Centralno logiranje

Svi znamo da je logove potrebno redovito pratiti. Međutim, njihovo čuvanje samo na uređaju koji ih je i generirao nije dobro iz više razloga. Primjerice, ako sustav bude kompromitiran, prvo što će napadač napraviti jest promijeniti logove i time izbrisati svoje tragove. Cilj centralnog logiranja jest skupljanje logova različitih uređaja na jedan, centralni poslužitelj.

Za centralno skupljanje logova koristit ćemo rsyslog. To je novija inačica dobro nam poznatog syslog protokola, a koji sadrži mnoga poboljšanja u odnosu na prethodnika. Primjerice, prijenosni protokol jest TCP, čime je osiguran pouzdan prijenos preko mreže. Također, dodane su mogućnosti zapisivanja u bazu podataka (podržane su MySQL, PostGRE, Oracle, SQLite, Microsoft SQL i druge), podrška za IPv6, kriptiranje sadržaja (SSL i TLS) i druge. Na većini Linux operativnih sustava rsyslog je osnovni sustav za logiranje, a na Debianu se koristi umjesto sysklogd počevši od verzije 5 (Lenny). Ukoliko rsyslog nije instaliran, naredba je standardna:

```
apt-get update
apt-get install rsyslog
```

Sva konfiguracija se nalazi unutar /etc/rsyslog.conf datoteke. Na klijentima konfiguracija ne može biti jednostavnija - potrebno je samo na početak pravila unutar rsyslog.conf datoteke dodati sljedeće:

```
*.* @@192.168.50.10:10514
```

Time smo rekli klijentu da sve logove šalje poslužitelju na navedenoj adresi i portu. Dva znaka @ nisu greška, a moguće je navesti nekoliko poslužitelja na način da se svaki poslužitelj doda u svoj redak.

Što se konfiguracije poslužitelja tiče, prva stvar koju treba napraviti jest natjerati rsyslog da "sluša" na već navedenom portu i to za TCP protokol. Na početak konfiguracijske datoteke potrebno je maknuti komentar s već postojećih redaka i promijeniti predloženi port:

```
$ModLoad imtcp
$InputTCPServerRun 10514
```

Moguće je odabrati i UDP kao prijenosni protokol, ali, zbog nesigurnog prijenosa preko mreže, to nije preporučljivo. Naravno, nakon svake promjene unutar rsyslog.conf datoteke potrebno je ponovno pokrenuti rsyslog servis:

```
invoke-rc.d rsyslog restart
```

Za samo spremanje logova na poslužitelju postoji nekoliko opcija pa možemo krenuti po redu. Prva je opcija "obično" primanje logova, bez ikakvog razvrstavanja ili sortiranja. U ovom slučaju gornje dvije linije konfiguracije su dovoljne da poslužitelj počne primati logove od klijenta. Međutim, ti će logovi biti u istim datotekama kao i lokalni logovi poslužitelja, tj. svi logovi će bit izmiješani. Doduše, možemo ih razlikovati pomoću imena klijenta koje se automatski doda pri početku retka unutar loga /var/log/syslog:

```
Oct 12 18:30:37 client01 sshd[1340]: pam_unix(sshd:session): session closed for user
mirko
Oct 12 18:30:51 client01 sshd[1371]: Accepted password for mirko from 192.168.50.40 p
```


Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

```
ort 54260 ssh2
Oct 12 18:30:51 client01 sshd[1371]: pam_unix(sshd:session): session opened for user
mirko by (uid=0)
Oct 12 18:31:03 server sshd[1560]: Accepted password for mirko from 192.168.50.40 por
t 54262 ssh2
Oct 12 18:31:03 server sshd[1560]: pam_unix(sshd:session): session opened for user mi
rko by (uid=0)
Oct 12 18:31:15 client01 su[1399]: Successful su for root by mirko
Oct 12 18:31:15 client01 su[1399]: + /dev/pts/0 mirko:root
Oct 12 18:31:15 client01 su[1399]: pam_unix(su:session): session opened for user root
 by mirko(uid=1000)
Oct 12 18:31:21 server su[1588]: Successful su for root by mirko
Oct 12 18:31:21 server su[1588]: + /dev/pts/1 mirko:root
Oct 12 18:31:21 server su[1588]: pam_unix(su:session): session opened for user root b
y mirko(uid=1000)
```

Vidimo da ovaj zapis nije najpregledniji, pogotovo ako je u pitanju veći broj klijenata. Zato možemo, primjerice, logirati odvojeno po mrežama na kojima su klijenti. Konfiguracija je sljedeća:

```
$ModLoad imtcp
$InputTCPServerRun 10514
if $fromhost-ip startswith '192.168.1.' then /var/log/network1.log
& ~
if $fromhost-ip startswith '192.168.2.' then /var/log/network2.log
& ~
*.* /var/log/syslog
```

Obratite pažnju na znak ~ koji govori rsyslogu da prekine s procesiranjem poruke nakon što je ona zapisana u log datoteku. Bez tog znaka log bi se nastavio dalje zapisivati i lokalnu /var/log/syslog datoteku. Iz tog razloga gornju konfiguraciju treba dodati ispred standardnih rsyslog pravila.

