Postfix savjeti i trikovi - Željko Boroš

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

- Logirajte [1] se za dodavanje komentara

Kako omogućiti SASL autentikaciju (SMTP AUTH) samo nekim korisnicima?

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:

```
Dragi carnet.hr korisni?ki ra?un,


Ova poruka je od svog webmail usluga i održavanja vašeg ra?una e-pošte za
sve korisnike centra. Mi smo poboljšanje naše baze podataka i e-mail centra
zbog spama aktivnosti identificirane u našem sustavu e-pošte. Stoga, kako bi
se izbjeglo sve ra?une spam identificirali smo
poboljšanje i stvaranje prostora za nove.

Vi ste potrebni kako bi potvrdili svoj ra?un e-pošte putem e-pošte potvrdu
identifikacije.To ?e sprije?iti vaš korisni?ki ra?un iz zatvorena tijekom
ove vježbe.

Kako biste potvrdili svoj identitet e-mail, daju sljede?e podatke tražene u
nastavku:


* Korisni?ko Ime: (...........) (required)
* Lozinka: (...........) (required)
```

```
* Datum ro?enja: (...........) (Neobavezno)
* Država: (..............) (Neobavezno)
```

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 [2].

Više informacija o samom SASL-u možete naći u članku "SASL SMTP autentikacija u Postfixu [3]".

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). Konketno, 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:

```
MECHANISMS="sasldb"
```

Zatim treba dodali "privilegirane" korisnike u bazu:

```
# saslpasswd2 -c korisnik1 -u fqdn.ime.stroja.hr -f /etc/sasldb2
# saslpasswd2 -c korisnik2 -u fqdn.ime.stroja.hr -f /etc/sasldb2
# saslpasswd2 -c korisnik3 -u fqdn.ime.stroja.hr -f /etc/sasldb2
...
```

Provjera konzistentnosti i sadržaja baze:

```
# sasldblistusers2
korisnik1@fqdn.ime.stroja.hr: userPassword
...
```

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

```
# saslpasswd2 -d korisnik3 -u fqdn.ime.stroja.hr -f /etc/sasldb2
```

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

```
# /etc/init.d/saslauthd restart
```

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

```
Sep 14 11:22:43 po postfix/smtpd[2686]: D2745135951:
  client=fqdn.ime.stroja.hr[161.53.xx.yyy], sasl_method=PLAIN,
  sasl_username=korisnik1@fqdn.ime.stroja.hr
```

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

```
Sep 14 11:20:21 po postfix/smtpd[3230]: warning: SASL authentication failure:
  Password verification failed
Sep 14 11:20:21 po postfix/smtpd[3230]: warning:
  korisnik_izvan_sasldb@fqdn.ime.stroja.hr [1.2.3.4]: SASL PLAIN
  authentication failed: authentication failure
```

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

```
# /usr/sbin/saslauthd -d -a sasldb -c -m /var/run/saslauthd -n 5
```

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: http://sistemac.carnet.hr/node/388 [4]

- 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.

- Logirajte [1] se za dodavanje komentara

uto, 2010-11-23 12:45 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Software [6]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Kako prevesti bounce poruke Postfixa?

 *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 [7].

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 [8]:

```
# cd /etc/postfix
# vim bounces.cf
...
# postconf -e 'bounce_template_file = /etc/postfix/bounces.cf'
```

Tekst predložaka se upisuje kao "*Here document*" (što je to smo nedavno opisali u ovom članku na Portalu [9]), odnosno unutar dvaju identifikatora "END" (no može biti bilo koja riječ):

```
verify_template = <<END
Charset: us-ascii
From: MAILER-DAEMON (Mail Delivery System)
Subject: Status isporuke vaseg e-maila / Mail Delivery Status Report

Ovo je e-mail servis na posluzitelju $myhostname.

Vas zahtjev o statusu isporuke vaseg e-maila se nalazi ispod.

        E-mail sustav na posluzitelju $myhostname

END

delay_template = <<END
...
END
```

i tako za svaki željeni predložak.

Nakon toga bi bilo jako dobro testirati je li sve u redu s vašim predlošcima s naredbom "**postconf -b**" (s kojom smo vas upoznali u članku http://sistemac.carnet.hr/node/687 [8]). 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:

```
# postconf -b /etc/postfix/bounces.cf
```

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!):

```
failure_template = <<EOF
Charset: us-ascii
From: MAILER-DAEMON (Mail Delivery System)
Subject: Vracena posta / Undelivered Mail Returned to Sender
Postmaster-Subject: Postmaster Copy: Undelivered Mail

Ovo je e-mail servis na posluzitelju $myhostname.

Obavjestavamo vas da vasa e-mail poruka nije isporucena jednom
ili vise primatelja. Poruka se nalazi u privitku.

Ukoliko trebate dodatnu pomoc, molimo obratite se na adresu
<postmaster@$myhostname> ili <root@$myhostname>

Molimo, ukljucite i ovu poruku kod prijave problema. Ukoliko zelite
privatnost, mozete obrisati tekst svoje originalne poruke, jer nije
kriticna za rjesavanje problema.

        E-mail sustav na posluzitelju $myhostname

=============================================================================

This is the mail system at host $myhostname.

I'm sorry to have to inform you that your message could not
be delivered to one or more recipients. It's attached below.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system
EOF



delay_template = <<EOF
Charset: us-ascii
From: MAILER-DAEMON (Mail Delivery System)
Subject: Neisporucena posta (no jos se pokusava isporuciti) / Delayed Mail (still bei
ng retried)
Postmaster-Subject: Postmaster Warning: Delayed Mail

Ovo je e-mail servis na posluzitelju $myhostname.

############################################################################
#   OVO JE SAMO UPOZORENJE. NE MORATE PONOVO SLATI SVOJU POSTU.    #
############################################################################

Vasa posta nije mogla biti isporucena u vremenu od
$delay_warning_time_hours sata(i).
```

```
Slanje vase poste ce biti pokusavano dok ne bude stara
$maximal_queue_lifetime_days dana.

Ukoliko trebate dodatnu pomoc, molimo obratite se na adresu
<postmaster@$myhostname> ili <root@$myhostname>

Molimo, ukljucite i ovu poruku kod prijave problema. Ukoliko zelite
privatnost, mozete obrisati tekst svoje originalne poruke, jer nije
kriticna za rjesavanje problema.

        E-mail sustav na posluzitelju $myhostname

=========================================================================

This is the mail system at host $myhostname.

#########################################################################
# THIS IS A WARNING ONLY.  YOU DO NOT NEED TO RESEND YOUR MESSAGE. #
#########################################################################

Your message could not be delivered for more than
$delay_warning_time_hours hour(s).
It will be retried until it is $maximal_queue_lifetime_days day(s) old.

For further assistance, please send mail to <postmaster>

If you do so, please include this problem report. You can
delete your own text from the attached returned message.

                   The mail system
EOF
```

