Serveur Web "is.anonyme"

Installation du système

Installation

Fond-fonfon.ch

Révision: 4

26.08.2023

Anonyme SA

Serveur Web "is.anonyme"

Objet :	Installation du système
Catégorie :	Installation
Département :	Systèmes d'information
Mots clefs :	Linux; Web; anonyme.ch; Installation
Révision :	4

Index

Introduction

Le présent document est basé sur la procédure révision "1", qui implémentait un serveur Linux Ubuntu version 14.04.

La présente révision (4) de ce processus s'attache à décrire une installation sur Linux serveur Ubuntu 22.04.x LTS.

De même, l'installation des nouvelles versions de PHP (8.1) et de MySQL (8.1) sont prises en compte dans ce document.

La première partie concerne l'installation de base du système.

La seconde partie comprend l'installation de logiciels et modules supplémentaires.

La troisième partie comprend l'installation et la configuration d'Apache HTTPd.

Une quatrième partie comprend l'installation de mySQL Server et PHP, ainsi que de leur configuration respective.

Une cinquième partie est plus particulièrement dédiée à la sécurisation du serveur ainsi que des logiciels.

Notes

D'une manière générale les commandes adressées à la console sont affichées en police "Courrier-New" sur fond noir.

Avertissement

Ce document comporte des paramètres susceptibles de devoir être adaptés en regard des divers processus à réaliser lors de l'implémentation du serveur.

Il faudra donc prévoir la modification certaines commandes.

D'une manière générale, prévoir ces adaptations avant l'exécution de la procédure proprement dite.

1ère partie - Installation de base

Pré-requis

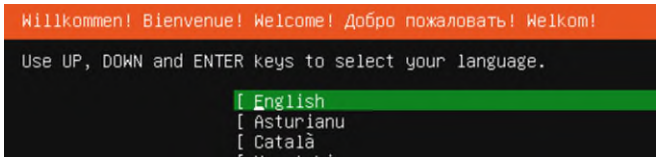
On présuppose une installation réalisée sur un serveur hyper-v Microsoft Windows version 2016 ou ultérieure.

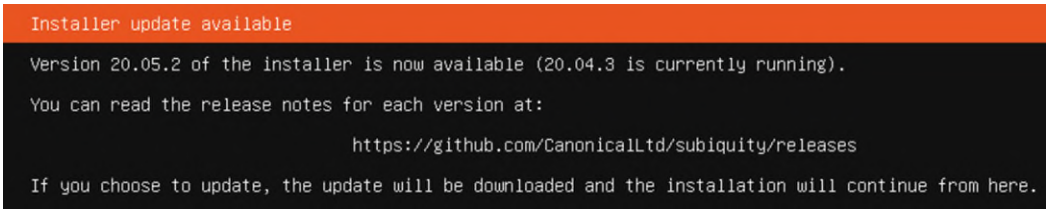
La création de la machine virtuelle présuppose les paramètres suivants:

- Génération de machine virtuelle : Génération 2
- Démarrage sécurisé activé avec option « Autorité de certification UEFI Microsoft » active.
- 256 Go de disque alloués dynamiquement
- 8192 Mo de RAM allouées dynamiquement
- Mémoire minimum : 512Mo
- Mémoire maximum : 8192Mo
- Mémoire au démarrage : 4096Mo
- Une carte réseau inscrite sur le VLAN DATA / sous-réseau : 192.168.xx.0.
- Une carte réseau inscrite sur le VLAN DMZ / sous-réseau : 192.168.xx.0.
- Modifier les paramètres suivants dans les propriétés de la machine :
    - 2 processeurs
    - Un lecteur DVD virtuel (modifier l'ordre de démarrage des périphériques)
- Conseil : en cas de haute disponibilité, appliquer des adresses MAC manuellement sur les cartes réseau.
- Un réplica de la machine sur un second serveur hyper-v (à réaliser en fin d'installation et de tests)
- Réalisation de clichés instantanés, afin de pouvoir reprendre une étape en cas de problème lors de l'installation.
- Sauvegarde du serveur web sur un système tiers (Veeam, p. ex.)
- Un fichier iso « Ubuntu Server 22.04.x LTS »

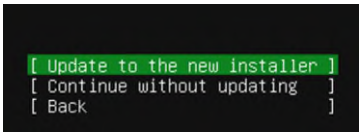
Déroulement de l'installation

1. Sélectionner l'anglais comme langue système

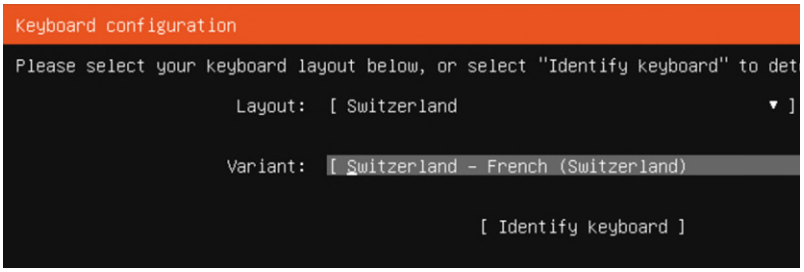




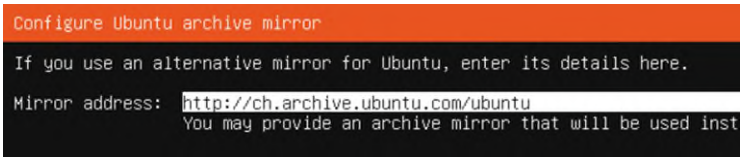
2. Sélectionner tel que ci-dessous



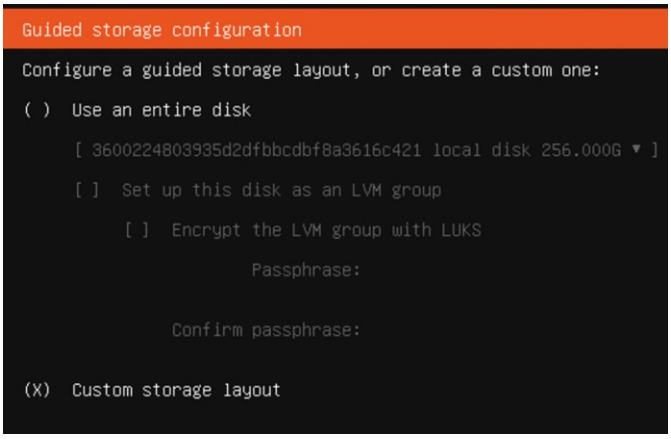
3. Configuration clavier



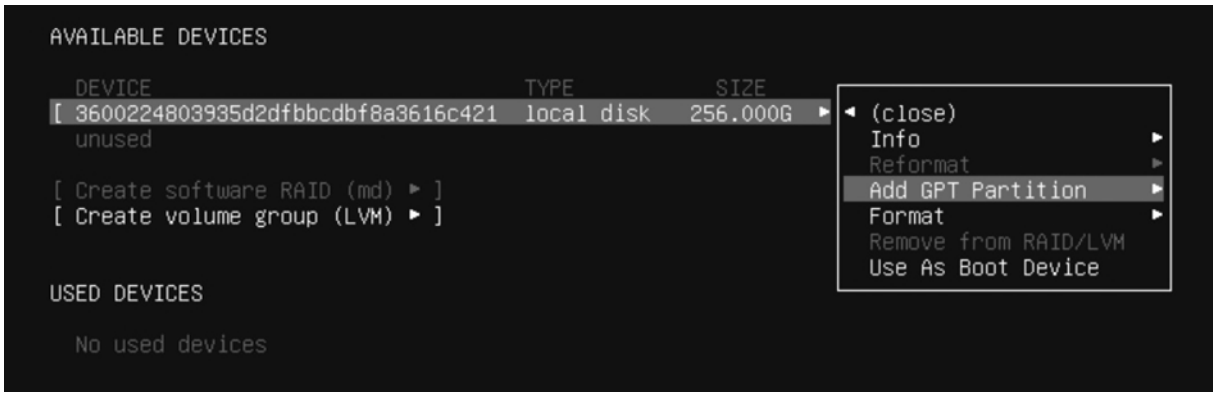
4. Laisser la configuration IP telle quelle, en DHCP
5. Ne pas utiliser de servuer proxy
6. Source Ubuntu : laisser tel quel



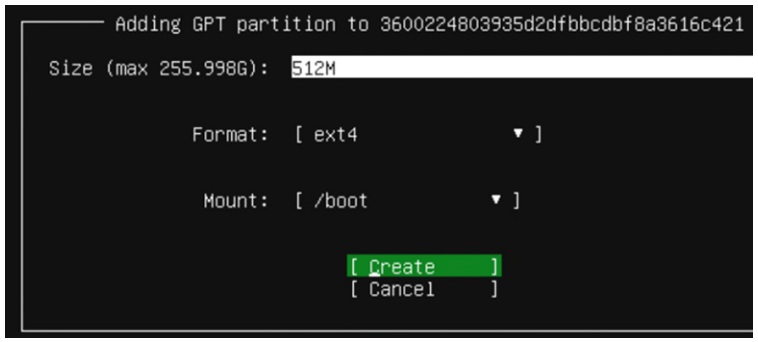
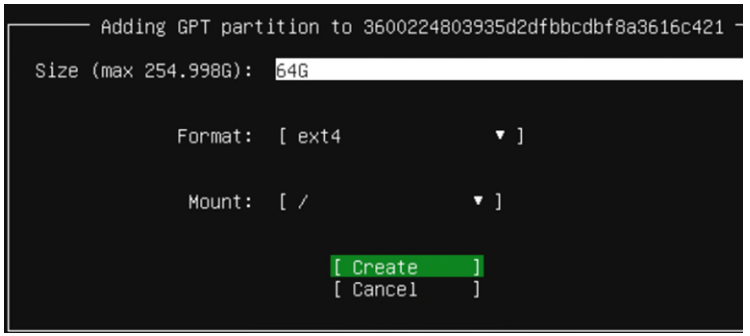
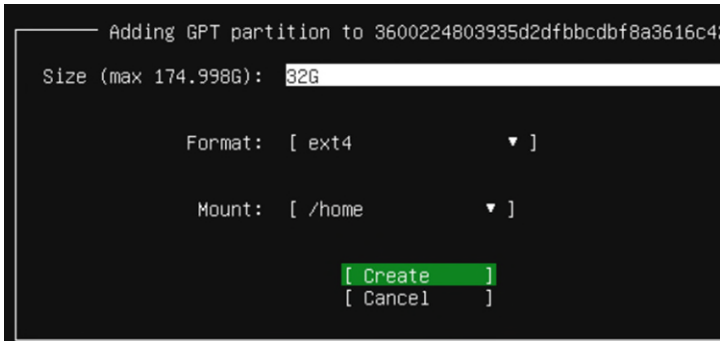
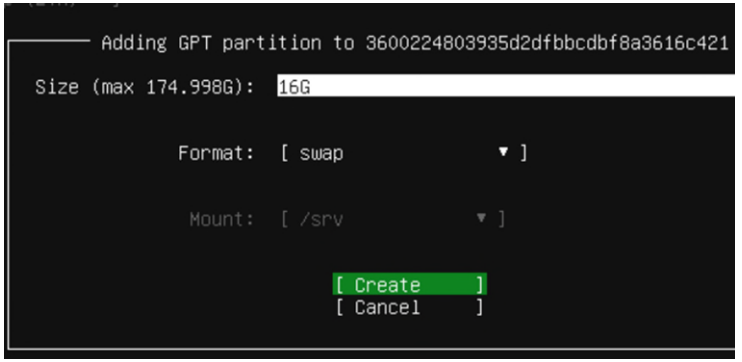
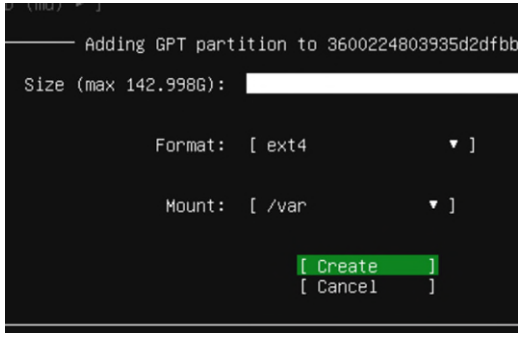
7. Partitionnement du disque dur manuel



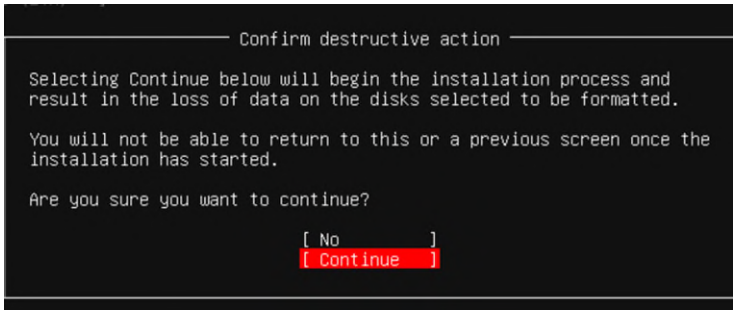
8. Sélectionner le disque pour créer les partitions



