Ariyathashan Nilanth
1TSIOC - SISR

05/03/13

Mise en place d'un serveur web à travers HTTPS

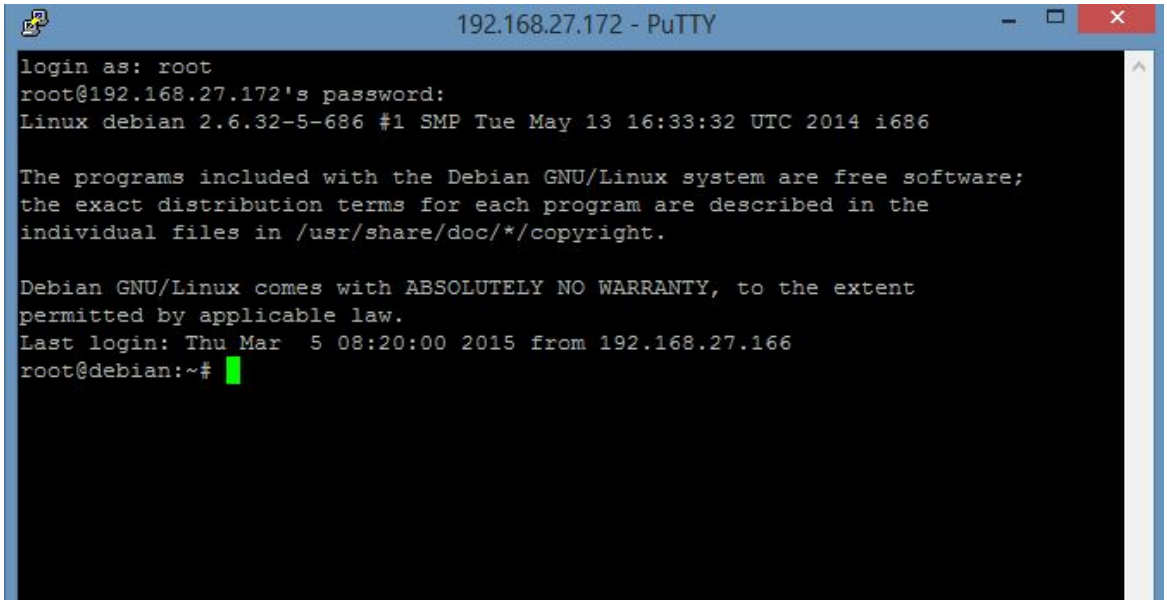
Objectifs: Être capable d'installer et de sécuriser un serveur web.
Conditions de réalisation: Environnement : debian
Durée: 2 H

Vous allez voir à travers ce TP, comment installer, paramétrer et sécuriser un serveur web sous linux en utilisant apache et les certificats.
Pour la réalisation de ce TP, vous aurez besoin d'une machine virtuelle debian. Vérifiez bien que votre carte réseau est en accès par pont et que vous avez bien une adresse IP sur le même réseau que la salle à l'aide de la commande ifconfig.

