

Servidor web/dades

Actualització d'HTTP a HTTPS amb certificats LetsEncrypt - Setembre de 2022

Cal convertir el servidor HTTP en HTTPS. He descartat les opcions de fer-ho amb un certificat auto-signat (self-signed) o amb un certificat aconseguit a través del Servei d'Informàtica perquè el primer no és acceptat per defecte pels navegadors i perquè el segon mecanisme implica força burocràcia i no sembla que sigui automatitzable.

Això ens deixa l'opció de fer servir certificats emesos per [Let's Encrypt](#), una Autoritat de Certificació sense ànim de lucre que actualment proporciona certificats TLS a 260 milions de llocs web.

Aquesta pàgina conté la descripció detallada del procés d'obtenció dels certificats i la configuració del servidor HTTPS amb Apache a Debian 10.12 "buster".

Desinstal·lació del paquet certbot de la distribució

El paquet certbot ([enllaç](#)) permet configurar automàticament la configuració d'HTTPS amb [Let's Encrypt](#),

automatically configure HTTPS using Let's Encrypt

The objective of Certbot, Let's Encrypt, and the ACME (Automated Certificate Management Environment) protocol is to make it possible to set up an HTTPS server and have it automatically obtain a browser-trusted certificate, without any human intervention. This is accomplished by running a certificate management agent on the web server.

This agent is used to:

1. Automatically prove to the Let's Encrypt CA that you control the website
2. Obtain a browser-trusted certificate and set it up on your web server
3. Keep track of when your certificate is going to expire, and renew it
4. Help you revoke the certificate if that ever becomes necessary.

This package contains the main application, including the standalone and the manual authenticators.

<https://packages.debian.org/buster/certbot>

La versió disponible per Debian 10 és la [0.31.0-1](#), mentre que la versió actual és la 1.30. Per aquest motiu, en comptes del paquet de la distribució, faig servir el [paquet disponible a la web del programa certbot](#).

Començo per desinstal·lar el paquet certbot de la distribució:

```
# apt purge certbot
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer
required:
  python-pyicu python3-acme python3-certbot python3-configargparse python3-
configobj python3-future python3-josepy python3-mock
  python3-parsedatetime python3-pbr python3-requests-toolbelt python3-
rfc3339 python3-tz python3-zope.component python3-zope.event
  python3-zope.hookable python3-zope.interface
Use 'apt autoremove' to remove them.
The following packages will be REMOVED:
  certbot*
0 upgraded, 0 newly installed, 1 to remove and 39 not upgraded.
After this operation, 70.7 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 254784 files and directories currently installed.)
Removing certbot (0.31.0-1+deb10u1) ...
Processing triggers for man-db (2.8.5-2) ...
(Reading database ... 254773 files and directories currently installed.)
Purging configuration files for certbot (0.31.0-1+deb10u1) ...
root@sermnserver:/etc/apache2# apt autoremove
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
  python-pyicu python3-acme python3-certbot python3-configargparse python3-
configobj python3-future python3-josepy python3-mock
  python3-parsedatetime python3-pbr python3-requests-toolbelt python3-
rfc3339 python3-tz python3-zope.component python3-zope.event
  python3-zope.hookable python3-zope.interface
0 upgraded, 0 newly installed, 17 to remove and 39 not upgraded.
After this operation, 6,955 kB disk space will be freed.
Do you want to continue? [Y/n]
(Reading database ... 254769 files and directories currently installed.)
Removing python-pyicu (2.2-2) ...
Removing python3-certbot (0.31.0-1+deb10u1) ...

[...]

Removing python3-zope.event (4.2.0-1) ...
Removing python3-zope.hookable (4.0.4-4+b4) ...
Removing python3-zope.interface (4.3.2-1+b2) ...
```

Instal·lació del gestor de paquets "snapd"

