Dernière mise-à-jour : 2020/01/30 03:27

208.1 - Gestion de Base du Serveur Web Apache 2.4 (4/60) - FIXME

LPI 208.1 - Implementing a web server

Weight: 4

Description: Candidates should be able to install and configure a web server. This objective includes monitoring the server’s load and performance, restricting client user access, configuring support for scripting languages as modules and setting up client user authentication. Also included is configuring server options to restrict usage of resources. Candidates should be able to configure a web server to use virtual hosts and customize file access.

Key Knowledge Areas:

- Apache 2.4 configuration files, terms and utilities
- Apache log files configuration and content
- Access restriction methods and files
- mod_perl and PHP configuration
- Client user authentication files and utilities
- Configuration of maximum requests, minimum and maximum servers and clients
- Apache 2.4 virtual host implementation (with and without dedicated IP addresses)
- Using redirect statements in Apache’s configuration files to customize file access

Terms and Utilities:

- access logs and error logs
- .htaccess
- httpd.conf
- mod_auth_basic, mod_authz_host and mod_access_compat
- htpasswd
- AuthUserFile, AuthGroupFile

- apachectl, apache2ctl
- httpd, apache2

Présentation d'Apache

Un serveur web est une machine doté d'un logiciel serveur qui attend des requêtes de la part de machines clientes afin de leur livrer de documents de types différents.

En 1994 le développement du serveur web le plus connue à l'époque, le démon **HTTP**, a été arrêté suite au départ de la NCSA de son principal développeur, **Rob McCool**.

Au début de l'année 1995, un groupe de webmestres indépendants s'est mis en place sous la direction de **Brian Behlendorf** et **Cliff Skolnick** pour reprendre le travail sur ce démon. Ce projet a pris le nom **Apache**. En même temps la NCSA a repris son propre travail de développement sur son démon HTTP. L'arrivée dans le groupe Apache de deux personnes de la NCSA en tant que membres honoraires, **Brandon Long** et **Beth Frank** a permis la mise en commun des connaissances des deux groupes.

Le projet **Apache** est un projet de développement d'un serveur web libre pour les plateformes Unix et Windows™. La première version *officielle*, la 0.6.2 est sortie en avril 1995.

La **Fondation Apache**, créée en 1999 par l'équipe Apache, gère aujourd'hui non seulement le projet Apache mais aussi un grand nombre d'autres projets. La liste des projets de la Fondation peut être trouvée **ici**.

Apache est modulaire. Certains modules fondamentaux conditionnent comment Apache traite la question du multitraitement. Les modules multitraitements - **MPM - Multi-Processing Modules** - sont différents selon le système d'exploitation utilisé et la charge attendue.

- **mpm-winnt** - module propre à Windows™ qui utilise son support réseau natif,
- **prefork** - module propre à Unix et Linux qui implémente un serveur mono-tâche à duplication,
- **perchild** - module propre à Unix et Linux qui implémente un serveur autorisant des démons servant les requêtes à être assigner à plusieurs id utilisateurs,
- **worker** - module propre à Unix et Linux qui implémente un serveur hybride multi-tâche et multitraitement.

Ces modules sont compilés statiquement au binaire Apache et sont mutuellement exclusifs.

Installation

Sous **RHEL / CentOS 7**, Apache n'est pas installé par défaut. Utilisez donc yum pour l'installer :

```
[root@centos7 ~]# rpm -qa | grep httpd
[root@centos7 ~]#
[root@centos7 ~]# yum install httpd
```

La version d'Apache est la **2.4.6** :

```
[root@centos7 ~]# rpm -qa | grep httpd
httpd-2.4.6-45.el7.centos.4.x86_64
httpd-tools-2.4.6-45.el7.centos.4.x86_64
```

Configurez le service pour démarrer automatiquement :

```
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[root@centos7 ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to
/usr/lib/systemd/system/httpd.service.
```

Lancez votre service apache :

```
[root@centos7 ~]# systemctl start httpd
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
```

```
   Active: active (running) since Tue 2017-08-22 11:19:18 CEST; 3s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 1293 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─1293 /usr/sbin/httpd -DFOREGROUND
           ├─1296 /usr/sbin/httpd -DFOREGROUND
           ├─1297 /usr/sbin/httpd -DFOREGROUND
           ├─1298 /usr/sbin/httpd -DFOREGROUND
           ├─1299 /usr/sbin/httpd -DFOREGROUND
           └─1300 /usr/sbin/httpd -DFOREGROUND

Aug 22 11:19:18 centos7.fenestros.loc systemd[1]: Starting The Apache HTTP Server...
Aug 22 11:19:18 centos7.fenestros.loc systemd[1]: Started The Apache HTTP Server.
```

Testez le serveur apache

Avec un navigateur

Lancez maintenant le navigateur et saisissez l'adresse http://localhost dans la barre d'adresses. Vous devez obtenir une page web servie par votre apache.

