

IDEJNO REŠENJE IT INFRASTRUKTURE

U dizajniranju novog tehničkog rešenja pošlo se od sledećih zahteva:

1. Javni DNS servis sadrži oko 50 hiljada zapisa sa tendencijom rasta do 100 000 hiljada u narednih godinu dana. Dnevno se u proseku ažurira oko 100 zapisa sa tendencijom rasta 300 zapisa u narednih godinu dana.
2. Veb sajt RNIDS sa informacijama o RNIDS kao organizaciji i uputstvima za korisnike.
3. Aplikacija i baza podataka za registraciju domena (Microsoft IIS i SQL) sa 150 konkurentnih korisnika i tendencijom rasta do 300 u narednih godinu dana. Veličina baze je manja od 5 GB sa tendencijom rasta do 10 GB u narednih godinu dana.
4. Sistem za razmenu elektronske pošte (klijentski i *webmail* pristup) sa 25 korisnika i prosečnom veličinom *mailbox*-a od 1 GB sa tendencijom rasta na 50 korisnika i prosečnom veličinom *mailbox*-a od 2 GB.
5. CA (Certificate Authority) servis za potrebe izdavanja klijentskih sertifikata kao dodatne kontrole pristupa.
6. Centralizovani bekap podataka baze za registraciju domena, baze email poruka, kao i svih servera na primarnoj lokaciji. Bekap baza i servera se radi svakodnevno i to kompletan (full) bekap. Tri poslednja bekapa su dostupna on-line, dok se svi stariji bekapi arhiviraju i čuvaju šest meseci.
7. Druge neophodne servise za podršku funkcionisanju prethodno navedenih servisa.

Dizajn tehničkog rešenja mora da ispunjava sledeće opšte zahteve:

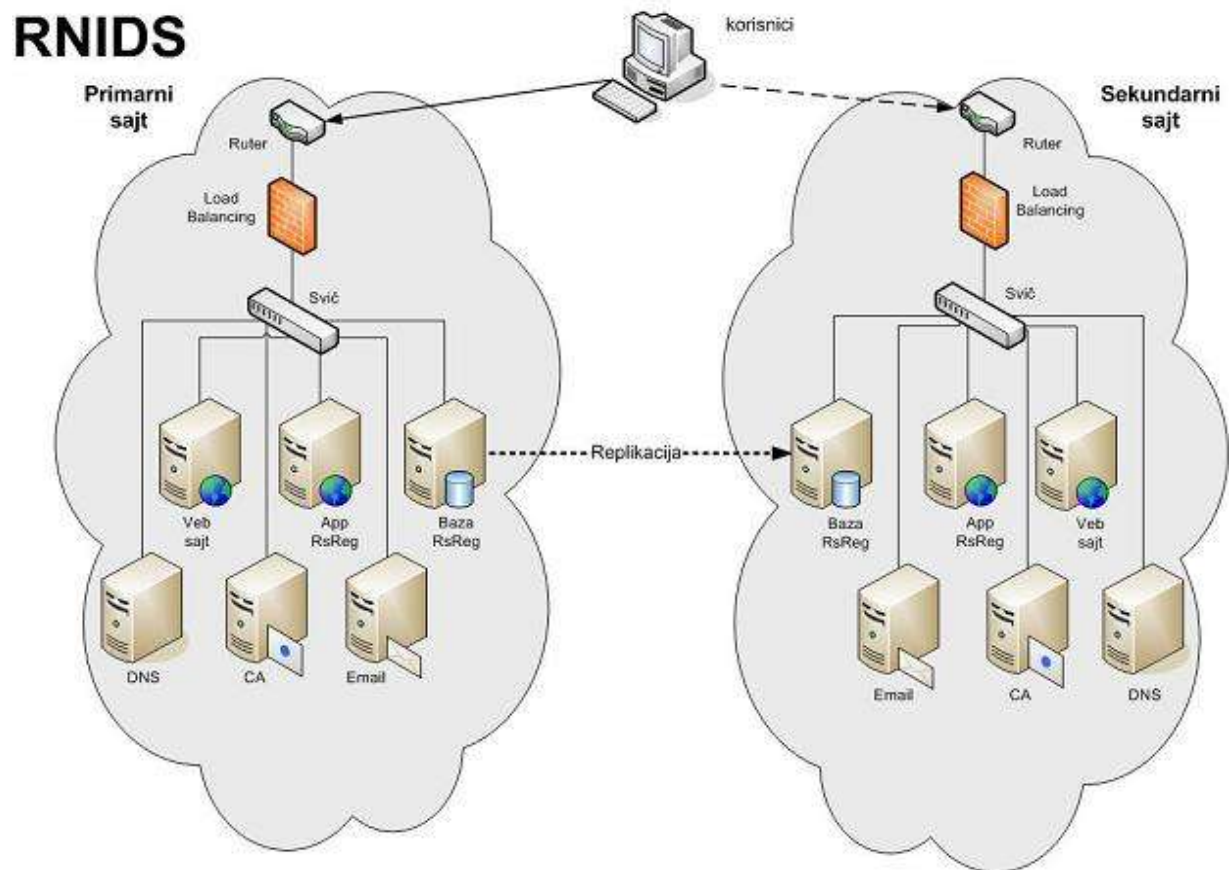
1. Rešenje treba da obezbedi pouzdan rad svih servisa i da pruža potrebne performanse.
2. Rešenje treba da omogući oporavak najvažnijih servisa (Registracija domena, DNS) na primarnom sajtu u roku od 2 sata, a ostalih u roku od 8 sati.
3. Rešenje treba da omogući prelazak na sekundarni sajt u roku od 4 sata.
4. Rešenje treba da spreči gubitak podataka o domenima.
5. Rešenje treba da pruži zaštitu sistema od neovlašćenog pristupa.

