Amavis savjeti i trikovi

Ova online knjiga je skup pojedinačnih članaka objavljenih kao pomoć sistemcima u konfiguraciji i korištenju Amavisa.

- Logirajte [1] se za dodavanje komentara

Amavis: kako zabraniti određene vrste priloga

Amavis podržava zabranu primanja maila s prilogom (*attachmentom*), i to po određenim kriterijima. Kriteriji mogu biti ekstenzija datoteke, tip datoteke koju vraća naredba *file(1)* ili MIME tip, kojeg svaki mail klijent danas šalje zajedno s prilogom. Na ovaj način možemo osujetiti pokušaje virusa i crva da se sakrivaju preko dvostrukih ili lažnih ekstenzija.

Iako email virusi danas nisu ni približno rašireni kao nekad, potreba zabrane slanja određenih tipova priloga i dalje ostaje.

Podešavanje se radi u Amavisovoj konfiguracijskoj datoteci /etc/amavis/conf.d/20-debian_defaults, odnosno /etc/amavis/conf.d/50-user (gdje možemo navesti vrijednosti koje će vrijediti umjesto *defaultnih*), u varijabli $banned_filename_re. Najčešće, i najlakše ćemo zabraniti prilog prema ekstenziji datoteke:

```
$banned_filename_re = new_RE(qr'.\.(mp3|mp4|wma|wmv|avi)$'i,);
```

Ovime postupkom smo zabranili neke (najčešće) nepoželjne datoteke. Naravno da ovdje možete upisati bilo koju ekstenziju koju želite zabraniti, u dogovoru sa odgovornim osobama i u skladu sa sigurnosnom politikom ustanove.

Ovo nije sve, jer amavis može zabraniti pojedine priloge po tipu, bez obzira na navedenu ekstenziju datoteke. Amavis ovo utvrđuje preko standardne Unix naredbe file(1) [2], koja se ne da zavarati ekstenzijom, nego tip datoteke traži u njenom zaglavlju.

Otkomentirajte sljedeće u amavisd.conf:

```
qr'^\.exe$'i
```

To će zabraniti bilo kakav prilog koji ima izvršnu datoteku, primjerice .com, .exe ili slično.

Nadalje, Amavis može zabraniti prilog prema njegovom MIME tipu, koji se nalazi u zaglavlju svakog maila s prilogom:

```
qr'^application/x-msdownload$'i, # banned MIME type
```

Ovime smo spriječili prolaz svim attachmentima tipa 'application/x-msdownload'. Ovaj tip

attachmenta često rabe virusi, kao što
je nekada činio virus Bagle-U.

Pogledajte i članak http://sistemac.carnet.hr/node/188 [3], koji rješava problem sa slanjem "message/partial" priloga.

Nakon prve instalacije Amavisa, jedina podrazumijevana postavka je to da je zabranjeno slanje priloga s dvostrukom ekstenzijom (.txt.pif, doc.exe, ...), što je bio pokušaj nekih virusa da zavaraju korisnika koji bi onda pokrenuo datoteku misleći da se radi o nečem drugom:

```
qr'\.[^.]*\.(exe|vbs|pif|scr|bat|cmd|com|dll)$'i
```

U amavisovoj konfiguraciji su navedeni dodatni primjeri, pa možete konfigurirati svoj sustav po želji. Sve ovisi o vašoj sigurnosnoj politici i potrebama na vašoj ustanovi.

- Logirajte [1] se za dodavanje komentara

pet, 2008-10-31 12:53 - Željko Borš**Vote:** 0

No votes yet

Amavis: ne prolaze "message/partial" attachmenti

Amavis, osim što omogućava pregled elektroničke pošte s antivirusnim i antispam programima, može blokirati poštu po tipu attachmenta. Primjerice, moguće je po datotečnim nastavcima blokirati attachmente sa zvučnim ili video zapisima, ali i po MIME tipu.