Vérification d'adresse IP à l'aide de la commande **ifconfig**

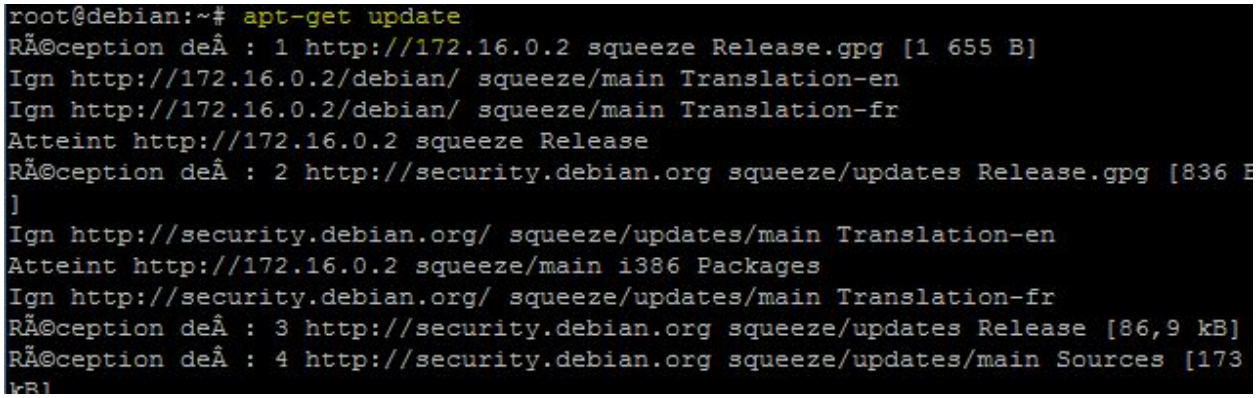
```
root@debian:~# ifconfig
eth2      Link encap:Ethernet  HWaddr 08:00:27:62:e9:81
          inet adr:192.168.27.172  Bcast:192.168.27.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe62:e981/64 Scope:Lien
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:1354 (1.3 KiB)  TX bytes:1026 (1.0 KiB)

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:8 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:560 (560.0 B)  TX bytes:560 (560.0 B)
```

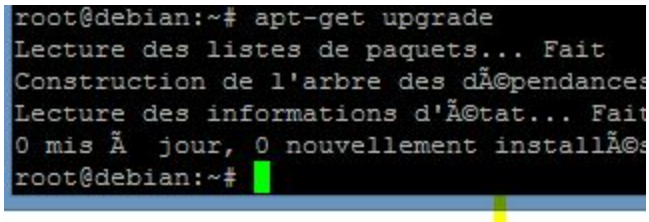
1. Pour administrer votre serveur, vous utiliserez un accès distant à l'aide de la commande ssh. Pour cela, vous pouvez taper la commande ssh root@IP_debian. On vous demande de vérifier que la signature du serveur est bien la bonne en l'acceptant puis le mot de passe de connexion. Ensuite, vous pouvez travailler comme si vous étiez sur votre serveur avec l'avantage du copier/coller.
En etant sur Windows , on peut utiliser Putty pour se connecter à distance avec une machine Debian à l'aide de son adresse IP.



2. Vous allez tout d'abord mettre à jour votre système.

Mise à jour du système avec les commandes **apt-get update** et **apt-get upgrade**





3. Sur votre machine debian, vous avez déjà tout ce qu'il vous faut. Cependant, apache utilise des modules additionnels pour augmenter ses fonctionnalités.
Ces modules sont présents dans le répertoire **/etc/apache2/mods-available/**
Pour qu'ils soient actifs, il faut placer un lien (un raccourci) dans le répertoire **/etc/apache2/mods-enabled/**
Cependant une commande peut le faire pour vous : **a2enmod** (apache2 enabled module).
Pour activer le support du https : **a2enmod ssl**. Il faut redémarrer le service.

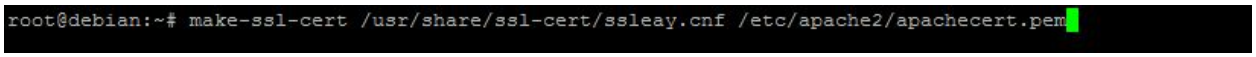
Activation du support du https avec la commande **a2enmod ssl**.