success_template = <<EOF

```
Charset: us-ascii
From: MAILER-DAEMON (Mail Delivery System)
Subject: Uspjesno isporucena posta / Successful Mail Delivery Report

Ovo je e-mail servis na posluzitelju $myhostname.

Vasa posta je uspjesno isporucena na adresu ili adrese navedene nize.
Ukoliko je posta uspjesno stigla u udaljeni sanducic, necete vise
primati dodatne obavijesti. U slucaju greske na drugim posluziteljima
moguce je da cete primiti dodatne poruke.

        E-mail sustav na posluzitelju $myhostname

=========================================================================

This is the mail system at host $myhostname.

Your message was successfully delivered to the destination(s)
listed below. If the message was delivered to mailbox you will
receive no further notifications. Otherwise you may still receive
notifications of mail delivery errors from other systems.

                   The mail system
```

```
EOF



verify_template = <<EOF
Charset: us-ascii
From: MAILER-DAEMON (Mail Delivery System)
Subject: Status isporuke vaseg e-maila / Mail Delivery Status Report

Ovo je e-mail servis na posluzitelju $myhostname.

Status isporuke vaseg e-maila se nalazi ispod.

        E-mail sustav na posluzitelju $myhostname

=========================================================================


This is the mail system at host $myhostname.

Enclosed is the mail delivery report that you requested.

                   The mail system
EOF
```

- Logirajte [1] se za dodavanje komentara

sri, 2010-01-13 10:42 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Postconf, ili kako bez editora uređivati main.cf

Postfix je standardni MTA (Mail Transfer Agent [11]) servis na CARNetovim čvornim računalima. Tu "čast" je zaslužio svojim brojnim kvalitetama i jednostavnom konfiguracijom, te laganim integiranjem 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:

```
# postconf -d
2bounce_notice_recipient = postmaster
access_map_reject_code = 554
address_verify_default_transport = $default_transport
address_verify_local_transport = $local_transport
address_verify_map =
address_verify_negative_cache = yes
address_verify_negative_expire_time = 3d
...
```

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:

```
# postconf -d content_filter
content_filter =
```

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

```
# postconf content_filter
content_filter = smtp-amavis:[127.0.0.1]:10024
```

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 variijablu, uzevši za primjer varijablu smtp_use_tls:

```
# postconf -n | grep smtp_use_tls
smtp_use_tls = yes
```

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

```
# postconf -d | grep smtp_use_tls
smtp_use_tls = no
```

Dakle, varijablu je uistinu mijenjana ili je to učinio netko drugi umjesto nas (ili neki paket). Sada možemo pokušati promijeniti vrijednost varijable pomoću opcije "**-e**" (*edit*):

```
po:/etc/postfix# postconf -e 'smtp_use_tls = no'
po:/etc/postfix# postconf -n smtp_use_tls
smtp_use_tls = no
```

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, objasnit ćemo opciju "**-b**". Ona provjerava sintaksu i ispisuje sve predloške za *bounce* poruke (http://en.wikipedia.org/wiki/Bounce_message [7]):

```
# postconf -b /etc/postfix/bounces.cf
expanded_failure_text = <<EOF
Ovo je e-mail servis na posluzitelju posluzitelj.carnet.hr.

Obavjestavamo vas da vasa e-mail poruka nije isporucena jednom ili vise
primatelja. Poruka se nalazi u privitku.
...
```

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

```
# postconf -b ""
```

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 post**fix** i post**conf**, što se zna u brzini dogoditi!

- Logirajte [1] se za dodavanje komentara

pon, 2009-12-28 15:41 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: Kako omogućiti relay maila drugim mrežama?

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:

```
mynetworks = 127.0.0.0/8, 161.53.xxx.0/24
```

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

```
mynetworks = 127.0.0.0/8, 161.53.xxx.0/24, 193.198.yyy.0/24
```

(za točno definiranje mreža možete se poslužiti naredbom ipcalc [12]).

Nakon toga je potrebno reloadati konfiguraciju na već standardan način:

```
# /etc/init.d.postfix reload
```

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:

```
mynetworks = 127.0.0.0/8, 161.53.xxx.0/24, 193.198.yyy.0/24, !193.198.yyy.xxx, !193.1
98.yyy.zzz
```

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:

```
mynetworks = 127.0.0.0/8, 161.53.xxx.0/24, !/etc/postfix/my_relays
```

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:

```
!193.198.xxx.zzx    REJECT
!193.198.xxx.zzy    REJECT
193.198.xxx.0/24    OK
```

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:

```
mynetworks = 127.0.0.0/8, 161.53.xxx.0/24, hash:/etc/postfix/my_relays
```

Nakon kreiranja ove *hash* datoteke, morate napraviti:

```
# postmap /etc/postfix/my_relays
```

uz obvezatni *reload* na kraju:

```
# /etc/init.d/postfix reload
```

Za dodatne informacije, svakako pročitajte http://www.postfix.org/postconf.5.html [13], sekciju mynetworks.

- Logirajte [1] se za dodavanje komentara

sub, 2009-02-28 21:36 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Software [6]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Postfix: dodatne alias datoteke

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:

```
alias_maps = hash:/etc/aliases, hash:/var/lib/postfix-cn/aliases_gecos
```

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:

```
alias_maps = hash:/etc/aliases, hash:/var/lib/postfix-cn/aliases_gecos,
   hash:/etc/mail/alias_baza
```

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:

```
# postalias /etc/mail/alias_baza
```

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:

```
alias_maps = hash:/etc/aliases, hash:/var/lib/postfix-cn/aliases_gecos,
   hash:/etc/mail/alias_baza
alias_database = hash:/etc/aliases, hash:/var/lib/postfix-cn/aliases_gecos,
   hash:/etc/mail/alias_baza
```

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

```
# newaliases -v
postalias: open hash /etc/aliases
postalias: open hash /var/lib/postfix-cn/aliases_gecos
postalias: open hash /etc/mail/alias_baza
```

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 svježe .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.

- Logirajte [1] se za dodavanje komentara

uto, 2007-03-20 09:59 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: filtriranje poruka na osnovu zaglavlja i/ili

sadržaja

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 opticaja 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 [15]) ili na osnovu pošiljatelja (Kako zabraniti primanje određenih dolaznih poruka? [16]).