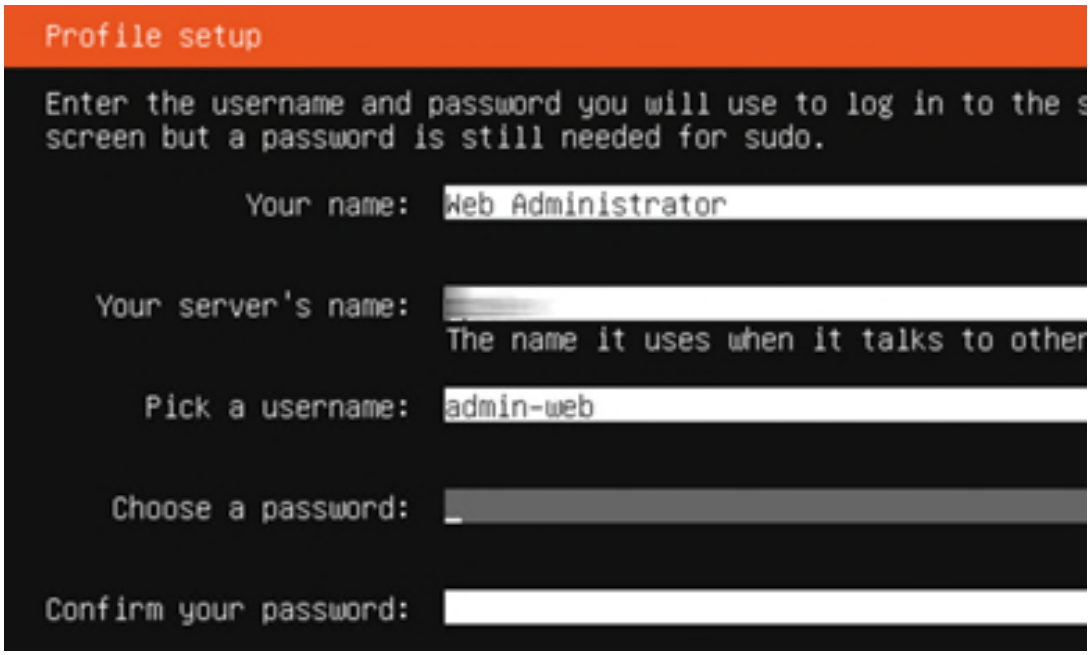
9. Créer les partitions tel que ci-dessous (de gauche à droite et de haut en bas)

<table>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td> 
</td>
<td> 
</td>
</tr>
<tr>
<td> 
</td>
<td></td>
</tr>
</table>

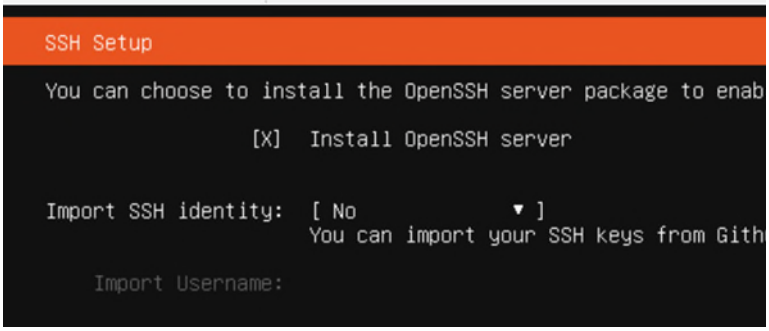
10. Valider le partitionnement



11. Nommer le serveur et créer l'urtilisateur administrateur



12. Installer SSH



13. Ne pas installer de composant supplémentaire

14. Redémarrer le serveur

15. Patienter avant de se connecter que l'ensemble des services soit démarré et configuré (2min.)

Après démarrage

16. Effectuer une recherche et appliquer les mises à jour:

```
sudo apt-get update

sudo apt-get upgrade

sudo apt-get dist-upgrade
```

17. Arrêter la machine.

```
sudo shutdown -P now
```

18. Effectuer un cliché instantané depuis hyper-v.

19. Démarrer le serveur.

Configuration des interfaces réseau

20. Configurer l'interface réseau "eth0"

```
sudo cp /etc/netplan/00-installer-config.yaml /etc/netplan/00-
installer-config.yaml.bak

sudo nano /etc/netplan/00-installer-config.yaml

network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: no
      addresses: [192.168.xxx.xxx/24]
      gateway4: 192.168.xxx.xxx
      nameservers:
        addresses: [192.168.xxx.xxx]
      dhcp6: no
```

Note : un routage static (ci-dessous) est programmé mais mis en commentaire pour l'instant. Une fois le serveur en place, on retirera le commentaire et on commentera la ligne « gateway4 » ci-dessus.

21. Si nécessaire configurer l'interface réseau "eth1" (on la commente pour l'instant).

```
 [...]

    #eth1:
      #dhcp4: no
      #addresses: [192.168.xxx.xxx/24]
      #gateway4: 192.168.xxx.xxx
      #nameservers:
      #  addresses: [xxx.xxx.xxx.xxx,xxx.xxx.xxx.yyy]
      #routes:
      #  - to: 192.168.xxx.xxx/xx
      #    via: 192.168.xxx.xxx
      #dhcp6: no
```

22. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

23. Appliquer la nouvelle configuration IP

```
sudo netplan apply
```

24. Vérifications IP :

```
Vérifier l'adresse IP:
ip addr

Vérifier les adresses IP de passerelle:
ip route

Vérifier les adresses IP des serveurs DNS configurés:
systemd-resolve --status | grep Servers
```

25. Changer le nom d'hôte si nécessaire

```
sudo nano /etc/hostname

[hostname]
```

26. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

```
sudo nano /etc/hosts

127.0.0.1  localhost
[adresse ens33] [nouveau nom d'hôte]
[adresse eth1]  [autre nom d'hôte]
```

27. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

28. Redémarrer le serveur

Configuration de SSH

29. Editer le fichier de config ssh:

```
sudo nano /etc/ssh/sshd_config
```

30. Configurer comme suit:

```
[…]

Port 10022
useDNS no

#ListenAddress ::
ListenAddress 192.168.xxx.xxx #(Décommenter et modifier)

[...]

PermitRootLogin no #(Décommenter et modifier)
StrictModes yes #(Décommenter)
```

31. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

32. Saisir la commande :

```
sudo service ssh reload
```

33. Fermer la session SSH et la relancer avec les nouveaux paramètres

34. Eteindre le serveur

```
sudo shutdown -P now
```

35. Effectuer un cliché instantané depuis hyper-v.

36. Relancer le serveur et se connecter en SSH et travailler depuis cet interface (avec "Putty" p. ex.).

Configuration des utilisateurs administrateurs

37. Restreindre l'accès "su" aux seuls administrateurs

```
sudo dpkg-statoverride --update --add root sudo 4750 /bin/su
```

Configuration de l'horloge

38. Paramétrage des sources NTP

```
sudo nano /etc/systemd/timesyncd.conf

[Time]
NTP=server 0.ch.pool.ntp.org # Décommenter et ajouter le
serveur
NTP=server 1.ch.pool.ntp.org # Ajouter le serveur
NTP=server 2.ch.pool.ntp.org # Ajouter le serveur
NTP=server 3.ch.pool.ntp.org # Ajouter le serveur
#FallbackNTP=ntp.ubuntu.com
#RootDistanceMaxSec=5
#PollIntervalMinSec=32
#PollIntervalMaxSec=2048
```

39. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

40. Sélectionner le fuseau horaire

```
sudo timedatectl set-timezone Europe/Zurich
```

41. Redémarrer le service et vérifier des paramètres de sychronisation

```
sudo systemctl restart systemd-timesyncd

systemctl status systemd-timesyncd
```

```
● systemd-timesyncd.service - Network Time Synchronization
     Loaded: loaded (/lib/systemd/system/systemd-
timesyncd.service; enabled; vendor preset: enabled)
     Active: active (running) since Tue 2021-05-18 13:33:13
CEST; 1h 55min left
       Docs: man:systemd-timesyncd.service(8)
   Main PID: 2706 (systemd-timesyn)
     Status: "Initial synchronization to time server
xxx.xxx.xxx.xxx:123 (xxx.xxx.xxx.xxx)."
      Tasks: 2 (limit: 9416)
     Memory: 1.8M
     CGroup: /system.slice/systemd-timesyncd.service
             └─2706 /lib/systemd/systemd-timesyncd
```

42. Vérifier l'horloge

```
timedatectl timesync-status
```

Réponse:

```
       Server: xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx)
Poll interval: 8min 32s (min: 32s; max 34min 8s)
         Leap: normal
      Version: 3
      Stratum: 3
    Reference: 52C5A42E
    Precision: 1us (-23)
Root distance: 53.855ms (max: 5s)
       Offset: +1.296ms
        Delay: 1.746ms
       Jitter: 1.084ms
 Packet count: 5
    Frequency: +7.354ppm
```

```
timedatectl
```

Réponse:

```
               Local time: Tue 2021-05-18 11:47:58 CEST
           Universal time: Tue 2021-05-18 09:47:58 UTC
                 RTC time: Tue 2021-05-18 09:47:58
                Time zone: Europe/Zurich (CEST, +0200)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
```

2ème partie - Installation du serveur Web Apache2

1. Installer le serveur

```
sudo apt-get update

sudo apt-get install apache2 apache2-utils libapache2-
mod-fcgid
```

2. Configuration du nom de serveur dans la configuration globale

```
sudo nano /etc/apache2/apache2.conf

[…]

# Global configuration
#
ServerName [nom d'hôte]
#

[…]

<Directory /var/www/vhosts/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

[…]

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Créer le répertoire /var/www/vhosts

```
sudo mkdir /var/www/vhosts
```

5. Vérifier l'activation des modules Apache suivants

```
sudo apache2ctl -M
```

   a. Parmi d''autres, les modules suivants doivent apparaître dans la liste des modules actifs:

```
sudo a2enmod autoindex deflate expires fcgid filter
headers rewrite setenvif unique_id
```

   b. Pour activer un module Apache:

```
sudo a2enmod [module]      (p. ex. "sudo a2enmod expires")

Puis

sudo apache2ctl graceful

sudo service apache2 restart
```

6. Supprimer le répertoire /var/www/html

```
sudo rm -rf /var/www/html
```

Pages par défaut

7. Configuration par défaut des pages d'accueil du site

   a. Mettre index.php en tête de la liste

```
sudo nano /etc/apache2/mods-enabled/dir.conf

     <IfModule mod_dir.c>
          DirectoryIndex index.php index.html index.cgi
index.pl ~~index.php~~ index.xhtml index.htm
     </IfModule>
```

   b. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

Configuration des protocols SSL acceptés

8. Configuration des protocoles SSL

    a. Modifier le paramètre SSLProtocol

```
sudo nano /etc/apache2/mods-available/ssl.conf

[...]

     SSLProtocol all -SSLv3

[...]
```

    b. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

9. Editer le fichier hosts et spécifier l'adresse IP à laquelle répondra l'hote "is.anonyme.ch"

```
sudo nano /etc/hosts

127.0.0.1  localhost
192.168.xxx.xxx isanonyme  is.anonyme
```

10. Modifier les ports d'écoute du site du serveur si nécessaire.

```
sudo nano /etc/apache2/ports.conf

[…]

Listen 80

Listen "N° de port pour un hôte supplémentaire"

<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mod_gnutls.c>
        Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

11. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

12. Modifier la rotation des fichiers journaux

```
sudo cp /etc/logrotate.d/apache2 /etc/logrotate.d/apache2.bak

sudo nano /etc/logrotate.d/apache2

/var/log/apache2/*.log {
        daily
        missingok
        rotate 30

[…]
```

13. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

14. Redémarrer le server Web

```
sudo service apache2 restart
```

15. Eteindre le serveur

```
sudo shutdown -P now
```

16. Effectuer un cliché instantané depuis hyper-v.

Configuration des hôtes virtuels

Sur cette installation, les hôtes virtuels sont envisagés selon le port de communication (80 ou 443 (SSL) par défaut.

Dans la configuration initiale on envisage de créer un hôte en port 80 redirigé sur un second en port 443 pour forcer l'usage de SSL (SSL) (La redirection est faite via un fichier .htaccess).

Configuration de l'hôte par défaut (port 80)

Répertoires des hôtes (A répéter pour chaque hôte souhaité)

1. Effectuer les opérations suivantes

```
sudo mkdir -p /var/www/vhosts/[nom du site]/httpdocs

sudo chown -R www-data:www-data /var/www/vhosts/[nom du site]

sudo chmod -R 775 /var/www/vhosts/[nom du site]
```

2. Editer une page html de test pour chaque hôte virtuel créé.

```
sudo nano /var/www/vhosts/[nom du site]/httpdocs/index.html

<html>
  <head>
    <title>Welcome to [nom du site]</title>
  </head>
  <body>
    <h1>Success! The [nom du site] site is working!</h1>
  </body>
</html>
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Editer le fichier de configuration de l'hôte virtuel "isanonyme", pour l'exemple (à faire pour chaque hôte virtuel)

```
sudo cp /etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-available/isanonyme.conf

sudo nano /etc/apache2/sites-available/isanonyme.conf

<VirtualHost *:80>
[…]
       ServerName localhost
       ServerAlias is.anonyme
       UsecanonicalName Off

       ServerAdmin webmaster@localhost

       DocumentRoot /var/www/vhosts/isanonyme/httpdocs

       ErrorLog ${APACHE_LOG_DIR}/error.isanonyme.log
       CustomLog ${APACHE_LOG_DIR}/access.isanonyme.log combined

[…]

         <Directory /var/www/vhosts/isanonyme/httpdocs>
             Options FollowSymLinks
             DirectoryIndex index.php index.html
             AllowOverride All
         </Directory>
         # Redirection vers https (on laisse en commentaire pour
         # l'instant
         #RewriteEngine on
         #RewriteCond %{HTTPS} !=on
         #RewriteRule ^/(.*)$ https://is.anonyme [ou adresse IP]/$1
[R=301,L,NC]

</VirtualHost>
```

5. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

6. Activer l'hôte virtuel:

```
sudo a2ensite isanonyme.conf
```

7. Vérifier la présence du fichier "000-default.conf" dans le dossier "sites-enabled". Si celui-ci est présent, il faut l'effacer.