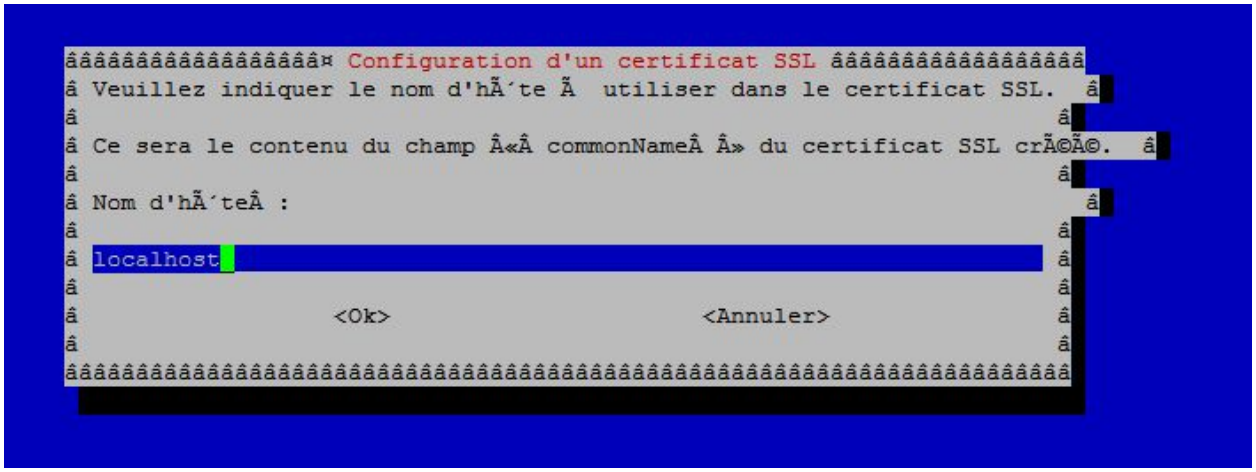
```
root@debian:~# a2enmod
Your choices are: actions alias asis auth_basic auth_digest authn_alias authn_an
on authn_dbd authn_dbm authn_default authn_file authnz_ldap authz_dbm authz_defa
ult authz_groupfile authz_host authz_owner authz_user autoindex cache cern_meta
cgi cgid charset_lite dav dav_fs dav_lock dbd deflate dir disk_cache dump_io env
 expires ext_filter file_cache filter headers ident imagemap include info ldap l
og_forensic mem_cache mime mime_magic negotiation php5 proxy proxy_ajp proxy_bal
ancer proxy_connect proxy_ftp proxy_http proxy_scgi reqtimeout rewrite setenvif
speling ssl status substitute suexec unique_id userdir usertrack version vhost_a
lias
Which module(s) do you want to enable (wildcards ok)?
ssl
Enabling module ssl.
See /usr/share/doc/apache2.2-common/README.Debian.gz on how to configure SSL and
 create self-signed certificates.
Run '/etc/init.d/apache2 restart' to activate new configuration!
root@debian:~#
```

Redémarrage du service avec la commande **service apache2 restart**

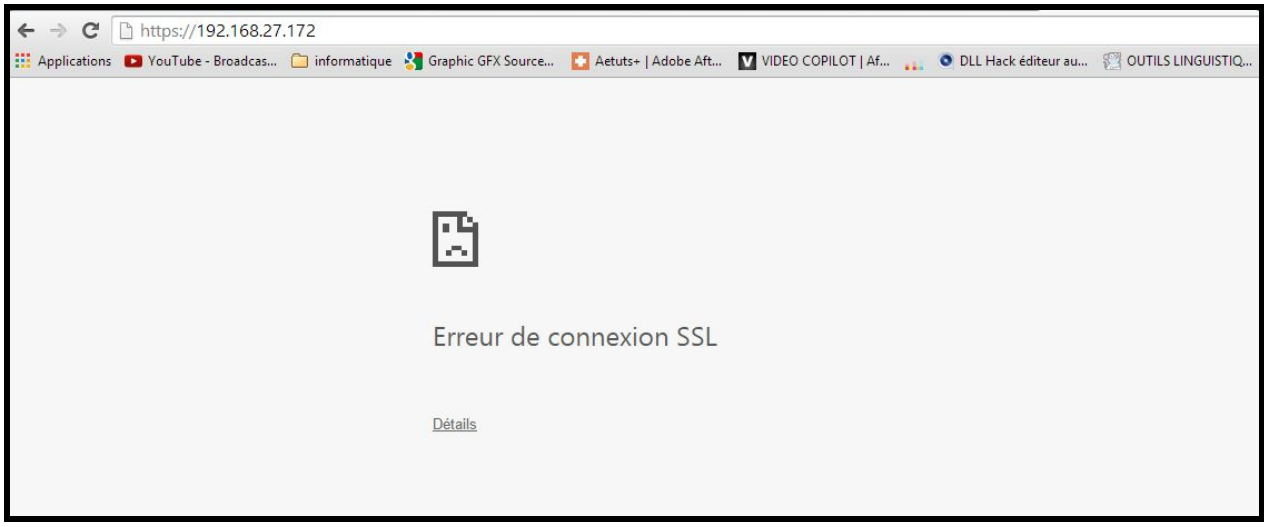
```
root@debian:~# service apache2 restart
Restarting web server: apache2 ... waiting .
root@debian:~#
```