Podešavanje se radi u standardnoj amavisovoj konfiguracijskoj datoteci, /etc/amavis/amavisd.conf. Varijabla "odgovorna" za podešavanje je $banned_filename_re, i u paketu amavisd-cn ona izgleda ovako (skraćeno zbog preglednosti):

```
$banned_filename_re = new_RE(
#  qr'^UNDECIPHERABLE$',  # is or contains any undecipherable components
   qr'\.[^.]*\.(exe|vbs|pif|scr|bat|cmd|com|dll)$'i, # some double extensions
   qr'[{}]',     # curly braces in names (serve as Class ID extensions - CLSID)
#  qr'^application/x-msdownload$'i,                  # banned MIME types
#  qr'^application/x-msdos-program$'i,
   qr'^message/partial$'i,  # rfc2046. this one is deadly for Outcrook
#  qr'^message/external-body$'i, # block rfc2046
);
```

Kao što se može vidjeti, blokirano je nekoliko tipova izvršnih datoteka, kao i MIME tip "message/partial". Message/partial tip attachmenta generiraju neki mail klijenti, najčešće će to biti Outlook Express uz uporabu opcije "Break apart messages larger than...". Tada se poruka šalje u nekoliko dijelova, po defaultu su to dijelovi veličine 60 kB (što je prilično malo i trebalo bi povećati na barem 1 MB).

Problem nastaje kad pokušavamo poslati takve poruke, jer će ih Amavis redom odbijati uz poruku:

```
<korisnik@domena.hr>: host 127.0.0.1[127.0.0.1] said:
 550 5.7.1 Message content rejected, id=02339-02 - BANNED: message/partial
 (in reply to end of DATA command)
```

Postoje dva rješenja ovog problema, jedan je u "Tools > Accounts > Mail > Properties > Advanced" isključiti opciju "Break apart messages larger than...". Ovo će pomoći, ali samo do veličine poruke koju ste odredili u Postfixu (pogledajte članak http://sistemac.carnet.hr/node/157 [4]), kada će poruke opet biti odbijene, ovaj put od strane Postfixa. No, slanje prevelikih datoteka preko maila ionako nije preporučljivo.

Drugo rješenje je jednostavno zakomentirati redak u amavisd.conf:

```
# qr'^message/partial$'i,
```

i naravno, napraviti

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

Na ovaj način ste trajno onemogućili zaustavljanje "message/partial" attachmenata, što vam iz sigurnosnih razloga ipak ne možemo preporučiti. Naime, ovaj način "distribucije" znaju rabiti virusi i crvi: http://www.securiteam.com/securitynews/5YP0A0K8CM.html [5]

- Logirajte [1] se za dodavanje komentara

uto, 2007-05-08 12:15 - Željko Boroš**Vote:** 0

No votes yet

Amavis: nedoumice oko startup skripte

 U službi za pomoć sistem-inženjerima ponekad znamo dobiti upit "koja je prava incijalizacijska datoteka za Amavis"? Uistinu, situacija može biti šarolika, pogotovo ako usporedimo stanje sa nekim drugim poslužiteljima. Ovdje ćemo pokušati malo objasniti "zavrzlamu".

Ako pogledamo što se nalazi u /etc/init.d direktoriju, a tiče se Amavisa, dobit ćemo ovakvu situaciju:

```
# ls -l /etc/init.d/amav*
lrwxrwxrwx 1 root root   10 Mar 28 15:05 /etc/init.d/amavis -> amavisd-cn
-rwxr-xr-x 1 root root 3501 Feb 24  2007 /etc/init.d/amavis.amavisd-new
-rwxr-xr-x 1 root root 3240 Apr  1 15:44 /etc/init.d/amavisd-cn
```

Na drugom poslužitelju situacija može biti ovakva:

```
# ls -l /etc/init.d/amav*
 lrwxrwxrwx 1 root root   10 Apr 21 12:48 amavis -> amavisd-cn
 -rwxr-xr-x 1 root root 2342 Dec  1  2004 amavis.amavisd-new
 -rwxr-xr-x 1 root root 3501 Feb 24  2007 amavis.amavisd-new.dpkg-new
 -rwxr-xr-x 1 root root 3236 Apr 21 12:48 amavisd-cn
```

Iako sve izgleda manje-više isto, veličine datoteka nisu jednake. Postoji i jedna datoteka više. Objasnit ćemo razlike.

U prvoj slučaju, korisnik je potvrdno odgovorio na pitanje želi li zamijeniti konfiguracijske datoteke s onima iz paketa (ili ih nikad nije ni dirao pa je to učinjeno automatski). U drugom slučaju, korisnik je odgovorio niječno, pa mu je ostala stara inačica datoteke, i pojavila se nova (amavis.amavisd-new.dpkg-new). Uočite da je ona jednaka datoteci amavis.amavisd-new na prvom poslužitelju (3501 bajtova), što potvrđuje činjenicu da su na dva poslužitelja odgovori bili drugačiji (datoteke *.dpkg-new obično zaostanu nakon nekog problema i inače ne bi trebale zaostati na sustavu, ali je nama izvrsno poslužilo za ilustraciju).

