:** jednostavno rečeno, DHCP raspon je obim IP adresa koji je moguće dodijeliti klijentima koji TCP/IP postavke primaju od DHCP poslužitelja. S osnovnim rasponom smo već upoznati iz kolegija OSMIS pa se u današnjoj vježbi nećemo previše baviti istime. Radije,



upoznat ćemo kako ga jednostavno i precizno podijeliti (eng. *Split*) između više poslužitelja u svrhu ravnomjernijeg opterećenja.

- **DHCP super-raspon:** super-raspon (eng. *Super Scope*) je mogućnost Windows Server DHCP poslužitelja namijenjena objedinjavanju dva ili više DHCP raspona. Nužno je da rasponi koje želite uključiti u super-raspon inicijalno budu neaktivni (eng. *Inactive*). Super-raspon je razmjerno lako konfigurirati putem DHCP konzole, a koristan može biti u nekoliko scenarija. Primjerice, ukoliko mijenjate adresnu shemu vaše mreže korištenje super-raspona može potpuno transparentno DHCP klijente migrirati u novi raspon IP adresa. Definirate novi raspon koji odražava novu adresnu shemu te on koegzistira s postojećim rasponom u super-rasponu. Klijente postepeno, nakon što im istekne dodijeljeno vrijeme (eng. *Lease time*) u starom rasponu, uvodite u novi raspon. Kad su svi klijenti u novom rasponu stari jednostavno isključite.
- **DHCP failover klaster:** Window Server 2012R2 poslužitelji s DHCP ulogom mogu međusobno dijeliti informacije o IP adresama koje su dodijelili klijentima. Postupkom replikacije riješen je stari problem koegzistencije više DHCP poslužitelja u istoj mreži (eng. *Subnet*), koji je gotovo sigurno dovodio do konflikta i duplikata na mreži. Kod DHCP failover klastera takve bojazni nema. U slučaju kvara jednog DHCP poslužitelja drugi poslužitelj uredno poslužuje klijente u cijeloj mreži.
- **DHCP zaštita imena:** značajka DHCP poslužitelja koja onemogućava prepisivanje (eng. *Overwrite*) unosa u DNS bazi. Prilikom ažuriranja DNS baze (uslijed promijene IP adrese klijenta) Window Server će provjeriti je li zahtjev zaista došao od računala koje je izvorni „vlasnik“ imena čija se IP adresa mijenja.

I DNS poslužitelj ima nekoliko mogućnosti kojih se valja prisjetiti:

- **Zaključavanje DNS keša** (eng. *DNS Cache locking*): sigurnosna značajka Windows Server 2012 R2 operacijskog sustava koja kontrolira kada je moguće prepisati informacije sadržane u DNS kešu. Prisjetimo se, prilikom rezolucije imena DNS poslužitelj informacije o upitu sprema u keš kako bi mogao brže odgovoriti na isti upit, jednom kada se pojavi. Trajanje zapisa u kešu je povezano s TTL (eng. *Time to live*) parametrom i predefinirano je postavljeno na 100% njegova vremena.
- **Raspon DNS portova:** Windows Server 2012 koristi tehniku nasumičnog dodjeljivanja DNS porta (eng. *Port randomization*). Maksimalni broj portova je 10000, a predefinirana vrijednost je 2500.
- **Global Names zona:** Global Names zona omogućava rezoluciju jednostavnih imena u drugim zonama. Primjerice, ukoliko klijent iz zone Racunarstvo.edu zatraži rezoluciju imena app1, takvo je ime moguće razlučiti isključivo u zoni racunarstvo.edu a ne, primjerice, u zoni algebra.edu. GlobalNames omogućava razlučivanje kratkih, jednostavnih imena u drugim zonama izradom odgovarajućeg CNAME zapisa u GlobalNames zoni.

I za kraj današnjeg uvoda pišimo infrastrukturu koju želimo postići:

- **SERVERDC:** domenski kontroler domene racunarstvo.edu, a ujedno DNS i DHCP poslužitelj. Na ovom računalu odrađujemo veliku većinu današnje vježbe.



- **SERVER1:** poslužitelj član domene racunarstvo.edu kojeg ćemo iskoristiti za konfiguraciju DHCP failover klastera.
- **CLI1:** klijentsko računalo u domeni racunarstvo.edu na kojem ćemo testirati konfigurirane opcije.