Tot seguit instal·lo el paquet snapd ([enllaç](#)) d'acord amb les [instruccions que hi ha a la web del](#)

programa:

```
# apt install snapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  liblzo2-2 squashfs-tools
The following NEW packages will be installed:
  liblzo2-2 snapd squashfs-tools
0 upgraded, 3 newly installed, 0 to remove and 39 not upgraded.
Need to get 14.4 MB/14.5 MB of archives.
After this operation, 61.5 MB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://ftp.es.debian.org/debian buster/main amd64 squashfs-tools amd64
1:4.3-12+deb10u2 [126 kB]
Get:2 http://ftp.es.debian.org/debian buster/main amd64 snapd amd64
2.37.4-1+deb10u1 [14.3 MB]
Fetched 14.4 MB in 2s (6,188 kB/s)
Selecting previously unselected package liblzo2-2:amd64.
(Reading database ... 253947 files and directories currently installed.)
Preparing to unpack .../liblzo2-2_2.10-0.1_amd64.deb ...
Unpacking liblzo2-2:amd64 (2.10-0.1) ...
Selecting previously unselected package squashfs-tools.
Preparing to unpack .../squashfs-tools_1%3a4.3-12+deb10u2_amd64.deb ...
Unpacking squashfs-tools (1:4.3-12+deb10u2) ...
Selecting previously unselected package snapd.
Preparing to unpack .../snapd_2.37.4-1+deb10u1_amd64.deb ...
Unpacking snapd (2.37.4-1+deb10u1) ...
Setting up liblzo2-2:amd64 (2.10-0.1) ...
Setting up squashfs-tools (1:4.3-12+deb10u2) ...
Setting up snapd (2.37.4-1+deb10u1) ...
Created symlink /etc/systemd/system/multi-
user.target.wants/snapd.seeded.service →
/lib/systemd/system/snapd.seeded.service.
Created symlink /etc/systemd/system/cloud-
final.service.wants/snapd.seeded.service →
/lib/systemd/system/snapd.seeded.service.
Created symlink /etc/systemd/system/multi-user.target.wants/snapd.service →
/lib/systemd/system/snapd.service.
Created symlink /etc/systemd/system/sockets.target.wants/snapd.socket →
/lib/systemd/system/snapd.socket.
Processing triggers for mime-support (3.62) ...
Processing triggers for libc-bin (2.28-10+deb10u1) ...
Processing triggers for man-db (2.8.5-2) ...
Processing triggers for desktop-file-utils (0.23-4) ...

root@sermnserver:/etc/apache2# snap install core ; snap refresh core
2022-09-27T13:24:51+02:00 INFO Waiting for restart...
core 16-2.57.1 from Canonical✓ installed
Channel latest/stable for core is closed; temporarily forwarding to stable.
```

```
2022-09-27T13:25:30+02:00 INFO Waiting for automatic snapd restart...
core 16-2.57.2 from Canonical✓ refreshed
```

Instal·lació del paquet certbot dels desenvolupadors

Instal·lo el paquet certbot per snapd distribuït pels desenvolupadors,

```
# snap install --classic certbot
certbot 1.30.0 from Certbot Project (certbot-eff✓) installed
```

i comprovo els contingut del paquet,

```
# ls -l /var/lib/snapd/snaps/certbot_2344.snap
-rw----- 2 root root 46661632 Sep 27 15:20
/var/lib/snapd/snaps/certbot_2344.snap

# unsquashfs -ll /var/lib/snapd/snaps/certbot_2344.snap | more
Parallel unsquashfs: Using 2 processors
6937 inodes (7574 blocks) to write

drwxr-xr-x root/root           190 2022-09-07 20:15 squashfs-root
drwxr-xr-x root/root           229 2022-09-07 20:14 squashfs-root/bin
-rw-r--r-- root/root          8834 2022-09-07 20:14 squashfs-
root/bin/Activate.ps1
-rw-r--r-- root/root          2244 2022-09-07 20:14 squashfs-
root/bin/activate
-rw-r--r-- root/root          1296 2022-09-07 20:14 squashfs-
root/bin/activate.csh
-rw-r--r-- root/root          2448 2022-09-07 20:14 squashfs-
root/bin/activate.fish
-rwxr-xr-x root/root           215 2022-09-07 20:14 squashfs-
root/bin/certbot
-rwxr-xr-x root/root           216 2022-09-07 20:14 squashfs-
root/bin/distro

[...]

-rw-r--r-- root/root          35611 2021-07-13 05:11 squashfs-
root/usr/share/python-wheels/wheel-0.34.2-py2.py3-none-any.whl
drwxr-xr-x root/root           77 2022-09-07 20:14 squashfs-
root/usr/share/python3
-rw-r--r-- root/root           412 2020-02-18 09:06 squashfs-
root/usr/share/python3/debian_defaults
drwxr-xr-x root/root           107 2022-09-07 20:14 squashfs-
root/usr/share/python3/debpython
-rw-r--r-- root/root          1877 2020-03-13 13:20 squashfs-
root/usr/share/python3/debpython/__init__.py
-rw-r--r-- root/root          3278 2020-03-13 13:20 squashfs-
```

```

root/usr/share/python3/debpython/files.py
-rw-r--r-- root/root          13511 2020-03-13 13:20 squashfs-
root/usr/share/python3/debpython/interpreter.py
-rw-r--r-- root/root          1886 2020-03-13 13:20 squashfs-
root/usr/share/python3/debpython/option.py
-rw-r--r-- root/root          14257 2020-03-13 13:20 squashfs-
root/usr/share/python3/debpython/version.py
-rwxr-xr-x root/root          11720 2022-09-07 20:14 squashfs-
root/usr/share/python3/py3versions.py

