Greške u ClamAV-u: "integrity tested BAD - SKIPPING"

ClamAV, kao jedino antivirusno rješenje na našim Debian poslužiteljima, pokazao se pouzdanim. No nije uvijek tako, povremeno se u logovima i mailovima znaju pojaviti poruke o nedostupnosti mirroring poslužitelja ili neke druge greške. Zajedničko im je to da s vremenom nestanu same od sebe. Ali, prije nekoliko dana pojavila se poruka koja nije nestala sama od sebe:

```
Clamscan reports Sanesecurity honeynet.hdb database integrity tested BAD - SKIPPING
Clamscan reports Sanesecurity securiteinfo.hdb database integrity tested BAD - SKIPPI
NG
Clamscan reports Sanesecurity vx.hdb database integrity tested BAD - SKIPPING
```

Zašto je odjednom baza SaneSecurityja prestala raditi? Možda je poslužitelj nedostupan ili je nastupio nekakav problem prilikom prijenosa baza sa poslužitelja? Najlogičnije bi bilo da pokušamo sami pokrenuti skriptu, da vidimo kakve se greške mogu pojaviti. Skripta se pokreće iz crona, ali mi ćemo je pokrenuti iz korisničke ljuske kako bi vidjeli sve greške i poruke:

```
# su -s /bin/sh clamav
# /usr/sbin/clamav-unofficial-sigs

======================================================================
SecuriteInfo Database File Updates
======================================================================

4 hours have not yet elapsed since the last SecuriteInfo update check

     --- No update check was performed at this time ---
...
```

Kako ne bi opterećivali poslužitelje na kojima se nalaze baze, skripta neće skidati ništa ukoliko nije prošlo dovoljno vremena između dva skidanja. To radi preko datoteke u kojem se zapisuje *timestamp* zadnjeg osvježavanja, a to je u konkretnom slučaju /var/lib/clamav-unofficial-sigs/configs/last-si-update.txt.

Kako skripta samo uspoređuje vrijednost u toj datoteci (ne radi nikakve *sanity* provjere), dovoljno je samo upisati jedinicu u tu datoteku:

```
# echo 1 > /var/lib/clamav-unofficial-sigs/configs/last-si-update
```

Nakon sto smo promijenili vrijednost u datoteci last-si-update.txt, pokušavamo ponovo:

```
Checking for updated SecuriteInfo database file: honeynet.hdb

  % Total    % Received % Xferd  Average Speed   Time    Time     Time
  % Current
                                 Dload  Upload   Total   Spent    Left
```

```
Speed
100   286  100   286    0     0   3601      0 --:--:-- --:--:-- --:--:--
6975

Testing updated SecuriteInfo database file: honeynet.hdb
Clamscan reports Sanesecurity honeynet.hdb database integrity tested BAD - SKIPPING
...
```

Download je krenuo, ali greška se i dalje javlja. Trebali bi pogledati što piše u samoj datoteci, koja je jako mala, samo nekoliko stotina bajtova. Znamo od prije da su te baze u tekstualnom obliku, pa se mogu pregledati običnim tekstualnim editorom ili pagerom:

```
# cd /var/cache/clamav-unofficial-sigs
# less si-dbs/honeynet.hdb
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>404 Not Found</title>
</head><body>
<h1>Not Found</h1>
<p>The requested URL /honeynet.hdb.gz was not found on this server.</p>
<hr>
<address>Apache Server at clamav.securiteinfo.com Port 80</address>
</body></html>
```

Dakle, sve je jasno, čini se da su opet problemi s mirrorima... ali kako to da do sada nisu riješeni? Google, kao i uvijek, može pomoći. Čini se da je u pitanju zastarjela skripta clamav-unofficial-sigs, što je malo čudno ("danas radi, sutra ne"), ali hajdemo provjeriti.