Ovime završava današnji uvod i možemo početi s vježbom.



## Prije vježbe

1. Pokrenite računalu u učionici sa Windows 8.1 operacijskim sustavom i prijavite se kao office:office.
2. Nakon učitavanja profila spojite se na cloud infrastrukturu korištenjem Horizon klienta, vašeg korisničkog imena i lozinke. Ove ćete podatke na prvim vježbama dobiti od profesora ili asistenta. Napomena: korisnička imena i lozinke su vaši, i **ne dijelite ih sa drugim kolegama studentima, jer bi to moglo utjecati na bodove koje "osvojite" na kolegiju.**
3. U Horizon clientu duplo kliknite na ikonicu PMI-CLI1, otvoriti će vam se prozor i biti ćete spojeni na CLI1 virtualnu mašinu, u koju se ulogiravate korištenjem standardne lozinke koju ste koristili i na AOS-u i OSMIS-u (Pa\$\$w0rd). Sa ove virtualne mašine spajate se na sve ostale virtualne mašine korištenjem Remote Desktop Connection-a. Adrese su slijedeće: a) CLI1 - 10.10.1.41  
b) CLI2 - 10.10.1.42  
c) SERVERDC - 10.10.10.1  
d) SERVER1 - 10.10.10.2  
e) SERVER2 - 10.10.10.3

Napomena: Ukoliko želite imati mogućnost spajanja na više virtualnih mašina odjednom korištenjem RDP protokola, u CLI1 virtualnu mašinu si instalirajte Remote Desktop Connection Manager. Url za preuzimanje dotične aplikacije je:

<https://www.microsoft.com/en-us/download/details.aspx?id=44989>

## Konfiguracija naprednih DHCP opcija

Kako je opisano u uvodnom dijelu vježbe, prvo ćemo se pozabaviti konfiguracijom naprednih opcija DHCP poslužitelja.

### Podjela raspona

Prvo povećajte kapacitet postojećeg DHCP raspona da vam **End IP address** bude **10.10.10.49**, te uključiti zaštitu imena na rasponu Klijeti.

Zatim na SERVER1 instalirajte DHCP poslužitelj.

Ne zaboravite da SERVER1 moramo autorizirati s AD-om kao DHCP poslužitelj.

Novi DHCP poslužitelj dodajte u DHCP konzolu na računalu SERVERDC.

Sad podijelite postojeći raspon između dva DHCP poslužitelja da svakom bude dodjeljeno pola raspona



Slika 1 Podjela DHCP raspona

DHCP raspon je podijeljen na način da je 50% kapaciteta IP adresa na računalu SERVERDC izuzeto od dodijele (engl. *Excluded from distribution*) klijentima. Vježbu nastavljamo konfiguracijom superraspona.

## DHCP super-raspon

Super-raspon se konfigurira od dva „obična“ raspona koji **ne smiju bit aktivni**.

Izradite prvi raspon imena **Raspon1**.

