

# Postfix savjeti i trikovi - Željko Boroš

Ivica Jurkić | 1 travnja, 2026

---

Postfix je popularan MTA preporučan za instalaciju na poslužiteljima unutar CARNet mreže. Ova online knjiga je skup pojedinačnih članaka objavljenih kao pomoć sistemcima u konfiguraciji i korištenju postfixa.

Zaprimili smo nekoliko uznemirenih upita kolega sistemaca koji su se uplašili da su im poslužitelji provaljeni. Razlog za to su unosi u logovima, gdje se moglo vidjeti kako se pojedini korisnici autenticiraju preko SASL-a sustava s ispravnim korisničkim podacima, te šalju mailove s različitih mrežnih adresa. Provjerom je ustanovljeno da u to vrijeme ti isti korisnici nisu uopće rabili mail ili računalo.

Jednom dijelu tih poslužitelja je, s druge strane, bio zabranjen pristup nekim besplatnim davateljima mail usluga, jer je s njih bio poslan veliki broj spam poruka. Spamovi su svi kroz poslužitelj prolazili na identičan način, autenticirajući se preko SASL-a i time preskačući određene zaštite koje standardno postoje u Postfixu. Što se zapravo događalo, odakle spamerima zaporke i je li uistinu poslužitelj provaljen?

Spameri su korisničke zaporke saznavali rabeći socijalni inženjering, u većini slučajeva preko ovakvih mailova:

Iako nemušto preveden preko nekog od servisa za prevođenje, mail je dovoljno razumljiv i neki korisnici su poslali zaporku. Što učiniti?

Prije svega, svakako **morate** promijeniti zaporke svim korisnicima koji su ih **poslali**, a još bolja opcija baš svim korisnicima, ukoliko je to moguće. Nove im možete priopćiti usmeno ili SMS-om, ili na neki drugi siguran način (npr. preko interne dostavne službe).

Dalje imamo dva puta: jednostavno onemogućiti SASL, ili probati ostaviti ovu mogućnost samo određenoj skupini korisnika, ukoliko je to moguće.

Onemogućiti SASL je jednostavno, i postupak je opisan u članku "SASL: Brute force napadi i kako ih onemogućiti" na Portalu za sistemce na adresi: <http://sistemac.carnet.hr/node/752>.

Više informacija o samom SASL-u možete naći u članku "[SASL SMTP autentikacija u Postfixu](#)".

Drugi put je pokušati naći rješenje koje će zadovoljiti potrebe vaših korisnika, odnosno postići da korisnici ne moraju mijenjati postavke na koje su se navikli (preko SASL autentikacije mogu bez brige slati mail iz bilo koje mreže). Konkretno, zahtjev je bio da zaposlenici (odnosno samo dio zaposlenika koji već rabi SASL) mogu i dalje nastaviti uporabu SASL-a, dok bi svima ostalima SASL bio zabranjen. Time bi se postiglo da čak i ako korisnici nekome ubuduće pošalju zaporku, spameri neće moći zlorabiti vaš poslužitelj.

Naravno, sasvim je druga priča da vaši korisnici ne bi trebali nikome slati zaporku, čak i ako se čini da zahtjev dolazi od CARNeta, uprave ili direktno vas. Tu može pomoći samo obrazovanje vaših korisnika, čime ćete u konačnici sebi uštedjeti neugode i gubitak vremena.

Vratimo se na osnovni problem. Daemon program saslauthd ne podržava nikakvo filtriranje korisnika po nekom kriteriju, primjerice grupi, ali podržava uporabu sustavske (/etc/shadow) ili vlastite baze podataka (/etc/sasldb) o korisnicima. Metodom pokušaja i pogreške, došli smo do zaključka kako bismo mogli postići traženo ukoliko rabimo bazu podataka u /etc/sasldb. Na ovaj način korisnici upisani u bazu u datoteci /etc/sasldb moći će rabiti SASL, dok oni koji nisu neće. Oni koji nisu upisani u /etc/sasldb morat će mail slati iz internih mreža (ili onih navedenih u /etc/postfix/main.cf u parametru mynetworks). Naravno, uvijek im ostaje i webmail, bilo lokalni bilo onaj na adresi <http://webmail.carnet.hr>.

Prvo što trebamo učiniti da bismo napravili ovaj način autentikacije je napraviti promjene u `/etc/default/saslauthd`:

Zatim treba dodati "privilegirane" korisnike u bazu:

Provjera konzistentnosti i sadržaja baze:

Ukoliko se kasnije ukaže potreba, korisnika možete obrisati pomoću naredbe:

Sada treba restartati `saslauthd` (kao uostalom i poslije svake izmjene baze!):

Korisnici koji su upisani i ukucaju dobru zaporku ostavljaju ovakav zapis u logovima:

Ako korisnik ne postoji ili je slučajno ukucao pogrešnu zaporku, zapis će izgledati ovako:

Ako nešto ne radi, možete ugasiti `saslauthd` i dobiti više informacija u *debug* načinu rada, tako da `saslauthd` pokrenete sa:

*Ne zaboravite pri tome ugasiti servis `saslauthd` u monitu (ukoliko rabite monit)!*

### **Napomene:**

- korisnici koji nisu u bazi neće moći rabiti SMTP AUTH, i dobit će poruku da su ukucali pogrešnu zaporku, što ih može zbuniti

- korisnici u bazi `/etc/sasldb` ne moraju uopće postojati na sustavu, a moći će slati mail

- *realm* je ime stroja, ali ako ne radi probajte staviti domenu

- također, korisnici i dalje mogu lažirati ime u MAIL FROM, ako ne napravite dodatne mjere, npr: [/sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postfix-kako-korisnicima-postaviti-uniformne-odlazne-adrese](#)

- ako vam poslužitelj odbija konekciju nakon par provjera u kratkom vremenu, provjerite imate li uključen `fail2ban` ili neki drugi vid aktivne zaštite (`iptables ipt_recent` modul!)

Ukoliko vam ovakve negativne posljedice ne smetaju, probajte ovakav način autenticiranja, ali ne zaboravite - obrazovanje vlastitih korisnika nema zamjene, ma koliko se činilo da uzima previše vremena. Uvijek se na kraju isplati.

*Bounce* poruke koje od mail sustava povremeno možemo primiti su vrlo korisne, bilo da se radi o prijavi problema isporuke pošte (NDR/NDN), bilo o statusu isporuke (DSN). Više o tipovima poruka i u kojim se slučajevima pojavljuju, provjerite na Wikipediji: [http://en.wikipedia.org/wiki/Bounce\\_message](http://en.wikipedia.org/wiki/Bounce_message).

No, *bounce* poruke su dosta šture, a kako odlaze najčešće krajnjem korisniku, za njih obično nejasne. Postfix nudi malu pomoć, te tako daje mogućnost promjene *bounce* poruka preko predložaka (*templatea*). Ukupno možete promijeniti 4 poruke preko 4 varijable, čiju funkciju možete naslutiti prema imenu:

### ***success\_template***

U ovu varijabli upisujete tekst koji će korisnik vidjeti kod uspješne isporuke poruke, ali samo ako takvo izvješće izričito zatraži.

### ***failure\_template***

Ovu poruku će krajnji korisnik najčešće susretati (jer označava bilo kakvu grešku kod isporuke), pa je preporučljivo pažljivo sročiti tekst, kako bi problem mogao pojasniti, te uputiti korisnika kome se obratiti kako bi svoj problem riješio. To je i u vašem interesu, jer vam može prištediti koji telefonski poziv ili posjetu korisnika.

### ***delay\_template***

Druga najčešća poruka je ona o tome da je poruku trenutno nemoguće isporučiti, ali da će se isporuka i dalje pokušavati poslati kroz neko vrijeme (uvijek piše koliko je to točno vremena).

## **verify\_template**

U ovaj predložak upisujete informacije koje vam mogu biti od koristi kod traženja problema. Ovaj predložak će se na izričit zahtjev korisnika vratiti pošiljatelju, bez obzira na status isporuke (no, ako je ona neuspješna, trebali bi dobiti i izvješće o neuspješnoj isporuci poruke).

Sve predloške možete staviti u istu datoteku proizvoljnog imena, i uključiti u konfiguraciju postfixa, što možete napraviti ručno ili preko [postconfa](#):

Tekst predložaka se upisuje kao "*Here document*" (što je to smo nedavno opisali u [ovom članku na Portalu](#)), odnosno unutar dvaju identifikatora "END" (no može biti bilo koja riječ):

i tako za svaki željeni predložak.

Nakon toga bi bilo jako dobro testirati je li sve u redu s vašim predloškima s naredbom "**postconf -b**" (s kojom smo vas upoznali u članku <https://www.hr/sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postconf-ili-kako-bez-edit-ora-uredivati-main-cf>). Ona će provjeriti je li sintaksa u redu, i izvršiti supstituciju varijabli, tako da možete vidjeti tekst onako kako će biti poslan korisniku. Sintaksa je:

Na kraju, par napomena:

1. Ne morate rabiti sve predloške, najzanimljiviji su vam vjerojatno **failure\_template** i možda **delay\_template**
2. Ostavite originalni engleski tekst pored prevedenog, i nemojte rabiti naše "šumnike"
3. **Obavezno ostavite jedan prazan redak na kraju datoteke!**

Slijedi primjer datoteke s prijevodom svih predložaka uz zadržan originalni engleski tekst, ali svakako preporučujemo da predloške prilagodite svojim potrebama, i potrebama svojih korisnika (u tekstu možete rabiti bilo koju varijablu iz main.cf!):

Postfix je standardni MTA ([Mail Transfer Agent](#)) servis na CARNetovim čvornim računalima. Tu "čast" je zaslužio svojim brojnim kvalitetama i jednostavnom konfiguracijom, te laganim integranjem s drugim servisima, najčešće onima s antispam i antivirusnim predznakom. Tu funkciju u CARNetovoj distribuciji preuzima amavisd-new, iako sami možete dodati i druge pomoćne servise.

