BIND/DNS savjeti i trikovi

Matko Kosmat | 31 ožujka, 2026

BIND je na CARNetovim računalima oduvijek bio u ulozi poslužitelja za DNS, te je gotovo postao sinonim za DNS sustav. Iako je konfiguracija kompleksna, preko CARNetovih paketa BIND dolazi konfiguriran i spreman za uporabu. Sistem inženjeru jedino preostaje redovito održavati sustav i dodavati, mijenjati i brisati podatke iz zonskih datoteka.

Kako je DNS izuzetno važan servis, valja posvetiti posebnu pažnju problemima koji se javljaju u radu, što ćemo pokušati riješiti s nizom članaka na tu temu.

U zonskim datotekama vaših DNS poslužitelja se nalazi serijski broj, kojeg obično povećamo kada dodajemo nove hostove ili jednostavno mijenjamo podatke u nasim zonama. Ovo radimo kako bi sekundarni DNS poslužitelji znali da je nastupila promjena i da trebaju skinuti novu inačicu zonske datoteke.

Podsjetimo se kako izgleda dio datoteke sa serijskim brojem:

Serijski broj nema službeno definirani format, i možemo početi od jedinice, povećavati na dva, tri i tako dalje. No, zgodno je znati kada smo nešto mijenjali, kako bi lakše utvrdili kada je (i ako) došlo do greške. Zato se serijski broj obično piše u obliku datuma:

Oznaka G je, naravno, godina, M mjesec, a D dan promjene. Kako u jednom danu možemo imati više izmjena, ostavili smo dva polja slobodna za broj revizije (R) toga dana. Ovo je znatno praktičnije i jednostavnije nego pisanje sata, minuta ili sekundi u tom polju.

Ukoliko se pitate zašto je predloženi format "obrnut" od "standardnog" DDMMGGGG, odgovor je jednostavan: zbog numeričkog sortiranja. Datum 2010101201 (12. listopada 2010.) će numerički uvijek biti ispred kasnijeg datuma, primjerice 2010121001 (10. prosinca 2010.). Na taj način ne morate misliti je li broj veći ili nije, nego jednostavno upišete datum na predviđeno mjesto, i ukoliko ima revizija povećate zadnju znamenku.

No, neiskusniji sistemci mogu napraviti pogrešku ukoliko nisu upoznati s ovim načinom obilježavanja. Naime, kako na prvi pogled znati je li prvi datum iz primjera 12. listopada ili 10. prosinca? No, zabune se u praksi događaju. Navest ćemo konkretan primjer sa helpdeska za sistem-inženjere:

Nagađamo da je nepažnjom sistemca jednom zapisan datum u pogrešnom obliku (2010270204, 27. veljače), te da je nakon neke promjene u zonskoj datoteci zapisan pravilni oblik datuma (2010091701, 17. rujna). No, sada taj broj više nije veći od prethodnog i - imamo problem.

Ukoliko ne pratite logove (**no, vi ih redovito pratite, zar ne?**), ovu grešku nećete ni primijetiti, sve dok ne shvatite da se vaše promjene ne vide u DNS-u, ili vam netko ne javi da ne može pristupiti resursu za kojeg znate da ste ga dodali u DNS.

Grešku je, zapravo, lako popraviti, ukoliko stavimo veći serijski broj. No, on tada više neće moći održavati datum promjene (što možete staviti u komentar unutar datoteke). Dakle, najelegantnije rješenje je staviti sljedeći serijski broj:

Prvi siječnja 2011. je svakako veći od pogrešno zapisanog datuma, a sve što trebate napraviti u sljedećoj godini je vratiti se preporučenoj shemi GGGGMMDDRR. Ukoliko imate promjena i prije tog datuma, jednostavno povećavajte broj revizije - imate mogućnost napraviti još barem 98 revizija.

Ne možemo ovdje ne spomenuti specifičnost serijskog broja u BIND-u, a ona se pojavljuje i u drugim aspektima i primjenama u IKT. Serijski brojevi se računaju u tzv. SNA aritmetici - Serial Number Arithmetic (http://en.wikipedia.org/wiki/Serial_number_arithmetic), gdje je moguće da je 10 > 2500000000. Kako je to moguće?

Serijski broj u BIND zonama je 32-bitni broj (2^32), što kad izračunamo, dobijamo raspon mogućih vrijednosti od 0 do 4294967295. Nulu ne uzimamo u obzir, iako je nekad služila upravo za resetiranje serijskog broja, no danas to nije tako. U ovom načinu računanja, pola svih brojeva (2147483647) je veće, dok je druga polovica manja od trenutnog serijskog broja.

Nakon što ste dosegli najveći mogući broj, brojanje počinje iznova od jedan, pa je tako 10 manje od 11 do 11+2147483647, ali **veće** od brojeva od 11+2147483649 do 4294967295, a nakon prebacivanja maksimalne vrijednosti i od brojeva 1 do 8.

(Broj 2147483648 ne uzimamo u obzir, jer se nalazi točno u sredini raspona).

U konkretnom primjeru, a po preporuci iz O'Reilleyeve knjige "DNS and BIND" (strana 153.), kada želite smanjiti serijski broj, na trenutni broj dodajte vrijednost 2147483647.

Sada imamo dva moguća rješenja:

a) Zbroj nije prešao 4294967295 i ne morate dalje ništa računati. Kako smo gore objasnili, u ovakvom načinu računanja, broj 4157753851 je *manji* od brojeva u rasponu od 4157753852 do 4294967295, te nakon *prelamanja* i od 1 do 2010270202. 4157753851 je vaš novi Serial.

b) Zbroj je prešao maksimalnu vrijednost 4294967295, pa moramo od tog broja (npr. neka je točno 5000000000) oduzmite 4294967296:

To je vaš novi Serial koji morate unijeti u zonsku datoteku.

a) Serijski broj 4157753851 je *manji* od 2010270202, pa time i 2010091701

b) Serijski broj 705032704 je manji od 2010270202, pa time i 2010091701

U oba slučaja u ovom trenutku morate **reloadati ili restartati** DNS poslužitelj.

Kada svi slave DNS poslužitelji preuzmu vašu zonu, možete postaviti željenu vrijednost 2010091701 koja će sada biti veća od zadnjeg serijskog broja.

Ovime smo postigli naš cilj, u dva koraka. Komplicirano? Naravno da jest, pa preporučujemo način iz prvog primjera, ali zapamtite ovaj specifičan način računanja serijskog broja - možda vam uštedi koji sat rada.

Dodatni resursi: https://web.archive.org/web/20150811013651/http://www.brandonhutchinson.com/resetting_bind_serial_number.html

EDIT: 2023-09-12

DNS sustav je prilično osjetljiv na razne greške, a to obično rezultira prestankom rada jednog ili više servisa. Kada tome dodamo manje iskusnog sistem-inženjera, situacija vrlo brzo može postati jako loša. Jedna od najčešćih problema je nemogućnost isporuke elektroničke pošte, jer udaljeni poslužitelj zahtijeva da vaš mail poslužitelj ima ispravan reverzni zapis.

