Bachelier en informatique et Systèmes

Informatique industrielle

3ème année

HELHa
Haute École Louvain
en Hainaut

Catégorie technique

Laboratoire de réseaux

Apache

2015 – 2016

Haveaux Valentin

Tables des matières

Apache

1 Serveur Apache

Daemon du serveur Apache: httpd

Fichier de configuration: /etc/httpd/conf/httpd.conf

Localisation des modules: /usr/lib64/httpd/modules

Localisation du site principal: /var/www/html

Lancement/arrêt/redémarrage : service httpd start/stop/restart

2 Benchmark Apache

ab -n 1000 -c 500 http://www.mysite.be/

watch –n 0 'ps ax | grep httpd' ➔ sur un autre terminal

3 Les commandes de vérification

httpd –t ➔ vérifie la syntaxe du fichier http.conf

httpd –S ➔ Liste les VirtualHosts

4 Environnement globale

ServerName : nom d'hôte sur de la machine sur laquelle apache tourne.

Exemple: ServerName www.mysite.be

ServerRoot: Répertoire dans lequel les fichiers de configurations, log et modules sont gardés

Exemple: ServerRoot "/etc/httpd"

DocumentRoot: dossier dans lequel les documents du site sont déposés.

Exemple: DocumentRoot "/var/www/html"

ServerAdmin: Adresse mail du webmaster.

Exemple: ServerAdmin webmaster@mysite.be

ServerTokens: permet de contrôler le contenu de l'en-tête Server inclus dans la réponse envoyée au client (ServerTokens Prod).

Exemple: ServerTokens Prod[uctOnly] ➔ Le serveur renvoie (par ex.): Server: Apache

Listen: adresse IP et numéro de ports sur lesquels Apache attend et reçoit les connexions des clients.

Exemple: Listen 10.0.0.7:80 ➔ Apache écoute sur le port 80 sur l'interface d'IP 10.0.0.7.

ErrorDocument: pour remplacer les pages d'erreurs envoyées au client en cas de problème.

Exemples:

```
ErrorDocument 403 "Vous n'êtes pas autorisé à lire cette
page !
```
Ici on affiche simplement un texte adapté à l'erreur.

```
ErrorDocument 401 /missing.html
```
Ici on affiche une page html sensée se trouver à la racine du site web.

```
ErrorDocument 500 http://www.bidon.com/erreur.html
```
Ici on affiche une page html extérieure au site.

DirectoryIndex: page renvoyé lors d'un accès à la racine (par défaut index.html).

MinSpareServers: Nombre minimal de serveurs supplémentaires (qui attendent les connexions sans rien faire) dans la réserve des processus.

MaxSpareServers: Nombre maximum de serveurs supplémentaires dans la réserve des processus.

StartServers: Nombre de serveurs supplémentaires créés au démarrage d'Apache.

MaxClients: Limite le nombre de processus qui peuvent tourner simultanément (chaque connexion cliente en utilise un).

5 Les sites perso

- Elle est activée par la directive `Userdir`.

```
<IfModule mod_userdir.c>
        #UserDir disabled
        UserDir public_html
</IfModule>
```

Si le module 'userdir' est chargé, alors un utilisateur du système pourra y héberger son site Web dont la racine se trouvera dans le dossier 'public_html' de sa home directory.

- Le site sera accessible vial'URL: `http://ip_serveur/~login_utilisateur`
  Exemple: `http://www.mysite.be/~jean`

```
UserDir disabled <user1 user2 ...>

UserDir disabled

UserDir enabled <user1 user2 ...>
```

Pour les sites perso faite bien attention aux droit d'accès des dossiers !

chmod 755 /home/login_user

Pour avoir plus de facilité et ne pas devoir créer de dossier public_html à chaque fois:

mkdir /etc/skel/public_html

6 Les redirections simple

Alias /CentOS/ "/usr/share/doc/HTML"

7 Visualiser le contenu d'un répertoire

```
IndexOptions None (indexation classique)

IndexOptions FancyIndexing (indexation au look plus agréable)

IndexOptions FancyIndexing VersionSort
            (idem + tri des entrées contenant des numéros de versions)
```

8 L'arbre des processus

ps –ef | grep apache

9 Protection des sites Web

9.1 Contrôle sur l'origine du client

- Géré par le module mod_authz_host
- Ses directives agissent dans un contexte répertoire (bloc <Directory… >)
- Les restrictions sont imposées à tous les fichiers du répertoire.

