










Linuxtricks

[Accueil](#)[Blogue](#)











-  [Tout le blogue](#)
-  [Logiciels libres](#)
-  [Actus Linuxtricks](#)
-  [Le sac de chips](#)

[Wiki](#)

HTTPS

-  [VMware / Windows Server](#)
-  [Console](#)
-  [Env. de bureau](#)
-  [Généralités Linux](#)
-  [Logiciels](#)
-  [Scripts et Programmation](#)
-  [Services et Serveurs](#)
-  [Calculate / Gentoo](#)
-  [Fedora/CentOS](#)
-  [Debian](#)
-  [Autres distribs](#)
-  [Hors Linux](#)
-  [Cisco](#)
-  [En rédaction](#)
-  [Archives](#)

[COAGUL](#)

-  [Site coagul.org](#)
-  [Audit participatif pub](#)
-  [Conférence création RPM](#)
-  [Atelier Découverte PHPBoost](#)
-  [Atelier Conteneurs \(LXC et ProxMox\)](#)
-  [Atelier Owncloud](#)
-  [Atelier Débutant Installation Linux Mint - 2016](#)
-  [Atelier Débutant Installation Linux Mint - 2019](#)
-  [Table ronde : Utiliser Internet](#)
-  [marjo21 - Collecteur de liens](#)

[à propos](#)

-  [Support et Contact](#)
-  [Communauté Linuxtricks](#)
-  [Statut Services Linuxtricks](#)
-  [Mon Github](#)
-  [Ma chaine Youtube](#)
-  [RSS](#)
 -  [Wiki](#)
 -  [Blogue](#)
 -  [Commentaires](#)

-  [Miroir Calculate Linux](#)

-  [Liens utiles](#)

-  [Linuxfr.org](#)
-  [Le journal du hacker](#)
-  [CalculateLinux](#)
-  [pkgs.org](#)
-  [Overlays Gentoo](#)
-  [NetMarketShare](#)
-  [kernel.org](#)
-  [Distrowatch](#)
-  [Mirror Service](#)
-  [CERT-FR](#)
-  [CNIL](#)
-  [Loi n° 78-17 du 6 janvier 1978](#)

Recherche...



Faire un don

Options du module Wiki

Accueil

Explorateur

Accueil

Wiki

Services et serveurs

Let's Encrypt : Mise en place

Services et serveurs

Let's Encrypt : Mise en place

Historique

Version imprimable



Introduction

Let's Encrypt est une autorité de certification qui fournit des certificats gratuits X.509 pour le protocole cryptographique TLS. C'est un moyen d'un processus automatisé destiné à se passer du processus complexe actuel impliquant la création manuelle, la validation, la signature, l'installation et le renouvellement des certificats pour la sécurisation des sites internet. Le projet vise à généraliser l'usage de connexions sécurisées sur l'internet. De nombreux sponsors soutiennent ce projet comme Akamai, CloudFlare, Comodo, DigiNotar, Dyn, Fastly, GitHub, Google, IBM, Let's Encrypt, LinkedIn, Microsoft, NetScout Systems, OpenDNS, Oracle, Rackspace, Red Hat, Mozilla, Gemalto...

Prérequis

Il est nécessaire de satisfaire quelques prérequis pour l'installation, à savoir :

Avoir la commande **git** à disposition

Avoir un serveur connecté à Internet avec un nom de domaine pleinement qualifié (FQDN)

Avoir les droits d'administration ... évident !

Enfin, mettre en service les dépôts EPEL avec **yum install epel-release**.

J'ai effectué mes tests sur une machine Gentoo Linux. Let's Encrypt n'est pas noté comme stable, j'ai dû ajouter **--debug** à mes commandes.

Installation

Pour commencer, on clone le dépôt git :

Code BASH :

 Copier vers le presse-papier

```
git clone https://github.com/certbot/certbot /opt/certbot
```

d ensuite dans le dossier en question pour exécuter ensuite les commandes :

Code BASH :

 Copier vers le presse-papier

```
cd /opt/certbot
```

ande à utiliser sera **./certbot-auto** au lieu de **certbot**

HTTPS) S, il est possible d'installer le paquet certbot présent dans EPEL :

Code BASH :

 Copier vers le presse-papier

```
yum install certbot
```

io, on peut installer app-crypt/certbot :

Code BASH :

 Copier vers le presse-papier

```
emerge -av app-crypt/certbot
```

Ération du premier certificat

utiliser la commande «oneliner» qui est plus simple à utiliser :

Code BASH :

 Copier vers le presse-papier

```
certbot certonly -d oxygen.linuxtricks.fr -m adrien.d@mageialinux-online.org --agree-tos -a webroot
--webroot-path /var/www/localhost/htdocs/
```

r : ne générer que le certificat

en.linuxtricks.fr : le domaine à certifier

en.d@mageialinux-online.org : email associé au certificat

tos : accepter les conditions d'utilisation

oot : Obtenir un certificat en écrivant dans la racine d'un serveur fonctionnel (apache par exemple)

alone : Obtenir un certificat en lançant un serveur web autonome (port 80 doit être dispo, et pas d'apache)

oot-path /var/www/localhost/htdocs/ : la racine du site en question (pour webroot) ou un dossier disponible pour écrire les fichiers nécessaires

ait, on a un super message nous indiquant que l'opération a été faite avec succès :

Citation :

IMPORTANT NOTES:

- Congratulations! Your certificate and chain have been saved at /etc/letsencrypt/live/oxygen.linuxtricks.fr/fullchain.pem. Your cert will expire on 2016-08-14. To obtain a new version of the certificate in the future, simply run Certbot again.
- If you like Certbot, please consider supporting our work by:

rs se créent dans **/etc/letsencrypt/live/nom-du-domaine**.