Problem je lako rješiv: dodajte reverznu zonu, ili samo nedostajući zapis ukoliko zona već postoji. No što ukoliko se počnu pojavljivati greške poput ove, obično u datoteci /var/log/daemon.log:

Očigledno, radi se o nekakvoj greški imenovanja, što sprječava da se zona učita i time bilo koji zapis u zoni nije uvažen. Zonska datoteka na prvi pogled izgleda prilično uobičajeno:

U logu se može vidjeti da je greška u drugom retku datoteke (2:), dakle u samom SOA zapisu, no on izgleda prilično uobičajeno. Štoviše, identičan zapis već imate u forward zoni, a tu nemate nikakvih problema. No, zbog skraćenog oblika pisanja unutar zonske datoteke (**posluzitelj** umjesto **posluzitelj.domena.hr.**) događa se transformacija zapisa na sljedeći način (pretpostavimo da je vaša reverzna zona 1.53.161.in-addr.arpa):

Ne izgleda baš lijepo, zar ne? Ali, čak i ovakav neispravan zapis neće prouzrokovati grešku koju ovdje opisujemo. Potreban je još jedan element: morate imati ***parcijalnu* reverznu zonu**. Situacija onda izgleda ovako:

Sada u zonskoj datoteci imamo još jedan karakter, a nevolja je u tome što taj znak nije dopušten za uporabu za nazive hostova unutar DNS sustava. Za DNS u principu smijete rabiti samo alfanumeričke znakove (**a-z**, **0-9**) i crticu (**-**). Sve ostalo će izazvati grešku, koju možda nećete odmah ni primjetiti.

Iako je kraći način zapisa pregledniji, može dovesti do neželjenih situacija, ili ovakvih ozbiljnih smetnji. Da biste izbjegli ovakve situacije, u zonskim datotekama, barem u SOA recordu, stavite puni oblik:

Ne zaboravite točku na kraju (hr**.**) inače ćete dobiti gotovo pa "monstruozan" oblik zapisa:

Točka označava kraj zapisa, odnosno "root zonu", i nakon nje DNS neće "lijepiti" nikakve nazive. Dakle, upotrebljavajte dulje nazive i ne zaboravite točku na kraju, a možda je najbolje cijelu reverznu zonu (ili barem dio s PC-ima korisnika) napraviti pomoću direktive $GENERATE, koju smo opisali u članku /sys-trek-objave/bind-dns-savjeti-i-trikovi/#bind-pojednostavite-konfiguraciju-pomocu-direktive-generate.

Ukoliko u logovima primjetite poruku "**bad owner name (check-names)**", radi se o vrlo sličnoj greški kao i u slučaju koji smo opisali u članku /sys-trek-objave/bind-dns-savjeti-i-trikovi/#bind-greska-bad-name-check-names. Sama formulacija greške može navesti na krivi put, pa možete pomisliti da se radi o krivo podešenim pravima pristupa nad nekom od zonskih datoteka. No, ipak se radi samo o krivo upisanim podacima, najčešće jednostavno iskopiranim iz *forward* zona. Pogledajmo kako greška izgleda i što je uzrokuje.

(Namjerno smo *grepali* podatke iz starijih rotiranih logova, jer se ova greška pojavljuje kod restarta BIND servisa, pa ne mora biti prisutna u aktualnom logu **daemon.log**)

Kao i u maloprije spomenutom članku, uz grešku se vidi i broj retka, a to je u ovom slučaju 36:

Na prvi pogled sve je u redu, no baš i nije. Naime, adresnim zapisima ("A" *record*) nije mjesto unutar reverzne zone. U reverznim zonama bi se u pravilu trebali nalaziti samo pokazivački zapisi ("PTR", *pointer record*), dakle nešto poput ovog:

Ako se prisjetimo da zapisi bez točke na kraju dobijaju trenutnu ekstenziju ($ORIGIN, u ovom slučaju 0/25.XX.198.193.in-addr.arpa), zapis će nakon procesiranja izgledati ovako:

što je upravo ono što želimo. **Napomena**: ne zaboravite da bi PTR zapisi trebali pokazivati na "prava" (*canonical*) imena, ne na aliase (CNAME zapise). Ne zaboravite dodati domenu i točku na kraju, kako se ne bi string iz $ORIGIN nalijepio na kraj zapisa!

Spomenimo i još jedan slučaj iz prakse kada se može pojaviti "**bad owner name**" greška. Istu grešku bi mogao izbaciti i ovakav zapis:

Naime, uporaba "_" nije dopuštena, i iako greška nije fatalna, držite se samo slova, brojeva i crtice ("-").

Kako smo već pisali, inačica BIND DNS poslužitelja donosi neke novosti. Neke od njih mogu izazvati velik broj lažnih upozorenja od raznih sustava za nadzor logova (logcheck, OSSEC). Kako je ovo samo odraz činjenice da su uvedena neka ograničenja, ova se upozorenja mogu ignorirati. Na prvom mjestu, radi se o upozorenju o tome da je "EDNS ugašen", te da je nekom klijentu izvan vaše mreže uskraćen rekurzivni upit.

EDNS je proširenje DNS-a, u smislu proširenja postojećeg polja OPT kako bi se zadovoljile nove, poželjnije funkcije. Kako EDNS nije tema članka, za više informacija pogledajte Wikipediju na linku http://en.wikipedia.org/wiki/EDNS. Također, ukoliko želite provjeriti dolazi li do ovih poruka zbog nekog vašeg vatrozida, pogledajte poruku na Usenetu: http://groups.google.com/group/comp.protocols.dns.bind/browse_thread/thread/cfa8c63ec6bd08d6.

U većini slučajeva, pojavljivanje ovih poruka će biti dovoljno samo spriječiti putem direktive u named.conf.local (jer drugo i nećete moći učiniti). Dovoljno je upiati u *logging* blok:

Nakon restarta procesa "named", poruke se više ne bi trebale pojavljivati.

Drugi problem koji se pojavio je pojavljivanje mnogobrojnih poruka "denied", u obliku:

Zbog novosti uvedenih u novom BIND-u, ove poruke će se pojavljivati za svakog klijenta izvan "trusted" deklaracije. Nije baš razborito ukloniti u potpunosti ove poruke: bolje je da ih logcheck ignorira. Ovo ćemo postići tako da u /etc/logcheck/ignore.d.server/local upišete:

Za OSSEC, taj redak upišite u ovom obliku u datoteku /var/ossec/rules/local_rules.xml:

SID je broj koji vam se prikaže kod izvješća, pa ga prilagodite po potrebi. Stvar je jednostavnija za rule_id, samo odaberite prvi slobodni broj veći od 100000, što je rezervirano za korisnička pravila.