Kako startup skripte obično ne traže modifikaciju (osim u posebnim slučajevima), bilo bi poželjno da imate one najnovije, iz paketa. U ovakvoj situaciji može nam pomoći sljedeća naredba:

```
# apt-get install --reinstall --yes -o DPkg::Options::=--force-confnew amavisd-new
```

Ovako složena naredba će bez pitanja zamijeniti sve datoteke s onima iz paketa, bez obzira jeste li što mijenjali ili ne. Iako to u ovom slučaju nije problem, ako želite rabiti ovu sintaksu i na drugim paketima, budite upozoreni da će se sve konfiguracijske datoteke zamijeniti novima i tako anulirati vaše izmjene. U ovom slučaju to nije problem, jer imamo amavisd-cn paket, koji će podesiti osnovne postavke, baš kao da ste tek instalirali poslužitelj:

```
# apt-get install --reinstall --yes amavisd-cn
```

U ovom slučaju ne treba forsirati zamjenu konfiguracijskih datoteka, jer u tom paketu /etc/init.d/amavis nije *Conffile*. Dodatno, paket amavisd-cn preusmjerava (pomoću alata dpkg-divert) /etc/init.d/amavis iz paketa amavisd-new na sebe, tako da pokazuje na /etc/init./amavisd-cn. Ova nas činjenica vodi na drugi dio nejasnoća oko inicijalizacije Amavisa.

Naime, nije svejedno pod kojim imenom pozivate startup skriptu (iako je /etc/init.d/amavis samo symlink na /etc/init.d/amavisd-cn).

Iz razloga kompatibilnosti sa starijim inačicama paketa, zadržano je staro ponašanje ako skriptu pokrenete kao "/etc/init.d/amavisd-cn restart". To konkretno znači da će se izvršiti restart svih servisa vezanih uz Amavis: amavisa, postfixa i clamava. Ako skriptu pokrenete kao "/etc/init.d/amavis restart" onda ćete restartati samo amavis, odnosno bit će pozvana originalna inicijalizacijska datoteka /etc/init.d/amavis.amavisd-new.

Izuzetak postoji, a to je da se uvijek forsira start (ne i restart ili stop) svih servisa, bez obzira pod

kojim imenom ste skriptu pokrenuli. Drugim (matematičko-programerskim) riječima rečeno:

amavisd-cn start	==	amavis start
amavisd-cn restart	!=	amavis restart
amavisd-cn stop	!=	amavis stop

Ako ste u nedoumici, jednostavno rabite oblik:

```
# /etc/init.d/amavisd-cn start ili restart ili stop
```

Nadamo se da smo uspjeli malo pojasniti ove različitosti.

- Logirajte [1] se za dodavanje komentara

pet, 2008-09-26 11:15 - Željko Borš**Kuharice:** Linux [6]
Kategorije: Operacijski sustavi [7]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Amavis: Što u logovima znači "Hits: -"?

Vjerujemo da sve kolege sistem-inženjeri znaju što znači podatak "Hits" u mail logovima, koji se nalazi u retcima koje upisuje amavis (za one koji ipak nisu sigurni, to je spam ocjena - *score* - koji je tom mailu dodijelio SpamAssassin). No, na tom mjestu se može naći vrijednost koju ne očekujemo (jer smo stavili nekoga u black listu i slično), ili jednostavno oznaka "-". Što to znači? Je li to ocjena "0.0"?

Ukratko, odgovor je "ne". Kad na mjestu ocjene stoji samo crtica (ili minus, kako vam je lakše), to znači da se provjera maila SpamAssassinom **nije uopće obavila**. Postoji nekoliko razloga zašto.

Prvi razlog je taj što je SpamAssassin provjera dosta kompleksna i samim tim traje neko vrijeme, što može značiti znatno opterećenje sustava u slučaju većeg mail prometa. Iz tog razloga, autor Amavisa je ugradio zaštitnu mjeru, pa se ne pregledavaju mailovi veći od 200 kilobajta (spamovi su obično puno kraći od tog). Dakle, svi mailovi veći od 200 kiB neće biti pregledani, **pa čak i ako ste neku**

adresu stavili u black listu.

