NOM Prénom : Ethan Georget
BTS SIO SISR - Bloc 2
Compte-Rendu : Administration et sécurisation d'un serveur Web Apache2

DOSSIER TECHNIQUE : CONFIGURATION AVANCÉE APACHE2

1. Objectifs du laboratoire

L'objectif de ce TP est de maîtriser les mécanismes de configuration du serveur web Apache2 sous Debian. Il s'agit de manipuler les directives fondamentales, de gérer des hôtes virtuels (VirtualHosts) en HTTP et HTTPS, et de mettre en œuvre des mesures de sécurité comme l'authentification HTACCESS et le durcissement du serveur.

Les travaux ont été réalisés sur la machine DEBIAN_TRAINING_DMZ. Un snapshot nommé 'BEFORE_TRAINING' a été créé avant le début des configurations.

1.1 Vérification de l'état initial du service Avant de débuter les modifications de configuration, j'ai vérifié que le service Apache2 était bien démarré et que les processus tournaient sous l'identité de l'utilisateur www-data. Cette étape permet de valider le bon fonctionnement du serveur web après son installation initiale.

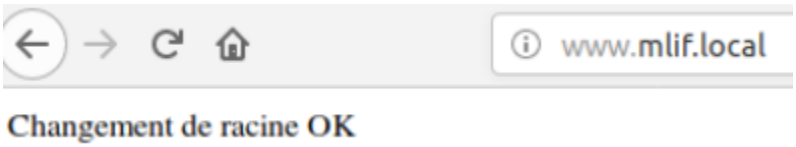
ps -ef | grep apache

```
root         653       1  0 08:40 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     655     653  0 08:40 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     656     653  0 08:40 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     657     653  0 08:40 ?        00:00:00 /usr/sbin/apache2 -k start
www-data     658     653  0 08:40 ?        00:00:00 /usr/sbin/apache2 -k start
```

2. Manipulation des directives principals

2.1 Modification du DocumentRoot

La directive DocumentRoot définit l'arborescence racine du site. Nous avons déplacé la racine par défaut de /var/www/html vers /var/lwww/html/sitea. Un bloc <Directory> a été ajouté dans 000-default.conf pour accorder les privilèges 'Require all granted'. La propriété récursive de l'arborescence a été attribuée à l'utilisateur www-data via la commande chown.



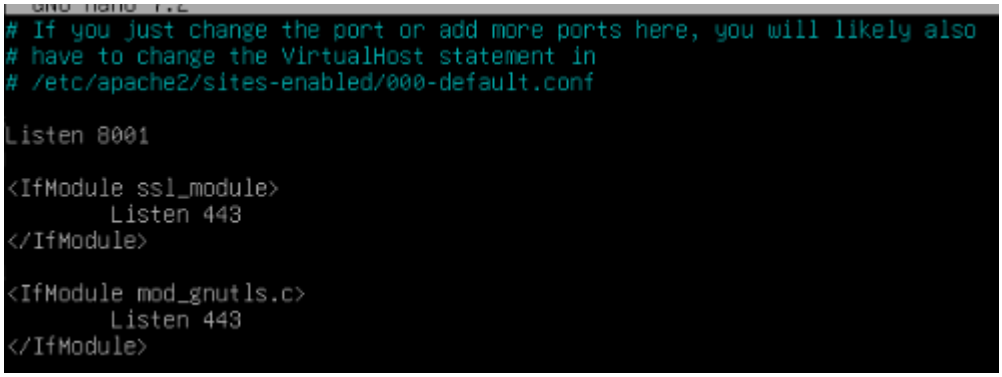
J'ai complété cette modification par l'ajout d'un bloc <Directory> spécifique dans le fichier de configuration du VirtualHost. Ce bloc est indispensable pour définir les options de parcours (Indexes) et accorder les droits d'accès (Require all granted) sur cette nouvelle arborescence personnalisée.

```
 GNU nano 7.2                                                  000-default.conf *
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and port that
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerName
        # specifies what hostname must appear in the request's Host: header to
        # match this virtual host. For the default virtual host (this file) this
        # value is not decisive as it is used as a last resort host regardless.
        # However, you must set it for any further virtual host explicitly.
        #ServerName www.example.com

        ServerAdmin webmaster@localhost
        DocumentRoot /usr/local/httpd/www

        # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

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

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For example the
        # following line enables the CGI configuration for this host only
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
<Directory /usr/local/httpd/www>
        Options Indexes
        Require all granted
```