- Directives:

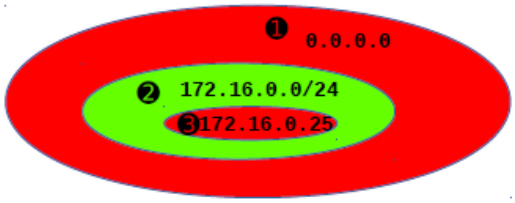
Allow: indique les hôtes autorisés à accéder aux ressources du dossier.
Deny: indique les hôtes à qui l'accès aux ressources est interdit.

Exemples:

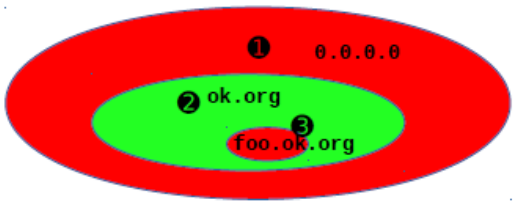
```
Deny from all
Deny from .autredomaine.com

Allow from 192.168.1.1
Allow from 192.168.1.2          } Allow from 192.168.1.1 192.168.1.2

Allow from 192.168.1
Allow from 192.168.1.0/255.255.255.0   } Ces 3 formes sont
Allow from 192.168.1.0/24              } équivalentes.
```

9.2 Directive Order

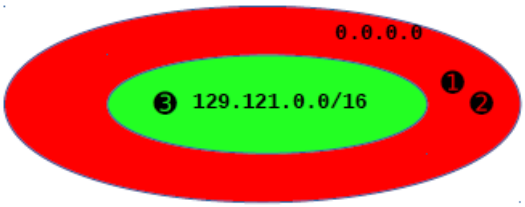
```
❶
Order Allow,Deny
    Allow from 172.16.0.0/24❷
    Deny from 172.16.0.25 ❸
```



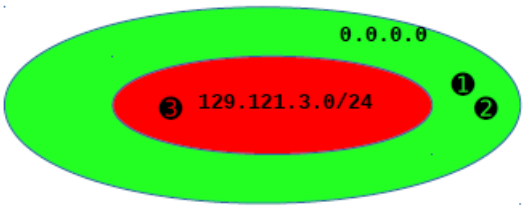

```
❶
Order Allow,Deny
    Allow from ok.org    ❷
    Deny from foo.ok.org ❸
```




```
❶
Order Deny,Allow
    Allow from 129.121❸
    Deny from all    ❷
```




```
❶
Order Allow,Deny
    Allow from all    ❷
    Deny from 129.121.❸
```



9.3 Controller par authentification

```
# htpasswd -c /var/www/securite/userfile toto   → création (en dehors du site... sécurité oblige ! )
# cat /var/www/securite/userfile
toto:cnVPtfAz2xw60
# htpasswd -b /var/www/securite/userfile albert secret → ajout avec mdp

        ☞       -m      → pour chiffrer le mdp en MD5
                -s      → pour chiffrer le mdp en SHA
                -p      → pour ne pas chiffrer le mdp
```

Activation de l'autorisation

```
<Directory rep_a_proteger>
   AuthName "Domaine de test" → message à afficher lors de l'authentification
   AuthType Basic → type d'authentification (Basic: valable pour auth. de base ou digest)

   AuthUserFile /var/www/securite/userfile → (1)

   Require valid-user → (2)
</Directory>
```

