

PARTIE A - HTTPS HTTPS : Hypertext transfert protocole secure

Création et utilisation d'un certificat auto-signé : on va premièrement procéder par l'installation d'Open SSL et la commande requise est:

```
apt-get install openssl
```

et ensuite, nous allons créer un répertoire pour la création des certificats en utilisant la commande

```
mkdir /etc/ssl/localcerts
```

l'étape suivant servira à générer un certificat : création de certificat le certificat se crée dans DIR=/etc/ssl/localcerts

la commande utilisée pour la création du certificat est :

```
openssl req -x509 -newkey rsa:4096 -nodes -keyout $DIR/mydomainkey.key -out $DIR/mydomaincert.pem -days 365
```

explication de la commande ci-dessus :

- -newkey rsa:4096 : Pour une clé RSA de 4096 bits
- -keyout : La clef
- -out : Le certificat
- -nodes : Pas de phrase de passe lors de l'utilisation pour le déverrouiller (no DES)
- -days 365 : Correspondant à la durée de validité du certificat

la Création du certificat TLS dans le répertoire /etc/ssl/localcert :

```
root@web1:~# tree -L 1 /etc/fail2ban
/etc/fail2ban
├── action.d
├── fail2ban.conf
├── fail2ban.d
├── filter.d
├── jail.conf
├── jail.d
├── paths-arch.conf
├── paths-common.conf
├── paths-debian.conf
└── paths-opensuse.conf

5 directories, 6 files
root@web1:~# cat /etc/resolv.conf
nameserver 10.31.96.54
nameserver 10.31.96.64
root@web1:~#
```

Paramétrons apache pour activer le Virtualhost SSL par défaut : pour le faire, on aura besoins des

commandes tels que :

Activation du Vhost SSL par défaut pour Apache et configuration

```
a2ensite default-ssl
```

Activation du module ssl pour Apache

```
a2enmod ssl
```

Il y a quelques modifications à effectuer dans le sur le Vhost SSL par défaut.

```
nano /etc/apache2/sites-available/default-ssl.conf
```

```
GNU nano 7.2 /etc/apache2/sites-available/default-ssl.conf
#Include conf-available/serve-cgi-bin.conf

# SSL Engine Switch:
# Enable/Disable SSL for this virtual host.
SSLEngine on

# A self-signed (snakeoil) certificate can be created by installing
# the ssl-cert package. See
# /usr/share/doc/apache2/README.Debian.gz for more info.
# If both key and certificate are stored in the same file, only the
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/ssl/localcerts/mydomaincert.pem
SSLCertificateKeyFile /etc/ssl/localcerts/mydomainkey.key
```

Vérifions que le port 443 est bien ouvert (LISTEN) : La commande :

```
netstat -tuln | grep :443
```

est utilisée pour vérifier si le port 443 est ouvert et en écoute sur un système Linux. On pouvait bien utiliser la commande

```
netstat -nat
```

mais la différence est que netstat -nat affiche toutes les connexions actives sur le système, tandis que netstat -tuln | grep :443 filtre spécifiquement les connexions TCP en écoute sur le port 443.

```
root@web1:~# netstat -tuln | grep :443n | grep :443
tcp6      0      0  :::443          :::*              LISTEN
root@web1:~#
```

Tester avec un navigateur : **voici mon certificat : le certificat n'a pas été délivré par une autorité de confiance du coup ils affichent une erreur indiquant que le certificat n'est pas valide.**



connection avec TLS :

```
ôte : 10.31.96.2   Nom d'utilisateur : intra
atut : Connexion TLS établie.
atut : Connecté
atut : Récupération du contenu du dossier...
atut : Contenu du dossier « /home/intra » affiché avec succès
```

Configurer de la même manière SSL/TLS pour intranet par exemple : le processus est le même que pour www,extranet, wiki : une fois dans web1 :

```
nano /etc/apache2/sites-available/intranet.m2l.org.conf
```

```
<VirtualHost *:443>
    ServerAdmin webmaster@beaupeyrat.com
    ServerName intranet.org
    ServerAlias intranet.m2l.org
    DocumentRoot /home/htdocs/m2l.org/intranet/

    ErrorLog /var/log/apache2/www-error.log
    CustomLog /var/log/apache2/www-access.log combined

    <Directory /home/htdocs/m2l.org/intranet/>
        Require all granted
    </Directory>

    # Activation de SSL
    SSLEngine on
    SSLCertificateFile /etc/ssl/localcerts/mydomaincert.pem
    SSLCertificateKeyFile /etc/ssl/localcerts/mydomainkey.key
</VirtualHost>
```