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:

```
 dpkg -l|grep pcre
```

pa ako vidite da nije, onda ga instalirate naredbom:

```
apt-get install postfix-pcre
```

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

```
header_checks = pcre:/etc/postfix/header_checks
body_checks = pcre:/etc/postfix/body_checks
```

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

```
touch /etc/postfix/body_checks /etc/postfix/header_checks
```

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

```
#Format zapisa je:
#/^HEADER: .*content_to_act_on/ ACTION
#
 /^To: .*Parris/ HOLD Spam Header Rule #AMG Header Par*ris#
 /^From: .*Canadian-Pharmacy/ HOLD Spam Header Rule #Cana*dian-Phar*macy#
 /^From: .*info\Sappastudio.it/ HOLD Spam Header Rule #appas*tudio.it#
 /.*hooshmand.yazd.*/ HOLD Spam Header Rule #hoosh--mand#
 /^Subject: .*viagra/ HOLD Spam Header Rule #via*-gra#
```

```
#Pozivi na  Facebook, LinkedIn... cesto u naslovu imaju rijec "Accept?" a vrlo cesto
#su laznjaci, da bi se dobila lozinka korisnika, u slijedecem redu je definirano da s
e
# pozivima  za druzenje na drustvenim mrezama naslov zamijeni u upozorenje #OPREZ!#
/^Subject: .*ccept/ REPLACE Subject: #OPREZ!#
#Iduci redci: Naslov je SIGURNO neprihvatljiv, poruku odmah odbij (ne stavljaj na cek
anje).
 /^Subject:(.*)penis|(.*)fuck|(.*)viagra|(.*)pr0n/ REJECT Dont Bother Sending Rubbish
 Emails
 /.*free money.*/ REJECT
```

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:

```
postmap header_checks
```

(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:

```
postfix reload
```

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

```
 /wants to follow you/ HOLD Body Rule #slijediti#
 /www.piramidasunca.ba/ HOLD Body Rule #pira*mide#
 /Dear Webmail Account User/ HOLD Body Rule #Dear W*ebmail..#
```

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

```
postmap body_checks #kreira ili ažurira bazu body_checks.db
postfix reload
```

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):

```
pfqueue
```

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:

```
CECB6859E
857F98B79
564157E84
1606D8AFB
930B68AA2
00AC98A9F
22CA28B7B
5C2C98B7A
A6B9E8541
```

Naredba:

```
postcat CECB6859E
```

prikazat će sadržaj poruke CECB6859E, a naredba:

```
mailq
```

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

```
cd /var/spool/postfix/hold; for a in $(ls);do echo;postcat $a|grep 'Subject:';echo "F
ilter:  #$(zgrep $a /var/log/mail.log*|grep '#'|cut -d'#' -f2)#";read -ep "brisati=b,
 dalje=Enter " b;if [[ $b == "b" ]];then rm $a;fi;done;cd -;
```

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 'I', kad se pozicioniramo u *hold queue* tipkom '4' u programu **pfqueue**. Za one koji hoće još više mogućnosti iz komandne linije prložena je skripta **hold.sh** pri dnu ovog članka - daje mogućnost pregledavanja, brisanja, proslijeđivanja, kopiranja itd.

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

Prilog	Veličina
hold.sh_.txt [17]	2.3 KB

- Logirajte [1] se za dodavanje komentara

čet, 2013-07-04 14:11 - Luka Ćavara**Kuharice:** Linux [5]

Kategorije: Servisi [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Postfix: kako kontrolirati brzinu isporuke maila na određene domene

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:

```
421-4.7.0 Our system has detected an unusual rate of
421-4.7.0 unsolicited mail originating from your IP address. To protect our
421-4.7.0 users from spam, mail sent from your IP address has been temporarily
421-4.7.0 rate limited.  Please visit
421-4.7.0 http://www.google.com/mail/help/bulk_mail.html to review our Bulk
421 4.7.0 Email Senders Guidelines.
```

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:

```
smtp_destination_concurrency_limit = 20
```

Ova postavka određuje koliko se istodobno poruka može isporučiti na istu domenu. Osnovna vrijednost je 20, a mi preporučujemo 1.

```
smtp_destination_rate_delay = 0s
```

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.

```
smtp_extra_recipient_limit = 50
```

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:

```
gmail   unix    -       -       n       -       -       smtp
yahoo   unix    -       -       n       -       -       smtp
sporo   unix    -       -       n       -       -       smtp
```

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:

```
gmail.com       gmail:
yahoo.com       yahoo:
domena.hr      sporo:
```

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

```
# postmap /etc/postfix/transport_mapa
```

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

```
transport_maps = hash:/etc/postfix/transport_mapa
```

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:

```
sporo_destination_concurrency_limit = 1
sporo_destination_rate_delay = 20s
sporo_destination_recipient_limit = 2
```

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.

- Logirajte [1] se za dodavanje komentara

pet, 2014-06-27 00:16 - Zdravko Rašić**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: kako korisnicima postaviti uniformne odlazne adrese?

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:

```
canonical_maps = hash:/etc/postfix/canonical
```

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

```
username1  Ime.Prezime1
username2  Ime.Prezime2
```

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

```
# postmap /etc/postfix/canonical
```

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*.

```
# postfix reload
```

Za dodatne informacije konzultirajte man stranicu sa "man 5 canonical", ili posjetite web stranicu http://www.postfix.org/rewrite.html#canonical [18].

Još jedno rješenje je jednostavno promjeniti 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 [19] koja će pokriti ovakve slučajeve, i imat ćete bazu na osnovu koje možete nekome uskratiti uslugu ukoliko uporno krši odluke donesene sigurnosne politike.

- Logirajte [1] se za dodavanje komentara

sri, 2008-05-21 13:01 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Postfix: kako obrisati mailove iz queuea?

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:

```
 # postsuper -d QUEUE_ID
```

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

```
# postqueue -p
-Queue ID- --Size-- ----Arrival Time---- -Sender/Recipient-------
F134C1838D    28300 Sun May 13 11:36:14  MAILER-DAEMON
          (connect to mail.pradella.biz[212.77.229.254]: Connection timed out)
                                         henry@pradella.biz

3C41518383    28352 Sat May 12 11:19:15  MAILER-DAEMON
           (connect to pistonheads.biz[195.225.218.139]: Connection timed out)
                                         john@pistonheads.biz

36FCE1838E    28328 Sat May 12 20:32:34  MAILER-DAEMON
           (connect to pistonheads.biz[195.225.218.139]: Connection timed out)
                                         john@pistonheads.biz

638221838B    28335 Sat May 12 18:06:48  MAILER-DAEMON
              (connect to 64.202.167.73[64.202.167.73]: Connection timed out)
                                         richard@guitarra.biz

-- 111 Kbytes in 4 Requests.
```

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 [21]):

```
#!/usr/bin/perl

$REGEXP = shift || die "no email-adress given (regexp-style, e.g.\
        bl.*\@yahoo.com)!";

@data = qx</usr/sbin/postqueue -p>;
for (@data) {
  if (/^(\w+)(\*|\!)?\s/) {
     $queue_id = $1;
  }
  if($queue_id) {
    if (/$REGEXP/i) {
      $Q{$queue_id} = 1;
      $queue_id = "";
    }
  }
}
```

```
open(POSTSUPER,"|postsuper -d -") || die "couldn't open postsuper" ;

foreach (keys %Q) {
  print POSTSUPER "$_\n";
};
close(POSTSUPER);
```

- Logirajte [1] se za dodavanje komentara

čet, 2007-05-17 14:46 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: kako podesiti da odlazne domene za pojedine korisnike budu drugog oblika?