Postfix dolazi s dosta pomoćnih alata, a danas ćemo se pozabaviti s alatom **postconf**, koji ispisuje parametre (ali ih može i promijeniti) iz konfiguracijske datoteke **/etc/postfix/main.cf**. Krenimo odmah:

Vidimo da se ispisuju sve varijable i njihove vrijednosti. Uporabom opcije "**-d**" (*default*) dobit ćemo ispis svih varijabli i njihovih vrijednosti, onako kako su ukompilirane u sam program. Dakle, uopće se ne gledaju vrijednosti varijabli u main.cf, nego one navedene u izvornom kodu (poneke se ipak isčitaju sa sustava prilikom pokretanja postfixa, primjerice ime hosta).

Najčešće, ipak, želimo vidjeti vrijednost samo određene varijable (ili više njih, ako ih navedemo). Evo primjera za jednu varijablu:

Ukoliko želite vidjeti trenutno važeće vrijednosti, jednostavno izostavite (bilo koju) opciju:

I zaista, ukoliko zavirite u main.cf, tamo je postavljena upravo ta vrijednost za varijablu `content_filter`.

Postoji jedna jako korisna opcija, "**-n**" (*new*). Ona će ispisati samo ako se razlikuje od ukompilirane vrijednosti. Ovo je jako korisno kad na brzinu želite provjeriti što je promijenjeno u konfiguraciji.

Kako je u Debianovoj distribuciji konfiguracijska datoteka main.cf već predpodešena, a u CARNetovoj i dodatno promijenjena pomoću paketa postfix-cn, lista promjena je zbog još uvijek prevelika. Iz tog razloga, opet ćemo se ograničiti na samo jednu varijablu, uzevši za primjer varijablu `smtp_use_tls`:

Provjerimo je li ta varijabla po *defaultu* zaista te vrijednosti:

Dakle, varijablu je uistinu mijenjano ili je to učinio netko drugi umjesto nas (ili neki paket). Sada

možemo pokušati promijeniti vrijednost varijable pomoću opcije **"-e"** (*edit*):

Provjerom možemo vidjeti da se vrijednost varijable uistinu promijenila iz "yes" u "no". Opcija "-e" se može rabiti u skriptama, i tu je možda njena najveća prednost nad ručnim editiranjem main.cf. Na ovaj način radi i CARNetov paket postfix-cn, koji preko opcije "-e" mijenja određena postavke koje odgovaraju vašem računalu.

Kako vas kasnije namjeravamo upoznati s predlošcima u Postfixu, objasniti ćemo opciju **"-b"**. Ona provjerava sintaksu i ispisuje sve predloške za *bounce* poruke ([http://en.wikipedia.org/wiki/Bounce\\_message](http://en.wikipedia.org/wiki/Bounce_message)):

Ukoliko želite saznati kako izgledaju originalni predlošci, upotrijebite naredbu u ovom obliku:

Za postconf postoje još neke opcije, ali ih nećemo objašnjavati jer se rjeđe rabe. Svakako zavirite u manual postconfa, kako biste mogli imati uvid u to što ta naredba još pruža, u slučaju da vam to zatreba.

I na kraju, nemojte pobrkati naredbu **postfix** i **postconf**, što se zna u brzini dogoditi!

Internet odavno nije bezopasno mjesto, a jedan od prvih servisa koji je počeo primjenjivati neke oblike zaštite je mail servis. Nekada ste bez problema mogli rabiti bilo koji mail poslužitelj kako biste poslali mail na bilo koji drugi poslužitelj, i to bez ograničenja broja mailova. Nakon pojave neželjene elektroničke pošte (spama), ovakvo stanje nije moglo biti održivo. Danas je uobičajeno da svaki poslužitelj prima i šalje mail (radi *relay*) samo za svoje korisnike.

Iako se kontrola relaya može raditi na više načina, u ovom ćemo se članku usredotočiti na načine kontrole preko definiranja mreža ili samo pojedinačnih IP adresa. Ovo se može postići na dva načina, ponešto različita, ali rezultat je u konačnici isti. Koji ćete upotrijebiti, ovisi o vašoj konkretnoj situaciji.

Inicijalna instalacija postfixa donosi otprilike ovakvu listu:

Ako želite dodati još koju mrežu, jednostavno je možete dodati na kraj liste:

(za točno definiranje mreža možete se poslužiti naredbom [ipcalc](#)).

Nakon toga je potrebno reloadati konfiguraciju na već standardan način:

Na ovaj način smo omogućili mreži 193.198.yyy.0/24 pristup i slanje maila preko našeg poslužitelja, a pretpostavka je da ta mreža pripada vašoj drugoj lokaciji, mrežnom segmentu ili nečem sličnom.

Ako unutar te mreže nekim računalima/IP adresama ne želite omogućiti relay, upišite ovo:

Naravno, ovo će onemogućiti relay samo za dvije IP adrese, a što je u slučaju da imate puno adresa kojima želite na ovaj način ograničiti mogućnost relaya?

U inačici Postfix 2.4 i višima (ovo uključuje i sad već stari Etch) je jednostavno, u zasebnu datoteku upišite sve IP adrese kojima želite onemogućiti relay, snimite je (recimo `/etc/postfix/my_relays`), i upišite:

Analogno tome, možete upisati i `/etc/postfix/my_relays` (bez uskličnika), što će omogućiti da je svim adresama navedenim u datoteci relay omogućen.

Alternativno, postfix razumije i miješani format datoteke, koja je (gotovo) jednaka kao i sendmail access datoteka:

```
/etc/postfix/my_relays:
```

Pravila se tumače od početka, a pretraga završava čim se nađe odgovarajuća adresa. Zato su zabrane na vrhu, a dopuštenja relaya na samom kraju. U skladu s tim pravilima, možete kreirati svoju listu.

U ovom slučaju je u `/etc/postfix/main.conf` potrebno upisati tip datoteke:

Nakon kreiranja ove *hash* datoteke, morate napraviti:

uz obvezatni *reload* na kraju:

Za dodatne informacije, svakako pročitajte <http://www.postfix.org/postconf.5.html>, sekciju mynetworks.

Osim osnovne datoteke s mail aliasima, postfix podržava dodatne datoteke, a jedini uvjet da cijela stvar proradi je da mu kažete gdje su. U osnovnoj CARNet konfiguraciji, u `/etc/postfix/main.cf` stoji slijedeće:

Uz osnovnu, CARNetov paket postfix-cn donosi i dodatnu alias datoteku, generiranu iz GECOS polja `/etc/passwd` datoteke (za podršku formatu e-maila `Ime.Prezime@ustanova.hr`). Na sličan način možemo dodati i naše datoteke:

Naravno, samo ime datoteke (alias\_baza) je proizvoljno. Važno je napomenuti da nastavak linije obvezno mora početi s prazninom (space ili tab). Nakon svega je potrebno izvršiti naredbu:

kako bi se kreirala `/etc/mail/alias_baza.db` datoteka. Ovu operaciju je potrebno izvršiti nakon svakog brisanja ili dodavanja aliasa, i vrlo je važna, jer bez kreiranja `.db` datoteka postfix će se pobuniti i cijeli e-mail sustav pada. Kako ne bi morali za svaku datoteku pokretati naredbu `postalias`, možete napraviti slijedeće:

Kopiranjem unosa iz `alias_maps` u `alias_database` postižete to da standardnom naredbom "newaliases" osvježavate sve datoteke navedene u `alias_database`:

Za daljnju automatizaciju, upotrijebite cron. Pogledajte, iskopirajte negdje i izmijenite skriptu `/usr/share/postfix-cn/make-aliases-gecos.sh` koja se svaki sat izvršava iz crona i generira svježije `.db` datoteke. Možete iskoristiti i datoteku `/etc/cron.d/postfix-cn` kao uzor za kreiranje vlastite cron datoteke.

Ukoliko ste aliase imali u posebnim datotekama (gdje su adrese upisane jedna po retku) i uključivali ih pomoću `:include:` iz `/etc/aliases` datoteke, ništa od gornjih primjera ne trebate raditi.

Kadkad baš i ne možemo biti sigurni da li ćemo pogoditi pravu metodu filtriranja neželjene pošte. U pravilu, što jače pooštrimo kriterije, veća je vjerojatnost da se iz optičaja povuče i korisna e-pošta, pa je često najbolje rješenje da se filtrirane poruke ne brišu automatski, već stave na čekanje u tzv. *hold queue*, gdje čekaju dok administrator ne odluči koje treba a koje ne treba proslijediti primatelju.

Podsjetimo prvo na ranije članke u kojima su opisana pravila, po kojima je moguće filtrirati e-poštu na osnovu primatelja ([Postfix: Selektivna zaštita korisnika](#)) ili na osnovu pošiljatelja ([Kako zabraniti primanje određenih dolaznih poruka?](#)).

U daljnjem tekstu bit će riječ o još dva pravila filtriranja, po zaglavlju i po sadržaju poruke a koja će se metoda ili čak kombinirane metode koristiti, ovisi o tome, s kako dovitljivim rasijačima *spam* i *phishing* poruka imamo posla.

Da bi e-poštu filtrirali po zaglavlju ili sadržaju (tijelu poruke), potrebno je imati instaliran dodatak postfixu za obradu *regularnih izraza*, najčešće se rabi ili **regexp** ili **pcre**. Recimo da ste se odlučili za *pcre* (=Perl Compatible Regular Expressions), onda prvo provjerite da li je instaliran:

pa ako vidite da nije, onda ga instalirate naredbom:

Ako želite mogućnost filtriranja i po zaglavlju (header) i po tijelu (body) poruke, onda u datoteku `/etc/postfix/main.cf` dopišite:

Kreirajte navedene datoteke (imena su proizvoljna), ako ne postoje:

U datoteku `/etc/postfix/header_checks` sada možete upisati filtere poput:

Primjetite da iza ključne riječi `HOLD Spam Header Rule` između dviju "taraba" (`#`) stoji opis o kojem se pravilu radi. To je korisno radi praćenja logova, ali treba paziti da ne bude isti kao i tekst koji se filtrira, jer će poruke logova koje daje *monit* ili OSSEC biti također zaustavljene (HOLD) ili odbačene (REJECT), (zato su ovdje stavljene zvjezdice ili crtice unutar njega!).

