Usare Let's Encrypt

Per l'uso della nuova Certification Authority libera e gratuita promossa da EFF, Mozilla e molti altri, il meccanismo più semplice (i pacchetti Debian sono disponibili al momento solo su testing e unstable) è quello di installare direttamente dal repository ufficiale, con:

```
git clone https://github.com/letsencrypt/letsencrypt
```

per verificarne il funzionamento occorrerà porsi nella directory in cui lo si è installato e per fargli installare i pacchetti mancanti eseguire (da root):

```
cd letsencrypt
./letsencrypt-auto --help
```

il programma inoltre si autoaggiornerà ad ogni esecuzione, e se lanciato senza argomenti cercherà di eseguire una installazione automatica, la verifica della richiesta per poter emettere i certificati ed infine anche la configurazione del web server per usare i certificati ottenuti, fornendo indicazioni qualora tutto ciò non sia possibile.

Le modalità di utilizzo dipendono infatti dalla disponibilità o meno di alcuni pacchetti nella propria distribuzione, ad esempio con Debian Wheezy non si può utilizzare l'autoconfigurazione automatica di Apache, mancando sufficiente supporto. Tratteremo comunque soltanto la modalità di configurazione non automatica, coprendo con questo anche la configurazione di altri servizi che non siano i server web, come la posta elettronica o la messaggistica.

La generazione dei certificati

In generale, quando non è possibile o non si vuole utilizzare la configurazione automatica dei servizi, e si deve ricorrere all'uso del comando certonly, come indicato anche dal programma stesso se l'automatismo è impossibile:

```
root@holland:~/letsencrypt# ./letsencrypt-auto
Checking for new version...
Requesting root privileges to run letsencrypt...
/root/.local/share/letsencrypt/bin/letsencrypt
No installers seem to be present and working on your system;
fix that or try running letsencrypt with the "certonly" command
```

L'uso del sottocomando certonly consente soltanto di ottenere i certificati, la configurazione dei servizi dovrà essere eseguita manualmente. Per emettere un certificato let's encrypt deve effettuare la validazione del dominio per cui questo viene richiesto, cosa che viene effettuata con una richiesta via web al dominio stesso, e l'uso di un meccanismo di challenge and response basato sulla possibilità di scaricare un file dal quel dominio.

Questa procedura può essere realizzata direttamente dal programma se si usa dopo il comando certonly l'opzione --standalone, che si incarica di far partire un servizio web sulla porta 80 o 443, ma in tal caso occorre fermare apache (o altro webserver) se attivi sul dominio.

Si può evitare tutto questo utilizzando l'opzione --webroot se si dispone dell'accesso alla document root del sito per cui si vuole ottenere il certificato, in tal caso infatti il programma crea i file necessari alla validazione sotto la directory /.well-known/acme-challenge, che però deve poter essere servita (occorre pertanto verificare che la configurazione del server web mantenga accessibile questa directory, per nginx è in genere necessaria un configurazione ad hoc, ci torneremo più avanti).

La directory della document root deve essere indicata con l'opzione -w, mentre il dominio (o i domini se sono più di uno, nel qual caso saranno aggiunti allo stesso certificato come nomi alternativi) devono essere richiesti con l'opzione -d. Se si hanno diversi siti con diverse document root in teoria si potrebbe eseguire l'operazione in un solo passo usando prima l'opzione -w per indicarle e poi l'opzione -d per indicare il dominio, quest'ultima infatti assume si stia usando come document root la directory indicata con l'ultima occorrenza precedente di -w, ma tutte devono essere egualmente accessibili, o si ripetere l'operazione per ciascun dominio, generando certificati separati, oppure si può usare la stessa document root per tutti i domini (usando le configurazioni descritte in seguito per consentire ad essa l'accesso via web per ciascuno di essi). Un esempio di invocazione del comando è il seguente:

```
      # ./letsencrypt-auto certonly --webroot -w /var/www/roundcubemail/ -d
mail.truelite.it
      [...]
      IMPORTANT NOTES:
       - Congratulations! Your certificate and chain have been saved at
         /etc/letsencrypt/live/mail.truelite.it/fullchain.pem. Your cert will
         expire on 2016-07-07. To obtain a new version of the certificate in
         the future, simply run Let's Encrypt again.
       - If you lose your account credentials, you can recover through
         e-mails sent to xxx@truelite.it.
       - Your account credentials have been saved in your Let's Encrypt
         configuration directory at /etc/letsencrypt. You should make a
         secure backup of this folder now. This configuration directory will
         also contain certificates and private keys obtained by Let's
         Encrypt so making regular backups of this folder is ideal.
       - If you like Let's Encrypt, please consider supporting our work by:

         Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
         Donating to EFF:                    https://eff.org/donate-le
```