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:

```
canonical_maps = hash:/etc/postfix/canonical
mydestin
ation = server.domena.hr, localhost.domena.hr, localhost, $mydomain, druga.domena.hr
```

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:

```
pero@domena.hr    pero@druga.domena.hr
marko@domena.hr   marko@druga.domena.hr
```

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

```
pero    pero@druga.domena.hr
```

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

```
# postmap hash:/etc/postfix/canonical
```

Ostaje još samo restartati postfix:

```
# /etc/init.d/postfix reload
```

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

KEYWORDS: postfix canonical mape domena odlazna adresa

- Logirajte [1] se za dodavanje komentara

čet, 2008-06-12 14:01 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: kako preusmjeriti mailove s određene domene jednom korisniku?

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? [16]". Radi se, opet, o restrikcijama pošiljatelja i već poznatim check_sender_access listama.

Evo što je kolegi zatrebalo:

```
Poštovani,

imam zahtjev da ukoliko mail dolazi sa odre?ene domene, ide isklju?ivo
odre?enom primatelju bez obzira što je poslan na drugoga?

Da li je tako nešto mogu?e te kako to podešavam?
```

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:

```
domena.hr          REDIRECT korisnik@nasadomena.hr
```

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

```
smtpd_sender_restrictions = check_sender_access hash:/etc/postfix/sender_access
```

Još treba napraviti:

```
# postmap /etc/postfix/sender_access
# /etc/init.d/postfix reload
```

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**.

- Logirajte [1] se za dodavanje komentara

sri, 2014-11-26 07:59 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: kako promijeniti maksimalnu dopuštenu veličinu poruka?

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 slijedeće:

```
message_size_limit = 20000000
```

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:

```
# /etc/init.d/postfix reload
```

da bi se nove postavke počele primjenjivati.

- Logirajte [1] se za dodavanje komentara

pet, 2007-04-06 12:18 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: kako zabraniti primanje dolaznih poruka pojedinim korisnicima ili aliasima?

 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:

```
smtpd_recipient_restrictions =
        check_recipient_access hash:/etc/postfix/recipient_access, ...
```

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:

```
smtpd_recipient_restrictions =
    reject_invalid_hostname, reject_unknown_sender_domain, reject_unknown_recipient_d
omain,
    reject_unauth_pipelining, permit_sasl_authenticated, permit_mynetworks,
    check_recipient_access hash:/etc/postfix/recipient_access,
    reject_unauth_destination, check_policy_service inet:127.0.0.1:60000, permit
```

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:

```
svi@    REJECT
nekiuser@  REJECT
```

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

```
# postmap /etc/postfix/recipient_access
```

Kako smo mijenjali konfiguraciju, moramo napraviti i:

```
# /etc/init.d/postfix reload
```

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

UPDATED: 2011-11-30

- Logirajte [1] se za dodavanje komentara

sri, 2007-12-19 15:29 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Postfix: kako zabraniti primanje određenih dolaznih poruka?

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 [22]), 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:

```
@domena.hr                DISCARD domena.hr spam message discarded
root@domena.hr            OK
netko@spam.hr             REJECT Odbijeno zbog spama.
```

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 http://sistemac.carnet.hr/node/569 [23].

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:

```
domena.hr                       554 Spam not welcomed here
```

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:

```
smtpd_sender_restrictions = check_sender_access
     hash:/etc/postfix/sender_access
```

Ostaje još samo konvertirati datoteku u binarni hash:

```
# postmap /etc/postfix/sender_access
```

i restartati, odnosno *reloadati* postfix:

```
# /etc/init.d/postfix reload
```

Više o svim ostalim načinima limitiranja unutar SMTP sesije pročitajte na adresi http://www.postfix.org/SMTPD_ACCESS_README.html [24].

- Logirajte [1] se za dodavanje komentara

uto, 2010-03-30 21:56 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: kako zabraniti slanje maila na određene adrese?

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 http://sistemac.carnet.hr/node/735 [16] 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 dobli 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 rješiti 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:

```
ured@drugadomena.hr    REJECT <neki tekst koji objasnjava situaciju>
```

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:

```
# postmap /etc/postfix/recipient_access
# ls -l /etc/postfix/recipient_access*
-rw-r--r-- 1 root root    58 Nov 29 23:08 /etc/postfix/recipient_access
-rw-r--r-- 1 root root 12288 Nov 29 23:13 /etc/postfix/recipient_access.db
```

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:

```
smtpd_recipient_restrictions = check_recipient_access hash:/etc/postfix/recipient_acc
ess, ...
```

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

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

```
# /etc/init.d/postfix restart
```

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

```
ured@drugadomena.hr    REDIRECT ured@pravadomena.hr
```

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 [25]

- Logirajte [1] se za dodavanje komentara

pet, 2011-12-09 15:45 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Postfix: ne rade poddomene u access listi?

Postfix nudi pristupne (access) liste za svaki dio SMTP konverzacije, ali možda vas je iznanadilo 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

```
parent_domain_matches_subdomains
```

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 [26].

Dakle, ako u main.cf imate

```
parent_domain_matches_subdomains = smtpd_access_maps
```

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.

```
primjer.com             REJECT
```

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:

```
.primjer.com             REJECT
```

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.

- Logirajte [1] se za dodavanje komentara

pet, 2009-04-10 11:59 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: nepostojeći RBL poslužitelji

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:

```
Dec 22 09:01:51 server postfix/smtpd[23876]: warning: 243.193.193.31.dnsbl.njabl.org:

    RBL lookup error: Host or domain name not found. Name service error for
    name=243.193.193.31.dnsbl.njabl.org type=A: Host not found, try again
```