```
cd /etc/apache2/sites-enabled

ls

sudo rm 000-default.conf
```

8. Redémarrer le service Apache

```
sudo service apache2 restart
```

9. Vérifier la config

```
sudo apache2ctl configtest

Réponse:

"Syntax OK"
```

Configuration de l'hôte par défaut avec SSL (port 443)

10. Activer le mode SSL

```
sudo a2enmod ssl

sudo service apache2 restart
```

11. Editer le fichier SSL de configuration de l'hôte virtuel "isanonyme",

```
sudo cp /etc/apache2/sites-available/default-ssl.conf
/etc/apache2/sites-available/ssl.isanonyme.conf

sudo nano /etc/apache2/sites-available/ssl.isanonyme.conf

<IfModule mod_ssl.c>
      <VirtualHost _default_:443>
            ServerName localhost
            ServerAlias is.anonyme
            UsecanonicalName Off

            ServerAdmin webmaster@localhost

            DocumentRoot /var/www/vhosts/isanonyme/httpdocs

            ErrorLog ${APACHE_LOG_DIR}/error.ssl.isanonyme.log
            CustomLog ${APACHE_LOG_DIR}/access.ssl.isanonyme.log
combined

            […]

            SSLEngine On

            […]

            <Directory /var/www/vhosts/isanonyme/httpdocs>
                  Options FollowSymLinks
                  DirectoryIndex index.php index.html
                  AllowOverride All
                  <IfModule security2_module>
                        SecRuleEngine On
                  </IfModule>
            </Directory>
      </VirtualHost>
</IfModule>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

12. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

13. Activer l'hôte virtuel:

```
sudo a2ensite ssl.isanonyme.conf
```

14. Redémarrer le service Apache

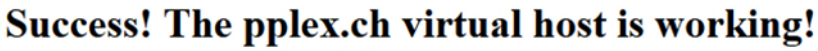
```
sudo service apache2 restart
```

Tests du serveur web

17. Tester le site normal en saisissant le http://ip-du-serveur dans un navigateur Web

18. Exécuter le même test en saisissant https://ip-du-serveur

19. Résultats port les deux adresses :



    Si ces pages n'apparaissent pas, contrôler la présence des seuls fichiers "isanonyme.conf" et "ssl.isanonyme.conf" dans le dossier "/etc/apache2/sites-enabled".

20. Eteindre le serveur

```
sudo shutdown -P now
```

21. Effectuer un cliché instantané depuis hyper-v.

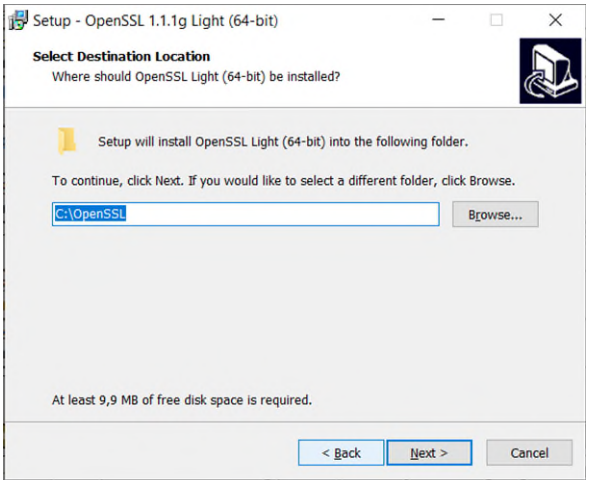
Traitement du certificat SSL

Ici, plusieurs étapes:

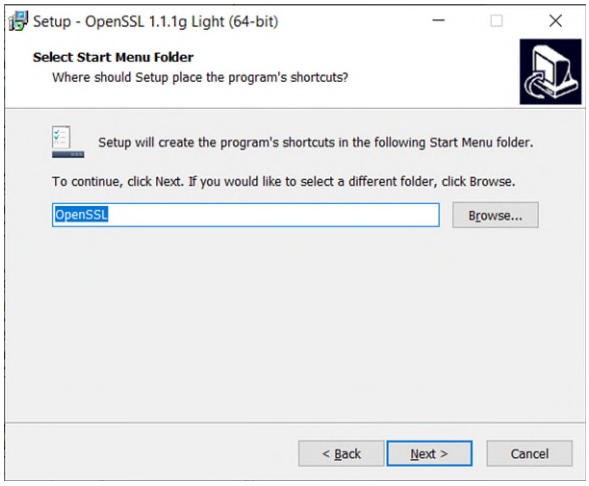
1. Extraire les certificats nécessaires au moyen de OpenSSL.
2. Importer le certificat au moyen de vsFTPd
    a. Installer et configurer vsFTPd.
    b. Créer un utilisateur provisoire FTP.
    c. Importer les certificats.
    d. Supprimer l'utilisateur provisoire FTP et la configuration attenante.
3. Mise en place du certificat et de la clef privée.
4. Configuration du fichier apache SSL pour appliquer le certificat importé.
5. Supprimer l'utilisateur ftp temporaire.

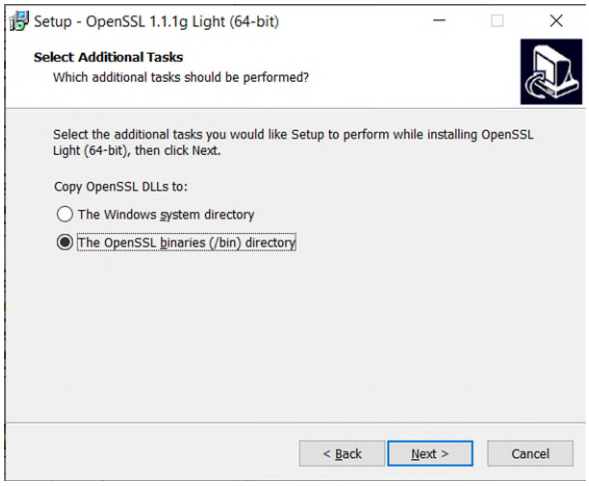
Extraction des certificats

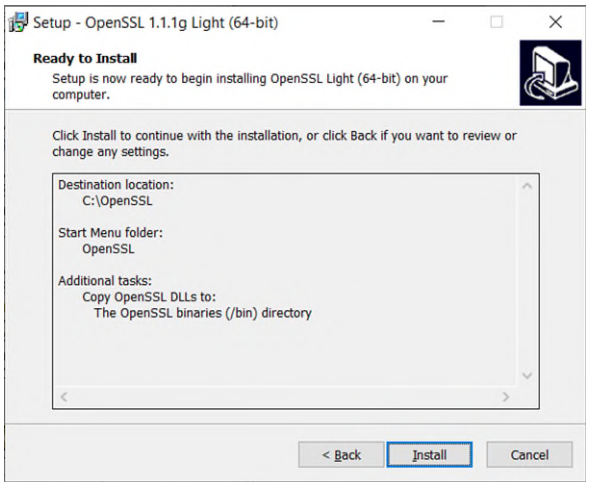
6. Télécharger la version binaire OpenSSL pour Windows. OpenSSL.org ne fournit plus de binaires de ce type. On se rabat donc sur le site "slproweb.com": https://slproweb.com/products/Win32OpenSSL.html
7. Installer OpenSSL

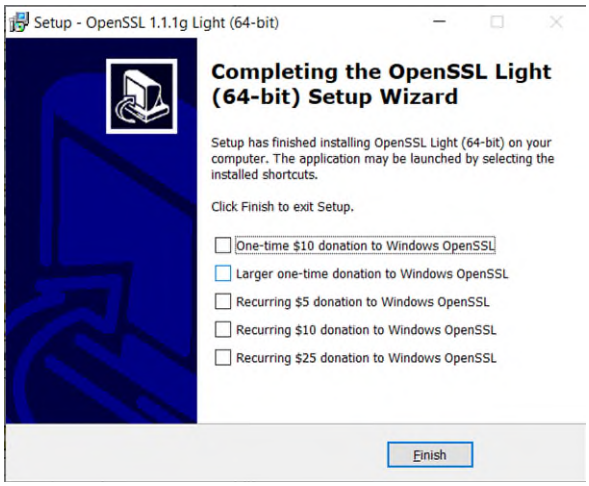


8. Installer OpenSSL (suite)









9. Se munir du certificat au format pfx pour le domaine « . ».

10. Copier le certificat pfx dans le répertoire d'installation d'OpenSSL « C:\OpenSSL\bin ».

11. Renommer le certificat comme suit : « isanonyme.pfx »

12. En ligne de commande, procéder comme suit depuis le répertoire d'installation OpenSSL.

    Lancer les commandes suivantes:

```
Extraction du certificate de domaine
openssl pkcs12 -in isanonyme.pfx -clcerts -nokeys -out
anonyme.cer

Extraction de la clef privée encryptée
openssl pkcs12 -in isanonyme.pfx -nocerts -nodes  -out en-
private.key

Décrpytage de la clef privée
openssl rsa -in en-private.key -out private.key
```

13. Renommer "isanonyme.cer" en "public.crt".

14. Depuis le site « globalsign », télécharger le certificat intermédiaire, le déplacer vers C:\OpenSSL\bin », puis le renommer en « globalsign-int.crt » (https://support.globalsign.com/ca-certificates/intermediate-certificates/organizationssl-intermediate-certificates)

15. Retour sur le serveur Ubuntu.

Installation du serveur FTP "vsFTPd"

16. Lancer la commande d'installation

```
sudo apt-get update

sudo apt-get install vsftpd

sudo mkdir /etc/vsftpd
```

17. Editer le fichier "/etc/vsftpd.conf" et ajouter :

```
sudo mv /etc/vsftpd.conf /etc/vsftp.conf.bak

sudo nano /etc/vsftpd.conf

listen=YES
listen_port=10021

anonymous_enable=NO
local_enable=YES
write_enable=YES

dirmessage_enable=YES

use_localtime=YES
xferlog_enable=YES
connect_from_port_20=YES
chroot_local_user=YES
allow_writeable_chroot=YES
secure_chroot_dir=/var/run/vsftpd/empty

pam_service_name=vsftpd

rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem

rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key

ssl_enable=YES
allow_anon_ssl=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
pasv_max_port=10200
pasv_min_port=10090

force_dot_files=YES
#hide_ids=YES
max_per_ip=20
max_clients=10
local_umask=002
chmod_enable=YES
file_open_mode=0775
```

18. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

Création d'un utilisateur FTP provisoire

22. Création d'un répertoire virtuel

```
sudo mkdir -p /var/www/vhosts/admin-ftp

sudo chown -R www-data:www-data /var/www/vhosts/admin-ftp

sudo chmod -R 775 /var/www/vhosts/admin-ftp
```

23. Création de l'utilisateur provisoire

```
sudo adduser admin-ftp

Enter new UNIX password:

Retype new UNIX password:

        Full Name []:[full_user_name]
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
```

24. Editer un fichier de redirection FTP

```
cd /etc/vsftpd

sudo nano admin-ftp

local_root=/var/www/vhosts/admin-ftp
```

25. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

26. Ajouter le nouvel utilisateur au groupe "www-data"

```
sudo adduser admin-ftp www-data
```

27. Modifier son répertoire de départ en le faisant pointer sur le répertoire /var/www/vhosts/admin-ftp

```
sudo mount --bind /var/www/vhosts/admin-ftp /home/admin-ftp/
```

28. Redémarrer le service FTP

```
sudo service vsftpd restart
```

Import des certificats et de la clef privée

1. Lancer un client FTP depuis Windows.
2. Données d'accès:
    - Adresse IP: 192.168.xxx.xxx
    - Port: 10021
    - Type: Connexion FTP explicite sur TLS
3. Se connecter avec les coordonnées de l'utilisateur provisoire.
4. Télécharger les certificats "public.crt", la clef privée "private.key" et le certificat « globalsign-int.crt » sur le serveur web.
5. Se déconnecter.
6. On conserve l'utilisateur et le répertoire ftp provisoire en cas de nécessité pour l'instant, le temps de configurer et tester les sites web virtuels http et https.

Mise en en place des certificats

7. Créer le répertoire /etc/apache2/ssl et appliquer les droits suivants:

```
sudo mkdir -p /etc/ssl/certs

sudo mkdir -p /etc/ssl/private

sudo chmod -R 755 /etc/ssl/certs

sudo chmod 755 /etc/ssl/private
```

8. Copier les fichiers certificats dans les répertoires ad-hoc.

```
sudo cp /var/www/vhosts/admin-ftp/wildanonyme.crt /etc/ssl/certs

sudo cp /var/www/vhosts/admin-ftp/wildanonyme.key /etc/ssl/private

sudo cp /var/www/vhosts/admin-ftp/GlobalSign_Root_RSA-OV-SSL_CA-
2018.crt /etc/ssl/certs
```

9. Appliquer les droits d'accès suivants pour les fichiers et répertoires

```
sudo chmod 644 /etc/ssl/certs/*.crt

sudo chmod 640 /etc/ssl/private/*.key

sudo chmod 710 /etc/ssl/private

sudo chown -R root:root /etc/ssl/

sudo chown -R root:ssl-cert /etc/ssl/private/
```

Configuration du site ssl

10. Editer le fichier SSL de configuration de l'hôte virtuel "is.anonyme",

```
sudo nano /etc/apache2/sites-enabled/ssl.isanonyme.conf

<IfModule mod_ssl.c>
      <VirtualHost _default_:443>
            ServerName localhost
            ServerAlias is.anonyme
            UsecanonicalName Off

            ServerAdmin webmaster@localhost

            DocumentRoot /var/www/vhosts/isanonyme/httpdocs

            ErrorLog ${APACHE_LOG_DIR}/error.ssl.isanonyme.log
            CustomLog ${APACHE_LOG_DIR}/access.ssl.isanonyme.log
combined

            […]

            SSLEngine On

            […]

            SSLCertificateFile    /etc/ssl/certs/wildanonyme.crt
            SSLCertificateKeyFile /etc/ssl/private/wildanonyme.key

            […]
            SSLCertificateChainFile
/etc/ssl/certs/GlobalSign_Root_RSA-OV-SSL_CA-2018.crt
            […]

            <Directory /var/www/vhosts/isanonyme/httpdocs>
                  AllowOverride All
            </Directory>
      </VirtualHost>
</IfModule>
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

11. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

12. Redémarrer le service Apache

```
sudo service apache2 restart
```

Tests du serveur web

13. Exécuter le même test qu'auparavant en saisissant https://ip-du-serveur

14. A ce stade, une erreur du type "BAD SSL CERT". C'est normal car le nom de domaine final n'est pas encore en usage pour le serveur web.

15. On ajoute une exception et la page de garde s'affiche.

Retrait de l'utilisateur admin-ftp

16. Suppression de l'utilisateur et des paramètres provisoires

```
sudo rm -rf /var/www/vhosts/admin-ftp

sudo deluser admin-ftp

sudo rm /etc/vsftpd/admin-ftp

sudo service vsftpd restart
```

Fin de configuration SSL

17. Eteindre le serveur.