PARTIE B - FTPS (File Transfer Protocol)

le processus est le même, il faut cependant créer un répertoire où stocker le certificat et la clé qu'on va générer: **NB:vous devez bien aller dans FTP et non sur le web pour effectuer ce travail**

```
mkdir /etc/proftpd/ssl/
</file bash>
```

Génération du certificat SSL auto-signé et de la clé :

```
<file bash>
DIR=/etc/proftpd/ssl/
```

```
openssl req -x509 -newkey rsa:4096 -nodes -keyout
$DIR/mydomainkey.key -out $DIR/mydomaincert.pem -days 365
```

l'explication de la commande se trouve dans **la partie A**

Nous allons Éditer le fichier /etc/proftpd/proftpd.conf et activer TLS en décommentant la ligne suivante:

```
#
# This is used for FTPS connections
#
Include /etc/proftpd/tls.conf
#
# This is used for SFTP connections
```

À présent nous éditons le fichier `/etc/proftpd/tls.conf` et paramètrons au minimum les directives suivantes et paramètrons les directives suivantes :

nano `/etc/proftpd/tls.conf`

Réaliser dans les deux captures d'ecrans ci-dessous:

1. • TLSEngine (activer/désactiver TLS)
2. • TLSLog (logguer les connexions chiffrées dans un fichier à part)
3. • TLSRSACertificateFile (chemin vers le certificat)
4. • TLSRSACertificateKeyFile (chemin vers la clé)

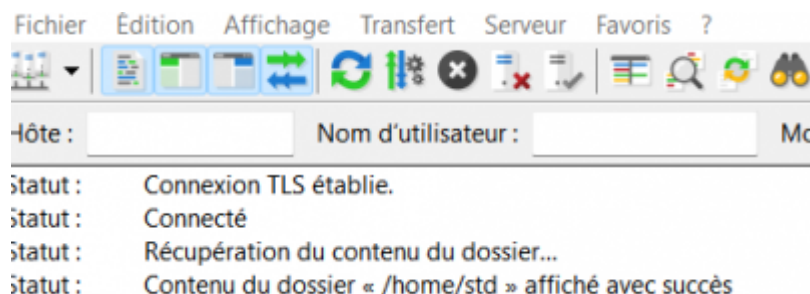
les voici : • TLSRSACertificateFile (chemin vers le certificat) • TLSRSACertificateKeyFile (chemin vers la clé)

```
GNU nano 7.2 /etc/proftpd/tls.conf
#TLSProtocol                                SSLv23
#
# Server SSL certificate. You can generate a self-signed certificate using
# a command like:
#
# openssl req -x509 -newkey rsa:1024 \
#   -keyout /etc/ssl/private/proftpd.key -out /etc/ssl/certs/proftpd.crt \
#   -nodes -days 365
#
# The proftpd.key file must be readable by root only. The other file can be
# readable by anyone.
#
# chmod 0600 /etc/ssl/private/proftpd.key
# chmod 0640 /etc/ssl/private/proftpd.key
#
# TLSRSACertificateFile                      /etc/proftpd/ssl/mydomaincert.pem
# TLSRSACertificateKeyFile                  /etc/proftpd/ssl/mydomainkey.key
```

- TLSEngine (activerTLS)

```
GNU nano 7.2 /etc/proftpd/tls.conf
#
# Proftpd sample configuration for FTPS connections.
#
# Note that FTPS impose some limitations in NAT traversing.
# See http://www.castaglia.org/proftpd/doc/contrib/ProFTPD-mini-HOWTO-TLS.h
# for more information.
#
# IfModule mod_tls.c>
#
# TLSEngine                                on
# TLSLog                                  /var/log/proftpd/tls.log
# TLSProtocol                              SSLv23
```

3. Tester avec un client FTP



From:

<https://sisr2.beaupeyrat.com/> - **Documentations SIO2 option SISR**

Permanent link:

https://sisr2.beaupeyrat.com/doku.php?id=sisr1-g6:ssl_tls

Last update: **2024/03/25 09:41**