Kako smo već spomenuli, nije razborito ove poruke potpuno izbrisati iz logova. No, i to se može:

U ovom slučaju nemate nikakve indikacije o odbijanju upita, iako je ta informacija izuzetno korisna kod prvotnog postavljanja DNS sustava na računalo. Rješenje je ili odgoditi postavljanje ove direktive dok ne postavite sustav DNS-a, ili filtrirati ove unose u vašem omiljenom *log checkeru*.

U prethodnim člancima smo se dotaknuli teme o načinima *logginga* u BIND-u, odnosno kako napraviti da se određene kategorije log zapisa uopće ne pojavljuju u logovima. Naravno da tu nije kraj, te da BIND može puno više. Vratimo se malo u povijest... BIND inačice 4 je imao samo rudimentarne mogućnosti logiranja, odnosno samo uobičajeni način povećanja ili smanjivanja razine zapisa (*verbosity*), kao što to ima većina drugih servisa.

Novije inačice BIND-a uvode pojam kanala (*channela*), preko kojih možete definirati što će se (koje informacije iz BIND-a) i gdje logirati (zapisivati u posebnu datoteku ili slati u syslog). Pri tome je u kanalu moguće kombinirati obje opcije, i tako definirati način logiranja kako vam u određenim situacijama najviše odgovara.

Neki su kanali već ugrađeni, ali njih ne možete mijenjati, nego možete samo dopisivati nove kanale. To znači da ako određeni kanal zapisuje i u syslog i u posebnu datoteku, nećete moći promijeniti to ponašanje. Ali, vrlo je jednostavno kreirati drugi kanal koji će raditi po vašim potrebama.

Iako ovaj sustav logiranja nudi veliku fleksibilnost, i nije tako jednostavan za definirati, pa ćemo se ograničiti samo na praktičnu primjenu. Za više informacija pogledajte odličnu O'Reillyevu knjigu "BIND & DNS", ili dokumentaciju na Internetu (npr. http://www.bind9.net/).

Primjer 1: kako spriječiti pojavljivanje "*lame server*" poruka u logovima?

Ova se poruka pojavljuje zbog loše podešenosti drugih DNS poslužitelja, ne vašeg, stoga je razumljiva ideja da se te poruke ne bilježe u vašem syslogu. Te poruke se ponekad mogu pretjerano pojavljivati i oduzimati vam mrežne i procesorske resurse.

U named.conf.local ukucajte sljedeće retke:

Ovime smo kateogoriju "lame-servers" presumjerili na ugrađeni kanal "null", što, jasno, znači da se poruke o *lame* poslužiteljima jednostavno neće bilježiti. Ipak, u slučaju da imate problema s konfiguracijom DNS poslužitelja, zakomentirajte ove linije kako biste mogli vidjeti sve poruke koje će vam možda pomoći u rješavanju problema.

Naravno, morat ćete BIND-u reći da se konfiguracija promjenila:

Pažljiviji će čitatelji primjetiti da ove retke donosi paket bind9-cn, pa ih ne treba posebno unositi.

Primjer 2: kako vidjeti koje upite naš poslužitelj prima?

U named.conf.local ukucajte slijedeće:

Ovdje smo kreirali novi kanal, i nazvali ga "moja_datoteka", da nas podsjeća da na to zapisi idu samo u jednu datoteku, /var/cache/bind/log.queries. Direktiva "severity" može biti jedna od:

Slično kao i kod sysloga, ova direktiva određuje da će se zapisivati samo ta razina informacija i viša. Pretpostavljena vrijednost je **info**. "Dynamic" znači da razinu određujemo preko naredbenolinijskog parametra "-d" ili preko naredbe "rndc trace".

U ovom primjeru, potrebno je pokrenuti **debug** način rada putem naredbe:

Kao što smo prije spomenuli, ovaj sustav logiranja je kompleksan, te će se uključivanjem debug načina rada odjednom pojaviti i datoteka named.run u istom direktoriju. U njoj se nalaze dodatni debug podaci, koji nas u ovoj
konfiguraciji ne zanimaju, pa ćemo ih isključiti. Cijela konfiguracija tada izgleda ovako:

I opet:

Sa cijelom ovom konfiguracijom isključili smo logiranje poruka o "*lame* serverima", preusmjerili standardne poruke u syslog i ugasili dodatne debug podatke, te na kraju logiranje upita preusmjerili u datoteku po želji.

Logovi znaju jako brzo narasti, pa ih je upitno staviti u neki logrotate sustav, ukoliko na dulje vrijeme želite pratiti rad DNS sustava.

Ukoliko ste ikad rabili CARNetovu uslugu provjere ranjivosti vaše mreže, vrlo vjerojatno ste dobili uputu da bi bilo dobro sakriti inačicu BIND-a.
Ova operacija se provodi u svrhu povećane sigurnosti, jer eventualni napadač nema informaciju o kojoj se točno inačici softvera radi.

Samim tim prvo mora saznati tu informaciju, ili napadati na slijepo, što mu oduzima više vremena. Ako zna točnu informaciju o inačici, napadač može upotrijebiti već gotove alate za provaljivanje, a za to ne mora imati nikakva posebna znanja (tzv. "script kiddies").

Informaciju o inačici BIND-a možete saznati na više načina:

DNS_SERVER je adresa poslužitelja čiju inačicu želite saznati:

Drugi način je preko alata dig:

U svakom slučaju, inačica poslužitelja je upisana u zapisu "version.bind".

Moramo spomenuti da ova informacija napadaču nije od presudne važnosti ukoliko je vaš sustav redovito održavan i patchiran, jer onda napadač nema ulazni vektor. No, ukoliko želite, vrlo lako možete sakriti tu informaciju. Dovoljno će biti u datoteci named.conf upisati opciju:

To morate napraviti u bloku "options", pa će izmjena izgledati otprilike ovako:

te napraviti

Provjerite postoje li kakve poruke o greškama u log datoteci /var/log/daemon.log. Sad bi DNS poslužitelj na upit o inačici trebao
odgovarati ovako:

Čestitamo, upravo ste dodali jedan mali dodatak sigurnosti vašeg poslužitelja.

Konfiguracija DNS sustava je, vjerujemo, jedna od stvari koji sistem-inženjer početnik ne voli raditi. Kriptična konfiguracija, ovisnost o drugim poslužiteljima, papirologija koja se mora slati ukoliko se rade veće promjene - sve to odbija od istraživanja mogućnosti DNS sustava.

No, nakon inicijalne konfiguracije (koja je olakšana ukoliko imate paket **bind9-cn**) stvari kasnije idu nešto lakše, jer je potrebno samo dodavati nove hostove u konfiguraciju. Ni to nije bez opasnosti, jer jedna zaboravljena točka na kraju zapisa može omesti rada DNS servisa. Kod unošenja većeg broja hostova ovo je svakako moguće, a kako bi umanjili ovu mogućnost, možemo rabiti direktivu **$GENERATE**.