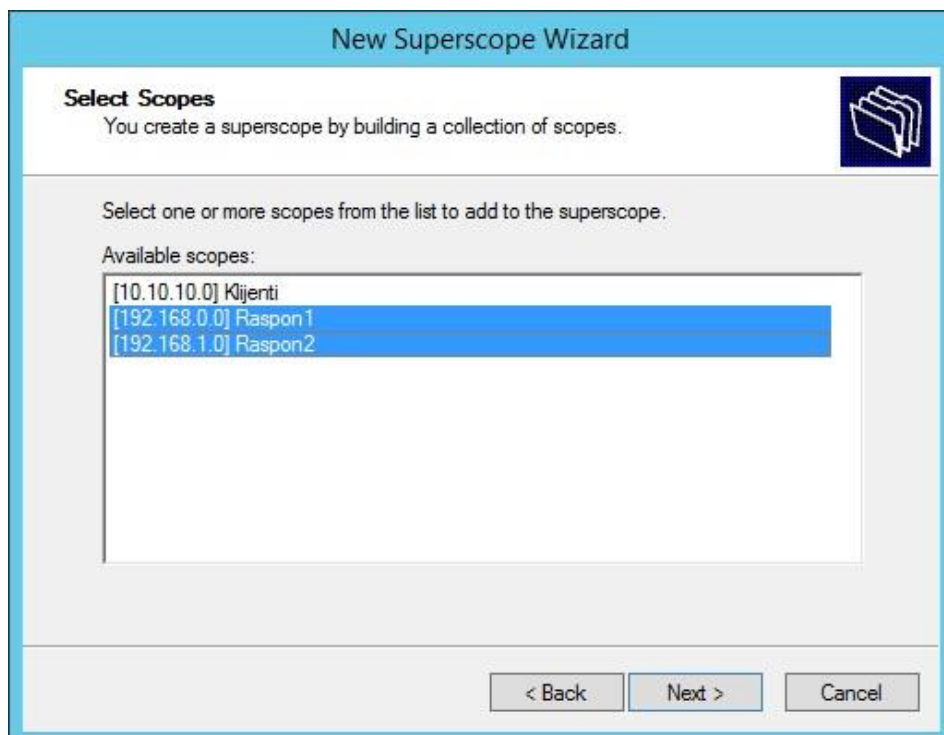
- Start IP address:** 192.168.0.50
- End IP address:** 192.168.0.100
- Lenght:** 24
- Router (Default Gateway):** 192.168.0.1
- DNS:** serverdc

Na isti način izrađujemo drugi raspon imena **Raspon2**.

- Start IP address:** 192.168.1.50
- End IP address:** 192.168.1.100
- Lenght:** 24
- Ostale postavke kao i na prvom rasponu**



Sada konfigurirajte super-raspon imena **SuperRacunarstvo**:



Slika 2 Rasponi za uključenje

**Napomena:** Opis slijedećeg koraka je samo radi potpunosti informacija. Nećemo raditi aktivaciju ovog superscope-a, ali, kada bismo to htjeli napraviti, procedura bi izgledala ovako. Unutar lijevog okna, pod poslužiteljem **SERVERDC**, desnim gumbom miša kliknite na stavku **Superscope SuperRacunarstvo** te iz kontekstualnog izbornika odaberite opciju **Activate**.

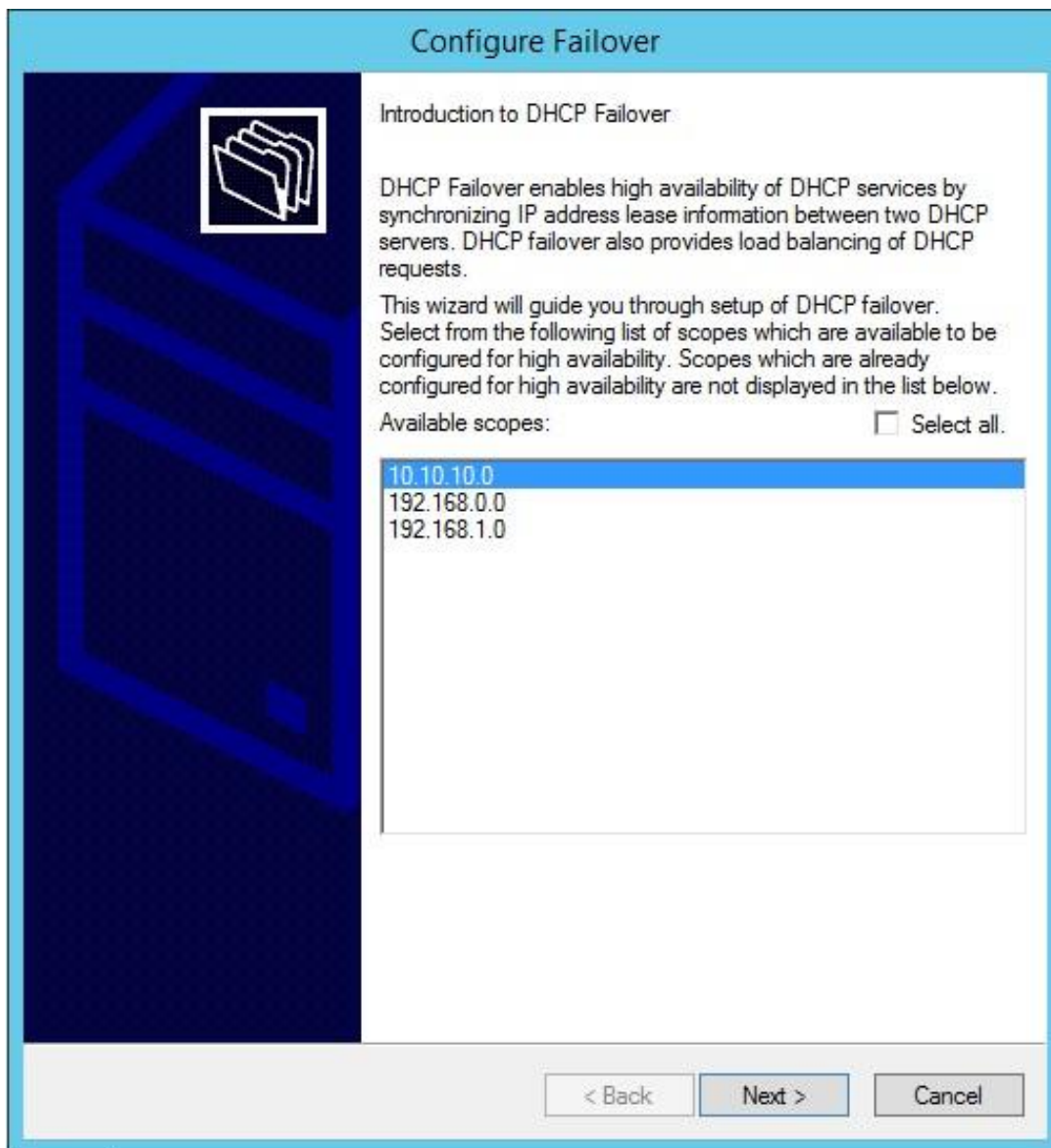
Super-raspon bi onda bio izrađen i aktiviran.