2.2 Modification du port d'écoute (Listen)

Pour des raisons de sécurité ou de services multiples, le port d'écoute a été modifié de 80 vers 8001. Cette modification implique une mise à jour du fichier /etc/apache2/ports.conf et du VirtualHost par défaut. Le redémarrage du service via systemctl a permis de valider l'écoute exclusive sur le nouveau port.

La modification s'est faite en deux temps : d'abord dans le fichier global ports.conf pour indiquer au serveur d'écouter sur le port 8001, puis dans le fichier du VirtualHost par défaut pour que les requêtes entrantes sur ce port soient correctement traitées.



2.3 Mise en œuvre d'Alias

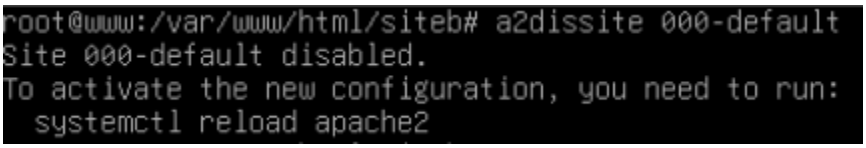
La directive Alias permet d'accéder à des ressources hors DocumentRoot. Nous avons créé un alias '/docs' pointant vers /usr/local/doc. Un bloc Directory correspondant a été configuré pour autoriser l'indexation et l'accès aux fichiers.

#ls /etc/apache2/mods-enabled | grep alias

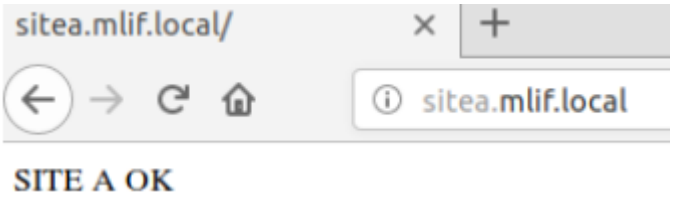
3. Hébergement multi-sites (VirtualHosts)

3.1 VirtualHosts HTTP et DNS

Pour rendre ces nouveaux sites opérationnels, j'ai utilisé les outils d'administration d'Apache pour désactiver le site par défaut (a2dissite) et activer les configurations de sitea et siteb (a2ensite). Un rechargement de la configuration a ensuite été nécessaire pour appliquer ces changements.

