

TP EXAMEN

APACHE 2.4 Installer, configurer Apache 2 et SSH
Admin LINUX Debian SUR DEBIAN 11

Matière : Administration Systèmes et Réseaux (Admin Linux Debian 11)

Niveau universitaire : FI GLSID 2 (23-24)

Professeur : M. KHIAT AZEDDINE

Durée de l'épreuve : 2H

Mentions spéciales : DOCUMENTATION AUTORISEE

Nom & Prénom de l'étudiant :

BOUHKKA Abdelilah

Sommaire

I. Contexte	1
II. Consignes et Cahier des Charges	1
III. Objectifs	1
IV. Livrables	2
V. Préparation de l'Environnement	2
VI. Instructions	3
VII. Installation d'Apache 2.4	3
VIII. Configuration de l'Accès HTTP	5
IX. Configuration de l'Accès HTTPS	6
X. Redirection des Requêtes HTTP vers HTTPS	9
XI. Configuration de l'Accès SSH	10
XII. Conclusion	11

I. Contexte

Vous êtes un administrateur système et réseaux dans une société. Vous avez pour mission d'installer et de configurer le serveur web Apache 2.4 sur une machine Debian 11. Votre objectif est de rendre votre site web accessible en HTTP et HTTPS, tout en assurant une sécurité optimale et une configuration adaptée à votre environnement.

II. Consignes et Cahier des Charges

III. Objectifs

- Installation et Configuration d'Apache 2.4 : Installer le serveur web Apache 2.4 sur une machine Debian 11 et le configurer pour qu'il soit accessible en HTTP et HTTPS.
- Sécurisation des Connexions : Mettre en place des certificats SSL auto-signés pour sécuriser les connexions HTTPS.
- Redirection des Requêtes HTTP vers HTTPS : Configurer une redirection automatique de toutes les requêtes HTTP vers HTTPS.

- Configuration de l'Accès SSH : Configurer l'accès SSH sur la machine Debian pour permettre une gestion à distance sécurisée.
- Utilisation de Fichiers de Configuration : S'assurer que les fichiers de configuration d'Apache sont correctement configurés pour la gestion des sites disponibles et actifs.

IV. Livrables

- Rapport d'installation : Document décrivant toutes les étapes de l'installation et de la configuration d'Apache 2.4.
- Fichiers de Configuration : Fichiers de configuration utilisés pour Apache et OpenSSL.
- Journal des Commandes : Liste des commandes exécutées lors de l'installation et de la configuration.
- Capture d'Écran des Pages Web : Captures d'écran des pages web affichées via HTTP et HTTPS, avant et après la redirection automatique.
- Guide d'Utilisation : Documentation pour l'administration du serveur Apache, incluant la gestion des sites et des certificats SSL.

