ClamAV savjeti i trikovi

ClamAV je antivirusni softver otvorenog koda, što ga je učinilo jednim od najpopularnijih komponenata antivirusne zaštite.

- Logirajte [1] se za dodavanje komentara

ClamAV: greška "Access to all MSRBL mirror sites failed"

 Na svojim poslužiteljima gotovo svi unutar CARNet mreže rabe antivirusni softver otvorenog koda - ClamAV. Iako većinu vremena ClamAV šuti i radi svoj posao, ponekad zna doći do zastoja. Ove godine je već bilo problema s oštećenim bazama, a sada se ugasio jedan od neslužbenih servisa koje rabi ClamAV. Ovo je prouzrokovalo desetke poruka, koje su stizale u mailbox svakih nekoliko sati:

```
Access to all MSRBL mirror sites failed - Check for connectivity issues or
signature database name(s) misspelled in the script's configuration file.
```

Poruka navodi na lažan trag, te bi se moglo pretpostaviti da je riječ o privremenom problemu, ili s mrežom ili nekakvom neuspjelom nadogradnjom. Činjenica je, zapravo, da neslužbeni servis MSRBL već duže vrijeme ne radi. Debianovci su ovo utvrdili još prošle godine i napravili novi paket **clamav-unofficial-sigs** za Wheezy (inačica je 3.7.1). U paketu clamav-unofficial-sigs popravljena je istoimena skripta, pa će i CARNetova grupa za pakete izdati novi paket **clamav-cn** koji će sadržavati ovu ispravku.

Za nestrpljive, rješenje u vlastitom aranžmanu je jednostavno, u konfiguracijsku datoteku /etc/clamav-unofficial-sigs.conf treba upisati sljedeće:

```
unset msrbl_dbs
```

Restart ClamAV-a nije potreban, a prilikom sljedećeg pokretanja skripte clamav-unofficial-sigs iz crona, obje baze iz direktorija /var/cache/clamav-unofficial-sigs/msrbl-dbs će biti automatski obrisane.

Ovo se može učiniti bez ikakve grižnje savjesti, jer starom i nepodržanom softveru jednostavno nije mjesto na poslužitelju u produkciji!

- Logirajte [1] se za dodavanje komentara

pon, 2012-05-14 14:45 - Željko Boroš**Kuharice:** Linux [2]

Kategorije: Servisi [3]
Vote: 0

No votes yet

ClamAV: greška 'lstat() failed'

 Nedavno se na nekim poslužiteljima pojavila nova greška povezana s ClamAV antivirusnim softverom. Riječ je o poruci 'lstat() failed', a puna inačica poruke izgleda otprilike ovako:

```
Jul 2 13:31:51 linux amavis[29062]: (29062-10) Clam Antivirus-clamd FAILED
 - unknown status: /var/lib/amavis/amavis-20070702T131611-29062/parts:
 lstat() failed. ERROR\n
Jul 2 13:31:51 linux amavis[29062]: (29062-10) WARN: all primary virus
scanners failed, considering backups
```

Poruka 'lstat() failed' označava problem gdje ClamAV proces (clamd ili clamscan, u ovisnosti o konfiguraciji) ne može pristupiti mail porukama koje trebaju biti pregledane. Razlog tome je pripadnost korisnika clamav i amavis različitim grupama:

```
# groups amavis clamav
amavis : amavis
clamav : clamav amavis
```

Iz gornjeg se primjera može vidjeti da clamav pripada grupi "clamav", ali i grupi "amavis", što je dodao CARNet paket clamav-cn u pokušaju da se baš ovakav problem izbjegne. To nije dovoljno, jer na adresi http://wiki.clamav.net/Main/FAQ#I_m_running_ClamAV_amavisd_new_a i u datoteci /usr/share/doc/clamav-base/README.Debian.gz piše da u datoteku /etc/clamav/clamd.conf treba dodati opciju AllowSupplementaryGroups, što je odavno i učinjeno. No, odnedavno se to pokazalo nedovoljnim, jer su (čini se) napravljene promjene u kodu koje više ne dopuštaju opcije bez argumenata. Imajte to na umu i provjerite svoj clamd.conf!