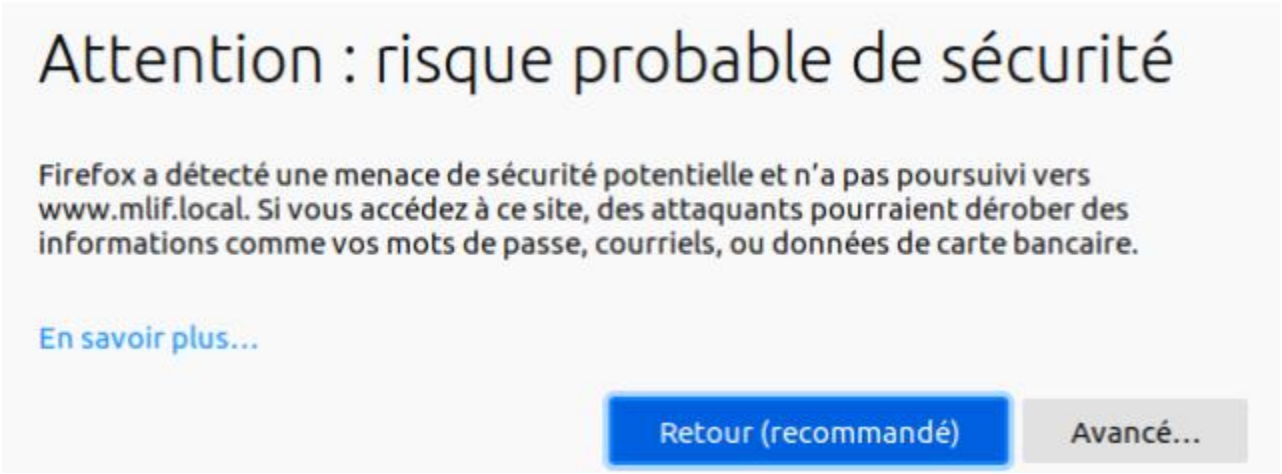


Deux nouveaux hôtes virtuels (sitea.mlif.local et siteb.mlif.local) ont été créés. Pour chaque site, un fichier de configuration distinct a été généré dans sites-available, puis activé avec la commande a2ensite. Côté DNS, des enregistrements de type CNAME ont été ajoutés sur le serveur Debian pour résoudre les nouveaux noms d'hôtes.



3.2 Activation du HTTPS (SSL)

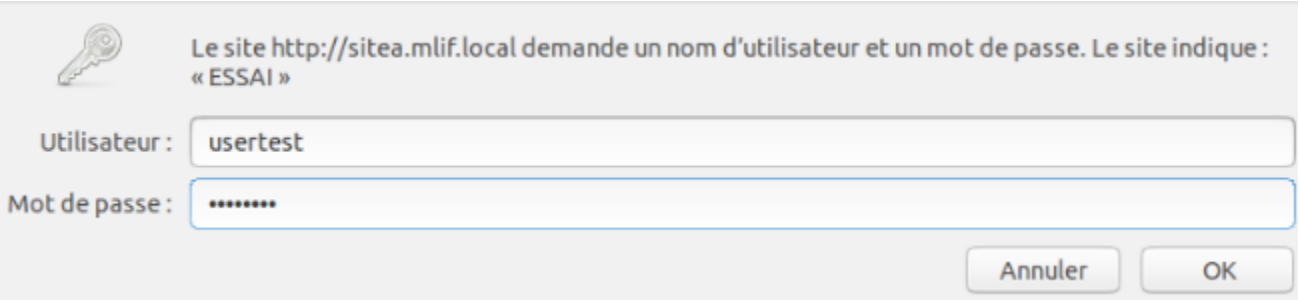
La sécurisation des échanges a été réalisée par l'activation du module SSL (a2enmod ssl) et du VirtualHost par défaut default-ssl. Nous avons configuré les directives SSLEngine, SSLCertificateFile et SSLCertificateKeyFile pour pointer vers les certificats fournis par Apache.



4. Sécurisation et contrôle d'accès

4.1 Authentification par .htaccess

Une politique de contrôle d'accès a été mise en place sur le site A. Nous avons activé la directive 'AllowOverride AuthConfig' et généré un fichier de mots de passe caché (.htpasswd) via la commande htpasswd. Le fichier .htaccess à la racine du site impose désormais une authentification 'Basic' pour tout utilisateur valide.