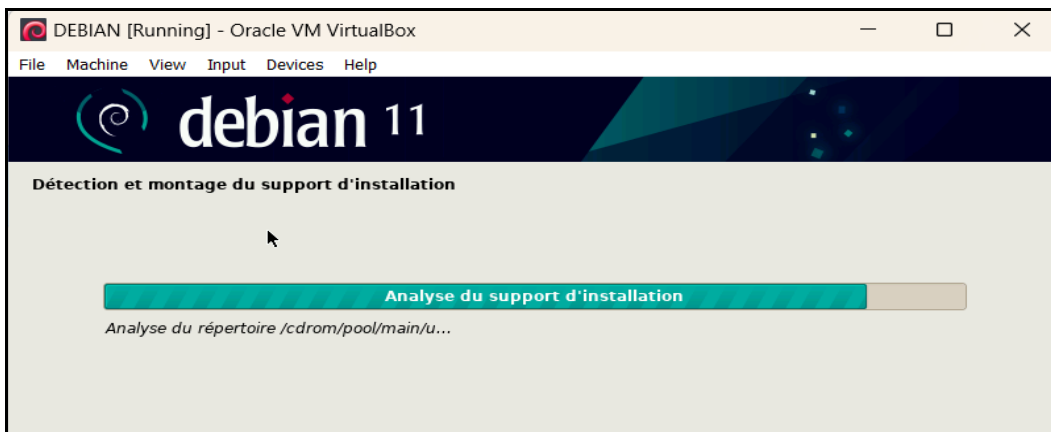
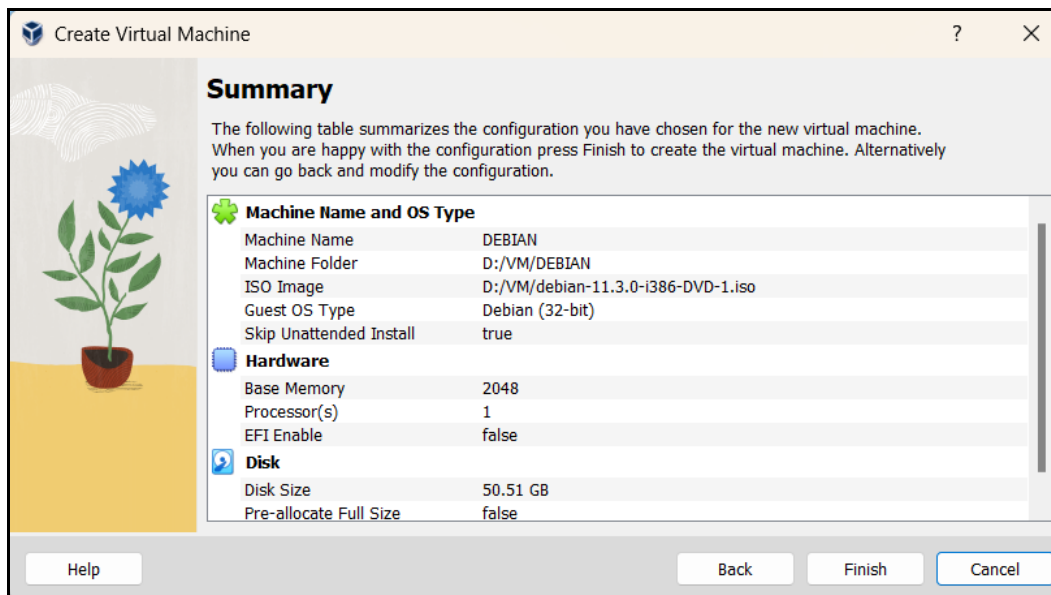
V. Préparation de l'Environnement

- Machine Virtuelle : Utiliser une machine virtuelle Debian 11.3 fraîchement installée.
- Accès Root : Ouvrir une session en tant que root pour avoir les permissions nécessaires.
- Mise à Jour des Paquets : Vérifier et mettre à jour les paquets existants avec apt update et apt upgrade.
- Installation d'Apache 2.4 : Installer Apache avec apt install apache2.
- Configuration SSH : Configurer l'accès SSH en installant OpenSSH-server, Putty et WinSCP.

VI. Instructions

VII. Installation d'Apache 2.4

L'installation d'une machine virtuelle Debian 11.3 :



- Mise à jour des paquets :
apt update



apt upgrade

```
abdelilah@debian: ~
root@debian:/home/abdelilah# apt upgrade
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:/home/abdelilah#
```

- Installation d'Apache 2.4 :
apt install apache2

```
abdelilah@debian: ~
root@debian:/home/abdelilah# apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  apache2-data apache2-utils
Paquets suggérés :
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Les NOUVEAUX paquets suivants seront installés :
  apache2 apache2-data apache2-utils
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 718 ko dans les archives.
Après cette opération, 2 012 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n] 0
Réception de :1 http://security.debian.org/debian-security bullseye-security/main i386 apache2-data all 2.4.59-1-deb11u1 [160 kB]
Réception de :2 http://security.debian.org/debian-security bullseye-security/main i386 apache2-utils i386 2.4.59-1-deb11u1 [274 kB]
Réception de :3 http://security.debian.org/debian-security bullseye-security/main i386 apache2 i386 2.4.59-1-deb11u1 [284 kB]
718 ko réceptionnés en 1s (666 ko/s)
```