Unutar direktorija **/etc/postfix/** je potrebno još samo utipkati:

(eventualno se pojave opomene tipa: "record is in "key: value" format; is this an alias file?" ili "postmap: warning: header\_checks.db: duplicate entry: "/^from:", no u pravilu se mogu ignorirati.)

Provjeriti da li je kreirana datoteka **header\_checks.db**, te ponovo učitati postfix konfiguraciju:

Ista je procedura i za filtriranje po tijelu poruke: u datoteku **/etc/postfix/body\_checks** upišemo pravila filtriranja, npr:

ili bilo koji tekst koji je jednoznačan za neželjenu poštu, te potom u direktoriju **/etc/postfix/** izvršite:

Primijetite da se u gornjim primjerima maltene sva filtrirana pošta stavlja da čeka odluku administratora (ključna riječ HOLD) tj. posprema u *queue* direktorij **/var/spool/postfix/hold**.

Kad su filtrirane poruke stavljene na čekanje, može se putem zgodnog *ncurses* programčića **pfqueue** obaviti pregled, brisanje, isporuku pojedine ili istovremeno više poruka koje su na čekanju. Program treba pokrenuti (pod *root* ovlastima):

i u sučelju tipkama 1-4 se pozicionirati u odgovarajući *queue* direktorij (1=deffered, 2=active, 3=incoming, 4=hold). Ostale važne naredbe su: strelice gore-dolje=pozicioniranje na poruku, 'Enter'=vidi poruku, 'd'=brisanje poruke, 'l'=oslobađanje poruke s liste čekanja primatelju bez nanovog filtriranja, 'r'=oslobađanje poruke s liste čekanja, ali će ponovo proći filtriranje, 't'=(de)selektiranje više poruka, ';'=iduća naredba se odnosi na sve odabrane (selektirane) poruke, '?'=kompletan ispis naredbi.

Taj **pfqueue** je vrlo koristan, kad je u pitanju manji broj poruka (do cca 200) koje čekaju na odluku administratora. Mnogo toga je moguće napraviti i direktno iz komandne linije, treba se samo pozicionirati u direktorij **/var/spool/postfix/hold** U njemu su sve poruke pohranjene kao datoteke imena kojih su jedinstveni heksadecimalni nizovi kao npr:

Naredba:

prikazat će sadržaj poruke CECB6859E, a naredba:

poruke i njihove primatelje i pošiljatelje u svim *queue* direktorijima. Mi možemo i sami konfekcionirati naredbu, primjerice:

koja će npr. izlistavati naslove svih poruka u direktoriju uz pravilo po kojemu su filtrirane (zapisano u log datoteci), pa ako vidimo da se nedvojbeno radi o smeću s 'b' možemo brisati datoteku, tj. poruku. Umjesto 'Subject' (naslov) možemo koristiti i neku drugu ključnu riječ, 'From', 'Reply-To' i sl. Poruke, koje nismo obrisali odnosno, za koje znamo da nisu smeće, možemo proslijediti kome su upućene tipkom 'l', kad se pozicioniramo u *hold queue* tipkom '4' u programu **pfqueue**. Za one koji hoće još više mogućnosti iz komandne linije priložena je skripta **hold.sh** pri dnu ovog članka - daje mogućnost pregledavanja, brisanja, prosljeđivanja, kopiranja itd.

Testiranje efikasnosti pojedinih pravila za filtriranje ( zar to treba reći ☺ ) je slanje poruke s kompromitirajućim sadržajem i/ili zaglavljem - samom sebi.

Svi su se susreli s problemom crnih lista kod raznih mail providera, na koje ste sasvim sigurno stigli barem jednom. Scenarij je najčešće ovakav: netko od vaših korisnika proslijedio je svoju lozinku na neku adresu ili je ukucao u neku formu, vjerujući napisanom u phishing mailu.

Nakon što uspijete odblokirati vašu domenu, stvar nije gotova. Reputacija vaše domene je narušena, pa će svaki sljedeći put sankcije biti brže i teže. Nakon toga, neke mjere protiv vas provideri mogu uvoditi s lakoćom. Primjerice, mogu vam uvesti "*rate throttling*", odnosno usporavati primanje mailova s vaše domene. U logovima će se pojavljivati ovakve poruke:

Dobra je vijest da se ovakve stvari mogu spriječiti u samom Postfixu uz pomoć nekoliko postavki, odnosno direktiva. One omogućavaju kontrolu nad brojem primatelja, razmakom između slanja pojedinih poruka i brojem istodobnih isporuka na istu domenu. Te opcije su:

Ova postavka određuje koliko se istodobno poruka može isporučiti na istu domenu. Osnovna

vrijednost je 20, a mi preporučujemo 1.

Ovime određujemo vremenski period između slanja pojedinih poruka na istu domenu. Osnovna vrijednost je 0, a mi preporučujemo bilo koji period za koji smatrate da će biti dovoljno dugačak, primjerice 10 ili 20 sekundi.

Time smo ograničili broj primatelja u jednom mailu. Spameri znaju napisati desetke primatelja u polje "To", pa je ograničavanje broja primatelja način smanjivanja štete.

Postavke se upisuju u `/etc/postfix/main.cf`, nakon čega napravimo *restart*, odnosno *reload* postfixa. Točne vrijednosti za sve ove postavke najbolje je odrediti praćenjem logova i slušanjem zahtjeva korisnika.

Ako ste pomisli da će ovakva (vrlo restriktivna) ograničenja možda smetati određenim odredištima, u pravu ste. Ovako zadana ograničenja vrijede za sve domene i primatelje, pa ćete tako ograničiti slanje mailova i za servere koji nemaju nikakva ograničenja, poput nekih lokalnih poslužitelja.

Ima li tome pomoći? Naravno da ima.

Rješenje leži u pravljenju novih "transporta" i pripadajućih mapa. Postfix omogućava definiranje više "puteva" za isporuku mailova, pa je tako moguće definirati transport sa specifičnim postavkama. Na ovaj način je moguće fino podešavati isporuku po domenama, jednostavno pridružujući domenu određenom transportu.

Prvo je potrebno definirati transporte, koje ćemo ovaj put upisati u `/etc/postfix/master.cf`:

Definirali smo tri transporta, dva specifična i jedan generički ("sporo"), kojeg ćemo koristiti za više domena.

Kreiramo datoteku `/etc/postfix/transport_mapa` i u nju upišemo:

Kao i uvijek kod mapa, pokrenemo naredbu **postmap**:

Zatim zadamo putanju do transportne mape u `/etc/postfix/main.cf`:

Zadnje što je ostalo je definiranje opcija za svaki transport zasebno. Na početku smo definirali postavke za transport "smtp", ali princip je i dalje isti, samo se mijenja početno ime varijable:

Slično je i za druge transporte, samo treba promijeniti početno ime varijable, dakle **gmail\_destination\_concurrency\_limit**, **yahoo\_destination\_concurrency\_limit** itd.

Nakon restarta postfixa, sve bi mape trebale biti aktivne, a u logovima ćete moći pratiti idu li poruke po zadanim ograničenjima.

Ostaje pitanje koje vrijednosti koristiti? Na to je teško odgovoriti, jer sve ovisi o potrebama vaših korisnika. Nećete pogriješiti uvođenjem restriktivne politike. Uvijek naknadno možete povećati ograničenja, ako korisnici primjete da mailovi ne prolaze ili vam poruke previše čekaju u queueu.

Još jedna zanimljivost: ako varijablu **\*\_destination\_recipient\_limit** postavite na **1**, onda se ostale dvije postavke ne odnose više na domenu, nego na točno jednog primatelja s određene domene. Tako će mail upućen na drugog primatelja iste domene biti isporučen paralelno s prvim mailom, iako je **\*\_destination\_concurrency\_limit** postavljen na 1!

Uz pomoć ovakvih posatavki poruke će odlaziti "urednije" prema domenama s agresivnim metodama suzbijanja spama (poput gmaila), te više ne bi trebalo biti problema s usporavanjima koja nameću takvi mail provideri.

Jedno od pitanja koje dobijamo na helpdesku za sistem-inženjere je kako podesiti da u svim odlaznim mail porukama adrese korisnika budu "ime.prezime@domena.hr", a ne "username@domena.hr"? Pitanje je sasvim legitimno i može se riješiti, no nije univerzalno i nekima neće bitno pomoći, odnosno pomoći će samo djelomično. No, to ćemo kasnije malo prokomentirati.

Dakle, za prepisivanje (*rewrite*) adresa u ovom slučaju rabit ćemo kanonske mape (*canonical maps*).

U datoteci `/etc/postfix/main.cf` dodajte redak:

U navedenoj datoteci (`/etc/postfix/canonical`) upišite mapiranja za sve adrese kojima želite promijeniti oblik. Važno je napomenuti da ova datoteka nema isti oblik kao alias datoteka, jer nema dvotočki nakon prvog retka. Oblik je zapravo još jednostavniji:

Nakon toga pokrenite `"postmap /etc/postfix/canonical"` kako bi se izgradila baza (istu naredbu treba pokrenuti nakon svake promjene te datoteke):

Ovakvo prepisivanje adresa vrijedi i za odlazne i za dolazne adrese. Ukoliko želite potpuniju kontrolu, možete upotrijebiti opcije **"sender\_canonical\_maps"** i **"recipient\_canonical\_maps"**. Ove mape služe za prepisivanje odlaznih i dolaznih adresa, kako im i samo ime govori. Čak možete kombinirati sve tri opcije, a prioritet kod izvršavanja imaju pojedinačne mape, pa tek onda zajednička mapa.