ieurs fichiers :

y.pem : c'est la clé privée pour le certificat. Doit être gardé secret. Le serveur doit y accéder (certIFICATEKEYFILE)

n : le certificat du serveur. (SSLCertificateFile) Apache < 2.4

m : les certificats requis par le navigateur (SSLCertificateChainFile)

n.pem : tous les certificats (chain.pem + cert.pem). Apache >= 2.4 (SSLCertificateFile)

HTTPS

Configurer le virtualhost sous Apache

Ensuite configurer apache, pour renseigner le certificat nouvellement généré. Editer votre fichier de virtualhost (peut varier selon votre OS) :

Exemple :

Code BASH :

 Copier vers le presse-papier

```
vi /etc/apache2/vhosts.d/00_default_ssl_vhost.conf
```

Exemple :

Code BASH :

 Copier vers le presse-papier

```
vi /etc/httpd/conf.d/ssl.conf
```

Remplacer les trois lignes :

Code BASH :


 Copier vers le presse-papier

```
SSLCertificateFile /etc/letsencrypt/live/www.linuxtricks.fr/fullchain.pem
SSLCertificateKeyFile /etc/letsencrypt/live/www.linuxtricks.fr/privkey.pem
SSLCertificateChainFile /etc/letsencrypt/live/www.linuxtricks.fr/chain.pem
```

Redémarrer apache après :

Exemple :

Code BASH :

 Copier vers le presse-papier

```
/etc/init.d/apache2 reload
```

Exemple :

Code BASH :

 Copier vers le presse-papier

```
systemctl reload httpd
```

Renouveler un certificat

uveler un certificat on exécute la commande «oneliner» suivante :

Code BASH :

 Copier vers le presse-papier

```
certbot certonly -d oxygen.linuxtricks.fr -m adrien.d@mageialinux-online.org --agree-tos -a webroot
--webroot-path /var/www/localhost/htdocs/ --renew-by-default
```

HTTPS a même que la première, avec **--renew-by-default** en plus pour éviter la question et que ça soit gérable par un

nérez tous les premiers du mois à minuit votre script et c'est joué !

:

Code BASH :

 Copier vers le presse-papier

```
vi /root/renew-lets.sh
```

Code BASH :

 Copier vers le presse-papier

```
#!/bin/bash
certbot certonly -d oxygen.linuxtricks.fr -m adrien.d@mageialinux-online.org --agree-tos -a webroot
--webroot-path /var/www/localhost/htdocs/ --renew-by-default
systemctl reload httpd
```

ontab :

Code BASH :

 Copier vers le presse-papier

```
0 0 1 * * /root/renew-lets.sh > /root/renew-lets.log
```

figurer le virtualhost HTTP pour rediriger le trafic HTTPS

, mais maintenant, voici comment, dans le virtualhost d'apache, on peut configurer pour rediriger **tout le trafic** PS.

lets tout le virtualhost du site **marjo21.linuxtricks.fr** mais regardez uniquement à partir du commentaire #Lets

Code BASH :

 Copier vers le presse-papier

```
<VirtualHost *:80>
    ServerName www.linuxtricks.fr
    ServerAlias marjo21.linuxtricks.fr
    DocumentRoot "/home/marjo21/public_html/"
    <Directory "/home/marjo21/public_html/">
        Options Indexes FollowSymlinks
        AllowOverride All
        Require all granted
    </Directory>
    # Redirection Lets Encrypt
    RewriteEngine on
    RewriteCond %{REQUEST_URI} !^/.well-known/acme-challenge/
    RewriteRule (.*) https://marjo21.linuxtricks.fr$1 [R=301,L]
```

```
</VirtualHost>
<VirtualHost *:443>
    ServerName marjo21.linuxtricks.fr
    ServerAlias marjo21.linuxtricks.fr
    # Certificat Lets Encrypt
    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/marjo21.linuxtricks.fr/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/marjo21.linuxtricks.fr/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/marjo21.linuxtricks.fr/chain.pem
    DocumentRoot "/home/marjo21/public_html/"
    <Directory "/home/marjo21/public_html/">
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

HTT

figurer le htaccess de votre CMS

ns CMS, il peut y avoir un problème d'accès notamment à cause de règles. (C'est le cas avec PHPBoost)
 placer ce code suivant

Code TEXT :

 Copier vers le presse-papier

```
RewriteCond %{REQUEST_URI} ^/\.well-known/acme-challenge/
RewriteRule "^.well-known/acme-challenge" - [L]
```

lignes :

Code TEXT :

 Copier vers le presse-papier

```
RewriteEngine on
RewriteBase /
```

ques problèmes

ecutableNotFound

is de cette erreur :

Code TEXT :

 Copier vers le presse-papier

```
An unexpected error occurred:
ExecutableNotFound
Please see the logfile 'certbot.log' for more details.
```

› supprimer le dossier local du programme :

Code BASH :

 Copier vers le presse-papier

```
rm -rf /root/.local/share/letsencrypt
```

la commande et ça devrait rouler.

rbidden

is où le site possède un fichier .htaccess, et que les URL non standards du CMS sont bloquées, le message suivant

Code RUBY :

[📋 Copier vers le presse-papier](#)

```
Domain: www.mageialinux-online.org
Type:   unauthorized
Detail: Invalid response from
http://www.mageialinux-online.org/.well-known/acme-
challenge/VxFva1I_aRm7WYwWJjeXhzqDFyvdhEvkF58_qKq0y7c:
"<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
```

la section **Configurer le htaccess de votre CMS**.



Cette page a été vue 9642 fois

[r PHPBoost](#) | [Mentions légales](#)

cs est mis à disposition selon les termes : [Licence Creative Commons](#)

