

# Sécurité Serveur Apache 2 (SSL)

Linux

## 1 Présentation de l'atelier :

Notre atelier vous offre en premier lieu l'occasion de :

- \* se familiariser avec le serveur web Apache2 sous Linux.
- \* savoir comment sécuriser ce serveur web grâce au protocole SSL.
- \* présenter la notion de VirtualHost sous Apache2.

- *Note : Nous avons travaillé cet atelier sous la version Mandrake 10.2.*

*Si vous choisissez de le faire fonctionner sous une autre distribution, il faut faire la correspondance dans les chemins.*

## 2 Installation :

- Télécharger la source Apache depuis <http://httpd.apache.org>
- Décompressez l'archive dans un répertoire de votre choix (*/usr/local* par exemple):

```
# tar -zxvf httpd-2-xxx.tar.gz
```

- Placez vous dans le répertoire nouvellement crée puis lancez la compilation

```
#cd httpd-2.0.x  
#./configure --enable-mod-shared=all -enable-ssl  
#make  
#make install
```

- Ou encore, on peut télécharger le fichier rpm du serveur Apache et l'exécuter :

```
# rpm -ivh httpd2-x.x
```

Vous remarquerez la création du répertoire */etc/httpd* et la création de l'exécutable httpd sous */etc/rc.d/init.d/*.

- Maintenant le serveur Web est prêt à fonctionner. Pour le démarrer, tapez la commande suivante :

```
# /etc/rc.d/init.d/httpd start
```

-Pour tester si le serveur Apache est bien lancé, il suffit de taper ***http://localhost/*** dans votre navigateur (Mozilla par exemple), si une page web Apache alors tout va bien.

### 3 Configuration :

Pour configurer le serveur Apache2 sécurisé, on se propose de réaliser les activités suivantes :

#### 3.1 Activité 1- La sécurité des pages Web

La configuration d'un serveur Web a des implications en matière de sécurité informatique.

- **Création des droits d'accès sur un domaine par login/mot de passe**
  - Créez un nouveau domaine appelé ***monsie***, l'emplacement de ce dernier sera :  
***/var/www/html/monsie***
  - Créez sous ce répertoire le fichier ***index.html*** qui a comme contenu:

```
<html>
<head><title>                Club                SécuriNets</title></head>
  <body>
    <p align="center">Atelier: Sécurité serveur Apache2
    </p>
  </body>
</html>
```

- Vérifiez que vous pouvez accéder à cette page avec l'URL ***http://localhost/monsie***
- Placez vous dans le répertoire ***/etc/httpd/conf/*** puis créez le répertoire ***sécurité***

```
# cd /etc/httpd/conf/
# mkdir securite
```

- Éditez le fichier de configuration apache ***/etc/httpd/conf/httpd2.conf*** et ajoutez les lignes suivantes :

```
<Directory
"/usr/local/apache2/htdocs/monsie">
```



**S E C U R I N E T S**  
Club de la sécurité informatique  
I N S A T

```
AllowOverride           None
Order                  allow,deny
Allow from all
AuthName "Vous allez accéder à mon site"
AuthType               Basic
AuthUserFile
/etc/httpd/conf/securite/htpasswd.users
require                user          securinets
</Directory>
```

-Placez vous dans le répertoire `/usr/sbin/` et tapez la commande qui permet de créer une liste d'utilisateurs possédant le droit d'accéder au domaine « monsite »

```
# cd /usr/sbin/
# ./htpasswd -c /etc/httpd/conf/securite/htpasswd.users securinets
```

- Redémarrez le serveur apache2 à l'aide de la commande :

```
# /etc/rc.d/init.d/httpd restart
```

- Accédez à la l'URL <http://localhost/monsite> uniquement avec l'authentification de l'utilisateur securinets.



- Voir le format du fichier `htpasswd.users`

## 3.2 Activité 2- Apache et SSL : La communication sécurisée

L'accès aux pages web se fait à l'aide du protocole http, en empruntant le réseau Internet. Aucune garantie de confidentialité n'est assurée lors de ces accès ; il est relativement simple à un pirate d'intercepter vos requêtes (votre code de carte bleue) et les réponses faites par le serveur.

En outre, vous n'avez pas une certitude absolue d'être en cours de consultation du site que vous croyez.

Afin de pallier à ces inconvénients, le protocole https avec l'authentification SSL peut être mis en oeuvre. D'une manière très schématique, il permet d'encapsuler et de crypter le trafic http. Ainsi, il sera quasiment impossible à un pirate d'intercepter les accès à des pages chargées via le protocole https, de décrypter cet échange, et donc de récupérer des informations confidentielles. En outre, https permet de s'assurer que le serveur auquel on accède est bien celui que l'on croit.

HTTPS offre d'autres possibilités qui ne sont pas abordées ici (par exemple, authentifier la personne qui accède au serveur).

Pour accepter les requêtes SSL, Apache a besoin de deux fichiers :

- \* une clé pour le serveur (server.key)
- \* un certificat signé (server.crt).

NB : Les noms des fichiers n'ont pas d'importance.

### 3.2.1 Les packages à installer :

- Mod-ssl est le module apache qui implémente https (http over ssl). Le serveur https écoute par défaut sur le port 443 au lieu de 80.

- OpenSSL fournit notamment une application pour créer des certificats.