Varijabla koja kontrolira ovu vrijednost se nalazi u datoteci **/etc/amavis/conf.d/20-debian_defaults**:

```
$sa_mail_body_size_limit = 200*1024;
```

Drugi razlog može biti da ste određene primatelje stavili u popis onih koji bezuvjetno primaju poštu. Ove primatelje možete definirati preko nekih od mapa iz skupine **@bypass_spam_checks_maps**, uz istovremeno podešavanje varijabli iz skupine **@spam_lovers_maps**. Više o podešavanju možete naći u dokumentaciji, ili na adresi http://www200.pair.com/mecham/spam/bypassing.html [8].

Treći razlog je jednostavno nekakva greška, ili *timeout* spamassassina. Ove ćete probleme lako uočiti, jer će svi mailovi biti neocjenjeni, ili se uopće neće isporučiti. Uglavnom, brzo ćete vidjeti da nešto "ne štima".

Zašto je uopće nekome bitno da su svi mailovi ocjenjeni? Prikazat ćemo to na primjeru iz prakse, kada se kolega požalio da mu korisnici ipak ponekad dobiju mail s adrese koju je davno blokirao:

```
Mar 27 21:36:32 server1 amavis[29875]: (29875-01) Blocked
SPAM, [IP1] [IP2] <korisnik@domena.hr> -> <user@local.hr>,
quarantine: 9/spam-9fHcA9EbdKvM.gz, Message-ID:
<01a701cacded$28826d60$79874820$@korisnik@domena.hr>,
mail_id: 9fHcA9EbdKvM, Hits: 98.229, size: 27742, 5644 ms

Mar 27 21:43:34 server1 amavis[30727]: (30727-01) Passed
CLEAN, [IP1] [IP2] <korisnik@domena.hr> -> <user@local.hr>,
Message-ID:
<01c401cacdee$196a2e20$4c3e8a60$@korisnik@domena.hr>,
mail_id: I6pZUFWkgKWs, Hits: -, size: 923456, queued_as:
3A5ED160376, 3067 ms
```

Sistem-inženjer je dodao mail adresu "korisnik@domena.hr" u black listu, u nadi da će spriječiti tu adresu da šalje spam mailove svojim korisnicima:

```
# cat /etc/spamassassin/local.cf
blacklist_from korisnik@domena.hr
```

No, iako je u prvom pokušaju mail blokiran, u drugom je propušten bez provjere. Sada kada znamo sve gore navedene činjenice lako je uočiti da je drugi mail daleko veći, svakako veći od navedenih 200 kiB, te je iz tog razloga jednostavno propušten. Lako je izračunati da bi pregledavanje 900 kiB drugog maila trajalo jako dugo, ako je prvi mail od 27 kiB pregledavan preko 5 sekundi.

Što učiniti da ipak blokiramo određene adrese? Najbolje bi bilo uopće ne blokirati pojedine adrese, nego ovakve slučajeve prijavljivati nadređenom ISP-u na adresu koju rabi abuse služba (npr. abuse@carnet.hr ukoliko je korisnik poslao mail iz CARNet mreže).

Ukoliko ipak želite blokirati adrese preko black lista, možete ih napraviti direktno u amavisu, ali i "ispred", u Postfixu. Ovo možete postići preko parametra smtpd_sender_restrictions.

Dakle, imamo čak tri mjesta gdje možemo postići blokiranje određenih adresa (ili domena), a svako mjesto ima određene prednosti i mane. Možda je najbolje ne rabiti sva tri sustava istovremeno, jer

ćete se teže snaći i pronaći problem ukoliko se pojavi. No, to ostavljamo vama da odlučite.

- Logirajte [1] se za dodavanje komentara

sri, 2010-03-31 11:57 - Željko Borš**Kuharice:** Linux [6]
Kategorije: Servisi [9]
Vote: 0

No votes yet

Amavisd-release: oslobodite svoj mail!

 Koliko je život sistem-inženjera ugodniji nakon pojave Amavisa (odnosno njegove poboljšane inačice, amavisd-new), ne treba puno govoriti. Blokirane stotine tisuće spamova, virusa i crva na svakom poslužitelju dovoljno govori o kvaliteti ovog softvera (naravno, uz pomoć SpamAssassina i nekog antivirusnog programa). No, kako određivanje što je spam, a što nije prilično teška zadaća, moguće su pogreške. U slučaju spama, greške možemo podijeliti u dvije skupine: lažni pozitivi i lažni negativi.

Lažni pozitiv je sasvim regularan mail koji je pogrešno označen kao spam. U obrnutom slučaju, spam nije prepoznat i propušten je korisniku. Iz navedenog se može zaključiti da lažni negativ i nije toliki problem, kao lažni pozitiv. Za lažni pozitiv uglavnom saznate kad se netko od korisnika pobuni da mu neki očekivani mail nije stigao, ili da je dobio odbijenicu od sustava s porukom da je njegov mail kategoriziran spam.