```
sudo shutdown -P now
```

18. Effectuer un cliché instantané depuis hyper-v.

3ème partie – Installation et configuration de MySQL 8.x et PHP 8.x

MySQL 8.x

1. Lancer la commande d'installation

```
sudo apt-get update

sudo apt-get install mysql-server
```

2. Sécuriser la base de données

```
sudo mysql_secure_installation
```

3. A la question concernant "Validate password plugin", répondre "non" (No).
4. (Appliquer un mot de passe root simple du type « 123 »)
5. Répondre aux questions qui suivent par "Oui" (Yes)

Modification de l'administrateur MySQL

1. Modifier le nom de l'administrateur MySQL "root" en "msql-adm"

```
sudo mysql -u root

use mysql

# Sélectionner les champs à modifier
SELECT user,authentication_string,plugin,host FROM mysql.user;

# Modifier le mot de passe root et le mode d'authentification
ALTER USER 'root'@'localhost' IDENTIFIED WITH
mysql_native_password BY '[password]'; # Remplacer par un mot
de passe fort.

# Remplacer l'utilisateur "root" par l'utilisateur « msql-adm »

update user set user='admin-sql' where user='root';


# Vérifier les modificatrions
SELECT user,authentication_string,plugin,host FROM mysql.user;

flush privileges;

quit

sudo service mysql restart

# Vérifier la connexion en se connectant avec « msql-adm »
sudo mysql -u 'admin-sql' -p

# Une fois connecté, quitter mysql
quit
```

(Option) Autoriser l'accès distant à MySQL

1. Editer le fichier "/etc/mysql/mysql.conf.d/mysqld.cnf"
2. Modifier le fichier

```
sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf

# Instead of skip-networking the default is now to listen only
on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0 # modifier
mysqlx-bind-address     = 127.0.0.1
#
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)
4. Pour autoriser la connexion au travers du pare-feu "iptables", voir la section "(Option) Insertion dans "iptables" des entrées pour l'accès mySQL distant (INPUT & OUTPUT)"

Installation de PHP

1. Lancer la commande d'installation

```
sudo apt-get update

sudo apt-get install php libapache2-mod-php php-mysql
php-dev libmcrypt-dev php-pear
```

2. installer l'extension « mcrypt »:

```
sudo pecl channel-update pecl.php.net

sudo pecl install mcrypt-1.0.6 # Attention à la version
qui peut changer

Durant l'installation, presser "Enter".
```

3. installer les extensions suivantes:

   - php-common
   - php-gd
   - php-mysql
   - php-mcrypt
   - […]

```
sudo apt-get install php-cgi php-cli php-common php-curl php-
phpdbg php-gd php-gmp php-pgsql php-sqlite3 php-tidy php-xmlrpc
php-xsl libphp-embed php-fpm php-imap php-intl php-sybase php-
json php-simplexml php-dom php-mysqlnd
```

4. Vérifier quel fichier de configuration php.ini est utilisé

```
php -i | grep "Configuration File"
```

5. Editer le fichier /etc/php/8.1/<Path to Config File>/php.ini

```
sudo nano /etc/php/8.1/cli/php.ini

[…]

max_execution_time = 300

[…]

memory_limit = 256M

[…]

allow_url_fopen = Off

[…]

disable_functions =

[…]
```

```
expose_php = Off

[…]

html_errors = Off ; Décommenter et modifier la valeur

post_max_size = 128M

realpath_cache_size = 16M ; Décommenter et modifier la valeur

realpath_cache_ttl = 300 ; Décommenter et modifier la valeur

serialize_precision = 100

short_open_tag = On

upload_max_filesize = 32M

[…]

;extension=xmlrpc
;extension=xsl
extension=mcrypt.so

[…]
```

6. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

7. Copier le fichier php.ini vers « Apache »

```
sudo cp /etc/php/8.1/cli/php.ini /etc/php/8.1/apache2
```

8. Redémarrer le server Web

```
sudo service apache2 restart
```

9. Tester si mcrypt est bien installé

```
php -m | grep mcrypt

Retour de valeur: mcrypt
```

(En option) Installation de l'extension LDAP pour PHP

10. Installation de l'extension LDAP pour PHP

```
sudo apt-get install php-ldap

sudo service apache2 restart
```

11. Vérifier l'installation

    Dans la section suivante "Tests Web", vérifier qu'une section "LDAP" existe lors de l'affichage de la page "phpinfo.php".

(En option) Activer le démarrage automatique des sessions pour PHP

```
sudo nano /etc/php/8.1/cli/php.ini

[…]

; Initialize session on request startup.
; http://php.net/session.auto-start
session.auto_start = 1

[…]
```

12. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

13. Copier le fichier php.ini vers « Apache »

```
sudo cp /etc/php/8.1/cli/php.ini /etc/php/8.1/apache2
```

14. Redémarrer le server Web

```
sudo service apache2 restart
```

Tests Web

Tester PHP

15. Création d'un fichier d'affichage des infos PHP

```
sudo touch /var/www/vhosts/isanonyme/httpdocs/phpinfo.php

sudo nano  /var/www/vhosts/isanonyme/httpdocs/phpinfo.php
```

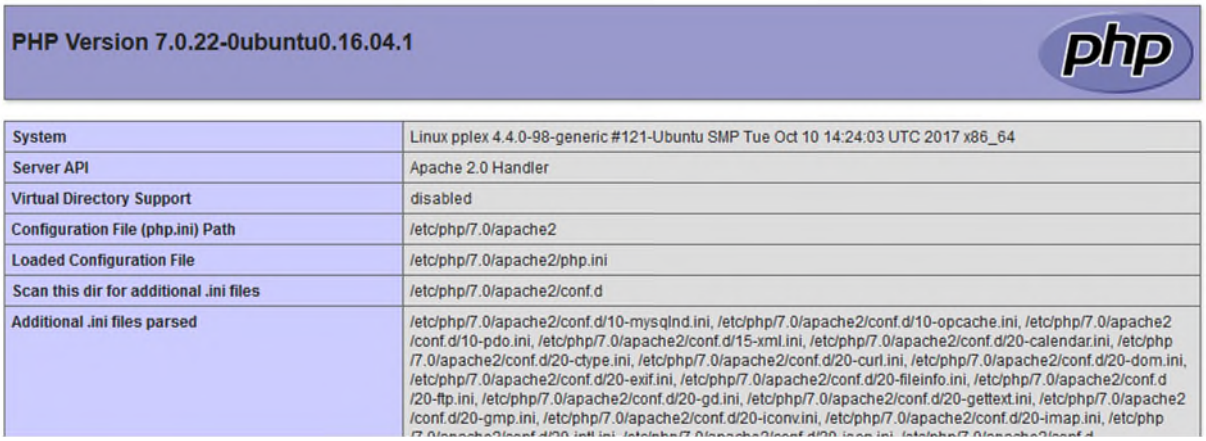
16. Ajouter la ligne suivante dans le fichier

```
<?php

$inipath = php_ini_loaded_file();

if ($inipath) {
    echo 'Loaded php.ini: ' . $inipath;
} else {
    echo 'A php.ini file is not loaded';
}

phpinfo();

?>
```

17. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

18. Tester la page PHP depuis le navigateur http://serveur/phpinfo.php

19. Résultat



PHP Version 7.0.22-0ubuntu0.16.04.1

System	Linux pplex 4.4.0-98-generic #121-Ubuntu SMP Tue Oct 10 14:24:03 UTC 2017 x86_64
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.0/apache2
Loaded Configuration File	/etc/php/7.0/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
Additional .ini files parsed	/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-ctype.ini, /etc/php/7.0/apache2/conf.d/20-curl.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-fileinfo.ini, /etc/php/7.0/apache2/conf.d/20-ftp.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gettext.ini, /etc/php/7.0/apache2/conf.d/20-gmp.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-imap.ini, /etc/php

Tester MySQL

20. Création d'un fichier d'affichage des infos PHP

```
sudo touch
/var/www/vhosts/isanonyme/httpdocs/phpmysql.php

sudo nano /var/www/vhosts/isanonyme/httpdocs/phpmysql.php
```

21. Ajouter le code suivant dans le fichier en remplaçant "password" par le mot de passe "root" MySQL

```
<?php
$link = mysqli_connect("127.0.0.1", "admin-sql",
"[password]", "mysql");

if (!$link) {
    echo "Error: Unable to connect to MySQL." . PHP_EOL;
    echo "Debugging errno: " . mysqli_connect_errno() .
PHP_EOL;
    echo "Debugging error: " . mysqli_connect_error() .
PHP_EOL;
    exit;
}

echo "Success: A proper connection to MySQL was made! The
mysql database is great." . PHP_EOL;
echo "Host information: " . mysqli_get_host_info($link) .
PHP_EOL;

mysqli_close($link);
?>
```

22. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

23. Tester la page depuis le navigateur http://serveur/phpmysql.php

24. Résultat

Success: A proper connection to MySQL was made! The mysql database is great. Host information: 127.0.0.1 via TCP/IP

25. Effacer les deux fichiers

```
sudo rm /var/www/vhosts/isanonyme/httpdocs/phpmysql.php

sudo rm /var/www/vhosts/isanonyme/httpdocs/phpinfo.php
```

4ème partie - Installation et/ou configuration de logiciels supplémentaires

Installation de PhpMyAdmin

6. Lancer la commande d'installation

```
sudo apt-get update

sudo apt-get install phpmyadmin
```

7. Durant l'installation, sélectionner l'option "Choose Apache2"

8. A la question "Configure database for phpmyadmin with dbconfig-common?" répondre "Yes"

9. Laisser le champ vide pour le mot de passe "MySQL application password for phpmyadmin".

10. Redémarrer le server Web

```
sudo service apache2 restart
```

11. Editer le fichier "/etc/phpmyadmin/apache.conf" comme suit:

```
sudo nano /etc/phpmyadmin/apache.conf

            # Alias /phpmyadmin /usr/share/phpmyadmin

            <Directory /usr/share/phpmyadmin>
                  Options FollowSymLinks
                  DirectoryIndex index.php
                  AllowOverride All
                  [...]
```

12. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

13. Editer le fichier de configuration du site web virtuel en mode SSL:

```
sudo nano /etc/apache2/sites-enabled/ssl.isanonyme.conf

<IfModule mod_ssl.c>
      <VirtualHost _default_:443>

            [...]

            Alias /PmA /usr/share/phpmyadmin

            <Directory /usr/share/phpmyadmin>
                  Options FollowSymLinks
                  DirectoryIndex index.php
                  AllowOverride All
                  <IfModule security2_module>
                        SecRuleEngine Off
                  </IfModule>
            </Directory>
      </VirtualHost>
</IfModule>
```

```
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

14. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

15. Modifier la configuration de "phpmadmin"

```
sudo nano /etc/phpmyadmin/config.inc.php

[…]

$cfg['Servers'][$i]['designer_settings'] = 'pma__designer_settings';
$cfg['Servers'][$i]['export_templates'] = 'pma__export_templates';
$cfg['Servers'][$i]['hide_db'] =
'^information_schema|mysql|phpmyadmin|performance_schema$';

    /* Uncomment the following to enable logging in to passwordless
accounts,

[…]

//$cfg['Servers'][$i]['host'] = '127.0.0.1'; //(Décommenter et
modifier)
```

16. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

17. Créer un répertoire pour les mots de passe

```
sudo mkdir -p /var/htpass/pma
```

18. Créer les utilisateurs pour le site "ssl.isanonyme"

```
sudo htpasswd -c -B /var/htpass/pma/.htpasswd [user_name_1]

sudo htpasswd -B /var/htpass/pma/.htpasswd [user_name_n]
```

19. Créer un fichier .htaccess dans le répertoire "/usr/share/phpmyadmin":

```
sudo nano /usr/share/phpmyadmin/.htaccess

AuthType Basic
AuthName "isanonyme Administration"
AuthUserFile /var/htpass/pma/.htpasswd
Require valid-user
```

20. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

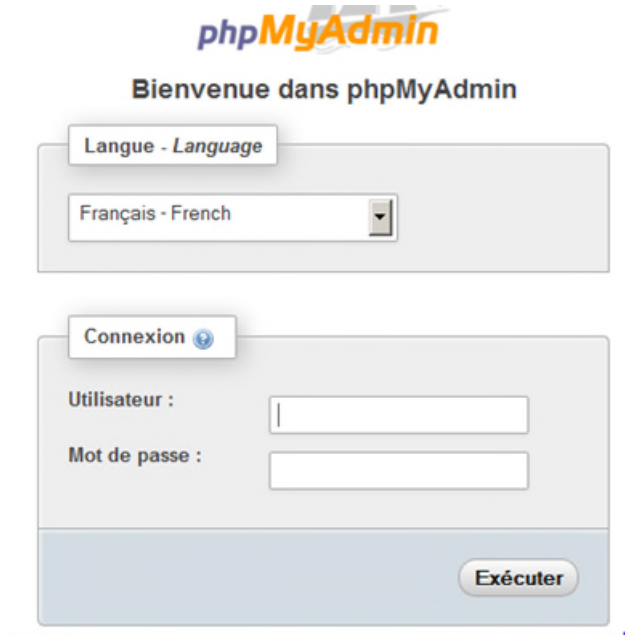
21. Redémarrer le serveur Web

```
sudo service apache2 restart
```

Tester PHPMyAdmin

1. Tester la page depuis le navigateur https://serveur/PmA

2. Résultat:



3. Eteindre le serveur.