9.3.1 Autorisation de certain utilisateurs

```
Require user toto albert
```

9.3.2 Autorisation par groupe d'utilisateurs

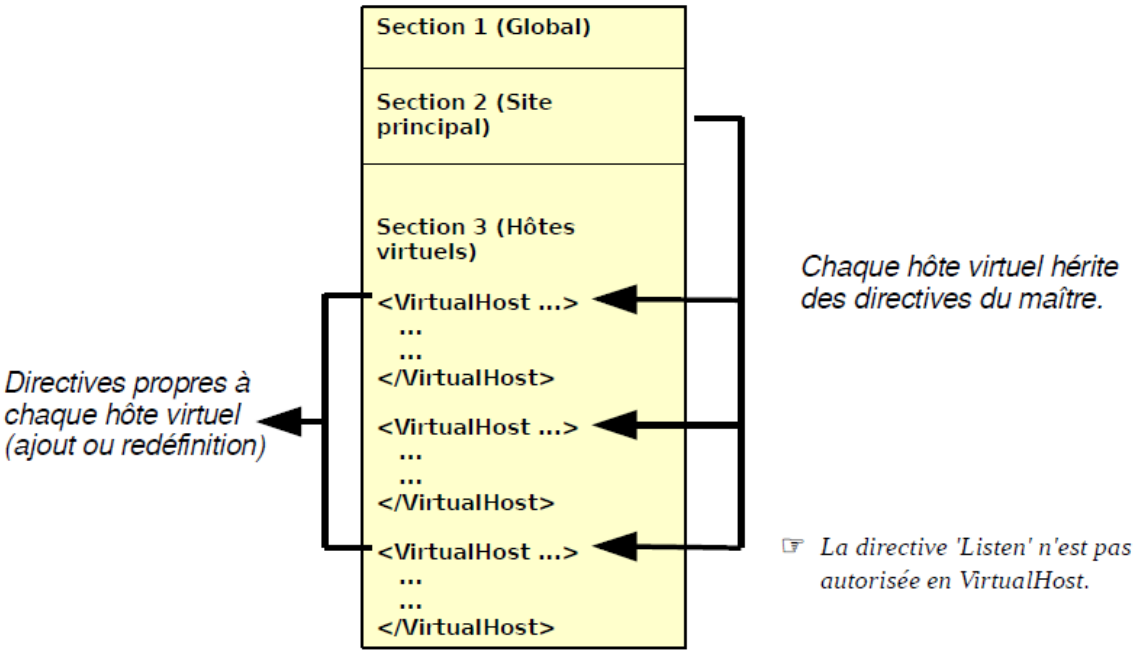
Soit un fichier texte /var/www/securite/groupfile contenant:

```
admins:toto albert
friends:toto linda
associates:bruno
```

alors:

```
<Directory rep_a_proteger>
   AuthName "Domaine de test"
   AuthType Basic
   AuthUserFile /var/www/securite/userfile
   AuthGroupFile /var/www/securite/groupfile
   Require group admins friends
</Directory>
```

10 Hébergement virtuel



10.1 Hébergement par IP

```
ServerName www.mysite.be
DocumentRoot /var/www/html

<VirtualHost 192.168.1.5>
  UseCanonicalName DNS
  ServerName vhost2.mysite.be
  DocumentRoot
/var/www/html/vhost2
</VirtualHost>
```

Création d'une alias: ifconfig ethx:y ***Ip*** netmask ***masque***

Si une adresse IP peut être atteinte mais qu'aucun hôte n'est défini sur celle-ci, c'est le site principal qui répondra à la requête.

10.2 Hébergement par nom

```
ServerName www.mysite.be
DocumentRoot /var/www/html
NameVirtualHost 192.168.1.1

<VirtualHost 192.168.1.1>
  UseCanonicalName off
  ServerName www.mysite.be
  DocumentRoot /var/www/html
</VirtualHost>

<VirtualHost 192.168.1.1>
  UseCanonicalName off
  ServerName vhost1.mysite.be
  DocumentRoot /var/www/html/vhost1
</VirtualHost>
```

Une seule directive NameVirtualHost par adresse Ip.

10.3 UseCanonicalName

DNS: adressage par IP

Off: hôte virtuel par nom

10.4 L'intervenant DNS

```
<VirtualHost 192.168.1.4>
  ServerName vhost1.mysite.be
  DocumentRoot /var/www/html/vhost1
</VirtualHost>
```

Il est conseillé de l'écrire de cette manière, car faire intervenir DNS peut provoquer la désactivation de l'hôte.

