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 [2]
Kategorije: Software [3]
Servisi [4]
Vote: 4.666665

Vaša ocjena: Nema Average: 4.7 (3 votes)

Source URL: https://sysportal.carnet.hr./node/526

Links
[1] https://sysportal.carnet.hr./sysportallogin
[2] https://sysportal.carnet.hr./taxonomy/term/17
[3] https://sysportal.carnet.hr./taxonomy/term/25
[4] https://sysportal.carnet.hr./taxonomy/term/28