Navest ćemo primjer: korisnik pero@domena.hr vam je prijavio da nije primio važan mail. Prvo što trebate napraviti je otići u karantenu i potražiti taj mail:

```
# find /var/lib/amavis/virusmails -name 'spam-*' | xargs zgrep pero@domena.hr
...
spam-lf+iS5Av9Hu0.gz:    for <pero@domena.hr>; Mon, 21 Feb 2009 14:59:14 +0200 (CEST)
banned-kdjiZh7dsHdf:To: pero@domena.hr
```

Ovo je najbrži i najjednostavniji način da saznate je li poruka određenenom primatelju zaustavljena i stavljena u karantenu. Poruka ne mora biti zaustavljena kao spam, nego može biti zaustavljena i kao poruka sa nedopuštenim prilozima (*banned*) ili virus, pa se nemojte ograničavati samo na spam-* datoteke. Također, adresa primatelja se ne mora nalaziti u To: polju (čest slučaj s mailing listama), te

svakako pribavite i adresu pošiljatelja i Subject pa probajte pretražiti karantenu i po tim odrednicama. Ovo će smanjiti mogućnost da vam navedena poruka promakne zbog vaše greške, ukoliko se zaista nalazi u karanteni. Naredbu zgrep rabimo jer su po defaultu spam poruke komprimirane.

Ukoliko dobijete puno rezultata, probajte profilitrirati pronađene rezultate:

```
# find /var/lib/amavis/virusmails -name 'spam-*' | xargs zgrep e@mail | awk -F: '{pri
nt $1}' | uniq
```

Ova kombinacija naredbi će smanjiti ispis, i prikazati vam samo popis datoteka gdje se nalazi traženi pojam. Na vama je da pronađete pravu datoteku.

Kad pronađete navedenu datoteku s problematičnim mailom, dalje je jako jednostavno:

```
# amavisd-release spam-lf+iS5Av9Hu0.gz
```

Amavisd-release je naredba napisana upravo zbog potrebe da se povremeno iz karantene vade pojedini mailovi. Nalazi se u amavisd-new u distribuciji Etch i novijima (zapravo, autor ju je uveo u inačici 2.3.0). Kod uporabe, ne treba čak ni dekomprimirati mail u karanteni (može se ostaviti nastavak *.gz).

No, po *defaultu* ova naredba na standardnim Debianovim Etch poslužiteljima neće raditi, jer potrebno je izvršiti male preinake u konfiguraciji. Radi se o dva retka, pa to neće biti veliki problem. U /etc/amavis/conf.d/50-user (ovdje upisujete sve vaše promjene u konfiguraciji Amavisa!) upišite:

```
$interface_policy{'SOCK'} = 'AM.PDP-SOCK';
$policy_bank{'AM.PDP-SOCK'} = {
 protocol => 'AM.PDP',  # select Amavis policy delegation protocol
 auth_required_release => 0,  # don't require secret_id for amavisd-release
};
```

Ovakava dodatna konfiguracija će uključiti AM.PDP protokol na Unix socketu, koji ionako već postoji za komunikaciju s Amavis daemonom. AM.PDP će omogućiti naprednije stvari, baš poput ove. Socket je uobičajeno definiran kao:

```
$unix_socketname = "/var/run/amavis/amavisd.sock";
```

Direktiva $policy_bank{'AM.PDP-SOCK'} određuje koje će se sigurnosne i druge postavke primjenjivati na pojedinim Amavisovim modulima. Ovdje je, osim samog protokola, postavljeno "auth_required_release => 0". To znači da se neće tražiti dodatne zaporke za "oslobađanje" mailova, pa zato treba biti oprezan. U suprotnom, svatko na lokalnom sustavu će imati mogućnost puštanja bilo kojeg spama u karanteni! Dopuštenja na socketu koja će onemogućiti ovakvo ponašanje trebaju biti:

```
# ls -l /var/run/amavis/amavisd.sock
srwxr-x--- 1 clamav amavis 0 Feb 21 07:38 /var/run/amavis/amavisd.sock
```

Naravno, moguće je podesiti da se rabe i zaporke, odnosno secret_id, no to zahtijeva zapisivanje zaglavlja svake poruke koja stigne na sustav u SQL bazu, pa se u ovom članku nećemo time baviti.