```
sudo shutdown -P now
```

4. Effectuer un cliché instantané depuis hyper-v.

Installation de Postfix mail server

1. Lancer la commande d'installation

```
sudo apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules
```

2. Durant l'installation répondre comme suit:

   a. `General type of mail configuration:` `Satellite system`
   b. `System mail name:` `is.anonyme`
   c. `SMTP relay host:` `mail.anonyme`

3. Copier puis éditer le fichier "/etc/postfix/main.cf"

```
sudo cp /etc/postfix/main.cf /etc/postfix/main.cf.bak

sudo nano /etc/postfix/main.cf

[…]

relayhost = mail.anonyme
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = 192.168.xxx.xxx loopback-only
inet_protocols = ipv4

debug_peer_list=mail.anonyme.ch # (en option)
debug_peer_level=3 # (en option)
```

4. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

5. Relancer postfix

```
sudo /etc/init.d/postfix reload
```

6. Tester la configuration

```
echo "Test mail from postfix" | mail -s "Test Postfix" you@example.com
```

   En cas de problème, le fichier /var/log/mail.log fourni des explications sur les erreurs rencontrées.

7. Visualiser la queue e-mail

```
mailq
```

8. Supprimer les mails en attente

```
sudo postsuper -d ALL
```

Installation de "apticron"

Automatiser la recherche de mises à jour et avertir par mail avec "apticron"

1. Installer cron-apt

```
sudo apt-get update

sudo apt-get install apticron
```

2. Editer le fichier "/etc/apti/config/apticron.conf" et ajouter l'entrée suivante

```
sudo nano /etc/apticron/apticron.conf

EMAIL="webmaster@localhost"
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Pour supprimer les mails en attente en cas de nécessité:

```
sudo postsuper -d ALL
```

Installation de "AutoMySQLBackup"

Automatiser la sauvegarde des bases de données "MySQL"

1. Installer "automysqlbackup"

```
sudo apt-get update

sudo apt-get install automysqlbackup
```

2. Editer le fichier "/etc/automysqlbackup"

```
sudo nano /etc/default/automysqlbackup

[...]

BACKUPDIR="/var/lib/automysqlbackup"

[...]

MAILCONTENT="quiet" # voir les différentes options

MAILADDR=”webmaster@localhost” " # voir les différentes options

[...]

MAXATTSIZE="8000"

[...]

# Include CREATE DATABASE in backup?
CREATE_DATABASE=yes

# Separate backup directory and file for each DB? (yes or no)
SEPDIR=yes

# Which day do you want weekly backups? (1 to 7 where 1 is Monday)
DOWEEKLY=6

[...]

ROUTINES=yes
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

Restaurer depuis une sauvegarde

```
1.  cd /var/lib/automysqlbackup

2.  Au choix:

      cd daily
      cd weekly
      cd monthly

3.  Selon la base à restaurer, au choix:

      cd anonyme
      cd oldanonyme
      cd phpmyadmin
      cd rest

4.  Décompresser la sauvegarde:

      sudo gunzip fichier_exemple.sql.gz

5.  Restaurer la base

sudo mysql -h localhost -u [MySQL user] -p[password] [name of the
database] < [name of your sql dump, e.g. sqldump.sql]

exemple:

sudo mysql -h localhost -u root -p[MotDePasse] isanonyme <
/var/lib/automysqlbackup/daily/isanonyme/fichier_exemple.sql

(Le mot de passe doit être accolé à l'option "-p")
```

Configuration d'un utilisateur VsFTPD (Serveur FTP)

A l'instar de la configuration d'un utilisateur FTP provisoire précédemment, nous allons configurer des utilisateurs FTP permanents.

Création des utilisateurs FTP

1. Répéter le processus suivant pour chaque nouvel utilisateur FTP

    a. Créer un nouvel utilisateur

```
sudo adduser [user_name]

Enter new UNIX password:

Retype new UNIX password:

        Full Name []:[full_user_name]
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
```

    b. Editer un nouveau fichier dans "/etc/vsftpd"

```
cd /etc/vsftpd

sudo nano [user_name]

local_root=/var/www/vhosts/[nom du site]/httpdocs
```

    On ajoute "httpdocs" pour le cas où il n'est pas nécessaire de donner accès au niveau supérieur du site web.

    c. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

    d. Ajouter le nouvel utilisateur au groupe "www-data"

```
sudo adduser [user_name] www-data
```

    e. Modifier son répertoire de départ en le faisant pointer sur le répertoire /var/www/vhosts/[nom du site]

```
sudo mount --bind /var/www/vhosts/[nom du site]/httpdocs
/home/[user_name]/
```

    On ajoute "httpdocs" pour le cas où il n'est pas nécessaire de donner accès au niveau supérieur du site web.

f. Appliquer la redirection du répertoire de façon permanente en éditant le fichier "/etc/fstab"

```
sudo nano /etc/fstab

[…]

# Redirect user [user_name] home dir
/var/www/vhosts/[nom du site]/httpdocs  /home/[user_name]/ none
bind            0       0
```

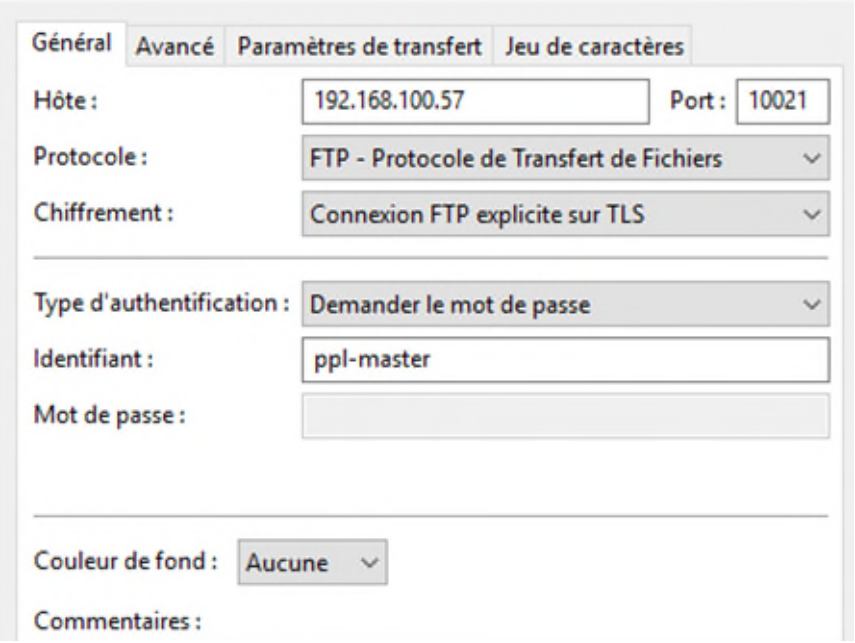
2. Redémarrer le service FTP

```
sudo service vsftpd restart
```

3. Tester la connexion à l'aide d'un client FTP.

Tester le service FTP

1. Lancer un client FTP du type "FileZilla"
2. Paramétrer la connexion comme l'exemple qui suit en adaptant :



3. Résultat: Obtention du listing du répertoire "/var/www/vhosts/nom du site" du serveur Web

4. Essai d'écriture. En cas d'échec, appliquer les commandes suivantes:

```
sudo chgrp -R www-data /var/www/vhosts/isanonyme

sudo chmod -R 775 /var/www/vhosts/isanonyme

sudo chmod -R g+s /var/www/vhosts/isanonyme

sudo service vsftpd restart
```

5. Répéter l'opération du point 4 pour les autres sites si nécessaire.

6. Arrêter le serveur

```
sudo shutdown -P now
```

7. Prendre un cliché instantané depuis hyper-v.

(En option) Installation de base de "Wordpress"

En tant que système de gestion de contenu pour le site isanonyme, wordpress peut être un outil convenable. L'installation proposée ici est basique et demande des travaux de développement additionnels, réalisés par des web designers professionnels.

Préambule

Avant l'installation, un nouvel utilisateur sera créé sur le serveur en tant qu'utilisateur "sudo". L'installation de Wordpress sera réalisée à l'aide de cet utilisateur. Egalement, il disposera des privilèges particuliers sur les répertoires Wordpress.

```
adduser admin-wpr

Indiquer un mot de passe dans le cours de la création

usermod -aG sudo admin-wpr
```

La poursuite de l'installation implique l'utilisation du nouvel utilisateur créé.

Aspect MySQL

1. Se déconnecter puis se reconnecter avec le nouvel utilisateur.

2. Créer une base de données

```
mysql -u msql-adm -p

CREATE DATABASE wordpress DEFAULT CHARACTER SET utf8 COLLATE
utf8_unicode_ci;
```

3. Créer un utilisateur MySQL spécifique à Wordpress

```
GRANT ALL ON wordpress.* TO 'wpr-adm'@'localhost' IDENTIFIED BY
'pp.lEx-17';

FLUSH PRIVILEGES;

Quit
```

Aspect PHP

4. Installer des extensions additionnelles pour php

```
sudo apt-get update

sudo apt-get install php-curl php-gd php-mbstring php-mcrypt
php-xml php-xmlrpc

sudo systemctl restart apache2
```

Aspects Apache2

5. Vérifier les directives de configuration afin de permettre les "overrides et "rewrites" du fichier ".htaccess".

```
sudo nano /etc/apache2/apache2.conf

[...]

<Directory /var/www/vhosts/>
        Options -Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

[...]
```

6. Si pas déjà réalisé, activer le module Apache "Rewrite"

```
sudo a2enmod rewrite
```

7. Tester la syntaxe de la configuration Apache

```
sudo apache2ctl configtest

Syntax OK
```

Aspects PHP

Installation de ImageMagik

```
sudo apt install imagemagick

sudo apt install php-imagick

sudo systemctl restart apache2
```

Vérifications

```
php -m | grep imagick

Réponse: imagick

php -r 'phpinfo();' | grep imagick

Réponse:

/etc/php/8.1/cli/conf.d/20-imagick.ini,
imagick
imagick module => enabled
imagick module version => 3.4.4
imagick classes => Imagick, ImagickDraw, ImagickPixel,
ImagickPixelIterator, ImagickKernel
imagick.locale_fix => 0 => 0
imagick.progress_monitor => 0 => 0
imagick.skip_version_check => 1 => 1
```

Aspects Wordpress

Téléchargement de WordPress

8. Suivre les directives suivantes:

```
cd /tmp

sudo curl -O https://wordpress.org/latest.tar.gz
```

9. Extraire le fichier téléchargé qui créera la structure des répertoires "Wordpress".

```
sudo tar xzvf latest.tar.gz
```

10. Créer le fichier ".htaccess" et paramétrer ses droits d'accès

```
sudo touch /tmp/wordpress/.htaccess

sudo chmod 660 /tmp/wordpress/.htaccess
```

11. Copier le fichier de configuration proposé en exemple en tant que fichier de configuration.

```
cp /tmp/wordpress/wp-config-sample.php /tmp/wordpress/wp-
config.php
```

12. Créer le répertoire "upgrade" afin de ne pas créer des problèmes de droits d'accès quand aux futures mises-à-jour de "Wordpress".

```
sudo mkdir /tmp/wordpress/wp-content/upgrade
```

13. Copier le répertoire "Wordpress" vers le dossier final.

```
sudo cp -a /tmp/wordpress/. /var/www/vhosts/isanonyme/httpdocs
```

Configurer le répertoire "Wordpress"

14. Prendre possession du répertoire

```
sudo chown -R www-data:www-data /var/www/vhosts/isanonyme
```

15. Paramétrer le bit "setgid" indiquant l'héritage des permissions des fichiers et répertoires

```
sudo find /var/www/vhosts/isanonyme -type d -exec chmod 755 {}
\;
```

16. Allouer les droits d'écriture sur le répertoire "wp-content" afin de permettre les modifications des thèmes et modules additionnels par l'interface web.

```
sudo chmod -R 755 /var/www/vhosts/isanonyme/httpdocs/wp-content
```

17. Allouer les droits d'écriture au serveur web sur ces répertoires

```
sudo chmod -R g+w /var/www/vhosts/isanonyme/httpdocs/wp-
content/themes

sudo chmod -R g+w /var/www/vhosts/isanonyme/httpdocs/wp-
content/plugins
```

Paramétrer le fichier de configuration "Wordpress"

18. Générer des clefs secrètes d'accès via le générateur de clefs "Wordpress".