Direktivu $GENERATE možemo shvatiti kao petlju u nekom programskom jeziku jer ima varijablu koja se povećava u svakoj iteraciji, u nekom određenom rasponu kojeg vi određujete. Najlakše je objasniti

kako to izgleda preko primjera:

Da ste umjesto preko direktive $GENERATE išli ručnim unosom, morali biste unijeti preko 250 redaka u ovom obliku:

Sada možemo vidjeti kako $GENERATE radi. Nakon same direktive navodimo raspon brojeva u kojem želimo da se varijabla povećava, zatim samu varijablu (označava se jednostavno sa '$'), te ostatak DNS zapisa kojeg želimo generirati. Dakle, sve je upravo kao u nekoj programskoj petlji, gdje će se varijabla uvećati u svakoj novoj iteraciji.

U primjeru smo rabili PTR zapis za reverznu zonu s privatnim adresama (0/16.0.168.192.in-addr.arpa), što je zgodno kada adrese dodjeljujete preko DHCP-a, kada možete navesti cijele *poolove* adresa koje možda imate u LAN-u:

Moramo napomenuti da radi jasnoće rabimo skraćeni oblik zapisa, puni zapis bi zapravo izgledao ovako:

$GENERATE vrijedi i za ove zapise: **A** (address), **AAAA** (IPv6 address), **NS** (Name Server), **CNAME** (Canonical Name odnosno Alias) i **DNAME** (Delegation Name odnosno Alias za domene). Opet ćemo posegnuti za primjerom, kada jednostavno želite uniformne nazive za računala u vašoj mreži:

što će se pretvoriti u niz adresnih (A) zapisa :

Napomena: oznaka "X" je naravno konkretna adresa vaše mreže, ne stoji kao varijabla ili bilo što slično!

Nadamo se da smo vam ovim člankom uštedili nešto tipkanja, te spriječili razne sitne greške unutar zonskih datoteka koje mogu spriječiti normalan rad vašeg DNS poslužitelja.

Nakon svake nadogradnje poslužitelja neminovno je da poneki od servisa treba ponovno podesiti, odnosno iskonfigurirati. Razlog ovome je nepostojanje automatizirane procedure koja će postavke, primjerice, freeradiusa 1.x prebaciti u postavke za freeradius 2.x. O nekoliko čimbenika ovisi što je bolje, ostaviti staru konfiguraciju ili uzeti novu pa prebaciti relevantne dijelove iz stare. No, o tome sada nećemo pisati, nego ćemo se ograničiti na promjene u konfiguraciji BIND-a u Lenny distribuciji, koje su neke sistem-inženjere zatekle nespremne jer su odgovorili da žele zadržati staru konfiguraciju, a ponašanje DNS servisa se promijenilo.

Problem se manifestira tako da DNS poslužitelj iznenada počinje odbijati upite s nekih vaših mrežnih segmenata, ili IP adresa koje rabite. U logovima se mogu pronaći unosi poput ovog:

Vidimo da se nekim klijentima odbija upit za autorativnim podacima (to su podaci o vašim zonama i svim zonama za koje ste sekundar), a isto se događa i kad upite šalje profesorov laptop koji se fizički nalazi na drugoj lokaciji u drugom mrežnom segmentu.

Što se promijenilo, pa kod nadogradnje nismo mijenjali konfiguraciju? Odgovor se nalazi u datoteci /usr/share/doc/bind9/NEWS.Debian.gz (ne možemo dovoljno naglasiti koliko je korisno pročitati datoteke u /usr/share/doc direktoriju, barem za najbitnije servise!).

Maintaineri kažu:

Komentar se odnosi na dvije-tri najbitnije zabrane u BIND-u: **allow-query**, **allow-query-cache** i **allow-recursion**. Do inačice BIND-a 9.4, sve tri su bile potpuno otvorene, dakle svi su klijenti mogli postavljati upite bilo kojeg tipa. Ovo je dovelo do ozbiljnih sigurnosih problema, pa je vaš DNS poslužitelj mogao biti upotrijebljen u DoS napadu, ili se preko njega moglo saznati koje stranice posjećuju vaši korisnici (uvjetno rečeno).

Iako to nigdje nije napisano u konfiguraciji, *default* u BIND-u iz Lennyja je:

Dakle, rekurzivni upiti i upiti iz *cachea* su ograničeni samo na "localhost" i "localnets". Po imenu možemo zaključiti o čemu se radi, i ujedno gdje je problem: BIND ne može znati da imate još nekoliko mrežnih segmenata kojima želite omogućiti neometane upite. On može samo pronaći

konfiguraciju na postojećim mrežnim sučeljima i po tome se ravnati.

Što trebamo učiniti: našim korisnicima trebamo omogućiti sve upite, a ograničiti upite za sve ostale. Kako danas situacija nije jednostavna (mrežno gledajući), najlakše je promjene napraviti preko pristupnih lista (ACL-ova). Obično je dovoljno u named.conf.local (ili named.conf.options) dodati:

Ovime smo kreirali ACL "**trusted**", gdje ćemo upisati sve mreže kojima vjerujemo, a to su naravno svi segmenti mreža nad kojima imamo nadzor, ili eventualno segmenti kakvog domaćeg ISP-a, ukoliko vaši korisnici to zahtijevaju i rabe vaš DNS umjesto DNS od tog providera. **Za izračun CIDR načina označavanja mrežnih segmenata (npr. 161.53.1.0/24) poslužite se alatom ipcalc**.

Definicija pristupne liste mora biti izvan "**options {}**" bloka, dok **allow-*** direktive mogu biti navedene ovako, u globalnom kontekstu, ili za svaku zonu pojedinačno. Obično želimo imati samo jednu konfiguraciju, pa **allow-*** direktive samo dopišite unutar "**options {}**" bloka.

Nakon toga samo treba restartati DNS poslužitelj. Svi bi DNS upiti vaših korisnika sada trebali biti odgovoreni, a u logovima i dalje pisati da je drugim klijentima zabranjen pristup (barem nekim vrstama upita).

Ukoliko primjetite da se opetovano s neke IP adrese ili mreže ponavljaju upiti, probajte kontaktirati administratora tog poslužitelja ili mrežnog segmenta. Ukoliko nema odgovora ni tada, možda bi za vas bilo dobro da napravite fail2ban pravilo koji će klijente koji naprave **daleko previše** upita unutar nekog vremena, jednostavno blokirati preko iptables pravila?

Na CARNetovim poslužiteljima funkciju DNS servisa već dugi niz godina obavlja Bind, najpopularniji softver za DNS. Iako se neki ne bi složili da je Bind alfa i omega DNS-a, svoj posao obavlja tiho i neprimjetno. Uz povremena dodavanja novih hostova, ni ne traži neku veliku pozornost. Možda baš zbog toga postoje mnogi loše konfigurirani poslužitelji na mreži, kako kod nas tako i na ostatku Interneta. No, sad nećemo pričati o njima. Skrenut ćemo vam pozornost na grešku koja se zna pojaviti kod nadogradnji, bilo cijelog poslužitelja bilo Bind-a. Greška obično spominje "rndc" (skraćeno od "Remote name daemon control"), alat za kontrolu Bind DNS poslužitelja (za više informacija pogledajte man stranicu).