Radi potpunosti, reći ćemo da se puštanje mailova može raditi i preko INET socketa, dakle s nekog drugog hosta. Kako ovo nije uobičajena situacija na poslužiteljima u CARNetovoj mreži, samo ćemo navesti kako to postići ukoliko imate potrebe za tom funkcionalnošću:

```
# apply policy bank AM.PDP-INET to some inet tcp socket, e.g. tcp port 9998:
$interface_policy{'9998'} = 'AM.PDP-INET';
$policy_bank{'AM.PDP-INET'} = {
 protocol => 'AM.PDP',  # select Amavis policy delegation protocol
 inet_acl => [qw( 127.0.0.1 [::1] 161.53.XXX.YYY 193.198.XXX.ZZZ )],  # restrict acce
ss to these IP addresses
# auth_required_release => 0,  # don't require secret_id for amavisd-release
};
```

Nakon podešavanja $interface_policy i $policy_bank{'AM.PDP-SOCK'}, poruka nakon puštanja maila iz karantene će biti:

```
# amavisd-release spam-lf+iS5Av9Hu0.gz
250 2.6.0 Ok, id=rel-
lf+iS5Av9Hu0, from MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as 6FC213E9A
```

a u logovima će pisati nešto slično ovome:

```
Feb 21 16:47:13 server amavis[8502]: (rel-spam-
lf+iS5Av9Hu0) Quarantined message release:
 spam-lf+iS5Av9Hu0 <korisnik@gmail.com> -> <pero@domena.hr>
```

Novi paket amavisd-cn će donijeti ove promjene automatski, a do tada možete ručno konfigurirati Amavis rabeći ove upute.

UPDATED: 2012-03-01

- Logirajte [1] se za dodavanje komentara

pon, 2009-02-23 07:15 - Željko Borš**Kuharice:** Linux [6]
Kategorije: Software [10]
Servisi [9]
Vote: 4.666665

Vaša ocjena: Nema Average: 4.7 (3 votes)

Označavanje SPAM pošte umjesto brisanja

Nekim korisnicima, a i sistemcima ne sviđa se činjenica da se SPAM poruke automatski brišu, odnosno spremaju u karantenu. Razlog je jasan - programi za detekciju SPAM-a ponekad pogriješe i neku od 'pravih' poruka proglase za SPAM. Iz osobnog iskustva znam da se to dešava vrlo rijetko ali se ipak događa. Zbog toga od početka imam konfiguriran sustav tako da se sve poruke primaju, uz promjenu naslova (Subject) SPAM poruke dodavanjem teksta *** SPAM *** na početak.

Do nedavno sam to podešavao u konfiguracijskoj datoteci Spamassassina, kojeg sam pokretao pomoću Procmaila. Ovo je ponekad izazivalo probleme, jer bi prilikom primanja veće količine pošte u kratkom vremenu došlo do usporenja rada servera. Za svaku poruku pokretao se poseban Spamassassinov proces i opterećenje bi naglo poraslo.

Na sreću, ista stvar se može podesiti i unutar Amavisa. Nakon promjena koje će biti opisane u nastavku server uredno radi bez prevelikog opterećenja koje se ranije povremeno dešavalo.

U konfiguracijskoj datoteci Amavisa, /etc/amavis/amavisd.conf treba napraviti sljedeće promjene:

1. ukoliko već nije, zakomentirati

```
#@bypass_spam_checks_acl = qw( . );
```

(ovo je u redovnoj konfiguraciji paketa amavisd-cn zakomentirano)

2. promijeniti

```
$final_spam_destiny = D_REJECT;
```

u

```
$final_spam_destiny = D_PASS;
```

(s ovom promjenom, Amavis će propuštati SPAM poruke, umjesto da ih stavlja u karantenu)

3. isključiti karantenu sa promjenom

```
$spam_quarantine_to = 'spam-quarantine';
```

u

```
$spam_quarantine_to = undef;
```

4. definirati promjenu subjecta

```
$sa_spam_subject_tag = '*** SPAM *** ';
```

i

```
$sa_spam_modifies_subj = 1;
```

(ovo otkomentirati iz standardne konfiguracije)

5. postaviti vrijednost iznad koje se spam poruke označavaju

```
$sa_tag2_level_deflt = 5.0;
```

(ovu vrijednost se može postaviti po želji)

6. ukoliko već nije postavljeno, postaviti

```
$final_banned_destiny = D_REJECT;
```