```
curl -s https://api.wordpress.org/secret-key/1.1/salt/

define('AUTH_KEY',         'BWDx*6IoPkO1#]
s[}ooIWSho(=dfAd$vK9@%!UX*2RNB4>8+3PJ9JSXo/LYjCOf');
define('SECURE_AUTH_KEY',  ',46442`m:V<SDoj][0G*&m5R7-*z-g._WnU;s[e})POt2
ykP@@t5z{mD0+6$nC*');
define('LOGGED_IN_KEY',    '&+`YG(CW9
[s+wQySnP`=>.,e<DQBHwEIs2$=3zF.x/jo&cVZy|70H|,>ud|0|gn');
define('NONCE_KEY',        'Dc%=`64J2r3XZo]1 ljoUB5%v|*IIm-
U~+PEGp+?>^%s,bD|.1kCX=}~cH^37f(x');
define('AUTH_SALT',
'cBJ6Hq5)R!GC/+6^Y|6p2gfA[Lo*wLA+|!CIBr/^h|`|RgsbOhq?Th>F/sM)V.?(');
define('SECURE_AUTH_SALT', 'D&m.+hrusym?J%@AJ-;{,OPXSh6KX-p<`TCq]_E-
Q{$|P#(pnYS8Iby.=g`O%qj/');
define('LOGGED_IN_SALT',   '+E[r<H }n9;Kd)vI~QZJ@ilI[8awI[my-hm^DS.WL8BB,H-
D/|:5B$D*7TL4(IjT');
define('NONCE_SALT',       'U/U$RBLr&zQNp:[lZ%u2B w
I`J5g{su+j;I4.qyHx:Xh+~f+z7Tb]~8DD,%pO,)');

Le valeurs ci-dessus sont des exemples et ne doivent pas être
copiées. Utiliser les valeurs obtenues lors du lancement de la
commande.
```

19. Ouvrir le fichier de configuration "Wordpress" et effectuer les modification suivantes:

```
sudo nano /var/www/vhosts/isanonyme/httpdocs/wp-config.php

[...]

define('DB_NAME', 'wordpress'); (Nom de la base de données)

/** MySQL database username */
define('DB_USER', 'wordpressuser'); (Utilisateur "Wordpress" de la
base de données)

/** MySQL database password */
define('DB_PASSWORD', 'password'); (Mot de passe de l'utilisateur)

[...]

define('AUTH_KEY',         'REMPLACER PAR LES VALEURS OBTENUES');
define('SECURE_AUTH_KEY',  'REMPLACER PAR LES VALEURS OBTENUES');
define('LOGGED_IN_KEY',    'REMPLACER PAR LES VALEURS OBTENUES');
define('NONCE_KEY',        'REMPLACER PAR LES VALEURS OBTENUES');
define('AUTH_SALT',        'REMPLACER PAR LES VALEURS OBTENUES');
define('SECURE_AUTH_SALT', 'REMPLACER PAR LES VALEURS OBTENUES');
define('LOGGED_IN_SALT',   'REMPLACER PAR LES VALEURS OBTENUES');
define('NONCE_SALT',       'REMPLACER PAR LES VALEURS OBTENUES');

define('FS_METHOD', 'direct');

[...]
```

Fin d'installation

20. Achever l'installation depuis l'interface web du serveur.

Note

1. Lorsqu'une mise-à-jour est disponible, se connecter sur le serveur avec l'utilisateur employé pour installer "Wordpress".

2. Accorder temporairement le droit d'accès au processus du serveur au répertoire racine complet du site.

```
sudo chown -R www-data /var/www/vhosts/isanonyme

Puis, une fois terminé:

sudo chown -R admin-web /var/www/vhosts/isanonyme
```

(En option) Installation des utilitaires DNS

1. Installation des outils DNS

```
sudo apt install dnsutils
```

2. Vérifier l'installation

```
dig -v

Réponse:

DiG 9.16.1-Ubuntu
```

Fin d'installation des logiciels

1. Mettre le serveur à jour

```
sudo apt-get update

sudo apt-get upgrade
```

2. Arrêter le serveur

```
sudo shutdown -P now
```

3. Prendre un cliché instantané depuis hyper-v.

5ème partie - Sécurisation du système

Pare-Feu "iptables"

Programmation

1. Vérifier que le pare-feu "iptables" accepte tous les paquets par défaut.

```
sudo iptables -L

Doit donner le résultat suivant:

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

2. Supprimer toutes les entrées dans "iptables".

```
sudo iptables -F
```

3. Supprimer les entrées de chaînes

```
sudo iptables -X
```

4. Dans le cas d'une installation réalisée à distance (avec ssh), on prêtera attention à s'assurer de programmer un accès SSH dans iptables AVANT de fermer les accès par défaut.

Configuration "iptables" en ENTREE (INPUT)

D'une manière générale, en orange les commentaires, en blanc les instructions, en gris foncé ce qui ne s'applique pas, mais à toutes fins utiles.

```
# Accepter le trafic de l'interface de bouclage
sudo iptables -A INPUT -i lo -p all -j ACCEPT

# Accepter la négociation à 3 voies
# sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

### Supprimer les paquets d'usurpation d'adresse (Spoofing)
sudo iptables -A INPUT -s 10.0.0.0/8 -j DROP
sudo iptables -A INPUT -s 169.254.0.0/16 -j DROP
sudo iptables -A INPUT -s 172.16.0.0/12 -j DROP
sudo iptables -A INPUT -s 127.0.0.0/8 -j DROP
sudo iptables -A INPUT -s 192.168.0.0/24 -j DROP
sudo iptables -A INPUT -s 224.0.0.0/4 -j DROP
sudo iptables -A INPUT -d 224.0.0.0/4 -j DROP
sudo iptables -A INPUT -s 240.0.0.0/5 -j DROP
sudo iptables -A INPUT -d 240.0.0.0/5 -j DROP
sudo iptables -A INPUT -s 0.0.0.0/8 -j DROP
sudo iptables -A INPUT -d 0.0.0.0/8 -j DROP
sudo iptables -A INPUT -d 239.255.255.0/24 -j DROP
sudo iptables -A INPUT -d 255.255.255.255 -j DROP

# Protection contre les attaques ICMP au moyen d'IP forgées (SMURF)
sudo iptables -A INPUT -p icmp -m icmp --icmp-type address-mask-request -j DROP
sudo iptables -A INPUT -p icmp -m icmp --icmp-type timestamp-request -j DROP
sudo iptables -A INPUT -p icmp -m limit --limit 1/second -j ACCEPT

# Suppression de tous les paquets invalides
sudo iptables -A INPUT -m state --state INVALID -j DROP

# Protection contre le Déni de service, rejet d'attaques "SMURF"
sudo iptables -A INPUT -p tcp -m tcp --tcp-flags RST RST -m limit --limit 2/second
--limit-burst 2 -j ACCEPT

# Protection contre le balayage de port
# Les adresses IP d'attaques seront bloquées pour 24h (3600 x 24 = 86400 Secondes)
sudo iptables -A INPUT -m recent --name portscan --rcheck --seconds 86400 -j DROP

# Retrait des adresses IP d'attaques de la liste noire
sudo iptables -A INPUT -m recent --name portscan --remove

# Ces rôles ajoutent les scanners à la liste des ports scannés et journalise les
# tentatives.
sudo iptables -A INPUT -p tcp -m tcp --dport 139 -m recent --name portscan --set -j
LOG --log-prefix "portscan:"
sudo iptables -A INPUT -p tcp -m tcp --dport 139 -m recent --name portscan --set -j
DROP

# Autoriser le serveur à accéder aux ports desservis depuis l'extérieur sur
l'interface  "ens33".
sudo iptables -A INPUT -i ens33 -p udp --match multiport --sports 53,123 -m state -
-state ESTABLISHED -j ACCEPT

sudo iptables -A INPUT -i ens33 -p tcp --match multiport --sports 80,443 -m state -
-state ESTABLISHED -j ACCEPT

# Autoriser l'accès aux sites web desservis par le serveur sur l'interface "ens33".
sudo iptables -A INPUT -i ens33 -p tcp --match multiport --dports 80,443,8080,8443
-m state --state NEW,ESTABLISHED -j ACCEPT

# Autoriser l'accès aux outils de maintenance desservis par le serveur sur
l'interface "ens33" (FTP, SSH, MySQL).
sudo iptables -A INPUT -i ens33 -p tcp -s 192.168.0.0/16 --match multiport --dports
3306,10021,10022,10443,20443 -m state --state NEW,ESTABLISHED -j ACCEPT
```

```
# Autoriser l'accès aux outils de maintenance desservis par le serveur sur
l'interface "ens33" (échange FTP).
sudo iptables -A INPUT -i ens33 -p tcp -s 192.168.0.0/16 --dport 10090:10200 -m
state --state NEW,ESTABLISHED -j ACCEPT

# Autoriser le flux SMTP depuis des serveurs de messagerie externes via l'interface
"ens33".
sudo iptables -A INPUT -i ens33 -p tcp --match multiport --sports 25,465 -m state -
-state ESTABLISHED -j ACCEPT

# Interdire les "pings" signifie que le port ICMP est fermé sur "ens33".
sudo iptables -A INPUT -p icmp -m icmp --icmp-type 8 -j REJECT
```

Configuration "iptables" en SORTIE (OUTPUT)

```
## Autoriser l'interface de bouclage en sortie
sudo iptables -A OUTPUT -o lo -j ACCEPT

# sudo iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# Suppression de tous les paquets invalides
sudo iptables -A OUTPUT -m state --state INVALID -j DROP

# Autoriser les ports et IP suivants en sortie sur l'interface "ens33"
sudo iptables -A OUTPUT -o ens33 -p udp --match multiport --dports 53,123 -m state
--state NEW,ESTABLISHED -j ACCEPT

sudo iptables -A OUTPUT -o ens33 -p tcp --match multiport --dports 80,443 -m state
--state NEW,ESTABLISHED -j ACCEPT

# Autoriser l'accès aux sites web desservis par le serveur sur l'interface "ens33".
sudo iptables -A OUTPUT -o ens33 -p tcp --match multiport --sports 80,443,8080,8443
-m state --state ESTABLISHED -j ACCEPT

# Autoriser l'accès aux outils de maintenance desservis par le serveur sur
l'interface "ens33" (FTP, SSH, MySQL).

sudo iptables -A OUTPUT -o ens33 -p tcp --match multiport --sports
3306,10021,10022,10443,20443 -m state --state ESTABLISHED -j ACCEPT

# Autoriser l'accès aux outils de maintenance desservis par le serveur sur
l'interface "ens33" (échange FTP).
sudo iptables -A OUTPUT -o ens33 -p tcp -d 192.168.0.0/16 --sport 10090:10200 -m
state --state ESTABLISHED -j ACCEPT

# Autoriser le flux SMTP vers les serveurs Exchange vis l'interface "ens33".

sudo iptables -A OUTPUT -o ens33 -p tcp --match multiport --dport 25,465 -m state -
-state NEW,ESTABLISHED -j ACCEPT

# Suppression des réponses "ping"
sudo iptables -A OUTPUT -p icmp -m icmp --icmp-type 8 -j REJECT
```

Configuration "iptables" en TRANSMISSION (FORWARD)

```
# Suppression de tous les paquets invalides
sudo iptables -A FORWARD -m state --state INVALID -j DROP

# Protection contre le balayage de port
# Les adresses IP d'attaques seront bloquées pour 24h (3600 x 24 = 86400 Secondes)
sudo iptables -A FORWARD -m recent --name portscan --rcheck --seconds 86400 -j DROP

# Retrait des adresses IP d'attaques de la liste noire
sudo iptables -A FORWARD -m recent --name portscan --remove

# Ces rôles ajoutent les scanners à la liste des ports scannés et journalise les
# tentatives.
sudo iptables -A FORWARD -p tcp -m tcp --dport 139 -m recent --name portscan --set
-j LOG --log-prefix "portscan:"

sudo iptables -A FORWARD -p tcp -m tcp --dport 139 -m recent --name portscan --set
-j DROP
```

Configuration "iptables" en "w00t" et "w00tchain" (Protection Apache2)

```
### Protection contre les attaques w00t (Apache)
# vérifie si l'IP est déjà présente dans la liste w00tlist.
sudo iptables -A INPUT -p tcp -m recent --name w00tlist --update --seconds 21600 -j
DROP

# Création de la chaîne w00t :
sudo iptables -N w00tchain

# Création de la chaine w00tchain qui rajoute l'IP à la liste w00tlist et reset la
# connexion

sudo iptables -A w00tchain -m recent --set --name w00tlist -p tcp -j REJECT --
reject-with tcp-reset

# création de notre chaîne w00t
sudo iptables -N w00t

# redirige les paquets TCP sur notre chaîne :
sudo iptables -A INPUT -p tcp -j w00t

### Protection contre les attaques w00t (Apache)
# chaîne w00t : recherche du premier SYN et création de la liste :
sudo iptables -A w00t -m recent -p tcp --syn --match multiport --dports
80,443,20443 --set

# recherche du paquet SYN,ACK et mise à jour la liste :
sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,SYN,ACK SYN,ACK --match
multiport --sports 80,443,8080,8443,10443,20443 --update

# recherche du paquet ACK et mise à jour la liste :
sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,SYN,ACK ACK --match
multiport --dports 80,443,8080,8443,10443,20443 --update

# Recherche de la signature hexadécimale dans le prenier PSH+ACK.
# Si elle est présente, on renvoie sur w00tchain pour blacklister et
# terminer la connexion.
# On supprime la liste pour ne pas filtrer les paquets suivants :
sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,ACK PSH,ACK --dport 80 --
remove -m string --to 80 --algo bm --hex-string '|485454502f312e310d0a0d0a|' -j
w00tchain

sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,ACK PSH,ACK --dport 443 --
remove -m string --to 443 --algo bm --hex-string '|485454502f312e310d0a0d0a|' -j
w00tchain

sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,ACK PSH,ACK --dport 443 --
remove -m string --to 8080 --algo bm --hex-string '|485454502f312e310d0a0d0a|' -j
w00tchain

sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,ACK PSH,ACK --dport 443 --
remove -m string --to 8443 --algo bm --hex-string '|485454502f312e310d0a0d0a|' -j
w00tchain

sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,ACK PSH,ACK --dport 20443 --
remove -m string --to 10443 --algo bm --hex-string '|485454502f312e310d0a0d0a|' -j
w00tchain

sudo iptables -A w00t -m recent -p tcp --tcp-flags PSH,ACK PSH,ACK --dport 20443 --
remove -m string --to 20443 --algo bm --hex-string '|485454502f312e310d0a0d0a|' -j
w00tchain
```