Kako bi promjene bile vidljive Postfixu, potrebno je napraviti *reload*.

Za dodatne informacije konzultirajte man stranicu sa "man 5 canonical", ili posjetite web stranicu <http://www.postfix.org/rewrite.html#canonical>.

Još jedno rješenje je jednostavno promijeniti odlazne adrese na klijentskoj strani. Mana ovog pristupa je što korisnik naknadno može upisati što god želi unutar polja From:, pa ima na taj način mogućnost zaobići prepisivanje adrese. Ovome nema pomoći, barem ne na jednostavan način. No, može pomoći donošenje adekvatne [sigurnosne politike](#) koja će pokriti ovakve slučajeve, i imat ćete bazu na osnovu koje možete nekome uskratiti uslugu ukoliko uporno krši odluke donesene sigurnosne politike.

Postfix pomoćni program 'postsuper' (skraćeno od "postfix superintendent") je namijenjen za rad sa Postfix queuevima, odnosno mailovima u njima. Postsuper je namijenjen sistem administratorima, a ukoliko korisnici žele dio mogućnosti postsupera (npr. ispisati mail queue), trebaju rabiti naredbu 'postqueue'.

U većini slučajeva, postsuper će se rabiti za brisanje mailova iz queuea. U tu svrhu služi opcija -d:

Queue ID broj možete naći preko naredbe "postqueue -p", odnosno "mailq" (koju donosi postfix radi zadržavanja kompatibilnosti sa sendmailom).

Kako ovo zna biti nepraktično, a počesto i sporo, donosimo kratku perl skriptu `delete_from_mailq.pl` koja će olakšati uporabu ove naredbe. Skriptu snimite primjerice u `/usr/sbin` (ili neki drugi direktorij koji je u `$PATH`-u root korisnika).

Uporaba je iznimno laka, jer kao parametar očekuje e-mail adresu, odnosno regularni izraz u obliku "spam.\*@domena.com", ".\*@spammerdomain.com" itd.).

E-mail adresa može biti i potpuna, primjerice "netko.negdje@domena.net".

Skripta `delete_from_mailq.pl` (možete je skinuti i [direktno](#)):

Nakon podešavanja mail servisa obično nema potrebe da se naknadno išta mijenja. No, postoje slučajevi kada želite određenoj skupini korisnika dodijeliti drugi oblik odlazne adrese. Primjerice, želite da studenti imaju odlaznu adresu @student.domena.hr, ili ste u potpunosti promijenili domenu, a ipak želite nastaviti primati mail na staru domenu. Ova se situacija može riješiti uporabom canonical mapa.

Dakle, u `/etc/postfix/main.cf` upišite:

Ovim ste definirali gdje se nalazi mapa za konverziju e-mail adresa i definirali ste da vaš mail poslužitelj prima mail i za drugu domenu. Datoteka `/etc/postfix/canonical` izgleda ovako:

Objašnjenje i nije potrebno, korisnik `pero@domena.hr` će postati `pero@druga.domena.hr` i tako dalje. Oblik može biti i samo:

ali je ovaj način ovisan o ostatku vaše konfiguracije, pa je bolje navesti puno ime. Dalje je već poznato, morate generirati bazu:

Ostaje još samo restartati postfix:

Sada će svi odlazni mailovi navedenih korisnika imati odlaznu adresu kako ste naveli u datoteci canonical.

KEYWORDS: postfix canonical mape domena odlazna adresa

U ovom članku nećemo okolišati. Direktno ćemo prenijeti upit jednog kolega, iako je pitanje usko vezano uz članak "[Postfix: kako zabraniti primanje određenih dolaznih poruka?](#)". Radi se, opet, o restrikcijama pošiljatelja i već poznatim `check_sender_access` listama.

Evo što je kolegi zatrebalo:

Rješenje je jednostavno (kada znate kako): potrebno je rabiti odgovarajuću direktivu unutar pristupne liste, koju možemo nazvati **/etc/postfix/sender\_access**. U njoj obično zabranjujemo ili dopuštamo nešto, no ona može i više od toga.

Osim ključne riječi **OK** i **REJECT**, imamo i **DEFER**, **BCC**, **HOLD**, **FILTER**, **PREPEND**, **WARN** i druge. Značenja svake od ovih ključnih riječi možete vidjeti u stranicama pomoći s "**man 5 access**", no nas zanima **REDIRECT**.

Ukoliko bude zadovoljen uvjet, mail će uporabom direktive REDIRECT biti preusmjeren na drugu adresu. Konkretno, odgovor na korisnikov upit je:

U `/etc/postfix/main.cf` morate imati ovaj redak:

Još treba napraviti:

I to je to. Svaki mail s domene "domena.hr" će biti preusmjeren korisniku "korisnik@nasadomena.hr". **U slučaju da mijenjate** bilo što unutar datoteke `/etc/postfix/sender_access`, **morate ponovo kreirati bazu pomoću naredbe postmap**.

Kad svladaju neki mrežni servis, korisnici imaju tendenciju rabiti ga za skoro sve potrebe. Takav je i e-mail, koji se sve češće rabi za slanje vrlo velikih datoteka. Iako ovo zbog prirode maila nije preporučljivo (uvećava sve attachmente za 30%), to je realnost i jedino što nam preostaje je ograničiti veličinu maila, odnosno prilagoditi veličinu poruka potrebama korisnika.

Ukoliko želite smanjiti, odnosno povećati veličinu poruka koje prolaze kroz postfix na način sličan opciji "MaxMessageSize" u sendmailu, u `/etc/postfix/main.cf` upišite sljedeće:

Vrijednost je izražena u bajtovima, što znači da je u gornjem slučaju maksimalna veličina poruke oko 20 MB. Inače, sve poruke veće od 10 MB neće biti isporučene niti zaprimljene, jer je osnovna vrijednost ove opcije 10240000, što iznosi 10 MB.

Neophodno je nakon bilo kakve promjene u `main.cf` pokrenuti naredbu:

da bi se nove postavke počele primjenjivati.

Ponekad je poželjno da pojedine e-mail adrese na vlastitom mail poslužitelju zaštitite od primanja pošte izvan vlastite lokalne mreže. Primjerice, lokalne aliase ("svi@domena.hr") ne želite izložiti svijetu, a time i spammerima. Postavlja se pitanje je li to u Postfixu moguće, i kako?

Rješenje je zapravo vrlo jednostavno, u `/etc/postfix/main.cf` dopišite:

Ovaj redak upišite **ispod unosa permit\_mynetworks** u parametru **smtpd\_recipient\_restrictions**. Ostavite ostale unose kako su i bili. Podsjetimo, argumenti parametara u postfixu mogu biti u više redaka, ali na početku dodatnih redaka mora biti barem jedan prazan znak (indentacija). To onda izgleda otprilike ovako:

U datoteci `/etc/postfix/recipient_access` (ime ne mora biti ovakvo, možete navesti neko drugo koje se više slaže s vašim sustavom naziva datoteka) upišite ovo:

Kako se radi o hash datoteci, moramo napraviti i sljedeće:

Kako smo mijenjali konfiguraciju, moramo napraviti i:

Slanje na adrese, odnosno aliase unutar vaše domene više neće biti moguće izvana. Unutar lokalne mreže će i dalje sve normalno funkcionirati.

Postfix podržava filtriranje poruka u bilo kojoj fazi SMTP sjednice (sessiona), dakle može blokirati ili propustiti mail na osnovu adrese pošiljatelja, IP adresi ili domeni s kojom se udaljeni poslužitelj predstavlja, kao i po drugim, manje korištenim parametrima. Filtriranje po adresi pošiljatelja može zvučati kao dobro mjerilo, no u realnosti to nije tako. Ova se adresa bez ikakvih problema može lažirati, pa nema smisla blokirati prema ovom mjerilu ukoliko mislimo spriječiti spam. No, ipak u određenim situacijama ima smisla rabiti ovo mjerilo.

Obično prepuštamo kombinaciji Amavis/SpamAssassin da se brine o spamu, koji to u velikom postotku uspješno i čini. No, zbog određenih postavki ili njihovih kombinacije (poput ovog primjera), moguće je da uporni korisnik ili korisnici s iste domene mogu slati spam. Obično se to događa kod korisnika unutar Hrvatske ili iz regije jer nisu pisani na engleskom pa izbjegnu standardnu detekciju.

Moramo napomenuti da je ovakve slučajeve najbolje prijaviti nadležnim Abuse službama, a tek nakon njihove eventualne neaktivnosti pribjeći ovakvim rješenjima. Dovoljno je da pošiljatelj promijeni odlaznu adresu i spam će proći, čineći ovu metodu neefikasnu kao sredstvo zaštite od spama. S druge strane, može uštedjeti nešto resursa, jer će odbiti mail odmah na ulazu u sustav i neće ga se proslijediti u Amavis/SpamAssassin.

Sve što vam treba je access datoteka s unosima adresa, cijelih ili djelomičnih, te s akcijama koje trebaju biti poduzete nad njima. Ovaj tip datoteka Postfix rabi u svim drugim načinima filtriranja koje podržava, a više o formatu datoteke pročitajte u man stranici sa "**man 5 access**".

Pojednostavljeno, datoteka izgleda ovako:

U prvom stupcu se nalazi puna e-mail adresa ili njen dio, a u drugom akcija koja će se provesti ako dolazni mail odgovara adresama navedenim u access datoteci.

U primjeru, svi mailovi u obliku "domena.hr" će biti ignorirani (udaljeni poslužitelj će vidjeti kao da je mail uredno zaprimljen), a poruku iza naredbe "DISCARD" ćete moći vidjeti u logovima. Poruka, inače, nije obavezna. No, poruke od root korisnika ("root@domena.hr") će biti propuštene.