Avec Telnet

Premièrement, ouvrez un console et en tant que root et installez telnet :

```
[root@centos7 ~]# yum install telnet
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.atosworldline.com
```

```
 * extras: mirrors.atosworldline.com
 * updates: ftp.ciril.fr
Resolving Dependencies
--> Running transaction check
---> Package telnet.x86_64 1:0.17-60.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================================
 Package                            Arch                              Version
Repository                         Size
================================================================================================================
=====================================
Installing:
 telnet                             x86_64                            1:0.17-60.el7
base                               63 k

Transaction Summary
================================================================================================================
=====================================
Install  1 Package

Total download size: 63 k
Installed size: 113 k
Is this ok [y/d/N]: y
```

Utilisez ensuite telnet pour vérifier le bon fonctionnement d'Apache :

```
[root@centos7 ~]# telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
```

```
GET /
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"><html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
        <title>Apache HTTP Server Test Page powered by CentOS</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">

    <!-- Bootstrap -->
    <link href="/noindex/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/css" />

<style type="text/css"><!--

body {
  font-family: "Open Sans", Helvetica, sans-serif;
  font-weight: 100;
  color: #ccc;
  background: rgba(10, 24, 55, 1);
  font-size: 16px;
}

h2, h3, h4 {
  font-weight: 200;
}

h2 {
  font-size: 28px;
}

.jumbotron {
  margin-bottom: 0;
  color: #333;
  background: rgb(212,212,221); /* Old browsers */
  background: radial-gradient(ellipse at center top, rgba(255,255,255,1) 0%,rgba(174,174,183,1) 100%); /* W3C */
}
```

```
.jumbotron h1 {
  font-size: 128px;
  font-weight: 700;
  color: white;
  text-shadow: 0px 2px 0px #abc,
               0px 4px 10px rgba(0,0,0,0.15),
               0px 5px 2px rgba(0,0,0,0.1),
               0px 6px 30px rgba(0,0,0,0.1);
}

.jumbotron p {
  font-size: 28px;
  font-weight: 100;
}

.main {
   background: white;
   color: #234;
   border-top: 1px solid rgba(0,0,0,0.12);
   padding-top: 30px;
   padding-bottom: 40px;
}

.footer {
   border-top: 1px solid rgba(255,255,255,0.2);
   padding-top: 30px;
}

    --></style>
</head>
<body>
  <div class="jumbotron text-center">
    <div class="container">
      <h1>Testing 123..</h1>
```

```
        <p class="lead">This page is used to test the proper operation of the <a href="http://apache.org">Apache
HTTP server</a> after it has been installed. If you can read this page it means that this site is working
properly. This server is powered by <a href="http://centos.org">CentOS</a>.</p>
        </div>
  </div>
  <div class="main">
    <div class="container">
       <div class="row">
            <div class="col-sm-6">
                <h2>Just visiting?</h2>
                      <p class="lead">The website you just visited is either experiencing problems or is
undergoing routine maintenance.</p>
                    <p>If you would like to let the administrators of this website know that you've seen this
page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster"
and directed to the website's domain should reach the appropriate person.</p>
                    <p>For example, if you experienced problems while visiting www.example.com, you should send
e-mail to "webmaster@example.com".</p>
                  </div>
                <div class="col-sm-6">
                      <h2>Are you the Administrator?</h2>
                      <p>You should add your website content to the directory <tt>/var/www/html/</tt>.</p>
                      <p>To prevent this page from ever being used, follow the instructions in the file
<tt>/etc/httpd/conf.d/welcome.conf</tt>.</p>

                      <h2>Promoting Apache and CentOS</h2>
                      <p>You are free to use the images below on Apache and CentOS Linux powered HTTP servers.
Thanks for using Apache and CentOS!</p>
                      <p><a href="http://httpd.apache.org/"><img src="images/apache_pb.gif" alt="[ Powered by
Apache ]"></a> <a href="http://www.centos.org/"><img src="images/poweredby.png" alt="[ Powered by CentOS Linux ]"
height="31" width="88"></a></p>
                </div>
              </div>
        </div>
        </div>
```

```
    </div>
      <div class="footer">
      <div class="container">
        <div class="row">
          <div class="col-sm-6">
            <h2>Important note:</h2>
            <p class="lead">The CentOS Project has nothing to do with this website or its content,
            it just provides the software that makes the website run.</p>
            <p>If you have issues with the content of this site, contact the owner of the domain, not the CentOS
project.
            Unless you intended to visit CentOS.org, the CentOS Project does not have anything to do with this
website,
            the content or the lack of it.</p>
            <p>For example, if this website is www.example.com, you would find the owner of the example.com
domain at the following WHOIS server:</p>
            <p><a href="http://www.internic.net/whois.html">http://www.internic.net/whois.html</a></p>
          </div>
          <div class="col-sm-6">
            <h2>The CentOS Project</h2>
            <p>The CentOS Linux distribution is a stable, predictable, manageable and reproduceable platform
derived from
               the sources of Red Hat Enterprise Linux (RHEL).<p>
            <p>Additionally to being a popular choice for web hosting, CentOS also provides a rich platform for
open source communities to build upon. For more information
               please visit the <a href="http://www.centos.org/">CentOS website</a>.</p>
          </div>
        </div>
          </div>
    </div>
  </div>
</body></html>
Connection closed by foreign host.
```