(Option) Insertion dans "iptables" des entrées pour l'authentification LDAP/Active Drirectory (INPUT & OUTPUT)

```
sudo iptables -I INPUT 29 -i ens33 -p udp --match multiport -s 192.168.1.0/24 --
sports 389,636 -m state --state ESTABLISHED -j ACCEPT

sudo iptables -I INPUT 29 -i ens33 -p tcp --match multiport -s 192.168.1.0/24 --
sports 389,636 -m state --state ESTABLISHED -j ACCEPT

sudo iptables -I OUTPUT 7 -o ens33 -p udp --match multiport -d 192.168.1.0/24 --
dports 389,636 -m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -I OUTPUT 7 -o ens33 -p tcp --match multiport -d 192.168.1.0/24 --
dports 389,636 -m state --state NEW,ESTABLISHED -j ACCEPT
```

(Option) Insertion dans "iptables" des entrées pour l'accès mySQL distant (INPUT & OUTPUT)

Le port par défaut de MySQL (3306) est uilisé

Le périmètre d'accès est dévolu à une seule adresse IP

```
sudo iptables -I INPUT 30 -i ens33 -s 192.168.1.0/24 -p tcp --destination-port 3306
-m state --state NEW,ESTABLISHED -j ACCEPT

sudo iptables -I OUTPUT 9 -o ens33 -p tcp --source-port 3306 -d 192.168.1.0/24 -m
state --state ESTABLISHED -j ACCEPT
```

Fin de configuration "iptables"

1. Interdire les communications par défaut

```
sudo iptables -P INPUT DROP

sudo iptables -P OUTPUT DROP

sudo iptables -P FORWARD DROP
```

2. Installer iptables-persistent

```
sudo apt-get update

sudo apt-get install iptables-persistent
```

3. Durant l'installation, répondez "Yes" à la question de savoir si vous souhaitez sauvegarder les règles.
4. La sauvegarde est effectuée dans le répertoire "/etc/iptables"
5. Pour sauver les règles iptables à nouveau :

```
sudo dpkg-reconfigure iptables-persistent
```

6. Répondre « yes » pour écraser les anciennes règles IPv4
7. Répondre « yes » pour écraser les anciennes règles IPv6
8. Si la sauvegarde ne fonctionne pas:

```
# Change to root first
sudo su

# Save current iptables ipv4 rules
iptables-save > /etc/iptables/rules.v4

# Save current iptables ipv6 rules
iptables-save > /etc/iptables/rules.v6
```

9. Arrêter le serveur

```
sudo shutdown -P now
```

10. Prendre un cliché instantané depuis hyper-v.

Tests

11. Démarrer le serveur.
12. Si tout se passe bien:
    a. On peut utiliser l'outil "NMAP" p. ex. pour scanner des ports, qui ne devrait retourner aucun résultat.

       Ceci fait, l'adresse de la machine utilisée pour le scan sera en liste noire pour 24h.

    b. Le serveur ne reçoit pas de réponse "ping".
    c. On peut se connecter au serveur en SSH (port 10022)
    d. On pourra se connecter au serveur en http (ports 80), https (port 443, 20443), ftp (port 10021), une fois ces services installés.
    e. Le système pourra envoyer des mails.
13. Pour une information complète de "iptables"

```
sudo iptables -L -nvx

ou

sudo iptables -L -n -v --line-numbers
```

14. Commandes utiles

```
# Autoriser l'ensemble du trafic

sudo iptables -P INPUT ACCEPT

sudo iptables -P OUTPUT ACCEPT

sudo iptables -P FORWARD ACCEPT

# Supprimer une ligne

sudo iptables -D <DIRECTION> <N° DE LIGNE>

Ex:

sudo iptables -D OUTPUT 5
```

Sécurisation du protocole IP

1. Copier et éditer les fichiers "/etc/sysctl.d/10-network-security.conf" et "/etc/sysctl.conf"

```
sudo mv /etc/sysctl.conf /etc/sysctl.conf.bak

sudo mv /etc/sysctl.d/10-network-security.conf /etc/sysctl.d/10-
network-security.conf.bak
```

2. Editer le fichier et ajouter les commandes suivantes en fin de fichier:

```
sudo nano /etc/sysctl.d/10-network-security.conf

# Ignore ICMP broadcast requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Disable ip forwarding
net.ipv4.ip_forward = 0
net.ipv6.conf.default.forwarding=0
net.ipv6.conf.all.forwarding=0

# Disable source packet routing
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
net.ipv4.conf.default.accept_source_route = 0
net.ipv6.conf.default.accept_source_route = 0

# Ignore send redirects
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.send_redirects = 0

# Block SYN attacks
net.ipv4.tcp_max_syn_backlog = 2048
net.ipv4.tcp_synack_retries = 2
net.ipv4.tcp_syn_retries = 5

# Log Martians
net.ipv4.conf.all.log_martians = 1
net.ipv4.icmp_ignore_bogus_error_responses = 1

# Ignore ICMP redirects
net.ipv4.conf.all.accept_redirects = 0
net.ipv6.conf.all.accept_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv6.conf.default.accept_redirects = 0

# Ignore Directed pings
net.ipv4.icmp_echo_ignore_all = 1
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Copier le fichier vers "/etc/sysctl.conf"

```
sudo cp /etc/sysctl.d/10-network-security.conf /etc/sysctl.conf
```

5. Relancer les processus liés "/etc/sysctl.conf"

```
sudo sysctl -p /etc/sysctl.conf

sudo service procps start
```

Sécurisation de la mémoire partagée

1. Editer le fichier "/etc/fstab" et inscrire la ligne suivante:

```
sudo nano /etc/fstab

# protect shared memory
tmpfs     /run/shm     tmpfs     defaults,noexec,nosuid     0     0
```

2. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

Protection contre le "spoofing"

1. Editer le fichier " /etc/host.conf" comme suit:

```
sudo nano /etc/host.conf

order bind,hosts
multi on
```

2. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

3. Redémarrer le serveur

```
sudo reboot now
```

Protection supplémentaire du site web

1. Créer un nouveau fichier « .htaccess » avec « nano » dans « /var/www/vhosts/nom du site/httpdocs/ ».

```
sudo nano /var/www/vhosts/isanonyme/httpdocs/.htaccess
```

2. Inscrire les commandes qui suivent pour empêcher des attaques de script inter-sites (cross-site scripting XSS)

```
<IfModule mod_headers.c>
      Header set X-XSS-Protection "1; mode=block"
</IfModule>
```

5. Sauvegarder et quitter (Ctrl + O, Ctrl + X).

Complément d'installation du (des) site(s)

Is.anonyme

1. Se connecter en "root" sur "MySQL" via "PhpMyAdmin"
2. Créer une base de données en interclassement "UTF8_general_ci" pour loger les donnéees
3. Créer un utilisateur "MySQL" employé lors de l'accès à la base de données depuis le site web.
4. Allouer des droits sur la base de données pour le nouvel utilisateur :
    a. Droits complets de modification des données
    b. Pas de droits concernant l'infrastructure des tables
    c. Pas de droits concernant l'administration
5. Créer un utilisateur "MySQL" employé lors de l'accès à la base de données depuis phpMyAdmin.
6. Allouer des droits sur la base de données à l'utilisateur chargé de la maintenance de la base :
    d. Droits complets de modification des données
    e. Droits complets concernant structure des tables
    f. Pas de droits concernant l'administration
7. Tester les comptes.
8. Vérifier l'accès à la base de données

Sécuriser PHP

9. Editer le fichier /etc/php/8.1/cli/php.ini
10. Modifier comme suit:

```
sudo nano /etc/php/8.1/cli/php.ini

[…]

disable_functions =
pcntl_alarm,pcntl_fork,pcntl_waitpid,pcntl_wait,pcntl_wifexited
,pcntl_wifstopped,pcntl_wifsignaled,pcntl_wexitstatus,pcntl_wte
rmsig,pcntl_wstopsig,pcntl_signal,pcntl_signal_dispatch,pcntl_g
et_last_error,pcntl_strerror,pcntl_sigprocmask,pcntl_sigwaitinf
o,pcntl_sigtimedwait,pcntl_exec,pcntl_getpriority,pcntl_setprio
rity,apache_child_terminate,apache_setenv,define_syslog_variabl
es,escapeshellarg,escapeshellcmd,eval,exec,fp,fput,ftp_connect,
ftp_exec,ftp_get,ftp_login,ftp_nb_fput,ftp_put,ftp_raw,ftp_rawl
ist,highlight_file,ini_alter,ini_get_all,ini_restore,inject_cod
e,mysql_pconnect,openlog,passthru,php_uname,phpAds_remoteInfo,p
hpAds_XmlRpc,phpAds_xmlrpcDecode,phpAds_xmlrpcEncode,popen,posi
x_getpwuid,posix_kill,posix_mkfifo,posix_setpgid,posix_setsid,p
osix_setuid,posix_setuid,posix_uname,proc_close,proc_get_status
,proc_nice,proc_open,proc_terminate,shell_exec,syslog,system,xm
lrpc_entity_decode,ezmlm_hash,

[…]
max_execution_time = 300
[…]
memory_limit = 256M
[…]
display_errors = Off
[…]
track_errors = Off
[…]
```

11. Sauvegarder et quitter (Ctrl + O, Ctrl + X)
12. Copier le fichier php.ini vers « Apache »

```
sudo cp /etc/php/8.1/cli/php.ini /etc/php/8.1/apache2
```

Sécuriser Apache2

1. Editer le fichier "/etc/apache2/conf-enabled/security.conf"
2. Modifier comme suit:

```
sudo nano /etc/apache2/conf-enabled/security.conf

[…]

ServerTokens Prod

[…]

ServerSignature Off

[…]

TraceEnable Off

[…]

Header set X-Content-Type-Options: "nosniff" (décommenter)

[…]

Header set X-Frame-Options: "sameorigin" (décommenter)

Header unset ETag
FileETag None

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)
4. Pour la prise en compte de ces changements, activer "mod_headers"

```
sudo ln -s /etc/apache2/mods-available/headers.load /etc/apache2/mods-enabled/headers.load
```

5. Redémarrer Apache2

```
sudo service apache2 restart
```

Installer et configurer "ModSecurity" et « OWASP »

1. Lancer la commande d'installation

```
sudo apt-get update

sudo apt-get install libapache2-mod-security2

sudo apachectl -M | grep security

sudo cp /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf
```

2. Editer le fichier "/etc/modsecurity/modsecurity.conf"

```
sudo nano /etc/modsecurity/modsecurity.conf

[...]

SecRuleEngine On

[...]

SecRequestBodyLimit 32768000 ou ()

[...]

SecRequestBodyInMemoryLimit 327680

[...]

SecResponseBodyAccess Off
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Redémarrer Apache2.

```
sudo systemctl restart apache2
```

5. Installer "Open Web Application Security Project Core Rule Set"

```
sudo mv /usr/share/modsecurity-crs
/usr/share/modsecurity-crs.bk

sudo git clone https://github.com/SpiderLabs/owasp-
modsecurity-crs.git /usr/share/modsecurity-crs
```

6. Editer le fichier “/etc/apache2/mods-enabled/security2.conf”

```
sudo nano /etc/apache2/mods-enabled/security2.conf

<IfModule security2_module>
        # Default Debian dir for modsecurity's persistent data
        SecDataDir /var/cache/modsecurity

        # Include all the *.conf files in /etc/modsecurity.
        # Keeping your local configuration in that directory
        # will allow for an easy upgrade of THIS file and
        # make your life easier
        IncludeOptional /etc/modsecurity/*.conf

        # Include OWASP ModSecurity CRS rules if installed
        IncludeOptional /usr/share/modsecurity-crs/*.load
        IncludeOptional /usr/share/modsecurity-crs/*.conf
        IncludeOptional /usr/share/modsecurity-crs/rules/*.conf
</IfModule>
```

7. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

8. Copier le fichier « crs-setup.conf »

```
sudo cp /usr/share/modsecurity-crs/crs-setup.conf.example
/usr/share/modsecurity-crs/crs-setup.conf
```

9. Redémarrer Apache2.

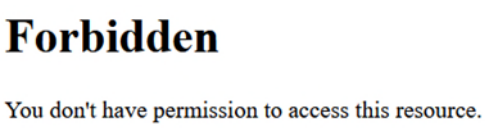
```
sudo systemctl restart apache2
```

Test de ModSecurity

10. Depuis un navigateur saisir le lien suivant:

```
http://[adresse du serveur]/aphpfilethatdonotexist.php?something=../../etc
```

11. Sur la page la réponse doit être :



12. Aller dans les journaux /var/log/apache2/error.isanonyme.log et vérifier :

```
[Fri May 29 13:20:21.919729 2020] [:error] [pid 45880] [client
192.168.104.150:50556] [client 192.168.xxx.xxx] ModSecurity: Access denied
with code 403 (phase 2). Operator GE matched 5 at TX:anomaly_score. [file
"/usr/share/modsecurity-crs/rules/REQUES>[…]

[Fri May 29 13:20:21.919986 2020] [:error] [pid 45880] [client
192.168.104.150:50556] [client 192.168.xxx.xxx] ModSecurity: Warning.
Operator GE matched 5 at TX:inbound_anomaly_score. [file
"/usr/share/modsecurity-crs/rules/RESPONSE-980-CORRELATION.con>[…]
```

Installer et configurer "mod_evasive"

1. Lancer la commande d'installation

```
sudo apt-get install libapache2-mod-evasive

sudo mkdir /var/log/mod_evasive

sudo chown www-data:www-data /var/log/mod_evasive
```

2. Editer le fichier "/etc/apache2/mods-available/evasive.conf"

```
sudo nano /etc/apache2/mods-available/evasive.conf

<IfModule mod_evasive20.c>
    DOSHashTableSize    3097 (décommenter)
    DOSPageCount        12 (décommenter)
    DOSSiteCount        400 (décommenter)
    DOSPageInterval     2 (décommenter)
    DOSSiteInterval     2 (décommenter)
    DOSBlockingPeriod   20 (décommenter)

    DOSEmailNotify      webmaster@localhost (décommenter)
    #DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    DOSLogDir           "/var/log/mod_evasive" (décommenter)
</IfModule>
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Si nécessaire lier symboliquement le fichier

```
sudo ln -s /etc/apache2/mods-available/evasive.conf
/etc/apache2/mods-enabled/evasive.conf
```

5. Redémarrer Apache2

```
sudo service apache2 restart
```

Installer et configurer "rootkit checker"

1. Lancer la commande d'installation

```
sudo apt-get install rkhunter chkrootkit
```

2. Editer le fichier "/etc/chkrootkit.conf"

```
sudo nano /etc/chkrootkit.conf

RUN_DAILY="true"
RUN_DAILY_OPTS=""
DIFF_MODE="false"
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

4. Editer le fichier "/etc/default/rkhunter"

```
sudo nano /etc/default/rkhunter

[...]