Ukoliko netko pošalje mail s adrese "netko@spam.hr", mail će mu biti odbijen (zato što rabimo "REJECT"), i moći će vidjeti našu poruku.

U prvom stupcu, osim pune adrese možete rabiti i sve druge načine koji su uobičajeni u postfix access datotekama. Izdvojit ćemo najčešće (ostale oblike možete naći s "man 5 access"):

### **korisnik@**

U ovom slučaju, domena se ne gleda, nego samo koji je korisnik poslao poruku

### **domena.hr**

Sve poruke s "@domena.hr" će biti obrađene. Podrazumijevano, ovo ne znači i poddomene, primjerice "@studenti.domena.hr". Ukoliko želite da se obrađuju i poddomene, stavite točku ispred: .domena.hr. Ukoliko je postavljena varijabla parent\_domain\_matches\_subdomains, točka ispred naziva domene nije potrebna, nego će se obrađivati i poddomene. Više o tome pročitajte u članku na [/sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postfix-ne-rade-poddomene-u-access-listi](#).

Akcija koje mogu biti provedene ima mnogo (DEFER, BCC, FILTER, REDIRECT...), no već smo naveli najčešće iz prakse. Mogli bi navesti još jedan čest primjer:

Gornji redak će, osim tekstom, poruku popratiti i standardnim SMTP kodom, pa ćemo time udaljeni poslužitelj ljubazno obavijestiti o čemu se radi, a on na osnovu toga odraditi njemu definirane akcije.

Kad jednom složite svoju access listu, tu datoteku nazovite prigodnim imenom (primjerice, /etc/postfix/sender\_access), te u /etc/postfix/main.cf upišite redak:

Ostaje još samo konvertirati datoteku u binarni hash:

i restartati, odnosno *reloadati* postfix:

Više o svim ostalim načinima limitiranja unutar SMTP sesije pročitajte na adresi [http://www.postfix.org/SMTPD\\_ACCESS\\_README.html](http://www.postfix.org/SMTPD_ACCESS_README.html).

O Postfixovim mogućnostima manipulacije mailom po različitim kriterijima smo već dosta pisali. U ovom članku ćemo se pozabaviti potrebom da zabranimo slanje maila na određene adrese, kao što smo u članku na adresi </sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postfix-kako-zabraniti-primanje-odredenih-dolaznih-poruka> obradili kako je moguće zabraniti primanje mailova s određenih adresa. Mehanizam koji ovo omogućava je, uostalom, isti.

Izravan povod za članak je upit sistem-inženjera koji je pristigao na sys.help. Njegovi su korisnici često slali mail na pogrešnu adresu radi izuzetne sličnost naziva njihove domene s onom udaljenog računala. Razlika je, naime, samo u jednom slovu. Naziv poštanskog sandučića je isti na obje domene, pa korisnici ne bi dobili obavijest o grešci, kada je i adresa na udaljenom računalu sasvim u redu. Problem je u neugodnostima koje si mogu priuštiti korisnici (a da to ni ne znaju) poslavši mail na ured druge institucije. Informacije u mailu mogu biti povjerljive, ili jednostavno neugodne po pošiljatelja.

Problem je lako riješiti uporabom mapa, s kojima smo se već susretali. Potrebno je upisati adresu (odnosno adrese) na koje ne želimo da korisnici šalju mail u datoteku, nazovimo je `/etc/postfix/recipient_access`:

Upišemo adresu koju želimo blokirati, zatim ključnu riječ REJECT, te tekst s objašnjenjem koji će korisnik vidjeti u svom mail klijentu i u logovima. Ovaj tekst nije obavezan, ali je svakako poželjan, kako bi korisnici bili upoznati s pravilom.

Kao i uvijek, treba napraviti binarnu .db datoteku:

Preostaje konfigurirati Postfix da bi koristio ovu datoteku i znao je tumačiti. U `/etc/postfix/main.cf` upišite na početak parametra `smtpd_recipient_restrictions` ovaj tekst:

Ukoliko su postojale neke druge direktive u tom parametru, ostavite ih nedirnute.

Na kraju, potrebno je napraviti reload, ili restart Postfixa:

Možda će Vam biti zanimljiva mogućnost preusmjeravanja mailova prema ovim adresama na neku drugu adresu. To možemo postići pomoću ovakve konfiguracije:

Iako je na tehničkoj razini ovakvo automatsko preusmjeravanje lako izvesti, nemojte su u to olako upuštati. Možda je korisnik zaista želio poslati mail na tu, "pogrešnu" adresu. Možda se raspituje za mogućnost zapošljavanja na drugoj instituciji, ili šalje neke privatne informacije? Ovakvo preusmjeravanje bi obavezno trebalo urediti sigurnosnom politikom, u dogovoru s upravom, te obavezno o tome obavijestiti korisnike.

Više o svim mogućnostima koje možete upotrijebiti u access mapi potražite na: <http://www.postfix.org/access.5.html>

Postfix nudi pristupne (access) liste za svaki dio SMTP konverzacije, ali možda vas je iznadanilo da se vama očekivano ponašanje jednostavno ne događa? Primjerice, naveli ste da ne želite nikakve mailove s domene primjer.com, jer vam od tamo stižu samo spam mailovi, ali mailovi u obliku `user@nesto.primjer.com` i dalje prolaze.

Problem je da u varijabli

mora postojati keyword "smtpd\_access\_maps". Ova varijabla prima i druge parametre, primjerice "mynetworks" ili "relay\_domains". Što sve prima, kao i uvijek, provjerite u [dokumentaciji](#).

Dakle, ako u main.cf imate

u svojim `smtpd_*` pristupnim listama možete očekivati da će domene uključivati i svoje vlastite

poddomene. U donjem primjeru, mailovi s domene primjer.com će biti zaustavljeni, ali mailovi s domene nesto.primjer.com hoće.

Ukoliko u parent\_domain\_matches\_subdomains ne postoji parametar smtpd\_access\_maps, morate koristiti oblik ".primjer.com" (dakle, s točkom ispred) kako bi i poddomene bile obuhvaćene:

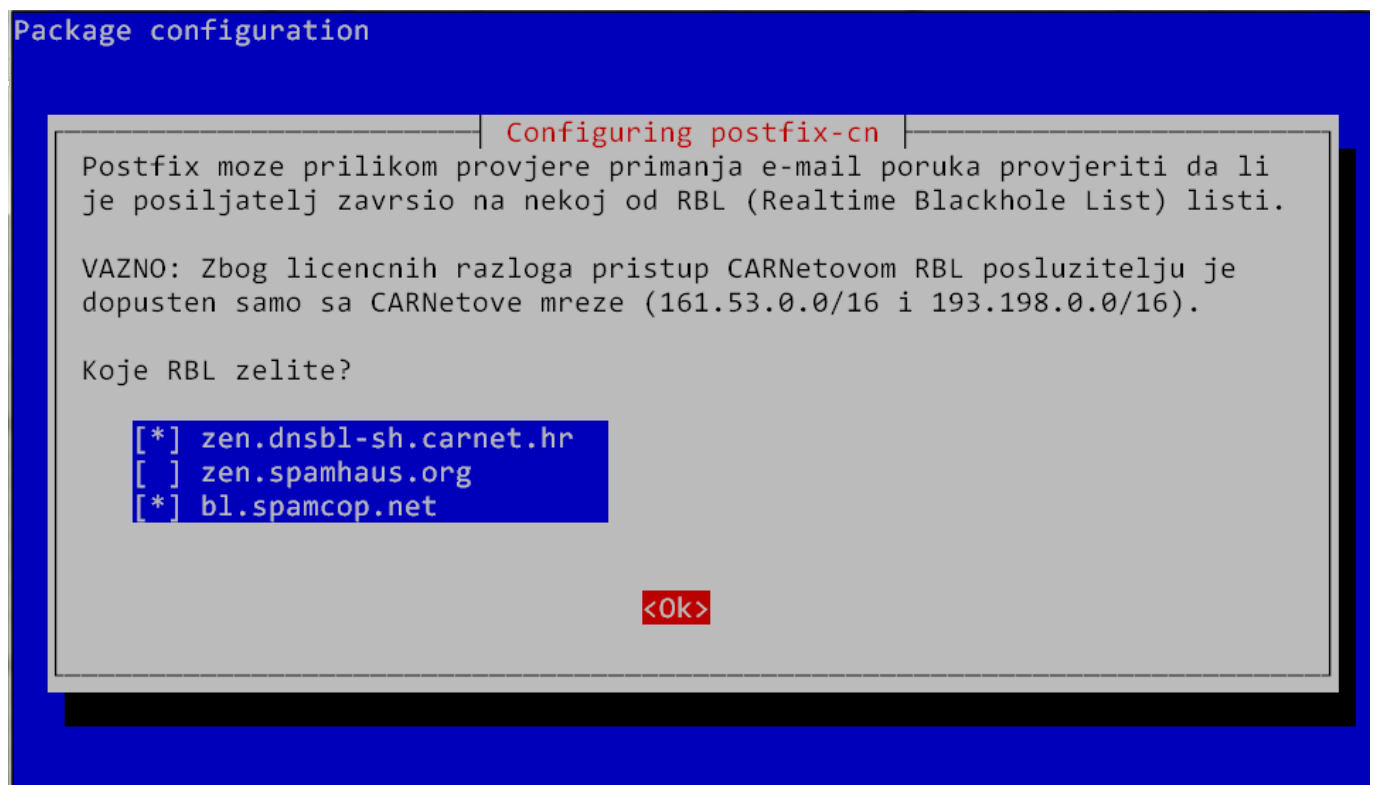
Naravno, vrijedi i obrnuto, tako da ako imate oblik domene s točkom, onda parametar "smtpd\_access\_maps" **ne smije** postojati u parent\_domain\_matches\_subdomains.