Također, moguće je i zasebno logirati svakog klijenta. Log datoteke će se stvarati dinamički neovisno o broju klijenata, a logovi će se razdvajati u te posebne datoteke, isto kao i lokalni logovi. Prvo je potrebno definirati klijente i log datoteke, a zatim odgovarajuće logove spremati u njihove datoteke. To se radi pomoću predložaka (eng. templates), a za primjer ćemo pokazati syslog, auth.log i kern.log datoteke za dva klijenta:

```
$template DYNauth,"/var/log/%HOSTNAME%/auth.log"
$template DYNsyslog,"/var/log/%HOSTNAME%/syslog"
$template DYNkern,"/var/log/%HOSTNAME%/kern.log"

##### client01
if \
    $source == '192.168.50.111' or $source == 'client01' \
then ?DYNsyslog
if \
    $source == '192.168.50.111' or $source == 'client01' \
    and $syslogfacility-text == 'auth' \
then ?DYNauth
if \
    $source == '192.168.50.111' or $source == 'client01' \
    and $syslogfacility-text == 'kern' \
then ?DYNkern
##### end client01

##### client02
if \
```


Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

```
    $source == '192.168.50.222' or $source == 'client02' \
then ?DYNsyslog
if \
    $source == '192.168.50.222' or $source == 'client02' \
    and $syslogfacility-text == 'auth' \
then ?DYNauth
if \
    $source == '192.168.50.222' or $source == 'client02' \
    and $syslogfacility-text == 'kern' \
then ?DYNkern
##### end client02
```

Posljedica ovog je klijentska direktorijska struktura unutar /var/log direktorija. Dakle, unutar svakog /var/log/clientXX direktorija bit će syslog, auth.log i kern.log datoteke tog klijenta.

Na kraju, moguće je iskoristiti i sigurnosnu komponentu rsyslogd protokola korištenjem kriptiranja te digitalnih certifikata radi utvrđivanja identiteta pošiljatelja i primatelja logova. Na taj se način onemogućava primanje logova s nepoznatih klijenata. U ovu je svrhu najjednostavnije koristiti samopotpisane certifikate. Potrebno je nekoliko certifikata tj. datoteka: certifikat kojem vjeruju sva računala unutar sustava (eng. certified authority, datoteku nazovimo ga ca.pem), te privatni ključevi (key.pem) i potpisani certifikati (cert.pem) za poslužitelj i svakog klijenta. Sami postupak kreiranja samopotpisanih certifikata ćemo preskočiti jer je opisan na mnogo mjesta, a konfiguracija poslužitelja je sljedeća:

```
# make gtls driver the default
$DefaultNetstreamDriver gtls

# certificate files
$DefaultNetstreamDriverCAFile /path/to/ca.pem
$DefaultNetstreamDriverCertFile /path/to/cert.pem
$DefaultNetstreamDriverKeyFile /path/to/key.pem

$ModLoad imtcp # load TCP listener

$InputTCPServerStreamDriverMode 1 # run driver in TLS-only mode
$InputTCPServerStreamDriverAuthMode anon # client is NOT authenticated
$InputTCPServerRun 10514 # start up listener at port 10514
```

Iza ovog može slijediti neki od opisanih načina za primanje udaljenih logova.
Konfiguracija klijenata ide kako slijedi:

```
# certificate files - just CA for a client
$DefaultNetstreamDriverCAFile /path/to/ca.pem

# set up the action
$DefaultNetstreamDriver gtls # use gtls netstream driver
$ActionSendStreamDriverMode 1 # require TLS for the connection
$ActionSendStreamDriverAuthMode anon # server is NOT authenticated
*.* @@192.168.50.10:10514 # send (all) messages
```

Rsyslog ima još dosta opcija poput tuneliranja, rada u NAT okruženju, komprimiranja logova i njihovog zapisivanja u različitim formatima. Također, moguće je primati logove s Windows i OS X operativnih sustava. Za sve opcije možete pogledati web stranicu alata, www.rsyslog.com.

čet, 2011-10-13 09:22 - Mirko Lovričević**Vijesti:** Linux [1]
Vote: 0

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr

No votes yet

Source URL: https://sysportal.carnet.hr/node/882

Links
[1] https://sysportal.carnet.hr/taxonomy/term/11

Copyright ©2003.-2017. CARNet. Sva prava pridržana.
Mail to portal-team(at)CARNet.hr