Puna poruka greške je sljedeća (javlja se nakon pokušaja pokretanja ili gašenja named daemona):

Greška se može manifestirati i u ovom obliku:

U logovima (obično /var/log/daemon.log) se mogu vidjeti ovakve poruke:

Problem je u nedostatku rndc.key datoteke, nepravilno postavljenim pravima nad njom ili konfiguraciji zaostaloj od prethodnih verzija. Ukoliko nedostaje /etc/bind/rndc.key datoteka, prvo učinite sljedeće:

Datoteka i njeni atributi trebaju biti postavljeni ovako:

Ukoliko rndc.key postoji, a u named.conf postoji unos sličan ovom, obrišite ga:

Obrišite i /etc/bind/rndc.conf i /etc/rndc.conf ako postoje. Ovo će prisiliti rndc i named da se vrate na default ponašanje, a to je upravo uporaba datoteke rndc.key. Naravno, prije brisanja valja napraviti zaštitnu kopiju svih datoteka koje se mijenjaju.

Problem je u tome što rndc i named mogu rabiti različite ključeve, što brisanjem konfiguracije svodimo na korištenje default vrijednosti i jedinstvenog ključa.

Drugi razlog je nemogućnost čitanja datoteke sa ključem rndc.key, što sprječava rndc u obavljanju svojih dužnosti. To što rndc pokrećete kao root nema nikakvih prednosti, jer se odmah po pokretanju programa privilegije spuštaju na razinu korisnika "bind".

Prije nekoliko godina smo na Portalu za sistemce pisali o problemu ***bogon*** ACL listi (*Access Control List*) u konfiguraciji BIND DNS poslužitelja, koje su onemogućavale pristup nekim dijelovima weba, odnosno internet prostora. Podsjetimo se što su zapravo bogon liste.

Bogon rasponi IP adresa u ACL listama su rasponi IP adresa koji još nisu dodijeljeni ni jednoj mreži, te stoga mogu izvrsno poslužiti za DoS napade. Zbog toga postoje filtri u DNS servisu i routing listama jer ni jedan paket ne bi smio doći s tih adresa. No, ove IP adrese se povremeno (svakih nekoliko mjeseci, u prosjeku svaka 4 mjeseca) dodjeljuju novim institucijama, odnosno ISP-ovima. Tako se može dogoditi da uslijed neažurnosti lista, koje nastavljaju blokirati novododijeljene raspone IP adresa, dio internet prostora postane nedostupan.

Dva su načina rješavanja ovog problema: uopće ne rabiti bogon liste, ili ih redovito osvježavati. Prvi način je jednostavniji, no otvara mogućnost napada izvan naše mreže. Drugi način traži veći angažman, jer automatiziranog osvježavanja nema. Nakon konzultacija sa kolegama koji se bave sigurnošću, možemo reći da je opasnost od napada iz bogon raspona zanemariva. Također, možemo dodati da je svakog dana opasnost zapravo sve manja, jer se gotovo svakodnevno smanjuje slobodni IPv4 adresni prostor, a time i manevarski prostor eventualnim napadačima.

Ukoliko Vam je slučajno zaostala u konfiguraciji, bogon listu možete pronaći u datoteci /etc/bind/named.conf (možda je odvojena u neku drugu datoteku u /etc/bind direktoriju, provjerite). Trebate ju jednostavno zakomentirati ili obrisati:

U "options" bloku još treba zakomentirati "blackhole" parametar:

Nakon toga treba restartati BIND sa:

Radi potpunosti, spomenut ćemo neke web stranice koje se bave bogon listama i uvijek imaju najsvježije popise adresa u slučaju da i dalje želite imati aktivne bogon liste.

Web site koji se bavi problematikom bogon lista i nudi download osvježene bogon liste. Tu je i mailing lista s najnovijim promjenama u bogon listi:

http://www.cymru.com/Bogons/

Tekstualna bogon lista spremna za ubacivanje u vaš DNS sustav ili router listu:

http://www.cymru.com/Documents/bogon-bn-nonagg.txt

Alat za provjeru dostupnosti pojedinih raspona IP adresa:

http://www.ris.ripe.net/debogon/

Potpuna lista Ipv4 adresnog prostora:

http://www.iana.org/assignments/ipv4-address-space

U zadnjih par tjedana bilo je nekoliko upita na sys.help kako dodati još jednu domenu (ili zonu) na poslužitelj, odnosno DNS servis. Postupak je jednostavan, a prvo je potrebno pripremiti tablicu za tu zonu.

Primjer tablice izgleda ovako:

Ono što treba u ovom predlošku izmjeniti je "cvorno.racunalo.hr" s nazivom postojećeg poslužitelja na kojem otvarate novu domenu. Ukoliko imate sekundarni DNS poslužitelj, njegovo ime upišite umjesto "sekundarni.dns.posluzitelj.za.novu.domenu.hr".

Tu tablicu snimimo kao datoteku **/etc/bind/novadomena.db** (mada samo ime datoteke ne ovisi o nazivu domene). Ako se pitate "pa dosada uopće nismo upisali naziv nove domene, gdje se to definira?", u pravu ste, to ćemo tek sada napraviti. U datoteku **/etc/bind/named.conf.local** dodajte:

Ovime smo "rekli" DNS poslužitelju da je odgovoran za zonu "novadomena.hr" i da podatke za nju može naći u datoteci novadomena.db. Naziv domene se automatski prenosi i dodaje na bilo koju labelu koja nema točku na kraju (**točka je jako bitna u zonskim datotekama!**). Tako će labela **www** postati **www.novadomena.hr**. Iz ovoga proizlazi da smo mogli odmah upisati

(obratite pažnju na točku na kraju!), ali je ovako jednostavno kraće.

Zatim je potrebno restartati bind, i nova domena je aktivna:

Provjerimo jesmo li sve dobro napravili naredbom host:

Sada možemo dodati i virtualni host u Apache, i dodati novu domenu u MTA (uobičajeno je to /etc/postfix/main.cf za Postfix MTA).

DNS, iako ga u većini slučajeva zanemarujemo, čini osnovicu internet prometa, i jednako je važan kao i sam TCP/IP protokol. Najbolje to znaju oni koji su imali bilo kakav veći kvar na DNS poslužitelju. U jednom trenutku sve može biti u redu, ali čim ispadne DNS poslužitelj, korisnici su prvi koji će to primjetiti i početi zvati sistem inženjera - vas.

No, ovdje se nećemo baviti sa problemima u radu DNS poslužitelja, nego ćemo opisati postupak koji možda nećete tako skoro provesti, ali ukoliko se ne pripremite - garantiramo glavobolju.