Nakon upisa ovih promjena treba spremiti konfiguraciju i reloadati amavis:

```
/etc/init.d/amavisd-cn reload
```

U slučaju da se ranije koristio Spamassassin preko Procmaila treba iz konfiguracijske datoteke /etc/procmailrc obrisati linije:

```
:0fw
| spamassassin
```

Nakon ovih promjena svi korisnici će dobivati spam poštu sa oznakom u naslovu poruke. Ovako to izgleda:

```
TraveLetter Pet, 3:41 am *** SPAM *** Cabo, Hawaii, Europe, Disney,
Rogert Sub, 3:50 pm + *** SPAM *** Any med for your girl to be happy!
MaupinTour Uto, 3:15 am *** SPAM *** Italy Tours - Save $150 Per Person
```

```
MaupinTour Ned, 10:59 pm *** SPAM *** Cruise Through the New Year With
MaupinTour Sub, 8:49 am *** SPAM *** The Best Way to See South America
```

Kako korisnici nikad nisu potpuno zadovoljni, nekima ovako nešto neće odgovarati. Jedan od načina brisanja poruka koje su ovako označene je uporabom Procmaila. Korisnik kojemu se ovako nešto ne sviđa trebao bi u svome home direktoriju stvoriti datoteku .procmailrc sa sljedećim sadržajem:

```
:0:
* ^X-Spam-Status: Yes
/home/korisnik/spam
```

Naravno, umjesto korisnik treba upisati svoje korisničko ime. Ovo može i sistemac napraviti kod korisnika koji to sami ne znaju ili ne žele.

Nakon upisa ove promjene, SPAM poruke za dotičnog korisnika spremat će se u datoteku spam u njegovom home direktoriju. Pa će tu datoteku korisnik u slučaju potrebe biti u mogućnosti pregledati.

Ovo može stvoriti jednu potencijalnu opasnost - zatrpavanje diska. Rješenje koje koristim je rotacija ovih datoteka preko logrotate daemona. Svo što treba je u /etc/logrotate.d stvoriti datoteku pod nazivom spam, sa sljedećim sadržajem:

```
/home/*/spam {
daily
missingok
rotate 7
compress
delaycompress
notifempty
create 644
sharedscripts
postrotate
endscript
}
```

Ovo se može podesiti po želji - kao što se vidi moja konfiguracija rotira spam datoteke dnevno i čuva zadnjih 7 dana. Kod jednog od korisnika to ovako izgleda:

```
# ls -al /home/korisnik/spam*
-rw-r--r-- 1 korisnik inst 8331 Jan 11 14:34 /home/korisnik/spam
-rw-r--r-- 1 korisnik inst 9129 Jan 10 19:42 /home/korisnik/spam.1
-rw-r--r-- 1 korisnik inst 7774 Jan 11 00:16 /home/korisnik/spam.2.gz
-rw-r--r-- 1 korisnik inst 6263 Jan 10 00:15 /home/korisnik/spam.3.gz
-rw-r--r-- 1 korisnik inst 5083 Jan 9 00:17 /home/korisnik/spam.4.gz
-rw-r--r-- 1 korisnik inst 27146 Jan 8 00:15 /home/korisnik/spam.5.gz
-rw-r--r-- 1 korisnik inst 4750 Jan 7 00:15 /home/korisnik/spam.6.gz
-rw-r--r-- 1 korisnik inst 3675 Jan 6 00:15 /home/korisnik/spam.7.gz
```

Na ovaj način bi trebali svi biti zadovoljni - i oni koji žele dobivati SPAM poštu i oni koji to ne žele.

Ovakva konfiguracija pokazala se korisnom u dosta slučajeva kada su neke poruke pogrešno označene kao SPAM.

- Logirajte [1] se za dodavanje komentara

čet, 2007-01-11 15:12 - Damir Mrkonjić**Kuharice:** Linux [6]
Za sistemce [11]
Vote: 0

No votes yet

Statistika antivirusnog poslužitelja

PAKET amavis-stats OD INAČICE SQUEEZE NIJE VIŠE DOSTUPAN NA DEBIANOVIM REPOZITORIJIMA!

Upotrebom različitih statističkih programa možemo dobiti korisne informacije o radu nekog servisa na poslužitelju. Obično takve informacije sadrže i grafički prikaz što povećava preglednost rezultata obrade.