11 Résumé certificat

Configuration de /etc/httpd/conf/httpd.conf

```
…
<VirtualHost 192.168.1.100:443>
UseCanonicalName off
ServerName secure.mysite.be
DocumentRoot /var/www/websecure
SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/secure.mysite.be.crt
SSLCertificateKeyFile /etc/pki/tls/private/secure.mysite.be.key
</VirtualHost>
```

Installation des modules openssl et mod_ssl (openssl est certainement déjà installé)

```
# yum install openssl mod_ssl –y
```

Implémentation des clés et des certificats

Création de la clé privée du serveur

```
# cd /tmp
# openssl genrsa -out secure.mysite.be.key 2048
```

Création du CSR

```
# openssl req -new -key secure.mysite.be.key -out
secure.mysite.be.csr
…

Remplir tous les champs d'information  concernant le formulaire.

…
```

Création du certifciat auto-signé

```
# openssl x509 -in secure.mysite.be.csr -out secure.mysite.be.crt
-req -signkey secure.mysite.be.key -days 3650
```

Copie des clés et certificats au bon endroit

```
# cp secure.mysite.be.crt /etc/pki/tls/certs
# cp secure.mysite.be.csr /etc/pki/tls/private
# cp secure.mysite.be.key /etc/pki/tls/private
```

Suppression des clés et certificats de /tmp

```
# rm –f /tmp/secure.mysite.be*
```

Relancer Apache

```
# service httpd restart
```

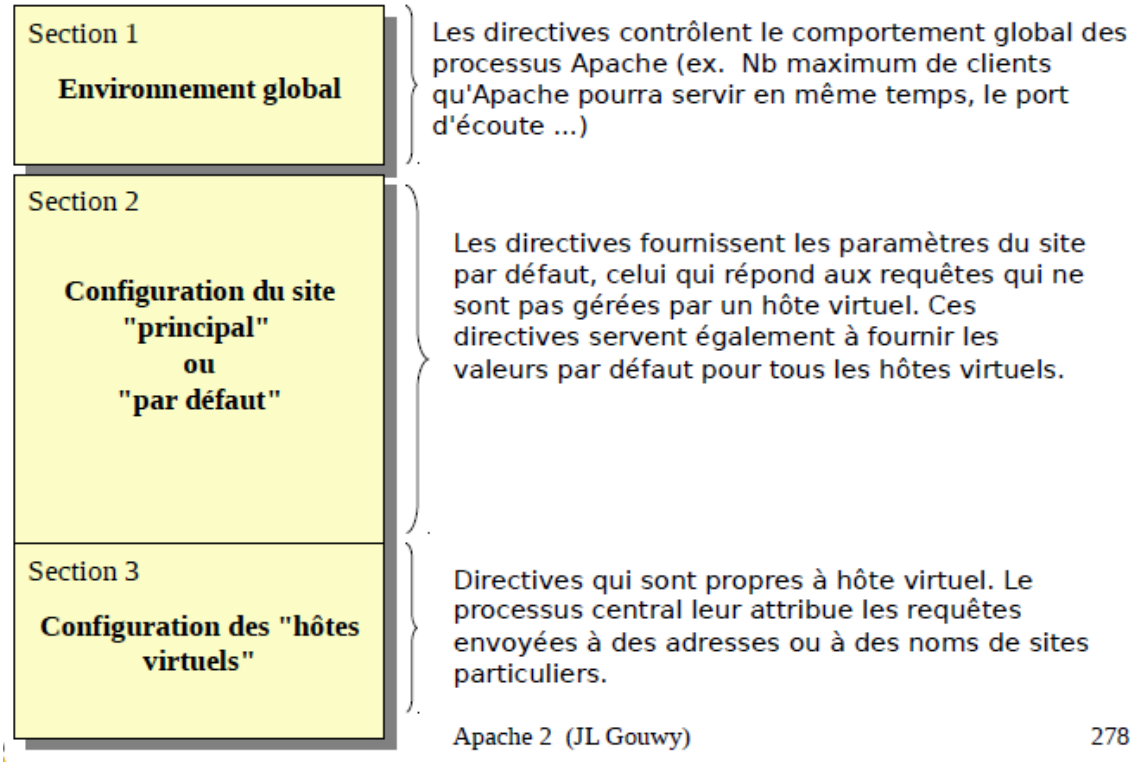
12 Tester si une requête fonctionne avec telnet

mcedit get-page.sh

```
echo "open $1 80"

sleep 2

echo "GET / HTTP/1.1"

echo "host: $1"

echo

echo

sleep 2
```