U novim inačicama Postfixa će podrazumijevana vrijednost biti da se eksplicitno **mora pisati točka** ukoliko želimo obuhvatiti i poddomene. Prilagodite svoje pristupne liste odmah u oblik s točkom, i ovaj parametar više neće biti potreban, niti ćete uopće morati znati da postoji.

Na sys.helpu smo zaprimili upit jednog kolege o problemu s mailom. Kako nam nije poslao logove, zatražili smo ih. Kada smo ih pogledali, pronašli smo zapis koji nije imao veze s problemom, ali je bio zanimljiv. Doduše, navikli smo da na raznim poslužiteljima nađemo različite "zaostatke", odnosno stvari koje su instalirali prethodnici ili trenutni sistemci (pa zaboravili na to). U ovom slučaju, radi se o zaboravljenom RBL poslužitelju, kojeg smo prepoznali u ovom retku u logovima:

Poslužitelj dnsbl.njabl.org je ugašen još 2013. godine, a u našem paketu postfix-cn je on tada i izbačen (izvadak iz skripte postinst):

Drugim riječima, potrebno je prekonfigurirati paket postfix-cn:



Možete izbaciti sve, osim **zen.dnsbl-sh.carnet.hr** i **bl.spamcop.net** (zen.spamhaus.org mi zrcalimo [još od 2008. godine](#)). Ukoliko želite rabiti dodatne blockliste, možete to učiniti direktno u /etc/postfix/main.cf, ali onda pripazite kod nadogradnji, jer će paket postfix-cn pregaziti te vaše postavke za RBL poslužitelje.

U ovom slučaju, velike štete nema, ali se za svaki mail slao upit DNS-u. Na to je potrošena tek po koja milisekunda, što nije puno, ali na jako opterećenim ili starijim poslužiteljima može nešto značiti. U svakom slučaju, nepotrebne i ugašene servise ne treba rabiti na poslužitelju u produkciji.

Danas uopće nije rijetkost da institucije imaju potrebe primati mail za više domena (primjerice, pojavila se domena tvrtke koja je u vlasništvu nekog instituta). Ovo uključuje i slučaj kad je riječ

samo o novoj poddomeni (primjerice, otvorio se novi laboratorij u sklopu fakulteta). U najvećem broju slučajeva za te domene nisu predviđeni dodatni poslužitelji (bilo iz razloga nedovoljnih tehničkih ili financijskih resursa, bilo iz nekog drugog razloga). No, na postojećem poslužitelju je moguće podesiti "virtualnu prisutnost" novog subjekta, kao što je primanje i slanje mailova. Postfix, mail servis koji dolazi sa CARNetovim poslužiteljima podržava ovu mogućnost, a problem se najlakše rješava preko virtualnih mapa.

Prije samog početka potrebno je urediti DNS. Ukoliko se DNS za novu domenu nalazi negdje dalje, treba s administratorom tog DNS poslužitelja dogovoriti da doda MX zapis koji će pokazivati na vaš poslužitelj. Ako će DNS biti kod Vas, na DNS poslužitelju će biti potrebno izvršiti određene preinake, odnosno dodati novu zonu u konfiguraciju. Pretpostavit ćemo da je "papirologija" s DNS službom već obavljena, jer u protivnom nova domena neće proraditi.

Dakle, treba kreirati novu zonu za novu domenu, ali i pripadajuće reverzne zapise. U `/etc/bind/novadomena.db` upišite (ili iskopirajte neku drugu zonu i samo izvršite modifikacije):

Treba uočiti da se nova domena služi istim mail (MX) poslužiteljem kao i osnovna domena.

Za reverzne zapise u `/etc/bind/novadomena.rev`, učinite sljedeće:

Nadalje, u `/etc/postfix/main.cf` treba dodati linije:

**Valja napomenuti da virtualnu domenu nikad ne smijete ujedno navesti i u opciji "\$mydestination"!**

Sadržaj `/etc/postfix/virtual`:

Sljedeći korak je, kako to piše u samoj datoteci, kreiranje *hash*-a baze:

Nakon upisa promjena, kao i uvijek, napravite reload:

Ukoliko je sve u redu, svaki će mail poslan na `@novadomena.hr` biti isporučen korisnicima lokalnog stroja. Ukoliko korisnik ne postoji (*catch-all* redak "`@novadomena.hr`"), mail će dobiti korisnik "root". Ovo je naravno veliki mamac za spamove, pa razmislite hoćete li zadržati ovu mogućnost. Ukoliko ne želite (samo zakomentirajte redak), posljedica je da će sva pošta za korisnike koji nisu navedeni u alias tablici biti odbijena, što je vjerojatno i najbolja opcija.

Ukoliko želite da odlazne adrese korisnika budu s novom domenom, podesite njihove klijente s novim odlaznim adresama (ili im samo kreirajte dodatni profil s novim podacima, a ostavite stari, osnovni). Također, možete probati upotrijebiti i canonical mape po savjetima iz članka [/sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postfix-kako-podesiti-da-odlazne-domene-za-pojedine-korisnike-budu-drugog-oblika](#).

Iako je uobičajeno da se pošta koju prima root korisnik preusmjerava na e-mail sistem-inženjera (ili više njih), neki preferiraju da tu poštu čitaju direktno preko root accounta.

Postfix tu praksu ukida, uz objašnjenje da ionako ne bi trebali rabiti root account za prijavu na sustav, osim u specifičnim slučajevima. Ovdje se misli da bi sve administrativne zadatke trebali obavljati preko `su` ili `sudo` naredbi, a nikako se ne koristiti root accountom za redovito logiranje (jer i najmanja nepažnja može biti katastrofalna). Zato i rootovu poštu ne bi trebali čitati direktno, nego preko svog accounta. Ukratko, da bi rootovu poštu primali, **mora** postojati alias na standardnom mjestu, u datoteci `/etc/aliases`:

U suprotnom, pošta jednostavno neće stizati na rootov korisnički račun. Kod uporabe `sendmaila`, pošta je stizala, ali postfix to eksplicitno brani: <http://www.postfix.org/faq.html#root>.

**Napomena:** nakon svake promjene alias datoteke, potrebno je pokrenuti naredbu "newaliases", inače novi aliasi neće biti prepoznati.

Dodatno, napomenut ćemo da je dužnost svakog sistem-inženjera da **redovito** čita sustavski mail i logove, jer to svakako pomaže kod sprječavanja većih problema, ili čak raspada sustava. S vremenom će to postati navika, a zauzvrat održavanje sustava lakše.

Postfix, mail poslužitelj kojeg smo odavno odabrali kao najfleksibilnijeg za uporabu na CARNetovim poslužiteljima na ustanovama članicama, većinu vremena radi svoj posao i ne "buni" se previše. Kad se pojavi problem, Postfix će svoje probleme prijaviti na adresu 'postmaster'. No, ponekad će Postfix (primjerice nakon nadogradnje sustava) početi prijavljivati određene stvari kao probleme, iako ti problemi ne utječu na rad sustava.

Jedan češći slučaj (sudeći po vašim upitima) se manifestira tako da za svaki poslani i/ili primljeni mail, na postmasterov mail stigne upozoravajući mail otprilike ovog sadržaja:

Kako ovakvih mailova može biti na desetke, normalna je želja sistemca da zaustavi navalu ovakvih mailova. Zanimljivo je da ćemo ovaj put činjenicu da bi trebalo riješiti osnovni problem koji izaziva ove poruke (jer je moguće da i drugi problemi uzrokuju jednako ponašanje), te ćemo samo "pospremiti problem pod tepih". To ćemo učiniti preko varijable **notify\_classes**, koja se nalazi u konfiguracijskoj datoteci /etc/postfix/main.cf.

Poslužimo se znanjem iz prethodnih članaka, i pogledajmo vrijednost te varijable:

Ono što trebamo učiniti je upisati "notify\_classes = resource" u main.cf i restartati Postfix:

Na ovaj način smo zaustavili poruke, jer smo isključili obavještanje o greškama u softveru, i ostavili samo obavještanje o nedostatku resursa. Koje još opcije ima direktiva notify\_classes? Navest ćemo ih sve:

**bounce** - Ukoliko je navedena, na adresu postmastera će biti poslana sva zaglavlja odbijenih poruka, uključujući i cijelu SMTP sjednicu (*session*). Ova opcija automatski uključuje opciju **2bounce**.

**2bounce** - Sva odbijena pošta će biti poslana na postmastera. Ovo ne uključuje SMTP sjednicu.

**delay** - Ukoliko mail kasni, kopija zaglavlja će biti poslana na adresu postmastera.

**policy** - Ukoliko je udaljeni poslužitelj odbijen zbog lokalne politike (*policy*), cijela sjednica će biti poslana na adresu postmastera. Obično se radi o lokalnim antispam mjerama.

**protocol** - Ukoliko se dogode greške u samom SMTP protokolu, zapis cijele sjednice će biti poslan na adresu postmastera.

**resource** - Kako smo već naveli, mail će biti poslan postmasteru u slučaju nedovoljnih resursa mail servisa.

**software** - Softverski problemi uključuju i pogrešnu ili djelomično ispravnu konfiguraciju, pa ćete uključivanjem ove opcije dobiti izvješće na adresu postmastera, ukoliko se takvi problemi pojave.

Adresa (zapravo, može biti posebna adresa za skoro svaku kategoriju) na koju će biti slana izvješća se može promijeniti (može se promijeniti parametrima **\*\_notice\_recipient**), no bit će dovoljno provjeriti je li alias postmaster postavljen:

Ukoliko to nije slučaj, upišite ga, a root alias (ukoliko to nekim čudom još nemate) postavite na svoj korisnički račun (ili više njih):

Nakon toga trebate izvršiti naredbu **newaliases**.

Više o direktivi notify\_classes možete naći na standardnom mjestu (man stranice, dokumentacija paketa), ili na Postfixovom web sjedištu:

[http://www.postfix.org/postconf.5.html#notify\\_classes](http://www.postfix.org/postconf.5.html#notify_classes)

Parametar "relay\_domains" određuje za koje domene će naš poslužitelj raditi "relay", odnosno zaprimanje i prosljeđivanje maila. Može ih biti više u istom retku.