### 3.2.2 Création de la clé et du certificat

Pour créer votre clé et votre certificat, tapez les commandes suivantes dans un terminal :

```
# mkdir /tmp/ssl_conf  
# cd /tmp/ssl_conf  
# openssl req -config /usr/lib/ssl/openssl.cnf -new -out monsite.csr
```

On génère un fichier de demande de signature de certificat (CSR Certificate Signing Request).

Là il vous demande un passphrase, entrez un mot de passe dont vous vous souviendrez. Finissez, en entrant des informations régionales. Ensuite, tapez :

```
# openssl rsa -in privkey.pem -out monsite.key
# openssl x509 -in monsite.csr -out monsite.crt -req -signkey monsite.key -days 3650
# openssl x509 -in monsite.crt -out monsite.der.crt -outform DER
```

Création de la clé privée (pointing to `privkey.pem`)

La durée de la validité de la clé. (pointing to `-days 3650`)

Notez que mon certificat est valable 3650 jours (presque 10 an). On peut protéger notre clé en interdisant toute modification ou accès de la part des autres utilisateurs. Ceci peut se faire facilement en tapant la commande:

```
# chmod 400 monsite.key
```

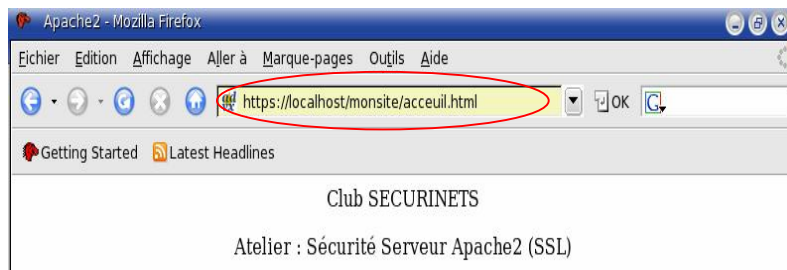
### 3.2.3 Configuration d'Apache pour le SSL

En tant que administrateur (root), copiez la clé et le certificat dans les dossiers ssl d'Apache (vous devrez peut-être les créer) :

```
# cd /tmp/ssl_conf
# cp monsite.crt /etc/httpd/conf/ssl.crt/
# cp monsite.key /etc/httpd/conf/ssl.key/
```

Editez le fichier /ssl.conf et modifiez les lignes qui suivent ainsi:

```
SSLCertificateFile /etc/httpd/conf/ssl.crt/monsite.crt
SSLCertificateKeyFile /etc/httpd/conf/ssl.key/monsite.key
```



### 3.3 Activité 3- Les serveurs Web sécurisés



# S E C U R I N E T S

Club de la sécurité informatique  
I N S A T

La mise en place de serveurs web virtuels, permet de faire cohabiter plusieurs serveurs sur une même machine. Nous verrons qu'il existe plusieurs techniques pour faire cela :

Pour les serveurs virtuels basés sur le nom, vous devrez désigner pour une adresse IP sur la machine (et si possible le port), quel est le nom utilisé (directive ServerName), et quelle est la racine du site (directive DocumentRoot).

On peut mettre en place des hôtes virtuels, en d'autres termes un utilisateur pour un même serveur Apache croira en voir plusieurs.

- Configuration du fichier Vhosts.conf

## # Configuration du 1er Virtual Host:

```
NameVirtualHost 192.168.13.11
<VirtualHost 192.168.13.11>
ServerAdmin webmaster@machine1.insat
DocumentRoot /var/www/html
ServerName machine1.insat
ServerAlias machine1.insat www.machine1.insat
ErrorLog logs/machine1-error_log
CustomLog logs/machine1-access_log common
ErrorDocument 404 /erreur.html
</VirtualHost>
```

## # Configuration du 2er Virtual Host:

```
NameVirtualHost 192.168.13.11
<VirtualHost 192.168.13.11>
ServerAdmin webmaster@machine2.insat
DocumentRoot /var/www/html
ServerName machine2.insat
ServerAlias machine2.insat www.Machine2.insat
ErrorLog logs/machine2-error_log
CustomLog logs/machine2-access_log common
ErrorDocument 404 /erreur.html
</VirtualHost>
```

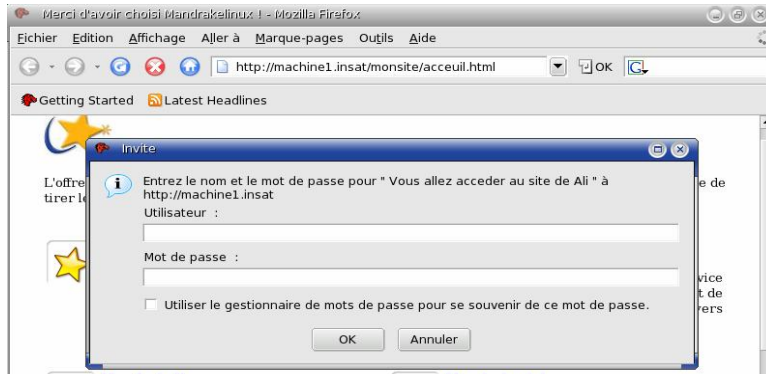
-Ensuite, il faut ajouter machine1.insat, [www.machine1.insat](http://www.machine1.insat) (de même pour la deuxième machine) dans le fichier /etc/hosts

→D'où on peut y accéder comme suit à notre site « monsite » :



# S E C U R I N E T S

Club de la sécurité informatique  
I N S A T



→ Accéder avec  
machine1.insat

Après authentification on obtient la page HTML suivante :

