

## Jalon 20 : Configuration HTTPS INETSRV

Nous n'avons pas eu le temps de déployer les certificats sur le domaine INTERNET mais nous avons configuré le serveur web en http. Pour cela, nous avons utilisé le serveur apache2 pour sa simplicité de mise en place et de configuration. Nous avons également installé un serveur PHP.

Voici le fichier de configuration de notre site web situé sous le répertoire /etc/apache2/sites-available/site.conf :

```
GNU nano 7.2 /etc/apache2/sites-enabled/site.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
    #
    # ServerSignature Off
    #
    # ServerTokens Prod
    DocumentRoot /var/www/html

    #
    # <FilesMatch "\.ht">
    #     Require all denied
    # </FilesMatch>
    #
    # 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>
```

Cette configuration reste assez basique mais est fonctionnelle. Elle indique que la racine du site web commence a partir du dossier /var/www/html.

Voici le contenu du fichier /var/www/html/index.php. Ce fichier héberge le serveur web Internet, simulant un site web réel. Ce site web devait afficher différentes informations :

- L'adresse IP du client qui demande la page web,
- L'user agent du navigateur client
- La date et l'heure actuelle.

```

Fichier Edition Onglets Aide
GNU nano 7.2 /var/www/html/index.php
<?php
//echo "ip: La date est : " . date("Y-m-d H:i:s") . "<br>";
//echo "ip: L'User-Agent est : " . htmlspecialchars($_SERVER['HTTP_USER_AGENT']) . "<br>";

<?php
// Définir la zone horaire pour s'assurer que la date est correcte
date_default_timezone_set('Europe/Paris');

// Afficher la date et l'heure actuelles
echo "<p>La date est : " . date("Y-m-d H:i:s") . "</p>";

// Récupérer l'adresse IP du client
if (empty($_SERVER['HTTP_CLIENT_IP'])) {
    $client_ip = $_SERVER['HTTP_CLIENT_IP'];
} elseif (empty($_SERVER['HTTP_X_FORWARDED_FOR'])) {
    $client_ip = $_SERVER['HTTP_X_FORWARDED_FOR'];
} else {
    $client_ip = $_SERVER['REMOTE_ADDR'];
}

// Afficher l'adresse IP du client
echo "<p>L'adresse IP du client est : $client_ip</p>";

// Récupérer l'User-Agent (navigateur et système d'exploitation du client)
$user_agent = $_SERVER['HTTP_USER_AGENT'];

// Afficher l'User-Agent
echo "<p>L'User-Agent du client est : $user_agent</p>";
?>

```

Nous devons également protéger le serveur web en faisant en sorte que pas d'information sensible soient transmises par les footer et header. Pour cela, nous avons modifié le fichier de configuration d'apache : /etc/apache2/apache2.conf

```

#
<FilesMatch "^\.ht">
    Require all denied
</FilesMatch>

```

Ce code empêche les pages en .ht d'être accessible et visible par les clients. Ce code est important car si on ne le fait pas et qu'un fichier .htaccess est présent, quiconque qui aura des intentions malveillantes pourrait y accéder en renseignant le fichier dans l'url.