Rešenje mora da sadrži opis sledećih komponenti

1. Dve lokacije (primarna i sekundarna) udaljenosti 5-10 km.
2. Mrežna infrastruktura sa specifikacijom opreme i opisom njene uloge u sistemu.

3. Serveri sa opštim opisom konfiguracije i ulogom u sistemu.
4. Replikacija podataka sa opisom mehanizma koji se predlaže.
5. Postupak prelaska produkcije sa primarne na sekundarnu lokaciju.
6. Bekap podataka i servera.
7. Oporavak podataka i servera kako na primarnom tako i na sekundarnom sajtu.
8. Migracija podataka i servisa sa postojeće platforme na novu.

Osnovni dizajn rešenja



Mreža

Osnovni dizajn čine sledeći mrežni elementi:

- Ruter

- Uređaj koji omogućava kontinuitet IT servisa (Load Balancing). Uloga ovog uređaja je da omogućí da svi servisi budu javno dostupni po virtualnim IP adresama. Za svaku virtualnu IP adresu se definišu fizičke adrese servera (jedan ili više) koji čine dati servis. Raspoloživost svakog od servisa, uređaj proverava pomoću unapred definisanih proba i po unapred definisanoj dinamici. Ukoliko servis nije raspoloživ, nije raspoloživa ni virtualna IP adresa na datom uređaju. U tom slučaju servis postaje dostupan preko drugog uređaja na drugoj lokaciji. Poznati uređaji ovog tipa su Cisco ACE, F5 BIG IP, ..

- Svič

Serveri

Osnovni dizajn čine sledeći serveri:

- Javni DNS server za domen
- Aplikativni server za registraciju domena
- Server baze podataka za registraciju domena
- CA server za izdavanje klijentskih sertifikata
- Javni Veb server
- Interni server za razmenu elektronske pošte.

Softver

Osnovni dizajn uključuje sledeći softver:

- Operativni sistem za DNS
- Operativni sistem za aplikativni server (Windows 2008 Server)
- Operativni sistem za server baze podataka (Windows 2008 Server Enterprise Edition)
- Softver za upravljanje bazom podataka (MS SQL 2008 Enterprise Edition)
- Operativni sistem za CA server (Windows 2008 Server)
- Operativni sistem za veb server
- Operativni sistem za server za razmenu elektronske pošte (Email).
- Softver za razmenu elektronske pošte (Email).
- Softver za bekap i oporavak podataka i servera.