Izvor informacije koji se jedini pokazao točan je man stranica, gdje se spominje sintaksa:

```
AllowSupplementaryGroups BOOLEAN
```

što upućuje na jedini mogući točan način upisivanja ove opcije:

```
AllowSupplementaryGroups true
```

Gornji redak trebate upisati u /etc/clamav/clamd.conf i restartati mail sustav, najbolje sa (iako možete probati restartati samo clamd):

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

U mail.log-u provjerite jesu li se svi potrebni servisi restartali (clamd, postgrey, postfix, amavis). Nakon ove promjene, problema više ne bi trebalo biti.

- Logirajte [1] se za dodavanje komentara

pon, 2007-07-02 15:01 - Željko Borš**Vijesti:** Linux [4]
Kuharice: Za sistemce [5]
Kategorije: Servisi [3]
Vote: 0

No votes yet

ClamAV: poruka "WARNING: getpatch: Can't download daily-16682.cdiff"

Nekim korisnicima našeg helpdeska za sistemce antivirusni program ClamAV ponovo počinje raditi "probleme". Ovi problemi ne sprječavaju rad antivirusa, no sprječavaju osvježavanje antivirusnih definicija. Ova činjenica s vremenom bi omogućila da pojedini virusi prođu nezamijećeni kroz cijeli antivirusni sustav, pa je potrebno posvetiti pažnju da se to ne dogodi. Poruke koje ste mogli primjetiti su bile:

```
LibClamAV Warning: ***The virus database is older than 7 days!***
LibClamAV Warning: ***Please update it as soon as possible.***
```

Ručnim pokretanjem programa za osvježavanje antivurnish definicija htjeli smo vidjeti zašto se antivirusne definicije ne skidaju, je li problem u mreži, mirrorima ili nečem drugom. Rezultat koji smo dobili:

```
# freshclam -v
Current working dir is /var/lib/clamav
Max retries == 5
ClamAV update process started at Wed Apr  3 14:25:46 2013
```

```
Using IPv6 aware code
Querying current.cvd.clamav.net
TTL: 712
Software version from DNS: 0.97.7
main.cvd version from DNS: 54
main.cld is up to date (version: 54, sigs: 1044387, f-level: 60, builder: sven)
daily.cvd version from DNS: 16950
Retrieving http://db.local.clamav.net/daily-16682.cdiff
Ignoring mirror 193.92.150.194 (has connected too many times with an outdated version
)
Ignoring mirror 195.222.33.229 (has connected too many times with an outdated version
)
Ignoring mirror 193.92.150.194 (has connected too many times with an outdated version
)
Ignoring mirror 195.222.33.229 (has connected too many times with an outdated version
)
WARNING: getpatch: Can't download daily-16682.cdiff from db.local.clamav.net
...
Whitelisting short-term blacklisted mirrors
Retrieving http://db.local.clamav.net/daily.cvd
Ignoring mirror 193.92.150.194 (has connected too many times with an outdated version
)
Ignoring mirror 195.222.33.229 (has connected too many times with an outdated version
)
Ignoring mirror 193.92.150.194 (has connected too many times with an outdated version
)
Ignoring mirror 195.222.33.229 (has connected too many times with an outdated version
)
WARNING: Can't download daily.cvd from db.local.clamav.net
Trying again in 5 secs...
```