Préparation

Désactivez le mode **enforcing** de SELINUX afin de pouvoir librement travailler avec Apache :

```
[root@centos7 ~]# setenforce permissive
[root@centos7 ~]# getenforce
Permissive
[root@centos7 ~]# vi /etc/sysconfig/selinux
[root@centos7 ~]# cat /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

Afin d'éviter les problèmes liés au pare-feu arrêtez le service firewalld :

```
[root@centos7 ~]# systemctl stop firewalld
[root@centos7 ~]# systemctl disable firewalld
[root@centos7 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)

Aug 21 16:23:02 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
```

```
Aug 21 16:23:07 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Aug 21 16:29:49 centos7.fenestros.loc systemd[1]: Stopping firewalld - dynamic firewall daemon...
Aug 21 16:29:49 centos7.fenestros.loc systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

Configuration

/etc/httpd/conf/httpd.conf

Sous Red Hat / CentOS 7 le fichier de configuration principal d'apache est **/etc/httpd/conf/httpd.conf**. Cette configuration est complémentée par les directives se trouvant dans les fichiers contenus dans les répertoires **conf.modules.d/*.conf** et **conf.d/*.conf** :

```
[root@centos7 ~]# ls -lR /etc/httpd
/etc/httpd:
total 4
drwxr-xr-x. 2 root root   35 Aug 22 11:17 conf
drwxr-xr-x. 2 root root   78 Aug 22 11:17 conf.d
drwxr-xr-x. 2 root root 4096 Aug 22 11:17 conf.modules.d
lrwxrwxrwx. 1 root root   19 Aug 22 11:17 logs -> ../../var/log/httpd
lrwxrwxrwx. 1 root root   29 Aug 22 11:17 modules -> ../../usr/lib64/httpd/modules
lrwxrwxrwx. 1 root root   10 Aug 22 11:17 run -> /run/httpd

/etc/httpd/conf:
total 28
-rw-r--r--. 1 root root 11753 Apr 12 15:50 httpd.conf
-rw-r--r--. 1 root root 13077 Apr 12 23:04 magic

/etc/httpd/conf.d:
total 16
-rw-r--r--. 1 root root 2926 Apr 12 23:03 autoindex.conf
-rw-r--r--. 1 root root  366 Apr 12 23:04 README
-rw-r--r--. 1 root root 1252 Apr 12 15:50 userdir.conf
```

```
-rw-r--r--. 1 root root  824 Apr 12 15:50 welcome.conf

/etc/httpd/conf.modules.d:
total 28
-rw-r--r--. 1 root root 3739 Apr 12 15:50 00-base.conf
-rw-r--r--. 1 root root  139 Apr 12 15:50 00-dav.conf
-rw-r--r--. 1 root root   41 Apr 12 15:50 00-lua.conf
-rw-r--r--. 1 root root  742 Apr 12 15:50 00-mpm.conf
-rw-r--r--. 1 root root  957 Apr 12 15:50 00-proxy.conf
-rw-r--r--. 1 root root   88 Apr 12 15:50 00-systemd.conf
-rw-r--r--. 1 root root  451 Apr 12 15:50 01-cgi.conf
```