Obrišimo sada raspon IP izuzetih IP adresa, ukoliko ga imamo na 10.10.10.0/24 subnetu:

Sada možete konfigurirati DHCP failover.

## DHCP failover

Failover ćemo konfigurirati za raspon Klijenti koji odgovara mreži 10.10.10.0/24:



Slika 3 Raspon za uključanje u failover

1. **Partner Server:** 10.10.10.2
  - a. **Relationship Name:** Racunarstvo
  - b. **Maximum Client Lead Time:** 0 sati i 15 minuta
  - c. **Mode:** Load balance
  - d. **Load Balance Percentage:** 50% za Local i Partner Server
  - e. **Shared Secret:** Pa\$\$w0rd
2. Ne zatvarajte **DHCP** konzolu!





## Konfiguracija naprednih DNS opcija

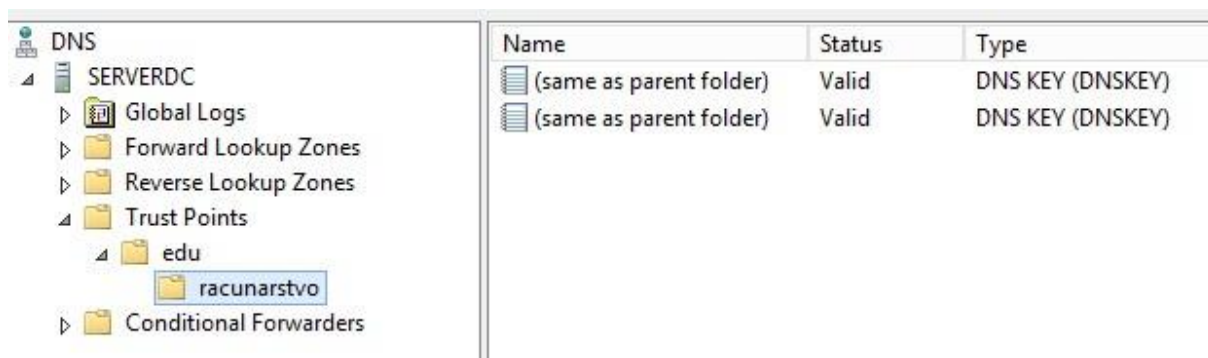
U drugome dijelu današnje vježbe konfiguriramo opcije DNS poslužitelja.

### DNSSEC

DNSSEC se konfigurira relativno jednostavno.