# Set this to yes to enable rkhunter daily runs
# (default: true)
CRON_DAILY_RUN="true"

# Set this to yes to enable rkhunter weekly database
updates
# (default: true)
CRON_DB_UPDATE="true"

REPORT_EMAIL="webmaster@localhost" # Voir si opportun

[...]
```

5. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

6. Déplacer les fichiers suivants:

```
sudo mv /etc/cron.weekly/rkhunter /etc/cron.weekly/rkhunter_update

sudo mv /etc/cron.daily/rkhunter /etc/cron.weekly/rkhunter_run

sudo mv /etc/cron.daily/chkrootkit /etc/cron.weekly/
```

7. Modifier le fichier « /etc/rkhunter.conf

```
sudo nano /etc/rkhunter.conf

UPDATE_MIRRORS=1

[…]

MIRRORS_MODE=0

[…]
ALLOWIPCPROC=/usr/sbin/apache2

WEB_CMD=""
```

8. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

9. Commandes de contrôle « rkhunter »

```
Vérifier que vous avez la dernière version :

sudo rkhunter --versioncheck

Mettre à jour le programme :

sudo rkhunter --update

Lister les différents tests effectués :

sudo rkhunter --list

Effectuer une vérification :

sudo rkhunter --checkall
```

10. Commande de « réalignement » « rkhunter »

    Lors d'une mise à jour du serveur, des fichiers systèmes peuvent être modifiés, induisant « rkhunter » en erreur puisqu'il détecte des changements inconnus sur des fichiers système.
    Dans ce cas, il faut ecxécuter la comande suivante pour réaligner la base de données du programme avec les nouvelles versions de fichiers installés :

```
sudo rkhunter --propupd
```

Installer et configurer "logwatch"

1. Lancer la commande d'installation

```
sudo apt-get install logwatch

sudo mv /etc/cron.daily/00logwatch /etc/cron.weekly/
```

2. Editer le fichier "/etc/cron.weekly/00logwatch"

```
sudo nano /etc/cron.weekly/00logwatch

#execute
/usr/sbin/logwatch --mailto webmaster@localhost --range 'between -7
days and -1 days'
```

3. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

Installer et activer "process accounting"

1. Lancer la commande d'installation

```
sudo apt-get install acct

sudo touch /var/log/wtmp
```

Installer et configurer "Fail2ban"

1. Lancer la commande d'installation

```
sudo apt-get update

sudo apt-get install fail2ban
```

2. Effectuer des copies du fichier "/etc/fail2ban/jail.conf"

```
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.bak

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

11. Editer le fichier "/etc/fail2ban/jail.local" (Début)

```
sudo nano /etc/fail2ban/jail.local

[…]

# defined using space separator.
ignoreip = 127.0.0.1/8 192.168.xxx.xxx 192.168.yyy.yyy 192.168.zzz.zzz

# "bantime" is the number of seconds that a host is banned.
bantime  = 86400

# A host is banned if it has generated "maxretry" during the last
"findtime"
# seconds.
findtime = 600
maxretry = 3

[…]

usedns = yes

#
# Destination email address used solely for the interpolations in
# jail.{conf,local} configuration files.
destemail = webmaster@localhost

#
# Destination email address used solely for the interpolations in
# jail.{conf,local,d/*} configuration files.
destemail = webmaster@localhost

# Sender email address used solely for some actions
sender = isanonyme-f2b@anonyme.ch

[…]

mta = mail

[…]

action = %(action_mwl)s
#
# JAILS

[…]

[sshd]

# To use more aggressive sshd modes set filter parameter "mode" in
jail.local:
# normal (default), ddos, extra or aggressive (combines all).
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage
example and details.
#mode   = normal

enabled = true
port    = ssh,10022
logpath = %(sshd_log)s
backend = %(sshd_backend)s

[…]

[apache-auth]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s
```

12. Editer le fichier "/etc/fail2ban/jail.local" (Suite)

```
[apache-badbots]
# Ban hosts which agent identifies spammer robots crawling the web
# for email addresses. The mail outputs are buffered.

enabled = true
port     = http,https
logpath  = %(apache_access_log)s
bantime  = 48h
maxretry = 1

[apache-noscript]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s

[apache-overflows]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2

[apache-nohome]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2

[apache-botsearch]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2

[apache-fakegooglebot]

enabled = true
port     = http,https
logpath  = %(apache_access_log)s
maxretry = 1
ignorecommand = %(ignorecommands_dir)s/apache-fakegooglebot <ip>

[apache-modsecurity]

enabled = true
port     = http,https
logpath  = %(apache_error_log)s
maxretry = 2

[apache-shellshock]

enabled = true
port    = http,https
logpath = %(apache_error_log)s
maxretry = 1
```

13. Editer le fichier "/etc/fail2ban/jail.local" (Suite)

```
[apache-scan]

enabled  = true
port     = http,https
filter   = apache-scan
logpath  = /var/log/apache*/error*.log
maxretry = 1


[apache-w00tw00t]

enabled = true
filter = apache-w00tw00t
action = iptables[name=Apache-w00tw00t,port=80,protocol=tcp]
logpath = /var/log/apache*/access*.log
maxretry = 1

[…]

[php-url-fopen]

enabled = true
port    = http,https
logpath = %(nginx_access_log)s
          %(apache_access_log)s
[…]

[vsftpd]
# or overwrite it in jails.local to be
# logpath = %(syslog_authpriv)s
# if you want to rely on PAM failed login attempts
# vsftpd's failregex should match both of those formats

enabled = true
port     = ftp,ftp-data,ftps,ftps-data,10021,10090:10200
logpath  = %(vsftpd_log)s

[postfix]
# To use another modes set filter parameter "mode" in jail.local:

enabled = true
mode    = more
port    = smtp,465,submission
logpath = %(postfix_log)s
backend = %(postfix_backend)s

[postfix-rbl]

enabled = true
filter   = postfix[mode=rbl]
port     = smtp,465,submission
logpath  = %(postfix_log)s
backend  = %(postfix_backend)s
maxretry = 1

[postfix-sasl]

enabled = true
filter   = postfix[mode=auth]
port     = smtp,465,submission,imap,imaps,pop3,pop3s
# You might consider monitoring /var/log/mail.warn instead if you are
# running postfix since it would provide the same log lines at the
# "warn" level but overall at the smaller filesize.
logpath  = %(postfix_log)s
backend  = %(postfix_backend)s
```

14. Editer le fichier "/etc/fail2ban/jail.local" (Suite)

```
[…]

[mysqld-auth]

enabled  = true
port     = 3306
logpath  = /var/log/mysql/error.log
backend  = %(mysql_backend)s

[…]

[phpmyadmin-syslog]

enabled = true
port    = http,https
logpath = %(syslog_authpriv)s
backend = %(syslog_backend)s
```

15. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

16. Vérifier que le fichier " /etc/mysql/my.cnf" contienne les lignes suivantes

```
sudo nano /etc/mysql/my.cnf

[…]

[mysqld]
log_error           = /var/log/mysql/error.log
log_error_verbosity = 3
[…]
```

17. Sauvegarder (si nécessaire) et quitter (Ctrl + O, Ctrl + X)

Fichiers "Jail"

18. Créer et modifier le fichier suivant:

```
sudo nano /etc/fail2ban/filter.d/apache-scan.conf

# Fail2Ban configuration file
#
# List of URL scanned
#
# Author: Etienne Jouvin
#

[Definition]

scannedurls =
admin|db|dbadmin|myadmin|mysql|mysqladmin|typo3|phpadmin|phpMyAdmin|ph
pmyadmin|phpmyadmin1|phpmyadmin2|pma|web|xampp|php\-my\-
admin|websql|phpmyadmin|phpMyAdmin\-2|php\-my\-admin|phpMyAdmin\-
2\.2\.3|phpMyAdmin\-2\.2\.6|phpMyAdmin\-2\.5\.1|phpMyAdmin\-
2\.5\.4|phpMyAdmin\-2\.5\.5\-rc1|phpMyAdmin\-2\.5\.5\-rc2|phpMyAdmin\-
2\.5\.5|phpMyAdmin\-2\.5\.5\-pl1|phpMyAdmin\-2\.5\.6\-rc1|phpMyAdmin\-
2\.5\.6\-rc2|phpMyAdmin\-2\.5\.6|phpMyAdmin\-2\.5.7|phpMyAdmin\-
2\.5\.7\-pl1|pp
scannedscripts = judge.*\.php|proxyheader\.php

# Option:  failregex
# Notes.:  regex to match the password failure messages in the
logfile. The
#          host must be matched by a group named "host". The tag
"<HOST>" can
#          be used for standard IP/hostname matching and is only an
alias for
#          (?:::f{4,6}:)?(?P<host>[\w\-.^_]+)
# Values:  TEXT
#
failregex = [[]client <HOST>[]] (File does not exist|script not found
or unable to stat): \/var\/www\/.*(?:%(scannedurls)s).*
            [[]client <HOST>[]] script
'\/var\/www\/.*(?:%(scannedscripts)s)' not found or unable to stat

# Option:  ignoreregex
# Notes.:  regex to ignore. If this regex matches, the line is
ignored.
# Values:  TEXT
#
ignoreregex =
```

19. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

20. Créer et modifier le fichier suivant:

```
sudo nano /etc/fail2ban/filter.d/apache-w00tw00t.conf

[Definition]

failregex = ^<HOST> -.*"GET \/w00tw00t\.at\.ISC\.SANS\.DFind\:\).*".*

ignoreregex =
```

21. Sauvegarder et quitter (Ctrl + O, Ctrl + X)

22. Modifier le fichier suivant:

```
sudo nano /etc/fail2ban/filter.d/php-url-fopen.conf


# Fail2Ban filter for URLs with a URL as a script parameters
# which can be an indication of a fopen url php injection
#
# Example of web requests in Apache access log:
# 66.185.212.172 - - [26/Mar/2009:08:44:20 -0500] "GET
/index.php?n=http://eatmyfood.hostinginfive.com/pizza.htm? HTTP/1.1" 200 114 "-"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; .NET $

[Definition]

# failregex = ^<HOST> -.*"(GET|POST).*\?.*\=http\:\/\/.* HTTP\/.*$ (Commenter)

failregex = ^<HOST> -.*"(GET|POST).*\?.*\=http\:\/\/.*\ HTTP\/1\..*$

ignoreregex =

# DEV Notes:
#
# Version 2
# fixes the failregex so REFERERS that contain =http:// don't get blocked
# (mentioned by "fasuto" (no real email provided... blog comment) in this entry:
# http://blogs.buanzo.com.ar/2009/04/fail2ban-filter-for-php-injection-
attacks.html#comment-1489
#
# Author: Arturo 'Buanzo' Busleiman <buanzo@buanzo.com.ar>
```

23. Redémarrer le service "fail2ban"

```
sudo service fail2ban restart
```

Tests

24. Vérifier le statut de "fail2ban"

```
sudo fail2ban-client status

Status
|- Number of jail:      19
`- Jail list:           php-url-fopen, apache-w00tw00t, apache-scan,
apache-noscript, postfix, ssh-ddos, apache-multiport, vsftpd, mysqld-
auth, ssh, apache-overflows, apache
```

25. Tester le filtre "apache-scan"

```
sudo fail2ban-regex /var/log/apache2/error.[un des nom de site créés].log
/etc/fail2ban/filter.d/apache-scan.conf

Running tests
=============

Use   failregex file : /etc/fail2ban/filter.d/apache-scan.conf
Use         log file : /var/log/apache2/error.[un des nom de site créés].log


Results
=======

Failregex: 0 total

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [189] WEEKDAY MONTH Day Hour:Minute:Second[.subsecond] Year
`-

Lines: 189 lines, 0 ignored, 0 matched, 189 missed
Missed line(s):: too many to print.  Use --print-all-missed to print all 189 lines
```

26. Tester le filtre "apache-w00tw00t"

```
sudo fail2ban-regex /var/log/apache2/access.[un des nom de site créés].log
/etc/fail2ban/filter.d/apache-w00tw00t.conf

Running tests
=============

Use   failregex file : /etc/fail2ban/filter.d/apache-w00tw00t.conf
Use         log file : /var/log/apache2/access.[un des nom de site créés].log


Results
=======

Failregex: 0 total

Ignoreregex: 0 total

Date template hits:
|- [# of hits] date format
|  [60] Day/MONTH/Year:Hour:Minute:Second
`-

Lines: 60 lines, 0 ignored, 0 matched, 60 missed
Missed line(s):: too many to print.  Use --print-all-missed to print all 60 lines
```

Retirer une adresse IP bannie

1. En ligne de commande (Remplacer [JAIL] et [MYIP] de façon appropriée)

```
sudo fail2ban-client set [JAIL] unbanip [MYIP]
```

7ème partie Maintenance générale du serveur

1. Mettre le serveur à jour et adapter la base de données de « rkhunter » (voir détail point 10 du chapitre Installer et configurer "rootkit checker")

```
sudo apt-get update

sudo apt-get upgrade

sudo apt-get dist-upgrade

sudo rkhunter --propupd
```

2. Redémarrer le serveur

```
sudo reboot now
```

Commandes utiles

1. Relancer les services réseau

```
sudo /etc/init.d/networking restart
```

2024.03.20 13:
43:41 +01'00'