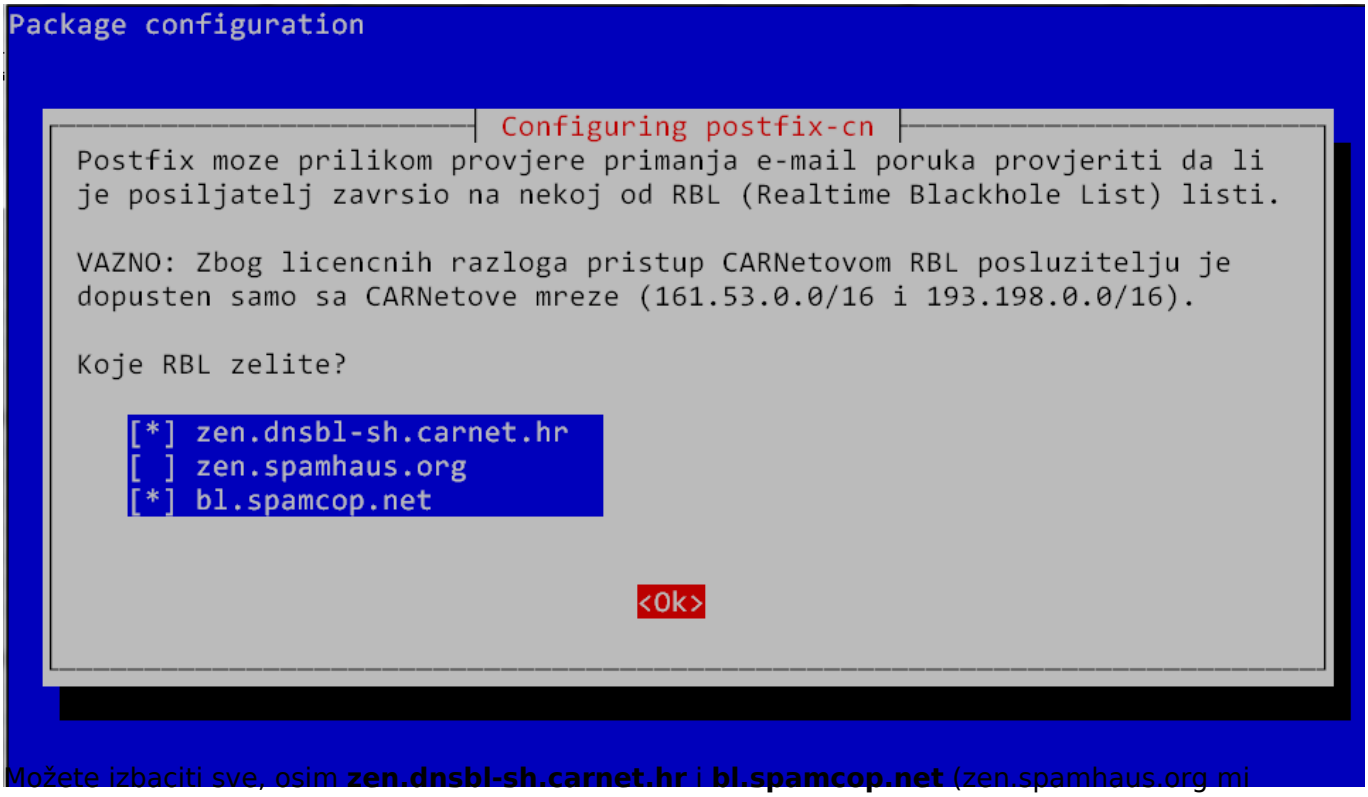
Poslužitelj dnsbl.njabl.org je ugašen još 2013. godine, a u našem paketu postfix-cn je on tada i izbačen (izvadak iz skripte postinst):

```
# Wed, 12 Jun 2013 15:15:28 +0200
# dnsbl.njabl.org je ugasen 2013-03
if echo $rbl | grep -q dnsbl.njabl.org; then
  rbl="`echo $rbl | sed 's/dnsbl.njabl.org, //g'`"
  # za svaki slucaj, ako je na kraju
```

```
  rbl="`echo $rbl | sed 's/dnsbl.njabl.org//g'`"
  db_set postfix-cn/rbl "$rbl" || true
fi
```

Drugim riječima, potrebno je prekonfigurirati paket postfixc-cn:

```
# dpkg-reconfigure postfix-cn
```



Možete izbaciti sve, osim **zen.dnsbl-sh.carnet.hr** i **bl.spamcop.net** (zen.spamhaus.org mi zrcalimo [još od 2008. godine] [27]). 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.

- Logirajte [1] se za dodavanje komentara

pet, 2015-01-09 15:39 - Željko Boroš**Kuharice:** Linux [5]
Vote: 0

No votes yet

Postfix: primanje e-maila za dodatne domene

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):

```
$TTL 3600       ; 1 hour
@       IN      SOA     server.novadomena.hr. hostmaster.novadomena.hr.
(
                              2008123101 ; serial
                                    1800 ; refresh (30 minutes)
                                     600 ; retry (10 minutes)
                                  604800 ; expire (1 week)
                                    3600 ; minimum (1 hour)
                IN      NS              server.domena.hr.
                IN      NS              neki.drugi.server.hr.
localhost       IN      A               127.0.0.1
bindmaster      IN      CNAME           server
;
novadomena.hr.            IN      MX      5       server.domena.hr.
```

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:

```
$TTL 3600       ; 1 hour
XXX.53.161.in-addr.arpa IN SOA server.novadomena.hr. hostmaster.novadomena.hr. (
                                1           ; serial
                                900         ; refresh (15 minutes)
                                600         ; retry (10 minutes)
                                86400       ; expire (1 day)
                                3600        ; minimum (1 hour)
                                )
                        NS      server.domena.hr.
                        NS      neki.drugi.server.hr.
; Iako IP adresa poslužitelja naj?eš?e završava s 3, promijenite po vlastitoj situaci
```

```
ji
3                       PTR     server.novadomena.hr.
```

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

```
virtual_alias_domains = novadomena.hr
virtual_alias_maps = hash:/etc/postfix/virtual
```

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

Sadržaj /etc/postfix/virtual:

```
#
#  Execute the command "postmap /etc/postfix/virtual" after changing
#  the virtual file
#
info@novadomena.hr      pero
marko@novadomena.hr   marko
@novadomena.hr            root
```

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

```
# postmap hash:/etc/postfix/virtual
```

Nakon upisa promjena, kao i uvijek, napravite reload:

```
# /etc/init.d/postfix 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 http://sistemac.carnet.hr/node/395 [28].

KEYWORDS: postfix domena virtual domain

- Logirajte [1] se za dodavanje komentara

uto, 2008-11-04 22:33 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 5

Vaša ocjena: Nema Average: 5 (2 votes)

Postfix: root alias obvezan!

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:

```
root: pperic
```

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.

- Logirajte [1] se za dodavanje komentara

uto, 2007-03-13 15:53 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: značenje parametra notify_classes

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:

```
Mail Delivery System [MAILER-DAEMON@server.hr]
Postfix SMTP server: errors from unknown[200.151.169.54]
Out: 220 server.domena.hr ESMTP Postfix (Debian/GNU)
 In:  EHLO [X.Y.Z.Z]
 Out: 250-server.domena.hr
 Out: 250-PIPELINING
 Out: 250-SIZE 18000000
 Out: 250-VRFY
 Out: 250-ETRN
 Out: 250-STARTTLS
 Out: 250-AUTH PLAIN LOGIN
 Out: 250-AUTH=PLAIN LOGIN
 Out: 250-ENHANCEDSTATUSCODES
 Out: 250-8BITMIME
 Out: 250 DSN
 In:  STARTTLS
 Out: 454 4.7.0 TLS not available due to local problem
 In:  MAIL FROM:<korisnik@domena.hr> SIZE=1625
 Out: 250 2.1.0 Ok
 In:  RCPT TO:<korisnik@domena.hr>
 Out: 554 5.7.1 Service unavailable; Client host [X.Y.Z.Z] blocked using
     zen.dnsbl-sh.carnet.hr; http://www.spamhaus.org/query/bl?ip=X.Y.Z.Z [29]
 In:  QUIT
 Out: 221 2.0.0 Bye
```

Kako ovakvih mailova može biti na desetke, normalna je želja sistemca da zaustavi navalu ovakvih mailova. Zanemarit 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:

```
# postconf notify_classes
notify_classes = resource, software
```

Ono što trebamo učiniti je upisati "notify_classes = resource" u main.cf i restartati Postix:

```
# postconf -e "notify_classes = resource"
```

```
# postconf notify_classes
notify_classes = resource
# /etc/init.d/postfix restart
```

Na ovaj način smo zaustavili poruke, jer smo isključili obavještavanje o greškama u softveru, i ostavili samo obavještavanje 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:

```
# grep ^postmaster /etc/aliases
postmaster:     root
```

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

```
# grep ^root /etc/aliases
root: sistemac1,sistemac2
```

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 [30]

- Logirajte [1] se za dodavanje komentara

čet, 2010-03-04 13:22 - Željko Boroš**Kuharice:** Linux [5]
Kategorije: Servisi [10]

Vote: 4

Vaša ocjena: Nema Average: 4 (1 vote)

Postfix: što znači parametar "relay_domains"?

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

Uobičajena je ovakva situacija:

```
relay_domains = $mydestination
```

iako nije neuobičajeno naći ovaj parametar prazan:

```
relay_domains =
```

Ovo je isto tako uobičajena situacija i prosljeđivanje će se dopuštati svima iz $mynetworks mreža (tzv. *trusted* klijenti), svima drugima relay će biti zabranjen. Ukoliko želite zaprimati i prosljeđivati mail za neke druge domene (primjerice, vaša institucija ima novu domenu, ali želi još neko vrijeme zadržati staru), samo ih upišite uz $mydestination (možda ćete trebati upisati tu IP klasu u $mynetworks).

Potpuni opis možete pronaći na adresi: http://www.postfix.org/postconf.5.html#relay_domains [31]

KEYWORDS: postfix relay relay_domains mydestination

- Logirajte [1] se za dodavanje komentara

pon, 2007-12-17 15:24 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

SASL SMTP autentikacija u Postfixu

 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 korisik 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 [32]. 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 poslane 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":

```
May 31 12:43:48 server postfix/smtpd[3298]: connect from
   pc-racunalo.domena.hr[161.53.XX.YYY]
May 31 12:43:59 server postfix/smtpd[3298]: 38BE9135957: client=
   pc-racunalo.domena.hr[161.53.XX.YYY], sasl_method=PLAIN,
   sasl_username=korisnik@domena.hr
```

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:

```
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
smtpd_sasl_local_domain = $myhostname
```

```
broken_sasl_auth_clients = yes
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated, ...
```

Jedino, možete provjeriti je li pokrenut saslauthd proces:

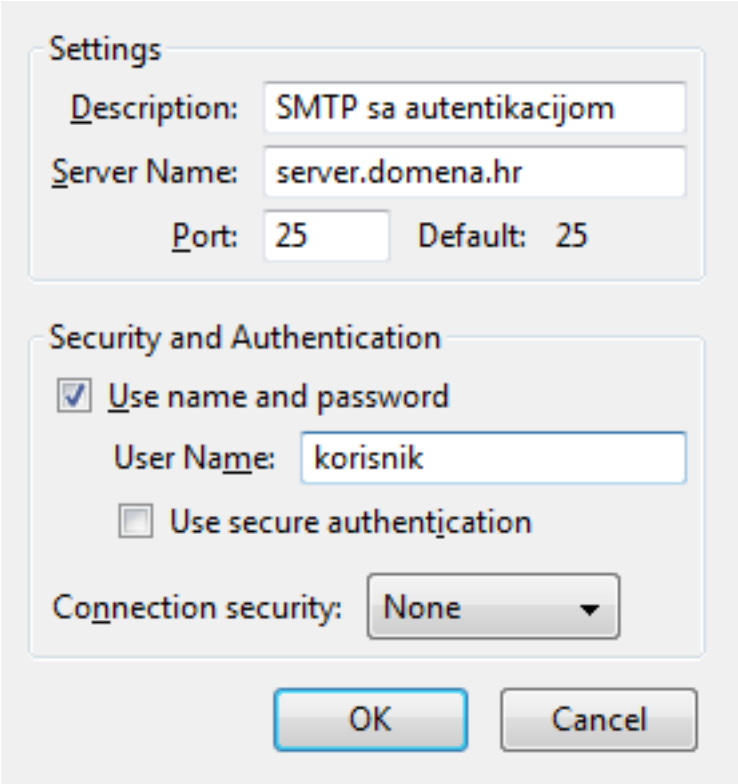
```
# ps -ef |grep saslauthd
root      3030     1  0 Apr08 ?        00:00:00 /usr/sbin/saslauthd
     -a pam -c -m /var/run/saslauthd -n 5
root      3036  3030  0 Apr08 ?        00:00:00 /usr/sbin/saslauthd
     -a pam -c -m /var/run/saslauthd -n 5
...
```

Dakle, sve je u redu, SASL daemoni su pokrenuti. Ukoliko nisu, provjerite zašto po uputama u članku http://sistemac.carnet.hr/node/122 [33].

Navest ćemo podešenja za dva najpopularnija mail klijenta:

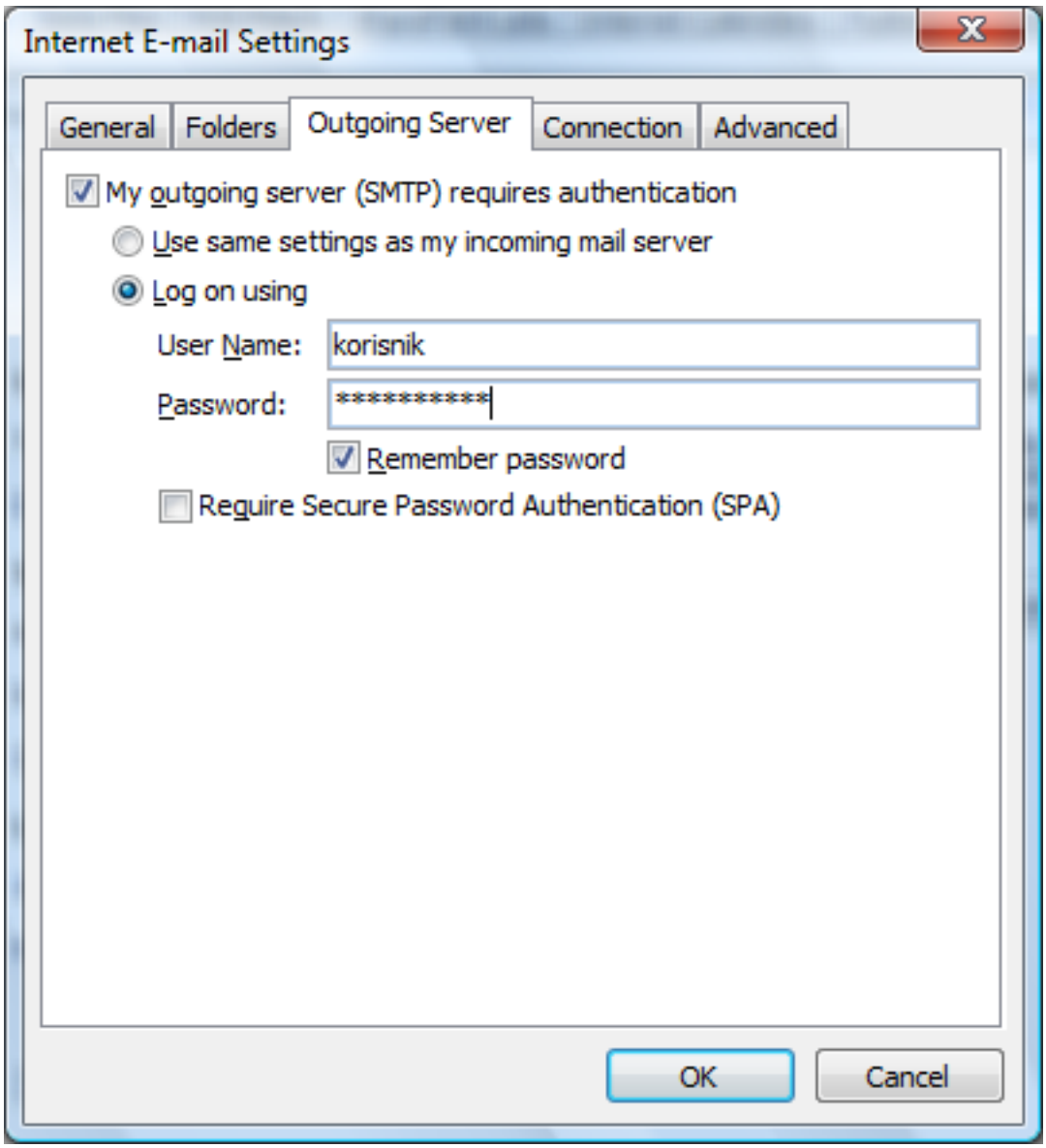
Mozilla Thunderbird:

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



Microsoft Outlook:

Tools -> Account Settings -> <dvoklik na profil>
-> More Settings -> Outgoing Server -> <upišite podatke> -> <isključiti SPA>



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 [34]"

- Logirajte [1] se za dodavanje komentara

pon, 2010-05-31 13:24 - Željko Boroš**Vote:** 5

Vaša ocjena: Nema Average: 5 (2 votes)

story_tag: SASL [35]
postfix [36]
SMTP AUTH [37]

SPA [38]
saslauthd [39]

Postfix: kako instalirati postfix preko sendmaila?

 U za današnje vrijeme zaista nevjerojatnom slučaju da još rabite sendmail, otkucajte slijedeću naredbu da biste prešli na postfix:

```
# apt-get install postfix-cn
```

Ako Vas debconf ništa ne pita, kasnije napravite:

```
# dpkg-reconfigure --priority=low postfix-cn
```

- 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 primati 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:

```
# pgrep sendmail
```

Ukoliko ih još ima, pobijte ih sve:

```
# pkill -9 sendmail
```

Restartajte mail sustav, najbolje s naredbom:

```
# /etc/init.d/amavisd restart
```

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

```
# pgrep postgrey
# pgrep saslauthd
```

Ukoliko se ID procesa ne pokaže, startajte te procese:

```
# /etc/init.d/postgrey start
# /etc/init.d/saslauthd start
```

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

```
Mar 14 11:12:53 linux postfix/qmgr[5248]: 7005178026: from=<root@os.carnet.hr>,
Mar 14 11:12:53 linux amavis[17885]: (17885-01) Passed, <root@os.carnet.hr> ->
Mar 14 11:12:53 linux postfix/smtp[31877]: 75BCB78025: to=<root@linux.os.carnet
Mar 14 11:12:53 linux postfix/qmgr[5248]: 75BCB78025: removed
Mar 14 11:12:54 linux postfix/local[11953]: 7005178026: to=<root@linux.os.carnet.hr
Mar 14 11:12:54 linux postfix/qmgr[5248]: 7005178026: removed
```

- Logirajte [1] se za dodavanje komentara

uto, 2007-12-18 18:25 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: mogući zaostali procesi prilikom nadogradnje sa sendmaila

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:

```
May 28 16:43:24 host sm-mta[9059]: l4SEhO8J009059: Milter (amavis-
milter): to error state
May 28 16:43:24 host sm-
mta[9059]: l4SEhO8J009059: Milter: initialization failed, temp failing commands
May 28 16:43:24 host sm-mta[9060]: l4SEhO3t009060: Milter (amavis-
milter): local socket
```

```
  name /var/lib/amavis/amavisd-new-milter.sock unsafe
```

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:

```
# pgrep milter
3543
# pgrep sendmail
4232
```

Navedene procese ubijte s naredbom "pkill":

```
# pkill -9 milter
# pkill -9 sendmail
```

Svakako provjerite jesu li se procesi uistinu pogasili:

```
# pgrep milter
# pgrep sendmail
#
```

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

```
# /etc/init.d/amavisd-cn restart
```

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

```
May 31 14:05:47 host postfix/smtpd[3972]: connect from localhost.carnet.hr[127.0.0.1]
May 31 14:05:47 host postfix/smtpd[3972]: 7AC5D4183: client=localhost.carnet.hr [127.
0.0.1]
May 31 14:05:47 host postfix/cleanup[3965]: 7AC5D4183: message-id=<Pine.LNX.4.62.0
  205311543520.3652@carnet.hr>
May 31 14:05:47 host postfix/smtpd[3972]: disconnect from localhost.carnet.hr[127.0.0
.1]
May 31 14:05:47 host amavis[3770]: (03770-05) Passed, <posiljatelj@domena.hr> ->
   <primatelj@carnet.hr>, Message-
ID: <Pine.LNX.4.62.070543534530.3932@carnet.hr>, Hits: -0.784
May 31 14:05:47 host postfix/smtp[3967]: 28C5F4681: to=<primatelj@carnet.hr>, relay=1
27.0.0.1[127.0.0.1],
   delay=3, status=sent (250 2.6.0 Ok, id=03770-05, from MTA: 250 Ok: queued as 7CC1D
4183)
May 31 14:05:47 host postfix/qmgr[1974]: 28C5F4681: removed
```

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):

```
# dpkg --purge sendmail-base
```

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 nardbom "mailq", iako istu stvar radi "postqueue -p".

- Logirajte [1] se za dodavanje komentara

čet, 2007-05-31 14:23 - Željko Boroš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: potencijalni problemi sa SASL autentikacijom

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:

```
Mar 14 12:45:22 linux postfix/smtpd[5219]: warning: SASL authentication failure: Pass
word verification failed
Mar 14 12:45:22 linux postfix/smtpd[5219]: warning: smtp.negdje.hr[161.53.XXX.YYY]: S
ASL PLAIN authentication failed
```

Razlog je taj što Thunderbird inicijalno rabi SASL PLAIN mehanizam autorizacije, dok Outloook 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:

```
# START=yes
```

Ukoliko je zakomentiran, odkomentirajte ga:

```
START=yes
```

Startajte saslauthd:

```
# /etc/init.d/saslauthd start
Starting SASL Authentication Daemon: saslauthd.
```

Provjerite radi li SASL mehanizam:

```
# testsaslauthd -u korisnik -p lozinka
0: OK "Success."
```

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

- Logirajte [1] se za dodavanje komentara

pon, 2007-03-19 10:15 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Postfix: "connect to 127.0.0.1:60000: Connection refused" problem

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:

```
Mar  9 11:18:16 server postfix/smtpd[26250]: warning: connect to 127.0.0.1:60000: Con
nection refused
```

rješenje je vrlo jednostavno: treba restartati postgrey daemon.