Uobičajena je ovakva situacija:

iako nije neuobičajeno naći ovaj parametar prazan:

U tipičnom slučaju kojeg možemo naći na institucijama članicama CARNeta mail poslužitelj se nalazi na lokaciji gdje se nalazi većina zaposlenika, a institucija ima eventualno još jednu lokaciju ili

nekoliko njih. Kako bi korisnici mogli slati mail preko tog poslužitelja, Postfix je potrebno konfigurirati tako da zaprima mailove (radi *relay*) iz "domaćih" mrežnih segmenata i šalje ih na odredište. Ovo je lako napraviti, jer samo treba u varijablu `$mynetworks` upisati novi segment i restartati Postfix.

Problem nastaje kada korisnici žele slati mailove od kuće, ili sa službenog puta. U tom slučaju nemamo izbora nego dodati sve segmente određenog ISP-a kako bi korisnik mogao slati mail iz mreže baš tog ISP-a. Kasnije, javit će se drugi korisnik koji rabi drugi ISP, pa moramo dodati i te segmente i tako unedogled. Jasno je da dodavanje drugih mrežnih segmenata otvara Vaš mail poslužitelj eventualnim spammerima iz Hrvatske (ili korisnicima koji ni ne znaju da su im računala zaražena kakvim crvom). Ukoliko korisnik putuje u inozemstvo, praktički je nemoguće saznati koji će segment korisnik rabiti za spajanje.

Postoji nekoliko načina da riješimo ovaj problem:

Možemo uputiti korisnike da na putu ili od kuće rabe webmail na vašim stranicama ili pak preko središnjeg servisa <http://webmail.carnet.hr>. U ovom slučaju se može pojaviti problem, ako korisnici rabe zastarjeli POP3 protokol. Tada neće imati sinkronizirano stanje na vlastitom računalu sa stanjem na poslužitelju (npr. neće imati poslone mailove u Outlooku ili Thunderbirdu, nego će ti mailovi biti samo na poslužitelju).

Najbolje je rješenje rabiti SMTP autentikaciju preko SASL daemona. Na ovaj način moguće je slati mailove preko poslužitelja na vašoj ustanovi preko bilo koje mreže. Jedini uvjet je da se korisnik prethodno "predstavi" sustavu, dakle upiše svoje podatke (username i password) u svoj mail klijent.

Svi mail klijenti podržavaju ovu mogućnost autentikacije, pa jedino ostaje da korisnicima podesite mail klijente ili im date upute kako da to sami učine. Jednom podešeni klijenti mogu nastaviti raditi i "kod kuće" i unutar lokalne mreže, samo će se u logovima vidjeti novi unosi poput "sasl\_username" i "sasl\_method":

Nikako **nemojte uključivati** opcije "Use Secure Authentication", "Secure Password Authentication (SPA)" i slično. Radi se o Microsoftovim metodama autentikacije i na Postfixu neće raditi. Sva potrebna podešavanja na Postfixu su već napravljena, ukoliko imate CARNET paket postfix-cn. U `/etc/postfix/main.cf` bi trebale biti uključene ove opcije:

Jedino, možete provjeriti je li pokrenut `saslauthd` proces:

Dakle, sve je u redu, SASL daemoni su pokrenuti. Ukoliko nisu, provjerite zašto po uputama u članku [/sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#postfix-potencijalni-problemi-sa-sasl-autentikacijom](#).

Navest ćemo podešenja za dva najpopularnija mail klijenta:

### **Mozilla Thunderbird:**

Tools -> Account Settings -> Outgoing Server -> Edit -> <pod "Security and Authentication" kliknuti na "Use Name and Password" -> <popuniti podatke>

Settings

Description: SMTP sa autentikacijom

Server Name: server.domena.hr

Port: 25 Default: 25

Security and Authentication

Use name and password

User Name: korisnik

Use secure authentication

Connection security: None

OK Cancel

### Microsoft Outlook:

Tools -> Account Settings -> <dvoklik na profil>

-> More Settings -> Outgoing Server -> <upišite podatke> -> <isključiti SPA>

Internet E-mail Settings

General Folders Outgoing Server Connection Advanced

My outgoing server (SMTP) requires authentication

Use same settings as my incoming mail server

Log on using

User Name: korisnik

Password: \*\*\*\*\*

Remember password

Require Secure Password Authentication (SPA)

OK Cancel

Za druge klijente je postupak, pretpostavljamo, vrlo sličan, pa ne bi trebao biti problem i njih podesiti.

Više o načinu rada SASL autentikacije, možete pročitati u članku "[SASL - Simple Authentication and Security Layer](#)"

U za današnje vrijeme zaista nevjerovatnom slučaju da još rabite sendmail, otkucajte slijedeću

naredbu da biste prešli na postfix:

Ako Vas debconf ništa ne pita, kasnije napravite:

- odgovorite "Internet Site"
- upišite svoj account (odnosno mail sistem inženjera) na pitanje "Where should mail for root go"
- upišite puno ime računala sa domenom na pitanje "Mail name?"
- samo potvrdite na pitanje "Other destinations to accept mail for?", osim u slučaju da će ovaj poslužitelj primiti poštu i za druge domene
- odgovorite No na pitanje "Force synchronous updates on mail queue?"
- uključite sve ponuđene RBL-ove sa tipkom SPACE
- uključite podršku za GECOS
- odgovorite Yes na pitanje "Zelite li nastaviti?"
- (sendmail-base i amavisd-milter će biti obrisani, to je u redu)
- ukoliko se pitanje za MatchGECOS pokaže još jednom, odgovorite kao i u prethodnom slučaju

Ukoliko poslije svega ne bude sve u redu, pogledajte ima li zaostalih sendmail procesa:

Ukoliko ih još ima, pobijte ih sve:

Restartajte mail sustav, najbolje s naredbom:

Ukoliko i dalje nešto ne radi (to će se najbrže vidjeti po logovima), provjerite jesu li pokrenuti procesi saslauthd i postgrey:

Ukoliko se ID procesa ne pokaže, startajte te procese:

U logovima (/var/log/mail/mail.log) će ispravan rad biti vidljiv ovako:

Kod nadogradnje složenijih servisa, koji imaju nekoliko daemona i međuovisnosti poput sendmaila (koji ovisi o clamavu, sophosu i milteru), lako je moguće da se pojave problemi. No, u gotovo svim slučajevima ti se problemi lako rješavaju.

Najčešći problem je zaostanak nekog od procesa, pa se tako Postfix ne može pokrenuti jer je port 25 još uvijek "zauzet" sa sendmail procesom, "nestao" je socket ili slično. Simptomi su lako uočljivi u mail.logu:

Poruke mogu biti i drugačije, ali problem je isti: mail ne radi. Problem je lako rješiv jednostavnim restartom poslužitelja, čime se ubijaju svi zaostali procesi i Postfix može nesmetano raditi.

No, problem nastaje u trenutku kad nije povoljan trenutak za restart poslužitelja, jer ipak treba obavijestiti korisnike da će nastupiti prekid - možda upravo korisnici objavljuju web stranice i slično. Srećom, ovu operaciju možete izvesti i ručno. Prvo treba provjeriti koji su procesi zaostali:

Navedene procese ubijte s naredbom "pkill":

Svakako provjerite jesu li se procesi uistinu pogasili:

Slijedeći korak je restart amavisa, koji će znati sam pokrenuti postfix i clamd:

U logovima sad ne bi trebalo biti problematičnih poruka, a ispravan rad će ostaviti otprilike ovakav trag:

Ukoliko ručno ne uspijete "probuditi" mail podsustav, uvijek ostaje opcija restarta poslužitelja, jer se ne isplati gubiti vrijeme na traženje greške, dok (nervozni) korisnici čekaju da mail proradi.

Kako instalacija postfixa ne briše postavke sendmaila, možete obrisati sve tragove sendmaila naredbom (ako imate access listu, sačuvajte je prije toga):

Naredba "sendmail" koja se pojavljuje u /usr/sbin/ je postfixova "dummy" naredba, uvedena smao zbog kompatibilnosti sa mnogim programima koji očekuju sendmail na tom mjestu. Ne treba ju miješati sa originalnim programom sendmail. Slično je i s naredbom "mailq", iako istu stvar radi "postqueue -p".

Nakon instaliranja paketa postfix-cn preko starog i nepodržanog paketa sendmail-cn, u nekim slučajevima je moguće da *odjednom* u nekim mail klijentima ne radi autentikacija, dakle "server ne prima password" i mail se ne može poslati. Ovo se poglavito odnosi na Mozilla Thunderbird, dok Microsoft Outlook (Express) i drugi nemaju tih problema.

Pri tome se u logovima pojavljuju unosi slični ovima:

Razlog je taj što Thunderbird inicijalno rabi SASL PLAIN mehanizam autorizacije, dok Outlook Express ne (iako se može uključiti). Konkretno, problem je u tome što proces saslauthd nije pokrenut, te ga stoga treba pokrenuti. Provjerite je li u datoteci `/etc/default/saslauthd` parametar `START` odkomentiran:

Ukoliko je zakomentiran, odkomentirajte ga:

Startajte saslauthd:

Provjerite radi li SASL mehanizam:

Morate dobiti poruku kao što je gore navedeno, i u tom slučaju je sve u redu.

Ukoliko vam se nakon instalacije postfix-cn paketa događaju problemi s primanjem mailova koji stižu izvan vaše lokalne mreže, a u logovima se pojavljuju poruke poput ove:

rješenje je vrlo jednostavno: treba restartati postgrey daemon.