sh get-page.sh www.helha.be | telnet > get-page.out

13 Structure de l'httpd.conf



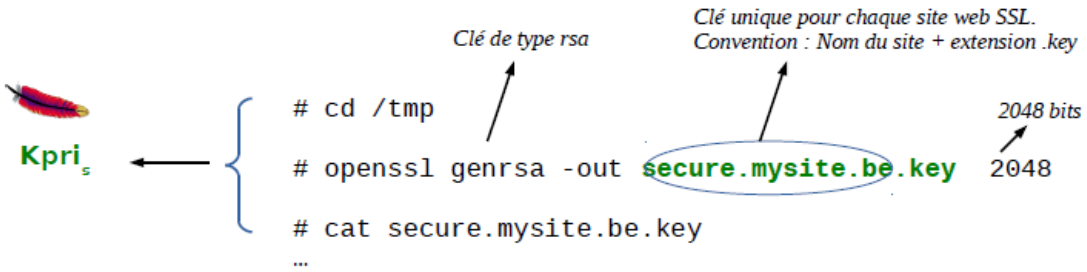
14 Les certificats

Etape 1: Installer OpenSSL

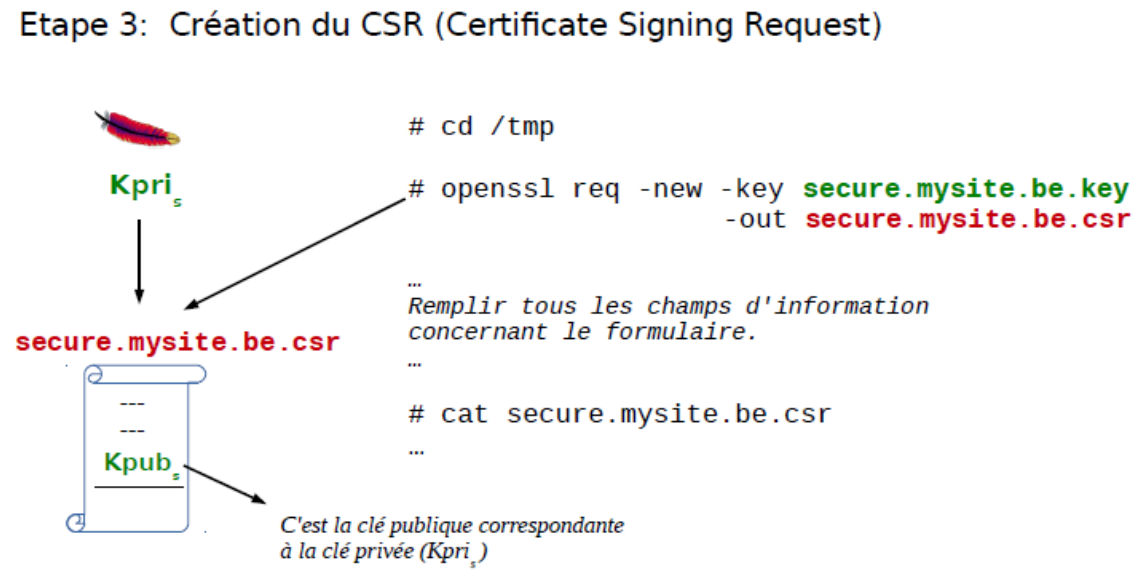
```
# yum install openssl
```

14.1 Clé privé du serveur

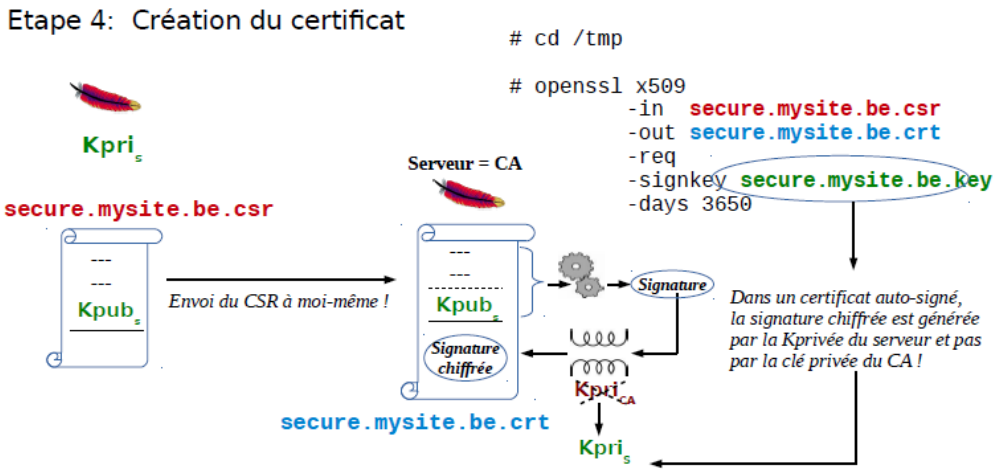
Etape 2: Création de la clé privée du serveur