Radi se o preseljenju DNS servisa na drugi poslužitelj, ili promjene naziva postojeće domene. Ukoliko cijeli postupak ne provedete bez dobre pripreme, možete onemogućiti svojim korisnicima uporabu interneta, ali i vanjskim posjetiteljima pristup vašim servisima, obično su to web i mail.

Cijeli postupak, neovisno o tome što trebate napraviti, počinje komunikacijom s DNS službom. Potrebno je obaviti svu potrebnu "*papirologiju*" sa DNS službom (http://www.dns.hr/), a točno što treba napraviti će vam oni objasniti.Pomoć možete sobiti preko standardnog Helpdeska preko e-mail adrese helpdesk@carnet.hr ili telefona 0800 227-638.

Svakako zatražite da staru domenu drže aktivnom što je moguće dulje. Ovo je nužno, jer sasvim sigurno postoje mnogi tiskani materijali i vizitke koje korisnici dugo čuvaju. Kako su na njima stare adrese, mailovi će im se vraćati, neće moći učitati web stranice i slično. Dakako, snalažljiviji će se korisnici snaći i nove podatke preko neke internet tražilice ili telefona, ali je svakako bolje ne napraviti nagli rez.

Nakon što ste poslali dokumente DNS službi, domena će biti aktivna za najviše 10 dana. U međuvremenu, potrebno je prirediti novu zonu, inače će DNS služba odbiti aktivirati tu novu zonu. Pri tome neće provjeravati sadržaj zone (jeste li dobro unijeli imena hostova i adrese), nego samo je li delegacija i definicija zone dobro provedena. Ispravnost zone možete ispitati pomoću alata **dnswalk** ili nekim drugim. Poslužite se DNS priručnikom D. Korunića: http://sistemac.carnet.hr/node/62

Prvo što trebate učiniti je da jučer smanjite TTL vrijednosti u zonskim datotekama. Jučer? Ne, ne šalimo se, obično je TTL vrijednost namještena na 24 sata, a njena funkcija je određivanje koliko će se podaci o vašoj zoni zadržati u cacheu klijentskih resolvera (resolver je klijentski dio DNS-a, i služi za dobivanje informacija od DNS poslužitelja). Ovo znači da stari podaci mogu "živi" još 24 sata (ili više ako je TTL tako podešen) nakon promjena, te tako učiniti nedostupnim neke ili sve od vaših servisa.

Promjena TTL-a je bitnija više kod promjene IP adrese DNS poslužitelja, nego kod dodavanja ili promjene naziva zona, jer će u potonjem slučaju vaši servisi biti dostupni pod starim nazivima.

TTL je najbolje smanjiti na 1 sat, ili čak manje. Nikako ne zaboravite TTL vrijednost vratiti na staru vrijednost (1 dan, ili 86400 sekundi). Ukoliko ostavite mali TTL, onda cete imati problem s prevelikim brojem DNS upita, jer će klijenti prekratko čuvati vaše podatke.

Tek sutradan je na redu "pravi posao".

Kao i uvijek, sačuvajte za svaki slučaj stare podatke (direktorij /etc/bind), najbolje je napraviti pun backup cijelog sustava, ali bit će dovoljno i samo sačuvati cijeli direktorij sa naredbom tar:

Sljedeći korak je kopiranje stare zone u novu:

Naravno, imena mogu biti i drugačija, mi smo se odmaknuli od ustaljene kombinacije hosts.db i hosts.rev, kako bi jasnije istaknuli razlike.

Reverzna zona je poseban slučaj, jer ne možete imati dvije iste zone. Kad se propagira nova forward zona, onda možete promijeniti unose iz staradomena.db u novadomena.db i preimenovati datoteku po zelji, ili ostaviti hosts.rev.

Da biste podesili i novu domenu, u iskopiranoj datoteci novadomena.db promijenite podatke na novadomena.hr:

Ne zaboravite povećati "Serial" u datoteci s novom domenom, a najbolje je zamijeniti cijeli broj za trenutnim datumom i dodavanjem brojke 01. Ovaj korak zaporavo i nije nužan, ali kako smo već rekli, dobro je znati vrijeme zadnje promjene.

Stari broj:

Novi broj:

Broj mora biti aritmetički veći od prethodnog, a na koji način ste ga dobili nije bitan (dakle, ne mora nuzno biti datum, mozete jednostavno povećavati brojeve: 1, 2, 3...). No, informacija o datumu zadnje promjene moze biti vrlo korisna kod pojave problema.

Uz staru, u /etc/bind/named.conf.local dodajte novu domenu:

Reverznu domenu ne treba dirati, ali kad jednom bude aktivna nova domena, možete promijeniti unose u reverznoj zonskoj datoteci na novu domenu.

NOvu domenu možete odmah upisati i u konfiguracijsku datoteku resolvera, /etc/resolv.conf upisati novo ime domene:
search staradomena.hr novadomena.hr

Nakon aktivacije nove domene, možete ili zamijeniti pozicije, ili ostaviti samo novadomena.hr.

Ukoliko imate dodatni sekundarni DNS poslužitelj (možete ih imati i više), morate kontaktirati sistem-inženjera koji taj DNS održava. Uz postojeću zonu, neka samo dodaju novu. bit će dovoljno dodati u njihovu named.conf.local datoteku:

Neka zadrže i sekundarni DNS za staru domenu i aktiviraju sekundarni DNS za novu. Direktorij gdje se spremaju podaci zona kojima ste sekundarni DNS poslužitelj je /var/cache/bind, umjesto /etc/bind.

Time su završene sve promjene na DNS/BIND konfiguraciji. Potrebno je restartati bind proces na poslužitelju, nije dovoljno napraviti samo "rndc reload":

Sve što je preostalo je sačekati da DNS sluzba aktivira novu domenu. Provjeru možete napraviti i sami, npr:

Nakon toga možemo prijeći na konfiguraciju servisa da se odazivaju na novu domenu, ili i na staru i novu domenu.

Nakon što smo u prošlom nastavku (nalazi se na adresi /sys-trek-objave/bind-dns-savjeti-i-trikovi/#kako-promijeniti-domenu-1-dio) opisali koje sve predradnje trebate obaviti, te kako podesiti BIND, u ovom dijelu ćemo opisati (za neke) lakši dio - konfiguracija servisa kako bi prepoznali i počeli rabiti novu domenu. Neke stvari se mogu napraviti i prije nego što DNS služba aktivira domenu, ali za to zapravo nema potrebe. Sve te promjene će vionako rijediti samo lokalno, pa nećete imati puni uvid u to radi li sve kako treba ili ne.

Prvo što treba podesiti je mail sustav, u našem slučaju Postfix. U konfiguraciji Postfix mail poslužitelja treba omogućiti primanje pošte za novu domenu. U /etc/postfix/main.cf prepravite tako da svugdje piše nova domena, ali svakako ostavite i staru:

Time smo riješili problem dolazne pošte, ali ostaje problem odlazne pošte. Taj problem možete riješiti i ručno, tako da odete do svakog klijentskog računala i promijenite podatke o adresi mail poslužitelja i mail adresi korisnika. Naravno da se možete poslužiti i automatiziranim procedurama, što ovisi kako je organiziran vaš LAN te koji je operativni sustav na
klijentskim računalima.