Čini se da mirrori imaju zastarjele inačice definicija, ili je možda greška ipak do nas? Najbrže je do informacija doći na izvoru, pa smo našli korisne informacije na adresi http://blog.clamav.net [6]. Čini se da su zbog izdavanja nove inačice ClamAV-a (0.97.7) i priprema za 0.98 napravili pogrešan korak, kojim su onemogućili osvježavanje na uobičajen način. Rješenje je jednostavno, treba obrisati datoteke daily.cvd i mirrors.dat u direktoriju /var/lib/clamav. Mi smo imali uspjeha i s brisanjem samo datoteke daily.cvd:

```
# rm /var/lib/clamav/daily.cvd
# freshclam -v
Current working dir is /var/lib/clamav
Max retries == 5
ClamAV update process started at Wed Apr  3 14:25:58 2013
Using IPv6 aware code
Querying current.cvd.clamav.net
TTL: 700
Software version from DNS: 0.97.7
main.cvd version from DNS: 54
main.cld is up to date (version: 54, sigs: 1044387, f-level: 60, builder: sven)
Retrieving http://db.local.clamav.net/daily.cvd
Trying to download http://db.local.clamav.net/daily.cvd (IP: 195.222.33.229)
Downloading daily.cvd [100%]
Loading signatures from daily.cvd
Properly loaded 1039355 signatures from new daily.cvd
daily.cvd updated (version: 16950, sigs: 1039355, f-level: 63, builder: neo)
Querying daily.16950.68.1.0.195.222.33.229.ping.clamav.net
bytecode.cvd version from DNS: 214
bytecode.cld is up to date (version: 214, sigs: 41, f-level: 63, builder: neo)
```

```
Database updated (2083783 signatures) from db.local.clamav.net (IP: 195.222.33.229)
```

Osvježavanje je, dakle, proradilo bez dodatnih intervencija. Ukoliko kod vas ovaj recept "ne upali", probajte obrisati i mirrors.dat.

- Logirajte [1] se za dodavanje komentara

sri, 2013-04-03 15:00 - Željko Boroš**Kuharice:** Linux [2]
Kategorije: Servisi [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

ClamAV: poruka "Your ClamAV installation is OUTDATED"

Ponekad se u logovima različitih servisa zna naći dosta poruka o greškama i problemima, koji mogu zvučati dosta ozbiljno. No, je li situacija uvijek ozbiljna kako se to na prvi pogled čini?

Primjerice, u datoteci /var/log/clamav/freshclam.log se mogu naći ovakvi unosi:

```
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.90.2 Recommended version: 0.90.3
```

Nije teško protumačiti da se ClamAV "buni" zbog starosti vlastite inačice, te preporučuje da se instalira nova, svježija inačica. No, zbog Debianove konzervativne politike izrade paketa, nove inačice paketa nisu usklađene sa inačicama ClamAV-a, odnosno paketi nisu dostupni na standardnim (stable) repozitorijima.

Upravo zbog tog problema paket clamav-cn sadrži backportanu inačicu paketa, odnosno najnoviju inačicu ClamAV-a prilagođenu aktualnoj CN-linux distribuciji (u ovom trenutku to je Sarge).

Jedino što treba učiniti je sačekati da izađe nova inačica paketa clamav-cn, što može potrajati nekoliko dana zbog postupka izrade i testiranja. U tom periodu čekanja, vaš poslužitelj nije nezaštićen i radi bez problema zahvaljujući redovitim nadogradnjama antivirusnih definicija, koje i dalje rade na "staroj" inačici ClamAV-a.

U samom logu ispod obavijesti piše i zgodna napomena:

```
DON'T PANIC! Read http://www.clamav.net/support/faq
```

Upravo tako i treba postupiti, pročitati FAQ (http://www.clamav.net/doc/install.html [7]) i jednostavno sačekati novu inačicu paketa, jer nema nikakve hitnosti unatoč toj poruci u logovima.
Dakako, uvijek možete sami iskompilirati ClamAV, ili naći gotov paket na volatile ili drugim repozitorijima (što ne preporučujemo ukoliko niste
iskusni u tome i znate točno što radite).

- Logirajte [1] se za dodavanje komentara

uto, 2007-06-05 13:58 - Željko Borš**Vijesti:** Linux [4]
Kuharice: Za sistemce [5]
Kategorije: Servisi [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/487

Links
[1] https://sysportal.carnet.hr/sysportallogin
[2] https://sysportal.carnet.hr/taxonomy/term/17
[3] https://sysportal.carnet.hr/taxonomy/term/28
[4] https://sysportal.carnet.hr/taxonomy/term/11
[5] https://sysportal.carnet.hr/taxonomy/term/22
[6] http://blog.clamav.net
[7] http://www.clamav.net/doc/install.html