Ukoliko to ne pomogne, restartajte i sam postfix sa

Problem je nastao jer iz nekog razloga postgrey daemon nije startan ili postfix ne vidi njegov mrežni socket. Postgrey je *policy daemon* za postfix, i opisan je u članku na CARNetovom portalu za sistemce [/sys-trek-objave/postfix-savjeti-i-trikovi-zeljko-boros/#greylisting-za-postfix-postgrey](#)

Postfix ne podržava opciju MatchGECOS, kao što to (kršeći pravila) čini sendmail, pa se može dogoditi da aliasi u obliku `Ime.Prezime@institucija.hr` ne rade. Jedan razlog je da prilikom instaliranja nije odabrana podrška za GECOS.

Provjerite trenutnu situaciju sa slijedećom naredbom:

Vrijednost 'matchgecos' mora biti true.

Ukoliko to nije slučaj, napravite slijedeće:

Tu svakako promijenite vaš odabir na "Yes" kod pitanja "Želite li podršku za GECOS?".

Drugi razlog može biti neispravni GECOS unos u `/etc/passwd` ili neminovno kašnjenje generiranja aliasa.

Alias oblika `Ime.Prezime` se iz datoteke `/etc/passwd` generiraju svaki puni sat. Generiranje se radi preko crona (skripta je `/etc/cron.daily/postfix-cn`), a učestalost osvježavanja možete povećati ili smanjiti po želji u datoteci `/etc/cron.d/postfix-cn`.

Ukoliko vas ni ovakvo rješenje ne zadovoljava, možete ručno pokretati skriptu `/usr/share/postfix-cn/make-aliases-gecos.sh` svaki put kad dodate korisnika. Tom će korisniku alias odmah biti aktivan.

Postoji još jedna razlika u odnosu na sendmail. Sve će greške iz `/etc/passwd` datoteke biti prijavljene odmah i u mail, dok je to sendmail radio samo u logove. Najčešće će to biti problemi s dvostrukim aliasima, slovima s dijakritičkim znakovima ili telefonskim brojem u GECOS polju. Takvim korisnicima aliasi neće raditi, a u slučaju dvostrukih korisnika mail će dobiti samo prvi pronađeni korisnik:

U datoteci `/var/lib/postfix-cn/aliases_gecos` (gdje se nalaze automatski generirani aliasi), situacija je onda ovakva:

Mail poslan na `Ime.Prezime@institucija.hr` će primiti samo `account1`, stoga korigirajte ime i prezime korisnika po vlastitim potrebama.

Datoteku `/var/lib/postfix-cn/aliases_gecos` nikad nemojte ručno mijenjati, jer će sve vaše promjene biti izgubljene kod prvog slijedećeg pokretanja skripte iz crona.

Postfix podržava i staru alias datoteku /etc/aliases (ili /etc/mail/aliases, ako je simbolički linkana na /etc/aliases). Ovu mogućnost uključuje opcija u /etc/postfix/main.cf, a načelo je "first come, first served", ili popularnije "tko prvi njemu djevojka":

Sve vaše posebne aliase (svi@, profesori@) dodavajte i dalje u /etc/aliases, postfix to neće nikad dirati.

Treći i posljednji razlog je opet povezan sa neispravnim unosima u /etc/passwd. Prilikom nadogradnje sa Solarisa i drugih Unixa moguće je da su korisnički id brojevi (UIDs) ostali ispod granice od 100, što je na linuxu rezervirano za sustavske potrebe. Ovako možete provjeriti imate li regularne korisnike ispod granice od 100:

Ovo će ispisati sve korisničke račune ispod UID-a 100. Ukoliko se ovdje mogu vidjeti računi "živućih" korisnika, promijenite im UID sa naredbom:

Datoteke i direktorije koji se nalaze izvan korisnikovog \$HOME direktorija morate ručno promijeniti sa ako cijeli direktorij (i poddirektoriji) trebaju pripadati tom korisniku ili ako je potrebno promijeniti samo nekoliko datoteka.

Na portalu za sistemce postoji članak (<http://sistemac.carnet.hr/node/101>) gdje je opisan način rada i implementacija greylistinga za sendmail. Ovdje ćemo opisati greylisting za postfix, postgrey.

Postgrey nema posebnu konfiguracijsku datoteku, osim /etc/default/postgrey. U principu, ovdje se nema što ni mijenjati, osim eventualno vremena usporenja za inicijalni primitak maila, --delay. U CARNetovom paketu je ova vrijednost podešena na 58 sekundi:

Ostatak retka govori da postgrey daemon sluša na lokalnom mrežnom sučelju na portu 60000. Naravno, odgovarajuća vrijednost mora postojati i u postfixu u main.cf (pored ostalih opcija):

Da se podsjetimo, greylisting radi na način da za svaku SMTP sesiju (session, sjednicu) zabilježi tri parametra: IP adresu udaljenog računala, envelope adrese pošiljalca i primatelja, takozvani triplet. Svaki put kad vidi jedinstvenu kombinaciju ova tri parametra, odnosno jedinstveni triplet, greylista odbije mail (uz standardnu poruku "450 <[netko@negdje.hr](mailto:netko@negdje.hr)>: Recipient address rejected: Greylisted for XX seconds") i zabilježi triplet u svoju whitelistu.

Ukoliko u navedenom periodu od XX sekundi udaljeni poslužitelj opet bude pokušao isporučiti mail, on će biti odbijen, ali se vrijeme odbijanja (delaya) i dalje smanjuje. Kad to vrijeme istekne, mail će uredno biti zaprimljen.

Razlog ovakvog ponašanja ovog filtera je jednostavan: svaki (ispravno podešeni) mail poslužitelj **\*mora\*** pokušavati isporučiti mail nekoliko puta, često i nekoliko desetaka puta u periodu od nekoliko sati do nekoliko dana, u ovisnosti o postavkama udaljenog poslužitelja. Spammeri rabe posebne programe, koji ne poštuju sve konvencije te se ni ne trude protumačiti poruke o greškama koje dobivaju od udaljenih poslužitelja. Njima je jedino bitno isporučiti što više spamova u što kraćem vremenu.

Zbog ove činjenice efikasnost greyliste je čak oko 97%, iako se može očekivati ovo smanjenje čim se spammeri budu prilagodili. Do danas ta prilagodba nije primijećena u znatnijoj mjeri.

Jedan manji problem kod greylistinga je zaustavljanje svih mailova koje sustav susreće po prvi put. Kako bi se ovo ponašanje ublažilo, defaultno je uključena opcija --auto-whitelist-clients=5. Ona jednostavno omogućava da se nakon 5 uspješno propuštenih mailova ta IP adresa stavi u whitelistu i na taj način trajno omogući primanje mailova s te adrese, bez ikakvih usporavanja. Da bi --auto-whitelist-clients opcija proradila, treba zadovoljiti dodatni uvjet da je IP adresa s koje je poslan mail "viđena" u zadnjih --max-age dana (default je 35).

Slična se operacija može napraviti i ručno (što je puno fleksibilnije), što ćemo obraditi u nastavku članka.

Kako ne bi bespotrebno usporavali e-mail promet unutar Hrvatske, paket postfix-cn donosi popis

većine MX poslužitelja u CARNetu. Ovi se poslužitelji nalaze u datoteci /etc/postgrey/whitelist\_clients(.local). Ovdje možete dopisati MX poslužitelje s kojih vam dolazi znatnija količina pošte. Primjerice:

Dakle, moguće je koristiti ime udaljenog računala, njegovu IP adresu ili regularni izraz koji opisuje poslužitelje koje želite propuštati bez zastoja.

U istom direktoriju postoji datoteka whitelist\_recipients. Kako samo ime govori, radi se o datoteci gdje možete upisati primatelje na lokalnom računalu za koje se greylista neće primjenjivati. Ovo ne znači da se mail neće dalje provjeravati u SpamAssassinu, te je moguće da mail bude odbijen (jer je spam) iako je prošao greylistu!

U obje datoteke možete upisati nazive poslužitelja, IP adrese, e-mail adrese, regularne izraze i slično. Potpuni popis potražite u man stranicama (man postgrey).

Nakon bilo kakve promjene u ovim (dodatnim) whitelistama, napravite reload postgreya:

U mail.logu će se moći vidjeti sljedeći redak:

Fizički, baza tripleta (whitelista) se nalazi u /var/lib/postgrey i ne briše se između restarta računala. Ne morate (ni nemojte!) ovdje ništa dirati.

Više informacija imate na URL-u <http://projects.puremagic.com/greylisting> i naravno, u manualu (man postgrey).

U proteklom razdoblju smo vas upoznali s načinom rada [greylistinga](#), kako člancima tako i paketom postgrey-cn. Podsjetimo se, greylisting radi na način da inicijalno odbija sve mailove, te nakon isteka određenog vremenskog perioda počne primati mailove koji se opet pojave s istim parametrima (IP adresa udaljenog poslužitelja, primatelj i pošiljatelj). Kako spam programi nisu provjeravali izlazne kodove mail poslužitelja, niti su pokušavali ponoviti isporuku, spam je bio zaustavljan u visokom postotku. Nažalost, bilo je samo pitanje vremena kad će se spameri prilagoditi, a to se upravo i dogodilo.

Sve manje i manje spama biva zaustavljeno na ovaj način, pa je CARNet u suradnji s grupom za izradu paketa odlučio da kroz pakete za CARNet-Etch distribuciju više ne bude distribuiran paket postgrey-cn. On je i dalje dostupan mimo CARNet paketa, kao osnovni Debian paket postgrey. Ukoliko tako želite i procjenite da vam je još uvijek koristan, možete ga nastaviti rabiti.

Greylisting preko postgreya će biti aktivan ako u /etc/postfix/main.cf imate redak `check_policy_service inet:127.0.0.1:60000`:

Ovime smo izgubili jedan alat za borbu protiv spama, ali zbog sve slabije efikasnosti i [uvođenja poboljšanja](#) u postojeće servise, sveukupna antispam zaštita mail poslužitelja neće doći u pitanje.