Podsjetnik na istek poslužiteljskih certifikata

Poslužiteljski certifikati davno su postali neizostavni dio sigurne svakodnevne komunikacije na internetu. Certifikate na koje imamo pravo (u suradnji s CARNetom) izdaje firma Comodo, a njihovo maksimalno trajanje je tri godine. Taj je period dovoljno dug da većina nas zaboravi pravovremeno provjeriti datum isteka certifikata. Naravno, istekli certifikat aktivira alarm za sve mail klijente i web preglednike, a time i naše korisnike.

Možemo pokušati sebi negdje zapisati podsjetnik, ali ni takav zapis nije otporan na previde. Kako su u svakom certifikatu zapisani datumi početka i kraja valjanosti certifikata, jedno od elegantnijih rješenja jest skripta koja će periodično provjeravati datum isteka te, kad se vrijeme približi, o tome obavijestiti administratora. Jedna takva jednostavna *bash* skripta je priložena.

```
#!/bin/bash
TO="administrator@domena.hr"
SERVER=$(</putanja/do/popisa/posluzitelja.txt)
set -- $SERVER
MESSAGE="/tmp/mail_message.txt"
for SERVER in "$@"
do
        openssl_output=$(echo "
        GET / HTTP/1.0
        EOT" \
         | openssl s_client -connect $SERVER:443 2>&1);
        if [[ "$openssl_output" = *"-----BEGIN CERTIFICATE-----"* ]]; then
                cert_expiry_date=$(echo "$openssl_output" \
                 | sed -n '/-----BEGIN CERTIFICATE-----/,/-----END CERTIFICATE-----/p
' \
                 | openssl x509 -enddate \
                 | awk -F= ' /notAfter/ { printf("%s\n",$NF); } ');
                seconds_until_expiry=$(echo "$(date --date="$cert_expiry_date" +%s) -
 $(date +%s)" |bc);
                days_until_expiry=$(echo "$seconds_until_expiry/(60*60*24)" |bc);
                if [[ ($days_until_expiry -lt 45) ]]; then
                        touch $MESSAGE
                        SUBJECT="Blizi se istek certifikata -  $SERVER"
                        echo "Do isteka certifikata na posluzitelju $SERVER je ostalo
 jos" \
                        "$days_until_expiry dana" > $MESSAGE
                        mail -s "$SUBJECT" "$TO" < $MESSAGE
                        /bin/rm -f "$MESSAGE"
                fi
        else
            echo "NOT_FOUND"> /dev/null 2>&1;
            exit 1
        fi
done
```

U varijabli "TO" se definira odredišna mail adresa, a u varijabli "SERVER" se nalazi putanja do tekstualne datoteke s popisom poslužitelja. Pomoću FOR petlje skripta se spaja na priključnu točku

443 svakog od definiranih poslužitelja, traži instalirani certifikat te provjerava njegov datum isteka. Ukoliko je taj datum unutar definiranog perioda od 45 dana od isteka, administrator će dobiti e-mail kao podsjetnik.

Skripta kao parametar prima popis poslužitelja koji se nalaze u tekstualnoj datoteci, a ona je jednostavna, po jedan poslužitelj u svakom retku. Ime poslužitelja može biti FQDN ili skraćeno, lokalno ime:

```
posluzitelj1.domena.hr
posluzitelj2.domena.hr
posluzitelj3.domena.hr
```

Broj poslužitelja je proizvoljan, a na ovaj način je dovoljno periodično pokretati skriptu na jednom poslužitelju i provjeravati sve ostale. Ja sam skriptu smjestio u direktorij */etc/cron.weekly*, što znači da će se ona izvršavati jednom tjedno. Vremenski period prilagodite svojim potrebama, a moguće je, naravno, i odrediti proizvoljni period izvršavanja skripte naredbom *crontab -e*.

pon, 2013-01-07 11:49 - Mirko Lovričević**Kategorije:** Operacijski sustavi [1]
Vote: 4.4

Vaša ocjena: Nema Average: 4.4 (5 votes)

Source URL: https://sysportal.carnet.hr/node/1178

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