Prvi korak je potpisivanje zone.

Provjerimo jesu li zapisi stvoreni:



Name	Status	Type
(same as parent folder)	Valid	DNS KEY (DNSKEY)
(same as parent folder)	Valid	DNS KEY (DNSKEY)

Slika 4 DNSKEY zapisi

1. Zatvorite **DNS Manager** konzolu.

Klijentima ćemo putem Group Policyja forsirati korištenje potpisane zone za DNS sufiks racunarstvo.edu.

1. Napravite novi Group polici objekt imena **DNSSEC**.
2. Te u njemu pronađite **Name Resolution Policy** i postavite **Suffix** na **racunarstvo.edu**
3. **Computer Configuration-> Policies-> Windows Settings-> Name Resolution Policy.**
4. **Enable DNSSEC in this rule**
5. **Require DNS clients to check that the name and address data has been validated by the DNS server.**

Name Resolution Policy Table

Namespace	CA	DNSSEC (Validation)	DNSSEC (IPsec)	DNSSEC (IPsec Encryption)	DirectAc...	DirectAc...	D
.racunarstvo.edu		Yes	No				

Slika 5 DNSSEC pravilo

Nastavljamo vježbu s konfiguracijom preostalih opcija.



## Raspon DNS portova

Promijenit ćemo predefiniranu vrijednost broja portova putem PowerShella.

1. S naredbom **Get-DNSServer** možemo pogledati trenutne postavke DNS poslužitelja
2. Uočimo da je trenutna veličina poola 2500
3. Uz pomoć naredbe **dnscmd** promijenite veličinu poola na 3000
4. Restartajte **dns** servis
5. Provjerite s naredbom **Get-DNSServer** novu vrijednost

Kao što vidite, promjena vrijednosti portova nije komplicirana. Ista opaska vrijedi i za sljedeći parametar.

## Zaključavanje DNS keša

Ispišimo ponovno konfiguraciju DNS poslužitelja.

1. Uz pomoć powershella promijenite dns cache na 75

## Izrada GlobalNames zone

GlobalNames ćemo demonstrirati putem nove zone. Novu primarnu zonu već znamo izraditi putem DNS Manager konzole a sada je probajte izraditi putem PowerShella.

Prvo izradimo zonu

1. Naziv zone: **algebra.edu**

Uključujemo podršku za GlobalNames zonu.

2. Naredbom **Set-DnsServerGlobalNameZone** omogućite GlobalNames

Sada možemo izraditi GlobalNames zonu.

3. Naredbom **Add-DnsServerPrimaryZone** napravite GlobalNames zonu

Izradimo odgovarajuće zapise u zonama.

1. U zoni algebra.edu dodajte **A** zapis za **app1** s adresom **10.10.10.5**

Sada možemo izraditi u GlobalNames novi CNAME zapis.

- a. **Alias name:** app1
- b. **Fully qualified domain name (FQDN) for target host box:** app1.algebra.edu

Ovime završava današnja vježba. Isključite sva virtualna računala. *Checkpoint* nije potreban.



## Rezultat vježbe

Rezultat današnje vježbe su izmjene na virtualnim računalima kako slijedi:

### SERVERDC:

- Podijeljen DHCP raspon klijenti
- Implementiran super-raspon bez aktivacije
- Organiziran u DHCP failover klaster sa računalom SERVER1
- Implementirana GlobalNames zona
- Implementiran DNSSEC **SERVER1**:
- Instaliran DHCP poslužitelj
- Organiziran u DHCP failover klaster sa računalom SERVERDC



## Što treba znati nakon ove vježbe?

1. Podijeliti DHCP raspon
2. Izraditi super-raspon
3. Izraditi DHCP klaster
4. Izraditi GlobalNames zonu
5. Konfigurirati DNS Cache Lock
6. Konfigurirati količinu DNS portova

## Dodatna literatura

- Technet dokumentacija za DNSSEC <http://technet.microsoft.com/en-us/library/jj200221.aspx>
- Technet dokumentacija za DHCP failover klaster [http://technet.microsoft.com/en-](http://technet.microsoft.com/en-us/library/dn338978.aspx)

[us/library/dn338978.aspx](http://technet.microsoft.com/en-us/library/dn338978.aspx)