```
 # /etc/init.d/postgrey restart
```

Ukoliko to ne pomogne, restartajte i sam postfix sa

```
# /etc/init.d/postfix restart
```

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 http://sistemac.carnet.hr/node/107 [40]

- Logirajte [1] se za dodavanje komentara

pet, 2007-03-09 14:13 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Problemi sa aliasima u obliku "Ime.Prezime@institucija.hr" u Postfixu

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:

```
# debconf-show postfix-cn
...
* postfix-cn/matchgecos: true
```

Vrijednost 'matchgecos' mora biti true.

Ukoliko to nije slučaj, napravite slijedeće:

```
# dpkg-reconfigure postfix-cn
```

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.

Aliasi 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 prijavljenje 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:

```
postalias: warning: /var/lib/postfix-cn/aliases_gecos.db: duplicate entry:
"ime.prezime"
```

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

```
ime.prezime: account1
...
ime.prezime: account2
```

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":

```
alias_maps = hash:/etc/aliases, hash:/var/lib/postfix-cn/aliases_gecos
```

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:

```
# awk -F: '$3 < 100 {print $1" "$3}' < /etc/passwd
```

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

```
# usermod -u NEKI_SLOBODNI_UID korisnik
```

Datoteke i direktorije koji se nalaze izvan korisnikovog $HOME direktorija morate ručno promijeniti sa

```
# chown -R korisnik /neki/direktorij
```

ako cijeli direktorij (i poddirektoriji) trebaju pripadati tom korisniku ili

```
# chown korisnik datoteka1 datoteka2 ...
```

ako je potrebno promijeniti samo nekoliko datoteka.

- Logirajte [1] se za dodavanje komentara

uto, 2006-12-19 00:00 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Greylisting za postfix: postgrey

Na portalu za sistemce postoji članak (http://sistemac.carnet.hr/node/101 [41]) 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:

```
POSTGREY_OPTS="--delay=58 --inet=127.0.0.1:60000"
```

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):

```
smtpd_recipient_restrictions = check_policy_service inet:127.0.0.1:60000
```

Da se podsjetimo, greylisting radi na način da za svaku SMTP sesiju (session, sjednicu) zabilježi tri parametra: IP adresu udaljenog računala, envelope adrese pošiljatelja 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> [42]: 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:

```
negdje.nesto.hr
161.53.xxx.yyy
/.*\.carnet\.hr/
```

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:

```
# /etc/init.d/postgrey reload
```

U mail.logu će se moći vidjeti sljedeći redak:

```
Mar  8 21:42:02 po postgrey[16648]: HUP received: reloading whitelists...
```

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 [43] i naravno, u manualu (man postgrey).

- Logirajte [1] se za dodavanje komentara

pet, 2007-03-09 10:41 - Željko Boroš**Kuharice:** Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Zašto u CARNet-Etchu više nema paketa postgrey-cn?

 U proteklom razodoblju smo vas upoznali s načinom rada greylistinga [40], 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:

```
smtpd_recipient_restrictions = permit_mynetworks,
                               permit_sasl_authenticated,
                               reject_unauth_destination,
...
                               check_policy_service inet:127.0.0.1:60000,
permit
```

Ovime smo izgubili jedan alat za borbu protiv spama, ali zbog sve slabije efikasnosti i uvođenja poboljšanja [27] u postojeće servise, sveukupna antispam zaštita mail poslužitelja neće doći u pitanje.

KEYWORDS: postgrey postgrey-cn

- Logirajte [1] se za dodavanje komentara

pon, 2008-06-16 12:59 - Željko Borš**Vijesti:** Linux [20]
Kuharice: Za sistemce [14]
Kategorije: Servisi [10]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr./node/126

Links
[1] https://sysportal.carnet.hr./sysportallogin
[2] https://sysportal.carnet.hr./node/752
[3] https://sysportal.carnet.hr./node/747
[4] https://sysportal.carnet.hr./node/388
[5] https://sysportal.carnet.hr./taxonomy/term/17
[6] https://sysportal.carnet.hr./taxonomy/term/25
[7] http://en.wikipedia.org/wiki/Bounce_message
[8] https://sysportal.carnet.hr./node/687
[9] https://sysportal.carnet.hr./node/693
[10] https://sysportal.carnet.hr./taxonomy/term/28
[11] http://en.wikipedia.org/wiki/Mail_transfer_agent
[12] https://sysportal.carnet.hr./node/330
[13] http://www.postfix.org/postconf.5.html
[14] https://sysportal.carnet.hr./taxonomy/term/22
[15] https://sysportal.carnet.hr./node/943
[16] https://sysportal.carnet.hr./node/735
[17] https://sysportal.carnet.hr./system/files/hold.sh_.txt
[18] http://www.postfix.org/rewrite.html#canonical
[19] https://sysportal.carnet.hr./system/files/sigurnosna_politika_ustanove.pdf
[20] https://sysportal.carnet.hr./taxonomy/term/11
[21] https://sysportal.carnet.hr./system/files/delete-from-mailq.pl_.txt
[22] https://sysportal.carnet.hr./node/734#primjer
[23] https://sysportal.carnet.hr./node/569
[24] http://www.postfix.org/SMTPD_ACCESS_README.html
[25] http://www.postfix.org/access.5.html
[26] http://www.postfix.org/postconf.5.html#parent_domain_matches_subdomains
[27] https://sysportal.carnet.hr./node/376
[28] https://sysportal.carnet.hr./node/395
[29] http://www.spamhaus.org/query/bl?ip=200.151.169.54
[30] http://www.postfix.org/postconf.5.html#notify_classes
[31] http://www.postfix.org/postconf.5.html#relay_domains
[32] http://webmail.carnet.hr
[33] https://sysportal.carnet.hr./node/122
[34] https://sysportal.carnet.hr./node/764
[35] https://sysportal.carnet.hr./taxonomy/term/143

[36] https://sysportal.carnet.hr./taxonomy/term/122
[37] https://sysportal.carnet.hr./taxonomy/term/144
[38] https://sysportal.carnet.hr./taxonomy/term/145
[39] https://sysportal.carnet.hr./taxonomy/term/146
[40] https://sysportal.carnet.hr./node/107
[41] http://sistemac.carnet.hr/node/101
[42] mailto:netko@negdje.hr
[43] http://projects.puremagic.com/greylisting