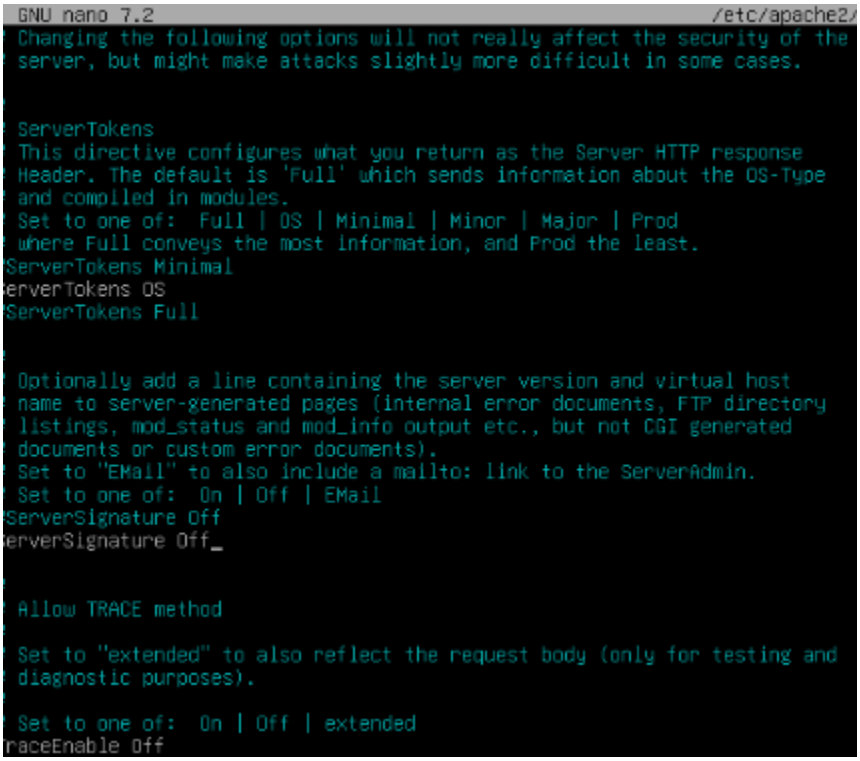
La directive AllowOverride AuthConfig a été ajoutée dans la configuration du VirtualHost de sitea pour autoriser le fichier .htaccess à surcharger la politique de sécurité. J'ai ensuite créé le fichier .htpasswd contenant les identifiants chiffrés pour restreindre l'accès à la racine du site.

```
  GNU nano 7.2
<VirtualHost *:80>
        # The ServerName directive sets the request scheme, hostname and
        # the server uses to identify itself. This is used when creating
        # redirection URLs. In the context of virtual hosts, the ServerN
        # specifies what hostname must appear in the request's Host: hea
        # match this virtual host. For the default virtual host (this fi
        # value is not decisive as it is used as a last resort host rega
        # However, you must set it for any further virtual host explicit
        ServerName sitea.mlif.local

        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html/sitea

        # Available loglevels: trace8, ..., trace1, debug, info, notice,
        # error, crit, alert, emerg.
        # It is also possible to configure the loglevel for particular
        # modules, e.g.
        #LogLevel info ssl:warn

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

        # For most configuration files from conf-available/, which are
        # enabled or disabled at a global level, it is possible to
        # include a line for only one particular virtual host. For examp
        # following line enables the CGI configuration for this host onl
        # after it has been globally disabled with "a2disconf".
        #Include conf-available/serve-cgi-bin.conf
</VirtualHost>
<Directory /var/www/html/sitea>
        Options Indexes
        Require all granted
        AllowOverride AuthConfig_
</Directory>
<Directory /usr/local/doc>
        Options Indexes
        Require all granted
</Directory>
```

4.2 Durcissement (ServerSignature)

Afin de limiter les informations divulguées par le serveur (Information Disclosure), la directive ServerSignature a été passée à 'Off' dans le fichier security.conf. Cela empêche l'affichage de la version d'Apache et de l'OS lors des erreurs 404 ou 403.

Cette modification a été effectuée dans le fichier security.conf. En passant la directive à Off, le serveur ne renvoie plus son nom ni sa version dans l'en-tête des pages d'erreur, ce qui limite les informations disponibles pour une éventuelle phase de reconnaissance par un attaquant.



5. Conclusion

Ce laboratoire a permis de valider les compétences d'administration système sur Apache2. La gestion des VirtualHosts et le durcissement de la configuration sont des briques essentielles pour l'exploitation d'un serveur web en environnement DMZ.