4. Qui dit https dit certificat.
Vous allez créer votre certificat à l'aide de la commande make-ssl-cert.
Cette commande va vous permettre de créer votre certificat à l'aide d'un modèle.
Pour cela, tapez **make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /etc/apache2/apachecert.pem**
En fait ce fichier contiendra votre certificat ainsi que votre clé privée.

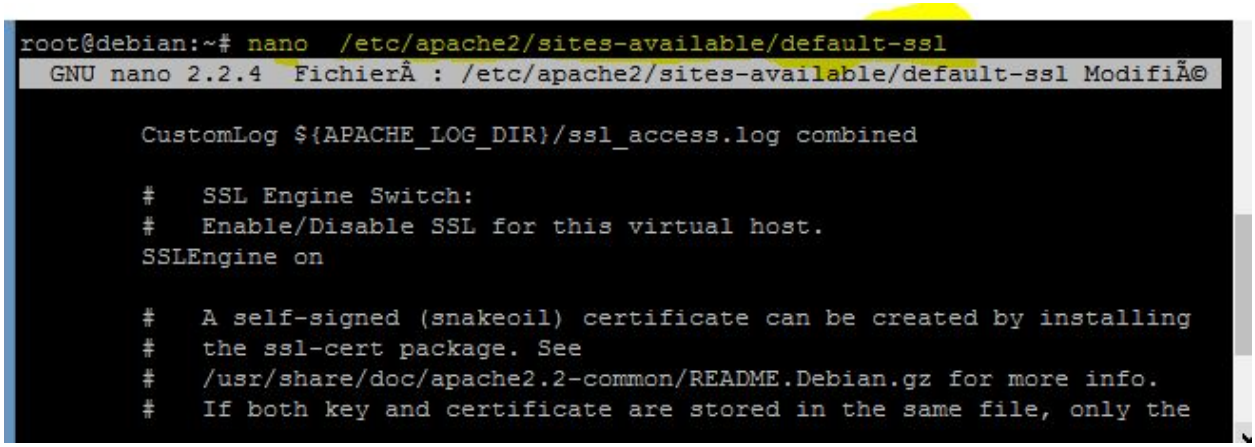


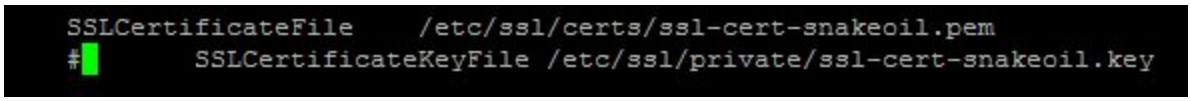


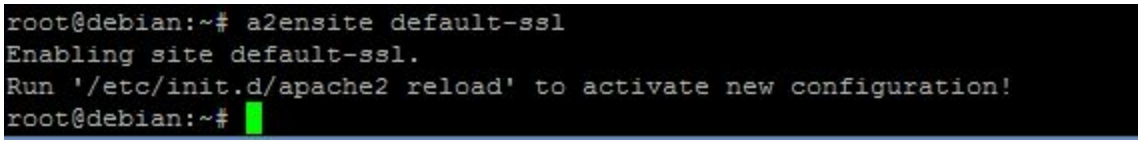
5. Testez le bon fonctionnement de votre serveur en utilisant le protocole https. Que se passe t il ?