Postoji i druga opcija, a o njoj smo već pisali prije godinu dana u članku na adresi /sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postfix-kako-podesiti-da-odlazne-domene-za-pojedine-korisnike-budu-drugog-oblika. Radi se o "canonical" mapama, kojima je svrha premapiranje jedne adrese u drugu. Ukratko, dovoljno je u main.cf dopisati (uz već gore navedene promjene parametra $mydestination):

U datoteku canonical treba upisati:

Na kraju, potrebno je napraviti i:

Ovime smo postigli da svaki mail poslan preko vašeg Postfixa bude "popravljen", tako da sadržava novu domenu umjesto stare.

Drugi servis kojemu treba posvetiti pažnju je, naravno, web servis. Apache podržava virtualne hostove gotovo od najranijih dana, pa je s njima fleksibilnost još i veća. Pri tome možete se odlučiti želite li obavijestiti korisnike o promjeni domene ili ne, te ukoliko želite, kako to izvesti.

Ukoliko ne želite, najjednostavnije je postojeći VHOST, primjerice www.staradomena.hr, iskopirati u www.novadomena.hr i urediti tako da su sve reference unutar te datoeke preimenovane na novu domenu. Kao što znate, virtualni hostovi su definirani u /etc/apache2/sites-available, stoga će postupak izgledati ovako:

Na ovaj način smo aktivirali novi VHOST, sa identičnim sadržajem kao i VHOST sa starim imenom domene.

No, bilo bi lijepo obavijestiti posjetitelje da je nastupila promjena, a još bolje bi bilo da nakon toga automatski preusmjerimo korisnike na nove stranice. Ovo možemo napraviti na dva načina: preko META Refresh zaglavlja
(ili preko Javascripta), ili preko Apache Redirect mehanizma (može i preko Rewrite mehanizma).

Prvi način omogućava da napišete poruku posjetiteljima stranica da se domena izmjenila, te ih zamoliti da osvježe svoje Bookmarks, odnosno Favorites unose. Nakon određenog broja sekundi korisnik će automatski biti preumjeren na nove stranice. Zaglavlje koje morate upisati na HTML stranici je:

Tek nakon odbrojavanja 20 sekundi, korisnik će biti preusmjeren na novi VHOST. HTML datoteku stavite u poseban direktorij, primjerice /var/www/www.staradomena.hr, i stavite taj direktorij kao DOC_ROOT u VHOST datoteku www.staradomena.hr (podrazumijevamo da www.staradomena nije istovremeno i DOC_ROOT za www.novadomena.hr).

Drugi način je automatski prebaciti korisnika na nove stranice bez da mu to date do znanja. Ovaj način je nešto neljubazniji prema korisniku, ali jednostavniji. Jednostavno, u definiciju starog VHOST-a stavite direktivu:

Ovo će preumjeriti sve zahtjeve na www.novadomena.hr. Radit će i poddirektoriji, jer će zahtjev http://www.staradomena.hr/mail biti preusmjeren http://www.novadomena.hr/mail.

Drugi servisi, iako možda i podržavaju virtualne hostove, obično tako ne rabimo, a ako i rabimo, prebacivanje obično nije problem (ne vjerujemo da želite imati različite sadržaje na ftp.staradomena.hr i ftp.novadomena.hr).

Kako provjeriti je li još u nekoj konfiguracijskoj datoteci postoji stara domena? Možemo se poslužiti dobrom starom naredbom grep:

Ovo će rekurzivno pretražiti cijeli /etc direktorij i ispisati gdje se pojavljuje naziv stare domene. Gdje se pojavi stara domena, zamijenite je sa novom i restartajte taj servis.

Poseban je slučaj AAI@EduHr sustav, no kako morate registrirati novu domenu kod njih, postupak se sastoji od javljanja na team@aaiedu.hr i praćenja njihovih uputa. Korisnike na vrijeme obavijestite o promjeni AAI@EduHr oznake.

Još bi valjalo spomenuti da editirate daoteku /etc/hosts i dodajte novu domenu. Stara može trajno

ostati.

Datoteka /etc/resolv.conf određuje ponašanje resolver rutina, pa tu upišite novu domenu, čime ste automatski promijenili i FQDN poslužitelja.

Sve što ostaje je pratiti logove u potrazi za nekim zaboravljenim servisom i adekvatnim promjenama u konfiguraciji istog. Trebate obavijestiti korisnike da što prije krenu u uporabu nove domene, kako bi se prijelaz što prije obavio. Neka promije sve unose na osobnim računalima (E-mail odlazne adrese, mrežne postavke itd.) da pokazuju na novu domenu, ukoliko imaju ovlasti ili vi to ne stignete. Također, javite korisnicima da promijene predloške i memorandume u Wordu, potpise u mail porukama, te daju tiskati nove vizitke i slično.

Promjena domene nije mala stvar, ali uz dobro planiranje sve može proći bez imalo glavobolje.

Prije više od pet godina pisali smo o koracima koje je potrebno provesti kako bi uspješno promijenili domenu vašem čvornom računalu (/sys-trek-objave/bind-dns-savjeti-i-trikovi/#kako-promijeniti-domenu-1-dio). Iako se potreba za ovime rijetko pojavljuje, neki kolege su morali proći cijelu ovu proceduru. Uspjeli su naletjeti na nekoliko problema, iako je sama promjena domene uspješno provedena.

Prvi problem je bio taj da je stara domena bila odmah ugašena. Kod kontaktiranja DNS službe (helpdesk at carnet.hr ili telefon 0800 227-638) važno je naglasiti da ne ukidaju staru domenu barem još šest mjeseci, inače su posljedice očigledne: nema vašeg maila ni weba za vanjske korisnike. Iznanada se počinju vraćati mailovi, a kontakt informacije na webu su nedostupne jer se domena weba promijenila, pa se ne može saznati ni broj telefona vaše institucije. Snalažljiviji će probati pogledati Googleov cache ili čak posjetiti archive.org, ali to ne možemo očekivati od svih korisnika.

Što se stranica sa starom domenom tiče, možda je najbolje na njima ostaviti samo poruku da je domena promijenjena, bez ikakve automatske redirekcije. Pretpostavka je da većina korisnika neće odmah osvježiti bookmarke, nego će se pouzdati u redirekciju i URL *history*, dakle natjerajmo ih da ručno unesu adresu i na taj način lakše zapamte ovu promjenu. Naravno, ukoliko vam tako više odgovara, napravite jednostavnu automatsku redirekciju, uz prikaz neke obavijesti ili čak bez nje.