U samoj skripti se nalazi točna verzija:

```
version="v3.6 (updated 2009-08-23)"
```

Dakle, zaista, za 4 godine koliko skripta postoji se moglo koješta dogoditi. Zašto Debian nije osvježio skriptu, ili je ovo skripta iz CARNetovog paketa pa nije najnovija? Čini se da nije, ovo je skripta iz najuobičajenijeg Debianovog paketa:

```
# dpkg -l clamav-unofficial-sigs
Desired=Unknown/Install/Remove/Purge/Hold
|Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-aWait/Trig-pend
|/ Err?=(none)/Reinst-required (Status,Err: uppercase=bad)
||/ Name           Version        Description
+++-==============-==============-============================================
ii  clamav-unoffic 3.6-1          update script for 3rd-party clamav signature
```

Dakle što možemo učiniti? Skripta ne radi, kako ćemo doći do novije skripte ako je nema u repozitoriju? Odgovor je dao onaj isti upit Googleu, gdje je spomenuto da se novija skripta može naći u "**debian backports**" repozitoriju.

Ukoliko ste navedeni repozitorij imali upisan od prije, vjerojatno niste ni primjetili ovaj problem. U suprotnom, upišite ga u /etc/apt/source.list:

```
deb ftp://ftp.at.debian.org/debian-backports/ squeeze-backports main
```

Navedeni mirror je iz Austrije jer nismo našli takav mirror u Hrvatskoj. Ako ga negdje ipak ima, sami ga upišite. Sljedeći korak je instalacija nove skripte:

```
# apt-get update
...
# apt-get -t squeeze-backports install clamav-unofficial-sigs
The following packages will be upgraded:
  clamav-unofficial-sigs
1 upgraded, 0 newly installed, 0 to remove and 157 not upgraded.
Get:1 ftp://ftp.at.debian.org/debian-backports/ squeeze-backports/main
clamav-unofficial-sigs all 3.7.1-1~bpo60+1 [44.2 kB]
```

Sama instalacija je prosla uredno, osim (dosadnog) problema s nadogradnjom konfiguracijskih datoteka:

```
Configuration file `/etc/clamav-unofficial-sigs.conf'
 ==> Modified (by you or by a script) since installation.
 ==> Package distributor has shipped an updated version.
   What would you like to do about it ?  Your options are:
    Y or I  : install the package maintainer's version
    N or O  : keep your currently-installed version
      D     : show the differences between the versions
      Z     : start a shell to examine the situation
 The default action is to keep your current version.
*** clamav-unofficial-sigs.conf (Y/I/N/O/D/Z) [default=N] ?
```

Nakon ispitivanja razlika (odabravši "D"), shvatili smo da vrijedi pregaziti datoteku (uvedene su neke promjene, poput konfiguracijskog direktorija /etc/clamav-unofficial-sigs.conf.d/ i slično), te ručno na kraj datoteke vratiti direktive iz prethodne verzije:

```
# By CARNet
unset msrbl_dbs
clam_user=clamav
clam_group=clamav
```

I to je to, skripta je sada verzije:

```
version="v3.7.1 (updated 2010-06-06)"
```

Napomena: ukoliko ste pokrenuli skriptu kao root, moguće je da su neke datoteke promijenile vlasništvo, te ih clamav više ne može mijenjati. Situaciju možete popraviti sa:

```
# chown -R clamav:clamav /var/cache/clamav-unofficial-sigs/*
# chown -R clamav:clamav /var/lib/clamav/*
```

Nova verzija skripte pazi na ovu situaciju, ali je potrebno dodati varijable "clam_user" i "clam_group" u /etc/clamav-unofficial-sigs.conf, kako smo i pokazali malo prije.

I još jedna napomena, ukoliko ponovo dođe do greške, probajte više puta pokrenuti skriptu

(resetirajući svaki put timestamp), jer neki mirrori nisu uvijek sinhronizirani s glavnim poslužiteljima.

uto, 2013-03-12 08:56 - Marko Jukić**Kuharice:** Linux [1]
Kategorije: Operacijski sustavi [2]
Vote: 4.666665

Vaša ocjena: Nema Average: 4.7 (3 votes)

Source URL: https://sysportal.carnet.hr/node/1226

Links
[1] https://sysportal.carnet.hr/taxonomy/term/17
[2] https://sysportal.carnet.hr/taxonomy/term/26