U ovom tekstu prikazati ćemo program **amavis-stats** za analizu rada antivirusne programske podrške na poslužiteljima koji koriste paket **amavis**. Kao rezultat instalacije ovog programa dobiti ćemo web stranicu sa grafičkim prikazom e-mail prometa s posebnim naglaskom na zaustavljene poruke s virusima. Stranica se sastoji od četiri grafikona koji prikazuju dnevnu, tjednu, mjesečnu i godišnju statistiku rada antivirusnog poslužitelja.

Instalacija ovog paketa sastoji se od instalacije deban paketa amavis-stats i nekoliko manjih izmjena u konfiguraciji poslužitelja.

Paket ćemo instalirati korištenjem programa *apt-get*:

```
 apt-get update
apt-get install amavis-stats
```

Uz amavis-stats instalirati će se još i paketi *wwwconfig-common* i *rrdtool* koji su nužni za njegovo normalno funkcioniranje. Instalacijski program će nam postaviti jedno pitanje:

```
 Amavis-stats keeps its database files under /var/cache/amavis-stats.
Should this directory be removed completely on purge?

Remove RRD files on purge?
```

Upit se odnosi na eventualnu deinstalaciju ovog paketa i čuvanje podataka koji su obrađeni za vrijeme njegovog rada. Ako odgovorimo sa 'no' podaci će biti sačuvani.

Instalacijski program otvoriti će korisnika `amavis-stats` pod čijim će se vlasništvom pokretati program.

Da bi se statistika mogla uspješno napraviti, korisnik `amavis-stats` mora imati pristup logovima e-mail poslužitelja koji se nalaze u direktoriju `/var/log/mail`. Datoteka `mail.info` koju amavis-stats analizira ima ovakva prava pristupa:

```
-rw-r-----   1 root adm  1098452 Oct 26 13:40 mail.info
```

Dakle, korisnik `amavis-stats` mora biti član grupe adm, što upisujemo u datoteku `/etc/group`:

```
adm:x:4:logcheck,amavis-stats
```

Sljedeći korak je dozvola pristupa `amavis-stats` programu u sam direktorij `/var/log/mail` koji obično ima ovakva prava:

```
drwxr-s---  2 root mail 4096 Oct 26 00:11 /var/log/mail/
```

Da bi korisnik `amavis-stats` mogao pristupiti datotekama unutar tog direktorija dovoljno je dodati pravo ulaska za sve:

```
chmod o+x /var/log/mail
```

nakon čega će stanje biti ovakvo:

```
drwxr-s--x  2 root mail 4096 Oct 26 00:11 /var/log/mail/
```

Da bi se statistika uspješno provodila potrebno je povremeno pokrenuti program `amavis-stats`, što se radi pomoću cron-a. Instalacijski paket postavlja datoteku `amavis-stats` u direktorij `/etc/cron.d` koja izgleda ovako:

```
 #
# cron job for the amavis-stats package
#
*/5 * * * * amavis-stats  [ -x /usr/sbin/amavis-stats ] && /usr/sbin/amavis-
stats /var/log/mail.info
```

Potrebno je ovo još prilagoditi konfiguraciji na našim poslužiteljima i popraviti direktorij gdje se nalazi log datoteka. Umjesto `/var/log/mail.info` napisati ćemo `/var/log/mail/mail.info` tako da imamo ovakav zapis u spomenutoj datoteci:

```
*/5 * * * * amavis-stats  [ -x /usr/sbin/amavis-stats ] && /usr/sbin/amavis-
stats /var/log/mail/mail.info
```

Kada cron prvi put pokrene statistiku generirati će se rezultati koje možemo vidjeti preko web preglednika, upisom adrese našeg web poslužitelja i direktorija amavis-stats,
npr. `http://www.domena.hr/amavis-stats/`

Kao primjer može se pogledati stranica `http://www.krs.hr/amavis-stats/`.

- Logirajte [1] se za dodavanje komentara

pon, 2007-10-29 12:21 - Damir Mrkonjić**Kuharice:** Linux [6]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/199

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://sysportal.carnet.hr/node/559
[3] https://sysportal.carnet.hr/node/188
[4] https://sysportal.carnet.hr/node/157
[5] http://www.securiteam.com/securitynews/5YP0A0K8CM.html
[6] https://sysportal.carnet.hr/taxonomy/term/17
[7] https://sysportal.carnet.hr/taxonomy/term/26
[8] http://www200.pair.com/mecham/spam/bypassing.html
[9] https://sysportal.carnet.hr/taxonomy/term/28
[10] https://sysportal.carnet.hr/taxonomy/term/25
[11] https://sysportal.carnet.hr/taxonomy/term/22