```

Finalment, creo un enllaç a la comanda certbot per tal que es pugui executar:

```
# ln -s /snap/bin/certbot /usr/bin/certbot
```

Obtenir i instal·lar el certificat

Executo la comanda següent per descarregar un certificat i fer que Certbot editi automàticament la configuració d'Apache per servir-lo i posar en marxa l'accés HTTPS en un únic pas:

```
# certbot --apache
```

Alternativament, la comanda següent descarrega el certificat però no fa cap canvi als fitxers de configuració, els quals s'hauran d'editar posteriorment.

```
# certbot certonly --apache
```

En aquest cas, faig servir la segona opció perquè prefereixo anar pas a pas, però primer faig un simulacre per comprovar que tot està ben configurat:

```

# certbot certonly --dry-run --apache -d uab.cat -d sermn.uab.cat
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Enter email address (used for urgent renewal and security notices)
(Enter 'c' to cancel): miquel.cabanas@uab.cat

- - - - -
- -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.3-September-21-2022.pdf. You must
agree in order to register with the ACME server. Do you agree?
- - - - -
- -
(Y)es/(N)o: Y
Account registered.
Simulating a certificate request for uab.cat and sermn.uab.cat

Certbot failed to authenticate some domains (authenticator: apache). The
Certificate Authority reported these problems:
  Domain: uab.cat
  Type:   unauthorized

```

Detail: 158.109.120.133: Invalid response from https://www.uab.cat/.well-known/acme-challenge/LiGiSsAoZIuH6bEXDBETZhvnijDGcnOfNqyWERSsx9Y: 404

Hint: The Certificate Authority failed to verify the temporary Apache configuration changes made by Certbot. Ensure that the listed domains point to this Apache server and that it is accessible from the internet.

Some challenges have failed.

Ask for help or search for solutions at <https://community.letsencrypt.org>. See the logfile /var/log/letsencrypt/letsencrypt.log or re-run Certbot with -v for more details.

El programa no aconsegueix comprovar que controlo el domini uab.cat i per això no genera el certificat.

En aquests casos, la millor opció és [general i descarregar el certificat de forma manual](#).

```
# certbot certonly --dry-run --manual --preferred-challenges http -d uab.cat
-d sermn.uab.cat
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Simulating a certificate request for uab.cat and sermn.uab.cat

- - - - -
- -
Create a file containing just this data:

gw2YmTM7enAzpx6_AKESSlrEcab1bRJv-
h_UgwduCTM.nkhY9qXPoLKISUKPBd_zwIeekrXGjCHWaN4VHmBAJeE

And make it available on your web server at this URL:

http://uab.cat/.well-known/acme-challenge/gw2YmTM7enAzpx6_AKESSlrEcab1bRJv-h
_UgwduCTM

- - - - -
- -
Press Enter to Continue
```

De nou, aquest camí tampoc em serveix perquè no tinc accés al servidor web de la UAB, de forma que no puc crear el fitxer necessari per confirmar que controlo el domini “uab.cat”.

Referències

- [LetsEncrypt - Debian Wiki](#)
- [Certbot Instructions | Certbot](#)
- [How To Secure Apache with Let's Encrypt on Debian 10 | DigitalOcean.](#)
- [Use Certbot to Enable HTTPS with NGINX on Debian | Linode.](#)

- [Let's Encrypt.](#)
- [How to Setup Free SSL Certificate for Apache on Debian 10.](#)
- [How to install Let's Encrypt on Apache2 | UpCloud.](#)

From:
<https://sermn.uab.cat/wiki/> - **SeRMN Wiki**

Permanent link:
https://sermn.uab.cat/wiki/doku.php?id=informatica:servidor_internet_2009_http_to_https&rev=1664291010

Last update: **2022/09/27 17:03**

