

Procédure : Authentification Apache

Dans ce tutoriel, je vais vous montrer comment aller plus loin en sécurisant votre site avec l'authentification de type *BASIC* et de type *DIGEST*.

NOTE : Ne pas confondre cryptage et chiffage. En effet le cryptage de données peut être décrypté avec un peu de connaissance informatique, tandis qu'un chiffrement utilise des algorithmes aléatoires qui ne peuvent pas être déchiffré.

Une fois ce tutoriel terminé, je vous conseille de passer à la partie du serveur DNS avant de continuer vers le tutoriel qui concerne HTTPS.

Table des matières

⇒ Mise en place de l'authentification de type <i>BASIC</i>	2
⇒ Mise en place de l'authentification de type <i>DIGEST</i>	4

⇒ Mise en place de l'authentification de type *BASIC*

1. Pour commencer nous allons d'abord créer un utilisateur qui aura le droit de se connecter au site avec la commande suivante : `htpasswd -c /etc/apache2/users toto`
Le fichier **users** n'existe pas mais il sera créé en même que l'utilisateur. Si par la suite vous décidez de voir ce fichier, vous verrez que le mot de passe a été crypté en Base64.

```
root@procedure-web:/# htpasswd -c /etc/apache2/users basic
New password:
Re-type new password:
Adding password for user basic
root@procedure-web:/# █
```

2. Nous allons activer le mode d'authentification avec la commande :
`a2enmod auth_basic.load` (activer par défaut)
3. Ensuite nous allons modifier le fichier de configuration de notre site, qui se trouve dans `/etc/apache2/sites-available/`

```
root@procedure-web:/# cd /etc/apache2/sites-available/
root@procedure-web:/etc/apache2/sites-available# vim robotech.conf █
```

Et ajouter les lignes suivantes :

<code><Directory /var/www/tryhard></code>	→ donne le chemin du site
<code>AuthType Basic</code>	→ Type de l'authentification
<code>AuthName "ma zone privée"</code>	→ Nom de l'authentification
<code>AuthBasicProvider file</code>	
<code>AuthUserFile /etc/apache2/users</code>	→ Fichier où sont situés les utilisateurs
<code>Require valid-user</code>	→ Requiert utilisateurs valide
<code></Directory></code>	→ fermeture de la balise

```

<VirtualHost 192.168.130.162:80>
    # 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.robotech.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/robotech

    <Directory /var/www/robotech>
        AuthType Basic
        AuthName "ma zone privée"
        AuthBasicProvider file
        AuthUserFile /etc/apache2/users
        Require valid-user
    </Directory>

    # 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>

```

4. Pour tester, entrez la commande `service apache2 reload` puis rendez-vous l'adresse de votre site depuis un navigateur. Normalement vous obtenez ça :

Authentification requise

Le site <http://192.168.130.162> demande un nom d'utilisateur et un mot de passe. Le site indique : « ma zone privée »

Utilisateur :

Mot de passe :

Annuler OK

Ainsi vous pouvez vous connecter avec l'utilisateur « basic » !

⇒ Mise en place de l'authentification de type *DIGEST*

1. Pour commencer nous allons d'abord créer un utilisateur qui aura le droit de se connecter au site avec la commande suivante :

```
htdigest /etc/apache2/users "ma zone privée" tata
```

Note: "ma zone privée" est la valeur que nous mettons dans AuthName.

```
root@procedure-web:/# htdigest /etc/apache2/users "ma zone privée" digest
Adding user digest in realm ma zone privée
New password:
Re-type new password:
root@procedure-web:/# █
```

2. Nous allons activer le mode d'authentification avec la commande :

```
a2enmod auth_digest.load
```

3. Ensuite nous allons modifier le fichier de configuration de notre site, qui se trouve dans /etc/apache2/sites-available/

```
root@procedure-web:/# cd /etc/apache2/sites-available/
root@procedure-web:/etc/apache2/sites-available# vim robotech.conf █
```

Et ajouter les lignes suivantes :

<Directory /var/www/tryhard>	→ donne le chemin du site
AuthType Digest	→ Type de l'authentification
AuthName "ma zone privée"	→ Nom de l'authentification
AuthDigestProvider file	
AuthUserFile /etc/apache2/users	→ Fichier où sont situés les utilisateur
Require valid-user	→ Requier utilisateurs valide
</Directory>	→ fermeture de la balise

```

<VirtualHost 192.168.130.162:80>
    # 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.robotech.local
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/robotech

    <Directory /var/www/robotech>
        AuthType Digest
        AuthName "ma zone privee"
        AuthBasicProvider file
        AuthUserFile /etc/apache2/users
        Require valid-user
    </Directory>

    # 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>

```

4. Pour tester, entrez la commande `service apache2 reload` puis rendez-vous l'adresse de votre site depuis un navigateur. Normalement vous obtenez ça :

5.

Authentification requise

Le site <http://192.168.130.162> demande un nom d'utilisateur et un mot de passe. Le site indique : « ma zone privee »

Utilisateur :

Mot de passe :

Annuler OK

Ainsi vous pouvez vous connecter avec l'utilisateur « digest » !