Principi funkcionisanja rešenja

- Komunikacija sa spoljnim svetom se odvija preko rutera. Na ruter dolaze bar dva nezavisna Internet linka.
- Saobraćaj sa rutera dolazi do uređaja koji omogućuje kontinuitet IT servisa. Sve što stiže na određenu virtualnu IP adresu usmerava se na odgovarajući server (ili više servera).
- Podaci iz baze podataka na primarnom sajtu se asinhrono repliciraju na sekundarnu lokaciju (nakon svake transakcije vrši se replikacija iste na sekundarnu lokaciju).
- Komunikacija između primarnog i sekundarnog sajta se odvija preko Interneta. Ne postoje direktne veze.
- Na sekundarnoj lokaciji, osim servera baze podataka, postoje spremni serveri: aplikativni, veb i DNS. Ovi serveri se ažuriraju istovremeno kada i odgovarajući serveri na primarnom sajtu. U slučaju prelaska produkcije na sekundarnu lokaciju CA i Email server se „podižu“ iz bekapa.
- U slučaju problema sa nekim od servisa na primarnoj lokaciji korisnici se preusmeravaju na sekundarni sajt uz pomoć nekog od poznatih uređaja ili mehanizama za tu namenu (Cisco GSS, RHI, ...). Sličan priča važi i u slučaju nedostupnosti cele lokacije). Po istom principu funkcioniše i povratak na primarnu lokaciju.

Udaljeni pristup

- Za administraciju mrežne opreme biće omogućen udaljeni pristup sa unapred definisanih IP adresa i odgovarajuća prava na opremi licima angažovani za administraciju.
- Udaljeni pristup serverima, a naročito podacima od strane lica angažovanih za administraciju sistema, biće regulisan posebnom procedurom. Procedura će podrazumevati da nije moguć pristup u bilo koje doba i sa bilo kog mesta.
- Za zaposlene će biti omogućen udaljeni pristup u bilo koje doba i sa bilo kog mesta.

Varijante rešenja

- Rešenje može da se realizuje i bez nabavke rutera. U tom slučaju bi zakup lokacije za smeštanje opreme uključivao i usluge rutiranja.

. Kritični serveri (aplikativni server i baza za RsReg, DNS) na primarnoj lokaciji mogu biti duplirani čime se izbegava prelazak na sekundarni sajt u slučaju manjih problema.

- Realno je očekivati da će se u budućnosti povećavati broj servera (dokumentacioni sistem, tiketing sistem, veb portal, whois server, ...). U tom slučaju bi bilo isplativo odlučiti se za virtualizaciju servera i time smanjiti investicije u budućnosti.

Prednosti rešenja

- Dobija se stabilna i bezbedna primarna lokacija. Na ovaj način se obezbeđuju uslovi da ogromnu većinu vremena produkcija bude na primarnoj lokaciji, bez prekida, pada performansi i slično. To su ujedno i najbolji uslovi za rad korisnika. S druge strane, sekundarna lokacija bi se u normalnim okolnostima koristila za testiranje novih softvera, novih verzija softvera, ispravki softvera, itd.

- Sve ključne funkcionalnosti infrastrukture se oslanjaju na poznata i u praksi dobro proverena rešenja (hardver i softver).

- Svi serveri mogu da imaju IP adrese iz privatnog opsega.

- Ne postoji treća lokacija. To znači da od manji firmi zavisi funkcionisanje sistema, manje ugovora, manje potencijalnih mesta za probleme. S druge strane to doprinosi jednostavnijoj implementaciji rešenja, jednostavnijem monitoringu, jednostavnijem otkrivanju uzroka potencijalnih problema i njihovom jednostavnijem rešavanju. Isto tako, budući razvoj infrastrukture će imati manje ograničenja.

- Izbegava se mogućnost konflikta sa podacima u bazi na primarnom u odnosu na bazu na sekundarnom sajtu. Pisanje je omogućeno samo na jednoj instanci baze podataka.

- Nema izmena DNS zapisa.