- Vérification du statut d'Apache :
systemctl status apache2

```
abdelilah@debian: ~
root@debian:/home/abdelilah# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Wed 2024-05-22 23:26:25 CEST; 26s ago
     Docs: https://httpd.apache.org/docs/2.4/
    Main PID: 7480 (apache2)
      Tasks: 55 (limit: 4747)
     Memory: 9.0M
        CPU: 438ms
    CGroup: /system.slice/apache2.service
            └─7480 /usr/sbin/apache2 -k start
              └─7481 /usr/sbin/apache2 -k start
                └─7482 /usr/sbin/apache2 -k start

mai 22 23:26:24 debian systemd[1]: Starting The Apache HTTP Server...
mai 22 23:26:25 debian apachectl[7479]: AH00558: apache2: Could not reliably de
mai 22 23:26:25 debian systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```

Vous devez obtenir cet affichage avec le statut 'active (running)'.

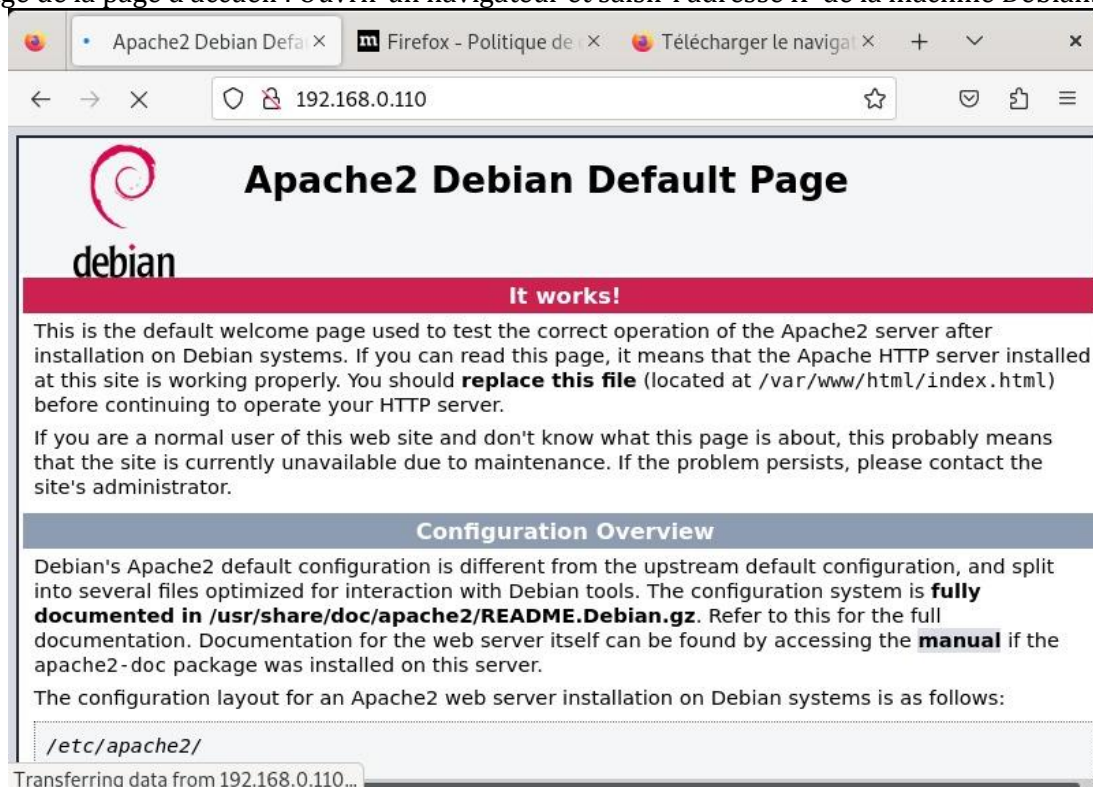
VIII. Configuration de l'Accès HTTP

- Vérifier l'adresse IP :

ip a