14.2 Création du CSR (Certificat Signing Request)

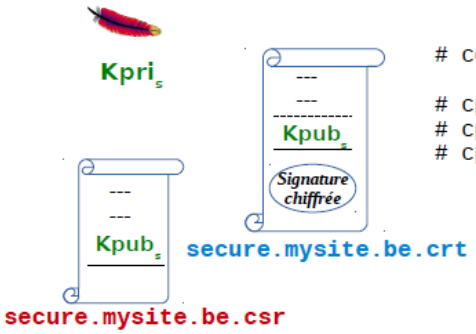


14.3 Création du certificat



14.4 Copie des clés aux bons endroits

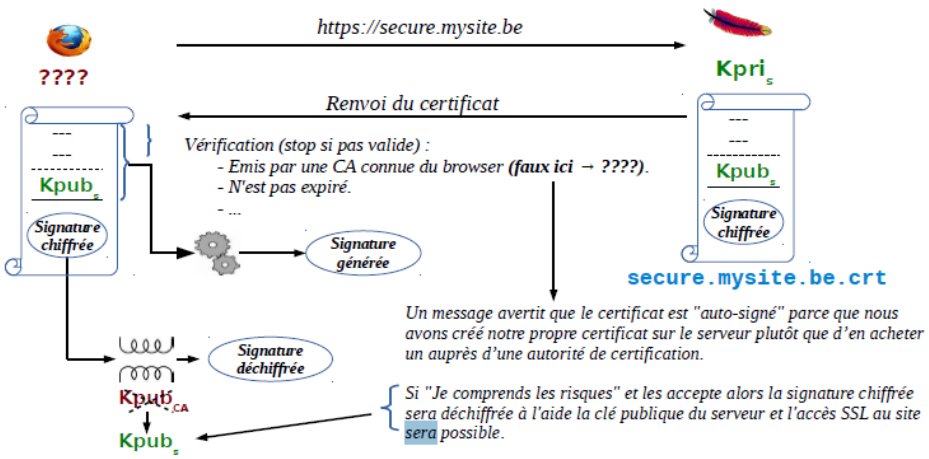
Etape 5: Copie des clés et des certificats au bon endroit




```
# cd /tmp

# cp secure.mysite.be.crt /etc/pki/tls/certs
# cp secure.mysite.be.csr /etc/pki/tls/private
# cp secure.mysite.be.key /etc/pki/tls/private
```

14.5 Connexion

Etape 6: Connexion SSL



14.6 Implémentation

14.6.1 Configurer /etc/httpd/conf/httpd.conf

Installer le module mod_ssl: # yum install mod_ssl

```
…
<VirtualHost 192.168.1.99:443>
   ServerName secure.mysite.be
   DocumentRoot /var/www/html/secure
   SSLEngine on  → Pour spécifier que SSL doit être utilisé pour un hôte virtuel et pas pour le serveur.
   SSLCertificateFile /etc/pki/tls/certs/secure.mysite.be.crt
                                                  → Nom complet du certificat pour ce site.
   SSLCertificateKeyFile /etc/pki/tls/private/secure.mysite.be.key
                                                  → Nom complet de la clé privée pour ce site.
</VirtualHost>
```

14.6.2 Configurer /etc/httpd/conf.d/ssl.conf

```
…
LoadModule ssl_module modules/mod_ssl.so  → Nécessaire aux certificats.
Listen 443  → Apache écoutera également sur le port 443 de toutes ses interfaces.
…
SSLPassPhraseDialog builtin  → Une passphrase éventuelle sera demandée
                               sur l'entrée standard.
SSLSessionCacheTimeout 300  → Timeout pour les sessions SSL (300 secondes).
…
```