La prima volta verrà richiesta una email di contatto (per comunicazione e recupero delle chiavi) e poi generato un certificato. La prima volta che si esegue il comando su una macchina oltre ad indicare la email di contatto si dovranno anche accettare le condizioni di letsencrypt. I certificati rilasciati durano tre mesi, e vengono installati sotto /etc/letsencrypt/live in una directory corrispondente al nome a dominio indicato (nel caso mail.truelite.it/). Ogni invocazione successiva si limiterà a creare i certificati richiesti con qualcosa del tipo:

```
      # ./letsencrypt-auto certonly --webroot -w /var/www/letsencrypt/ -d
bd2.truelite.it
      Checking for new version...
      Requesting root privileges to run letsencrypt...
         /root/.local/share/letsencrypt/bin/letsencrypt certonly --webroot -w
```

```
/var/www/letsencrypt/ -d bd2.truelite.it

      IMPORTANT NOTES:
       - Congratulations! Your certificate and chain have been saved at
         /etc/letsencrypt/live/bd2.truelite.it/fullchain.pem. Your cert will
         expire on 2016-07-07. To obtain a new version of the certificate in
         the future, simply run Let's Encrypt again.
       - If you like Let's Encrypt, please consider supporting our work by:

         Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
         Donating to EFF:                    https://eff.org/donate-le
```

Con lo script listlecert.sh si può stampare un elenco dei certificati creati, e dei domini da essi coperti.

Configurazioni per consentire la validazione

Come accennato per effettuare la validazione del dominio con la modalità --webroot è necessario che siano raggiungibili i contenuti corrispondenti alla URL:

```
http://mio.dominio.it/.well-known/acme-challenge/xxx
```

cosa che può dipendere dalla configurazione del proprio webserver. Nel caso di Nginx la modalità suggerita per consentire questa configurazione è creare un frammento di configurazione (nel caso /etc/nginx/snippets/letsencrypt-acme-challenge.conf) contenente le direttive necessarie per consentire l'accesso:

```
location ^~ /.well-known/acme-challenge/ {
    default_type "text/plain";
    root         /var/www/letsencrypt;
}
location = /.well-known/acme-challenge/ {
    return 404;
}
```

queste istruzioni consentono di eseguire la validazione indicando come webroot la directory /var/www/letsencrypt, posto che il frammento di cui sopra sia stato incluso come prima direttiva nelle configurazioni dei virtual host coinvolti (basta anche inserirlo solo nelle direttive in chiaro), ad esempio con qualcosa del tipo:

```
server {
        listen 80;
        root /var/www/html;
        server_name bd.truelite.it;
        include /etc/nginx/snippets/letsencrypt-acme-challenge.conf;
        location / {
            rewrite ^/(.*)$ https://bd.truelite.it/$1 permanent;
```

```
        }
    }
```

una analoga configurazione per Apache si può effettuare inserendo in /etc/apache2/conf.d (o con Jessie in /etc/apache2/conf-available/ per poi abilitarlo con a2enconf) il seguente frammento di configurazione:

```
    Alias /.well-known/acme-challenge/ /var/www/.well-known/acme-challenge/
    <Directory "/var/www/.well-known/acme-challenge/">
        Options None
        AllowOverride None
        ForceType text/plain
        # avoid access to anything not resembling a challenge
        RedirectMatch 404 "^(?!/\.well-known/acme-challenge/[\w-]{43}$)"
    </Directory>
```

Si tenga presente però che quando si usa Apache come reverse proxy occorrerà anche inserire una opportuna eccezione alle regole di proxy per la suddetta URL, in sostanza si dovrà aggiungere alla configurazione del virtual host una riga:

```
    ProxyPass /.well-known/acme-challenge !
```

Esempi di configurazione dei servizi
Una volta completata la validazione del proprio dominio, nella directory di installazione dei certificati (/etc/letsencrypt/live/mio.dominio.it) vengono sempre creati i file:

file	contenuto
cert.pem	cerficato
chain.pem	catena dalla CA
fullchain.pem	catena + certificato
privkey.pem	chiave privata

Dove chain.pem è il certificato intermedio (o la catena di certificati intermedi) che validano cert.pem che è il certificato del proprio dominio, mentre fullchain.pem è l'insieme completo del certificato e della catena. Infine la chiave privata è in privkey.pem.