Drugi problem se pojavio s vlastitim korisnicima. Iako su obavijesti poslane, neki to nisu vidjeli i/ili registrirali (to se svakako može dogoditi). Zato, bolje je poslati nekoliko obavijesti, a zadnju na sam dan prelaska. Ne zaboravite istaknuti isprintane obavijesti na oglasnim pločama i drugim prikladnim mjestima. Ukoliko zaista želite učiniti sve, pošaljite obavijesti i institucijama s kojima intenzivnije surađujete, kako bi oni mogli obavijestiti svoje korisnike. Isto tako, zamolite svoje korisnike da obavijeste sve svoje korespondente.

Treći problem o kojem smo obaviješteni je AAI@EduHr sustav. S promjenom tu nema problema (a prava adresa za to je paketi at aaiedu.hr), ali ima sa servisima koji rabe AAI@EduHr za autentikaciju. Prvi je CARNetov webmail. Nakon promjene AAI korisničke oznake, korisnik se više ne može ulogirati u svoj stari profil, te mu se otvara novi gdje nema njegovih postavki za IMAP poslužitelje. Potrebno je javiti se na adresu webmail at carnet.hr, kako bi se napravile izmjene u bazi i promijenili nazivi profila.

Slična situacija je s CARNetovim servisom Loomen. Ukoliko se studenti prijave s novim oblikom AAI oznake, neće više biti u mogućnosti pristupiti svojim podacima i tečajevima, nego će biti kreirani novi profili s kojima će se neki pokušati prijaviti na kolegije i time napraviti zbrku u bazi. Pojavit će se duplikati korisnika, pa će biti problem koji profil pobrisati, a koji ostaviti.

Iz tog razloga je potrebno iskoordinirati promjenu s administratorima sustava Loomen. Potrebno je blokirati kolegiji s vaše institucije, dok se ne napravi promjena oznake u sustavu AAI@EduHr. Adresa za kontaktiranje tima je loomen at carnet.hr.

Ovo nisu jedini servisi koji rabe AAI@EduHr, pa ukoliko ih rabite, svakako javite promjenu na vrijeme administratorima tih sustava. Na taj način ćete izbjeći probleme i dodatne napore sebi i drugima kod ionako "pipkavog" posla promjene domene.

Svi znamo je IP adresni prostor ograničen, i u našoj mreži sve više institucija dobiva samo pola, četvrtinu ili čak manji dio standardno dodijeljenih 256 adresa (samo numerički mogućih, sve se obično svodi na 254 adrese). Ovo je razumno, jer nije potrebno da svaki PC korisnika bude direktno dostupan s Interneta, dapače, povećava se sigurnost ukoliko upotrijebimo neku od NAT tehnika. Uz uporabu vatrozida (ili drugog specijaliziranog mrežnog uređaja), broj potrebitih IP adresa se smanjuje na svega nekoliko, uglavnom za poslužitelje (web, mail i slično), koji moraju biti dostupni na Internetu.

Problem nastaje kod reverznog DNS-a (rDNS, pretvaranje IP adrese u ime računala), jer u početku nije bilo predviđeno da se reverzne zone autoritativnosti dijele na manje dijelove. Reverzni DNS je dosta bitan, jer će mnogi mail i SSH poslužitelji i servisi odbiti mail sa poslužitelja koji nema reverzni DNS zapis. No, postoje načini za rješavanje ovog problema. Jedan način je da postoji samo jedan autoritativni poslužitelj za reverznu zonu, koji će opsluživati sve segmente te zone. Kako segmenti obično bivaju dodijeljeni drugim institucijama, ovaj pristup nije osobito fleksibilan, jer to znači da ćete morati prepustiti brigu o vašem segmentu nekome drugome (a to uključuje i dodavanje i brisanje hostova iz zonskih datoteka). U suprotnom slučaju, vi ćete se morati brinuti o tuđim zapisima.

Drugi način rješavanja ovog problema, koji ćemo ovdje opisati, je uporaba CIDR notacije (Classless Inter-Domain Routing) u zonskim datotekema, što je definirano kao "Classless IN-ADDR.ARPA delegation" u RFC-u 2317. Pretpostavimo da imate dodijeljen segment 193.198.XXX.0 do 193.198.XXX.64. CIDR notacija za ovaj segment je 193.198.XXX.0/26 (kako si olakšati izračun, pogledajte u članku /sys-trek-objave/naredbe-za-koje-mozda-niste-znali/#naredbe-za-koje-mozda-niste-znali-2-ipcalc). Ostala tri segmenta su 193.198.XXX.64/26, 193.198.XXX.128/26 i 193.198.XXX.192/26. Pretpostavimo da imate domenu (zonu odgovornosti) "institucija.hr". S forward DNS rezolucijom nemamo problema, jer zonu "institucija.hr" najčešće ne dijelimo s nijednom drugom institucijom. Reverznu zonu, u ovom slučaju, dijelimo s drugim institucijama.

Iz tog razloga ćemo podijeliti reverznu zonu, i umjesto:

pišemo

Ovime smo rekli "odgovoran sam za reverzni DNS za adrese 193.198.XXX.0 do 193.198.XXX.63". Uvijek se možete poslužiti naredbom ipcalc za izračun točnih vrijednosti, jer adresni prostor može biti bilo koji segment mreže, npr. 193.198.XXX.192 do 193.198.XXX.255 (što pišemo kao 193.198.XXX.192/26, odnosno zona je 192/26.XXX.198.193.in-addr.arpa).

Postupak je dalje jednostavan i možemo ga prikazati u svega nekoliko točaka:

1. U datoteci /etc/bind/named.conf.local reverzna zona treba biti konfigurirana ovako:

Ime datoteke nije bitno, sve dok vam je iz samog imena jasno što se u njoj nalazi. Vaš DNS poslužitelj može biti odgovoran za više segmenata, pa si na ovaj način olakšajte snalaženje. Primjerice, dolazi u obzir i oblik "193.198.XXX.0-26.institucija.rev" ili kraće "institucija.0-26.rev", kao i bilo koji oblik koji vama odgovara.

2. u datoteku s reverznim zapisima /etc/bind/193.198.XXX.institucija.rev upišite sljedeće:

Oblik "dns.institucija.hr" je samo primjer, najbolje je ostaviti što je već bilo (primjerice, "knjiga.ffos.hr", "oliver.efri.hr" itd). Komentare u zonskim datotekama označavajte isključivo sa znakom ";" i ne zaboravite ostaviti točke na kraju naziva hostova!

3. Treba restartati BIND, odnosno natjerati ga da prihvati novu konfiguraciju:

4. Također, treba provjeriti radi li sustav kako bi trebao:

Znak da je sve u redu bi trebao biti ispis poput ovog:

Ne bi trebalo biti ovakvih poruka:

5. S konfiguracijom smo gotovi, no valja javiti administratorima nadređenih poslužitelja da je konfiguracija gotova. Zasad, najbolje je da se javite na **helpdesk@carnet.hr** i priložite ispis (pomoću naredbe iz točke 4) koji pokazuje da je konfiguracija ispravno napravljena kako bi se cijeli proces ubrzao.