```
abdelilah@debian: ~  
root@debian:/home/abdelilah# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP  
    group default qlen 1000  
    link/ether 08:00:27:a6:d4:ee brd ff:ff:ff:ff:ff:ff  
    inet 192.168.0.110/24 brd 192.168.0.255 scope global dynamic noprefixroute e  
    inet6 fe80::a00:27ff:fea6:d4ee/64 scope link noprefixroute  
    valid_lft 4580sec preferred_lft 4580sec  
    valid_lft forever preferred_lft forever  
root@debian:/home/abdelilah#
```

Affichage de la page d'accueil : Ouvrir un navigateur et saisir l'adresse IP de la machine Debian.



IX. Configuration de l'Accès HTTPS

- Installation et configuration d'OpenSSL :

apt install openssl

```
abdelilah@debian: ~  
root@debian:/home/abdelilah# apt install openssl  
Lecture des listes de paquets... Fait  
Construction de l'arbre des dépendances... Fait  
Lecture des informations d'état... Fait  
openssl est déjà la version la plus récente (1.1.1n-0+deb11u5).  
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.  
root@debian:/home/abdelilah#
```

- Création d'une clé privée et d'un certificat auto-signé :

mkdir /etc/apache2/ssl

```
abdelilah@debian: ~  
root@debian:/etc/apache2# mkdir /etc/apache2/ssl  
root@debian:/etc/apache2# ls  
apache2.conf  envvars      mods-enabled  sites-enabled  
conf-available  magic        ports.conf    ssl  
conf-enabled   mods-available  sites-available  
root@debian:/etc/apache2#
```

cd /etc/apache2/ssl

openssl genrsa -out ca.key 4096

```
abdelilah@debian: ~  
root@debian:/etc/apache2/ssl# openssl genrsa -out ca.key 4096  
Generating RSA private key, 4096 bit long modulus (2 primes)  
.....++++  
.....++++  
e is 65537 (0x010001)  
root@debian:/etc/apache2/ssl#
```

openssl req -new -x509 -key ca.key -out ca.crt -days 365

```
abdelilah@debian: ~  
root@debian:/etc/apache2/ssl# openssl req -new -x509 -key ca.key -out ca.crt -days 365  
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]:MR  
State or Province Name (full name) [Some-State]:TEST  
Locality Name (eg, city) []:TEST  
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABDELILAH  
Organizational Unit Name (eg, section) []:TEST  
Common Name (e.g. server FQDN or YOUR name) []:TEST  
Email Address []:ABDELILAH@GMAIL.COM  
root@debian:/etc/apache2/ssl#
```

openssl genrsa -out cleprivapache.key 4096

```
abdelilah@debian: ~
root@debian:/etc/apache2/ssl# openssl genrsa -out cleprivapache.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
root@debian:/etc/apache2/ssl#
```

openssl req -new -key cleprivapache.key -out demandesignature.csr

```
abdelilah@debian: ~
root@debian:/etc/apache2/ssl# openssl req -new -key cleprivapache.key -out demandesignature.csr
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]:MR
State or Province Name (full name) [Some-State]:TEST
Locality Name (eg, city) []:TEST
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABDELILAH
Organizational Unit Name (eg, section) []:BOUHKKA
Common Name (e.g. server FQDN or YOUR name) []:ABDELILAH
Email Address []:ABDELILAH12@GMAIL.COM

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:glsid
An optional company name []:glsid
root@debian:/etc/apache2/ssl#
```

openssl x509 -req -in demandesignature.csr -out certifapache.crt -CA ca.crt -CAkey ca.key -CAcreateserial -days 365

```
abdelilah@debian: ~
root@debian:/etc/apache2/ssl# openssl x509 -req -in demandesignature.csr -out certifapache.crt -CA ca.crt -CAkey ca.key -CAcreateserial -days 365
Signature ok
subject=C = MR, ST = TEST, L = TEST, O = ABDELILAH, OU = BOUHKKA, CN = ABDELILAH
, emailAddress = ABDELILAH12@GMAIL.COM
Getting CA Private Key
root@debian:/etc/apache2/ssl#
```

- Modification du fichier de configuration :
nano /etc/apache2/sites-available/default-ssl.conf

```
abdelilah@debian: ~
root@debian:/# nano /etc/apache2/sites-available/default-ssl.conf
```

- Ajouter les lignes pour spécifier l'emplacement des fichiers de certificats :
 SSLCertificateFile /etc/apache2/ssl/certifapache.crt
 SSLCertificateKeyFile /etc/apache2/ssl/cleprivapache.key