In qualunque configurazione occorre sempre fare riferimento a questi file, che sono link simbolici, in quanto Let's Encrypt aggiornerà automaticamente gli stessi con la procedura di rinnovo automatico che vedremo più avanti.

I file cert.pem e chain.pem sono quelli che si usano nella configurazione di Apache, che li vuole separati, ad esempio con quelli ottenuti in precedenza la configurazione utilizzata è:

```
    SSLCertificateFile /etc/letsencrypt/live/mail.truelite.it/cert.pem
    SSLCertificateChainFile/etc/letsencrypt/live/mail.truelite.it/chain.pem
    SSLCertificateKeyFile/etc/letsencrypt/live/mail.truelite.it/privkey.pem
```


Truelite Srl
Via Monferrato, 6
50142 Firenze
055.7879597
www.truelite.it - info@truelite.it
P. Iva 05316110484 - Capitale sociale 15.000 euro i.v.
Registro imprese Firenze n. 05316110484 - R.E.A. Firenze n. 537498

Invece fullchain.pem è l'insieme del certificato e di tutta la sua catena di firma, che viene richiesto da Postfix, Dovecot e Nginx. Per Postfix occorrerà farvi riferimento in /etc/postfix/main.cf con le direttive:

```
smtpd_tls_cert_file=/etc/letsencrypt/live/mail.truelite.it/fullchain.pe
m
smtpd_tls_key_file=/etc/letsencrypt/live/mail.truelite.it/privkey.pem
```

mentre per Dovecot di dovanno utilizzare in /etc/dovecot/conf.d/90-user.conf le direttive:

```
ssl_cert = </etc/letsencrypt/live/mail.truelite.it/fullchain.pem
ssl_key = </etc/letsencrypt/live/mail.truelite.it/privkey.pem
```

ed infine per Nginx si dovrà inserire nella configurazione del proprio virtual host qualcosa del tipo:

```
server {
   listen 443 ssl;
   server_name bd.truelite.it;
   root /var/www/html;
   ssl_certificate /etc/letsencrypt/live/bd.truelite.it/fullchain.pem;
   ssl_certificate_key
/etc/letsencrypt/live/bd.truelite.it/privkey.pem;
   ...
```

Infine per configurare ejabberd (server jabber) occorre generare dai file di Let's Encrypt un unico file contenente in testa la chiave privata (il programma non consente di specificarli separatamente), se pertanto /etc/ejabberd/ejabberd.pem è il file usato dal programma, occorrerà rigenerarlo ogni volta che si generano o rinnovano i certificati con:

```
cat /etc/letsencrypt/live/jabber.truelite.it/privkey.pem \
    /etc/letsencrypt/live/jabber.truelite.it/fullchain.pem >
ejabberd.pem
```

In tutti i casi deve essere effettuato un riavvio completo dei servizi.

Il rinnovo dei certificati

La scadenza dei certificati emessi da Let's Encrypt è di tre mesi, ma una volta ottenuti questi possono essere facilmente rinnovati utilizzando il sottocomando renew, in particolare se si esegue il comando dopo averli ottenuti si otterrà qualcosa del tipo:

```
# ./letsencrypt-auto renew
Checking for new version...
Requesting root privileges to run letsencrypt...
   /root/.local/share/letsencrypt/bin/letsencrypt renew
```

Processing /etc/letsencrypt/renewal/mail.truelite.it.conf

The following certs are not due for renewal yet:

```
  /etc/letsencrypt/live/mail.truelite.it/fullchain.pem (skipped)
No renewals were attempted.
```

la cosa si può automatizzare inserendo banalmente nel cron il comando, ad esempio creando il file /etc/cron.d/letencrypt con il contenuto:

```
00 23 * * 6  root /root/letsencrypt/letsencrypt-auto renew
```

oppure usare lo script le-renew allegato (da adattare alle proprie esigenze), da inserire in /etc/cron.weekly.

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.