6. Vous allez dire à apache de prendre en compte votre certificat.
Pour cela, vous devez modifier le fichier /etc/apache2/sites-available/default-ssl et adaptant la ligne SSLCertificateFile et en commentant la ligne SSLCertificateKeyFile car vous n'avez pas de clé privée séparée.
Ensuite il faut activer votre site sécurisé : **a2ensite default-ssl**







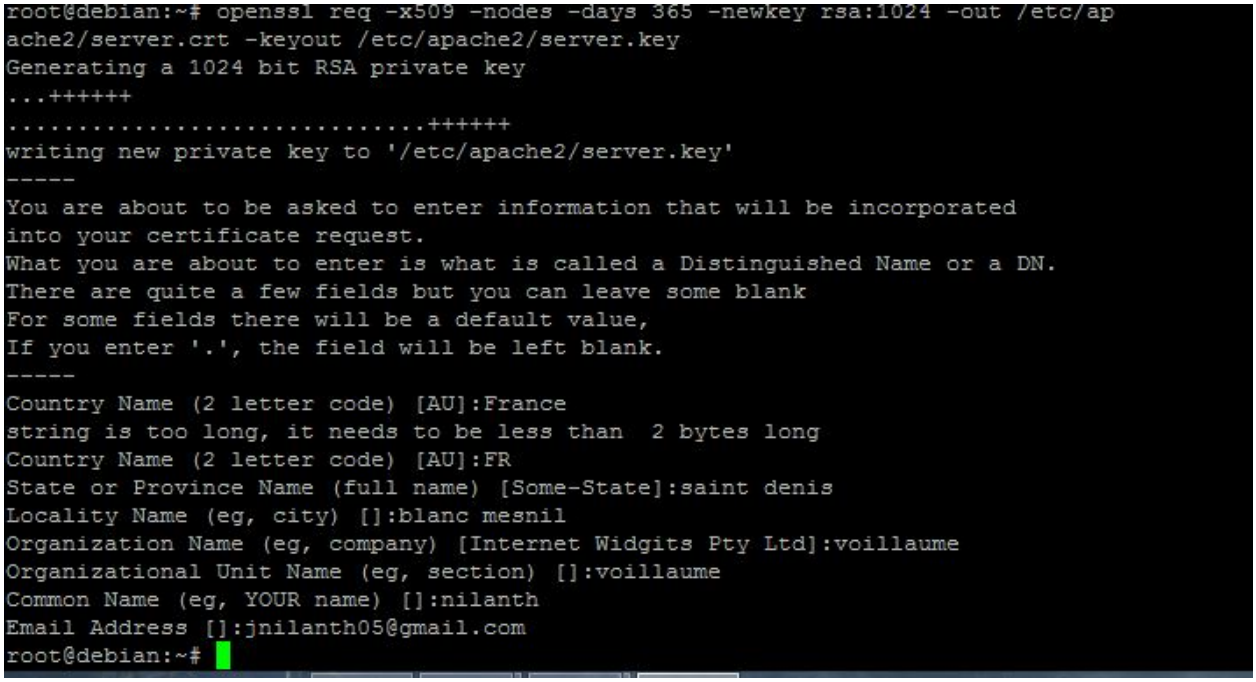
7. Testez le bon fonctionnement de votre serveur en utilisant le protocole https. Que se passe t il ?

10. Tout cela fonctionne mais vous n'avez pas eu la main sur la configuration de votre certificat. Vous allez maintenant créer un nouveau certificat où vous allez choisir toutes les caractéristiques.
Pour cela, vous allez utiliser openssl en utilisant la commande suivante :
openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key

où

- days indique la durée de validité,
- newkey indique le type de cryptage et la taille,
- out l'emplacement du certificat et
- keyout l'emplacement de la clé privée.

Il faut répondre à toutes les questions puis modifier la configuration de apache pour accepter votre nouveau certificat.


root@debian:~# openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out /etc/ap
ache2/server.crt -keyout /etc/apache2/server.key
Generating a 1024 bit RSA private key
...++++++
.............................++++++
writing new private key to '/etc/apache2/server.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:France
string is too long, it needs to be less than 2 bytes long
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:saint denis
Locality Name (eg, city) []:blanc mesnil
Organization Name (eg, company) [Internet Widgits Pty Ltd]:voillaume
Organizational Unit Name (eg, section) []:voillaume
Common Name (eg, YOUR name) []:nilanth
Email Address []:jnilanth05@gmail.com
root@debian:~#