```

abdelilah@debian: ~
GNU nano 5.4 /etc/apache2/sites-available/default-ssl.conf *
# include a line for only one particular virtual host. For exam>
# following line enables the CGI configuration for this host on>
# after it has been globally disabled with "a2disconf".
#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 inst>
# 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, on>
# SSLCertificateFile directive is needed.
SSLCertificateFile /etc/apache2/ssl/certifapache.crt
SSLCertificateKeyFile /etc/apache2/ssl/cleprivapache.key

# Server Certificate Chain:
# Point SSLCertificateChainFile at a file containing the
# concatenation of PEM encoded CA certificates which form the
Nom du fichier à écrire: /etc/apache2/sites-available/default-ssl.conf
^G Aide M-D Format DOS M-A Ajout (à la fin) M-B Copie de sécu.
^C Annuler M-M Format Mac M-P Ajout (au début) ^T Parcourir

```

- Activation du site HTTPS :
 a2ensite default-ssl
 systemctl reload apache2

```

abdelilah@debian: ~
root@debian:/# /usr/sbin/a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@debian:/# systemctl reload apache2
root@debian:/#

```

Test de l'accès HTTPS : Ouvrir un navigateur et saisir https://debian

```

abdelilah@debian: ~
root@debian:/# hostname -f
debian
root@debian:/#

```




La connexion a échoué

Une erreur est survenue pendant une connexion à debian.

- Le site est peut-être temporairement indisponible ou surchargé. Réessayez plus tard ;
- Si vous n'arrivez à naviguer sur aucun site, vérifiez la connexion au réseau de votre ordinateur ;
- Si votre ordinateur ou votre réseau est protégé par un pare-feu ou un proxy, assurez-vous que Firefox est autorisé à accéder au Web.

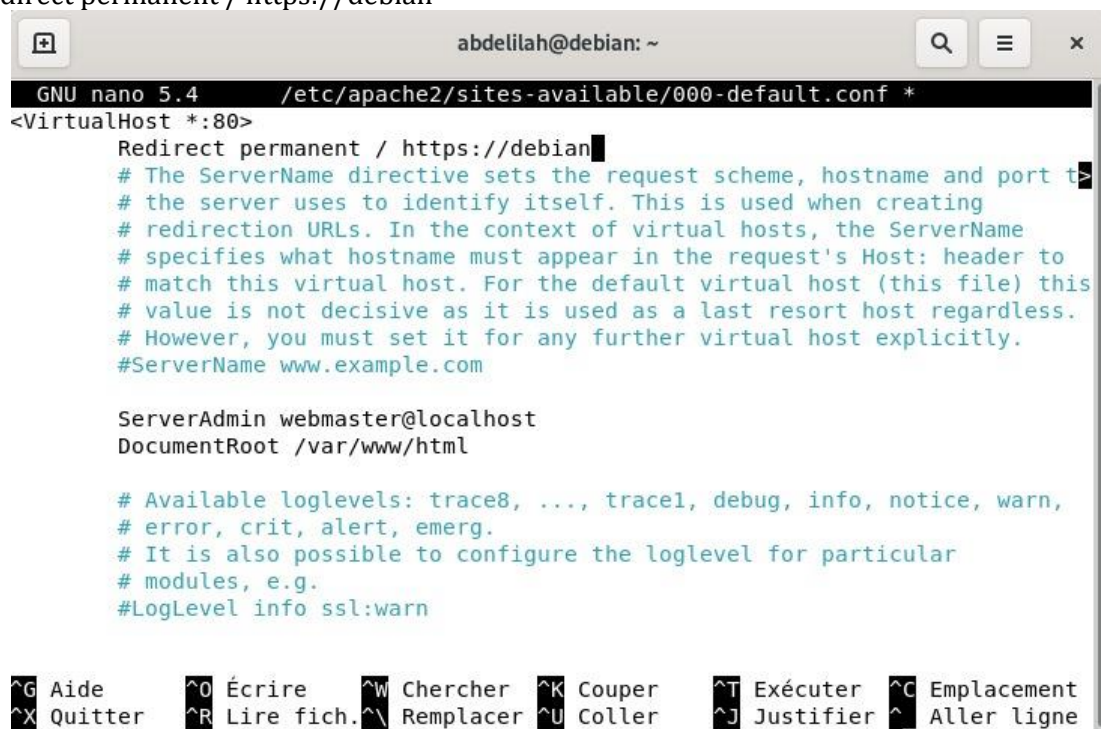
Réessayer

X. Redirection des Requêtes HTTP vers HTTPS

- Modification du fichier de configuration :
nano /etc/apache2/sites-available/000-default.conf

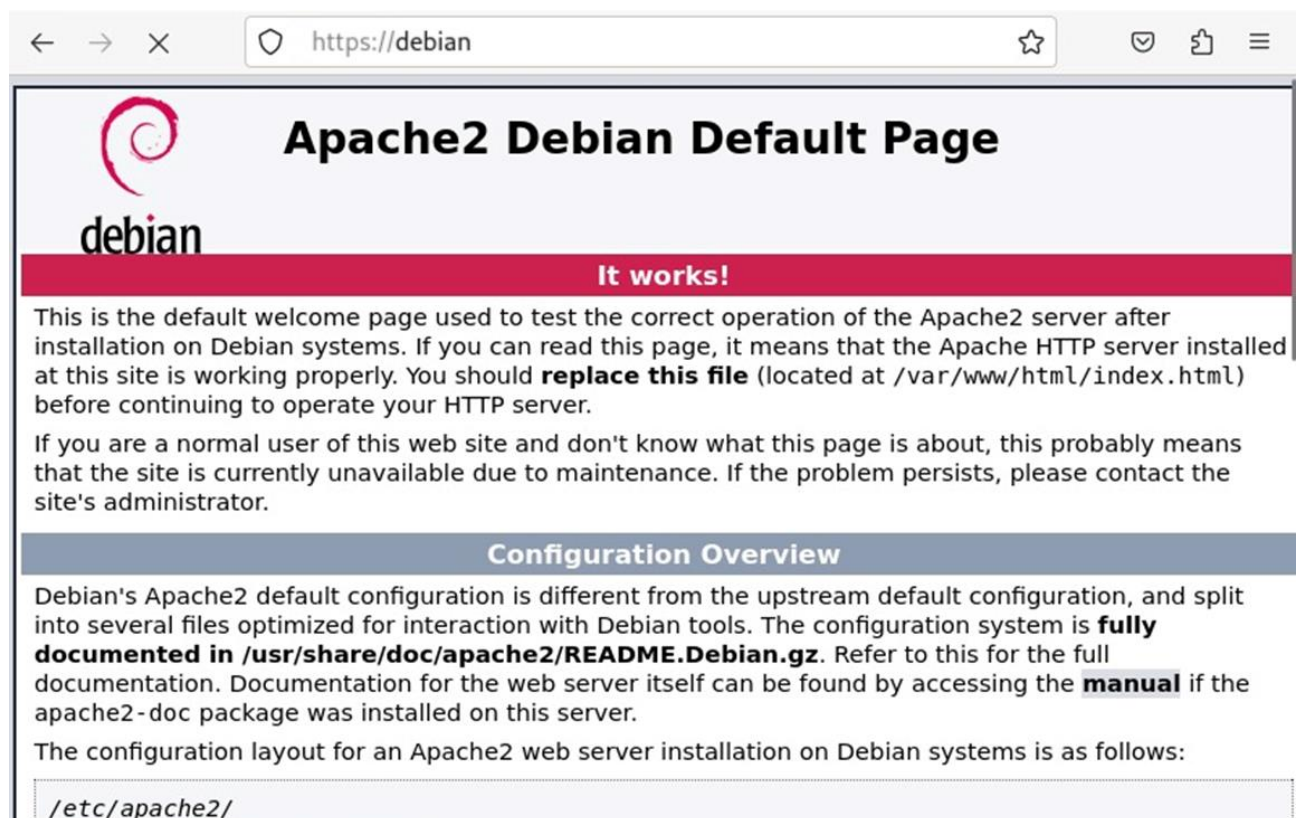
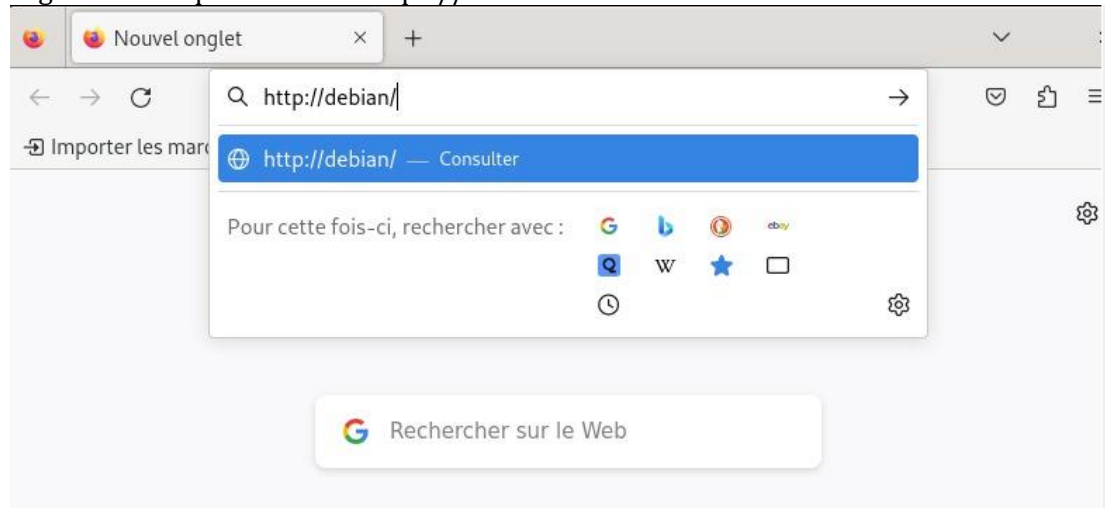


- Ajouter la ligne suivante :
Redirect permanent / https://debian



- Relance du service Apache :
systemctl restart apache2

Vérification de la redirection : Ouvrir un navigateur et saisir `http://debian` pour vérifier que vous êtes redirigé automatiquement vers `https://debian`.



XI. Configuration de l'Accès SSH

Installation d'OpenSSH-server :
apt install openssh-server

```

root@debian:/# apt install openssh-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  openssh-sftp-server runit-helper
Paquets suggérés :
  molly-guard monkeysphere ssh-askpass ufw
Les NOUVEAUX paquets suivants seront installés :
  openssh-server openssh-sftp-server runit-helper
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 483 ko/490 ko dans les archives.
Après cette opération, 1 944 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://security.debian.org/debian-security bullseye-security/main
i386 openssh-sftp-server i386 1:8.4p1-5+deb11u3 [59,2 kB]
Réception de :2 http://security.debian.org/debian-security bullseye-security/main
i386 openssh-server i386 1:8.4p1-5+deb11u3 [423 kB]
Changement de support : veuillez insérer le disque nommé
* Debian GNU/Linux 11.3.0 _Bullseye_ - Official i386 DVD Binary-1 20220326-11:23
»
dans le lecteur « /media/cdrom/ » et appuyez sur la touche Entrée

```

Téléchargement et installation de Putty et WinSCP sur la machine Windows.
 Configuration des fichiers hosts sur les machines Debian et Windows.

```

GNU nano 5.4 /etc/hosts *
127.0.0.1    localhost
127.0.1.1    debian

192.168.0.110  debian
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

Nom du fichier à écrire: /etc/hosts
^G Aide      M-D Format DOS  M-A Ajout (à la fin) M-B Copie de sécu.
^C Annuler   M-M Format Mac  M-P Ajout (au début) ^T Parcourir

```

XII. Conclusion

En suivant ce guide, vous serez en mesure d'installer et de configurer le serveur web Apache 2.4 sur une machine Debian 11, tout en sécurisant les connexions HTTPS et en configurant l'accès SSH pour une gestion à distance sécurisée. Assurez-vous de documenter toutes les étapes et de fournir les fichiers de configuration nécessaires pour une gestion optimale du serveur.