Les directives actives du fichier **/etc/httpd/conf/httpd.conf** sont les suivantes :

```
[root@centos7 ~]# egrep -v '^(#|$)'  /etc/httpd/conf/httpd.conf > /tmp/httpd.conf
[root@centos7 ~]# cat /tmp/httpd.conf
ServerRoot "/etc/httpd"
Listen 80
Include conf.modules.d/*.conf
User apache
Group apache
ServerAdmin root@localhost
<Directory />
    AllowOverride none
    Require all denied
</Directory>
DocumentRoot "/var/www/html"
<Directory "/var/www">
    AllowOverride None
    Require all granted
</Directory>
<Directory "/var/www/html">
    Options Indexes FollowSymLinks
    AllowOverride None
```

```
    Require all granted
</Directory>
<IfModule dir_module>
    DirectoryIndex index.html
</IfModule>
<Files ".ht*">
    Require all denied
</Files>
ErrorLog "logs/error_log"
LogLevel warn
<IfModule log_config_module>
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    <IfModule logio_module>
      LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
    </IfModule>
    CustomLog "logs/access_log" combined
</IfModule>
<IfModule alias_module>
    ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
</IfModule>
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
<IfModule mime_module>
    TypesConfig /etc/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
    AddType text/html .shtml
    AddOutputFilter INCLUDES .shtml
</IfModule>
AddDefaultCharset UTF-8
```

```
<IfModule mime_magic_module>
    MIMEMagicFile conf/magic
</IfModule>
EnableSendfile on
IncludeOptional conf.d/*.conf
```

Les Directives du fichier /etc/httpd/conf/httpd.conf

ServerRoot

Cette directive indique la racine de la configuration d'apache.

```
ServerRoot "/etc/httpd"
```

Listen

Cette directive indique le port écouté par apache.

```
Listen 80
```

Include

Cette directive indique que les fichiers de configuration inclus dans le répertoire **conf.modules.d/*.conf** doivent être inclus dans httpd.conf :

```
Include conf.modules.d/*.conf
```

User et Group

Cette directive indique l'UID et le GID de l'utilisateur qui exécute le service apache :

```
User apache
Group apache
```

ServerAdmin

Cette directive indique l'adresse email de l'administrateur du serveur apache :

```
ServerAdmin root@localhost
```

<Directory />

Cette directive permet de regrouper d'autres directives s'appliquant à un répertoire précis - dans ce cas la racine du site :

```
<Directory />
```

Require all

Cette directive autorise ou interdit l'accès. Dans ce cas l'interdiction concerne tout le monde.

```
Require all denied
```

AllowOverride

Cette directive stipule comment Apache doit utiliser les directives situées dans un éventuel fichier **.htaccess** La valeur **none** désactive l'utilisation du fichier **.htaccess** dans le répertoire.

```
AllowOverride None
```

</Directory>

Cette directive ferme le bloc **Directory**.

```
</Directory>
```

DocumentRoot

Cette directive indique l'emplacement par défaut des pages web à servir :

```
DocumentRoot "/var/www/html"
```

<Directory "/var/www">

Cette directive définit des règles pour le répertoire **/var/www/** :

```
<Directory "/var/www">
```

AllowOverride

Cette directive stipule comment Apache doit utiliser les directives situées dans un éventuel fichier **.htaccess** La valeur **none** désactive l'utilisation du fichier **.htaccess** dans le répertoire **/var/www/**.

```
AllowOverride None
```

Require all

Cette directive autorise ou interdit l'accès. Dans ce cas l'autorisation concerne tout le monde.

```
Require all granted
```

</Directory>

Cette directive ferme le bloc **Directory**.

```
</Directory>
```

<Directory "/var/www/html">

Cette directive définit des règles pour le répertoire **htdocs** :

```
<Directory "/var/www/html">
```

Indexes

La directive Options active (+) ou désactive (-) des fonctions spécifiques. Dans ce cas **Indexes** autorise au serveur apache de générer une liste du contenu du répertoire dans le cas ou le fichier index ne peut pas être trouve tandis que **FollowSymLinks** permet à apache de suivre les liens symboliques.

```
Options Indexes FollowSymLinks
```

AllowOverride

Cette directive stipule comment Apache doit utiliser les directives situées dans un éventuel fichier **.htaccess** La valeur **none** désactive l'utilisation du fichier **.htaccess** dans le répertoire **/var/www/html**.

```
AllowOverride None
```

Require all

Cette directive autorise ou interdit l'accès. Dans ce cas l'autorisation concerne tout le monde.

```
Require all granted
```

</Directory>

Cette directive ferme le bloc **Directory**.

```
</Directory>
```

IfModule

IfModule dir_module indique que le pavé ne sera interprété QUE dans le cas ou le module dir_module soit chargé.

```
<IfModule dir_module>
```

DirectoryIndex

La directive **DirectoryIndex** stipule la liste des pages servies par défaut.

```
DirectoryIndex index.html
```

</IfModule>

Cette directive ferme le bloc **IfModule**

```
</IfModule>
```

Files

La directive Files recherche des fichiers qui correspondent a l'expression régulière passée en argument.

```
<Files ".ht*">
    Require all denied
</Files>
```

ErrorLog

Cette directive indique l'emplacement du journal d'erreurs.

```
ErrorLog "logs/error_log"
```

LogLevel

Cette directive indique le niveau de journalisation au format **syslog**: debug, info, notice, warn, error, crit, alert, emerg.

```
LogLevel warn
```

IfModule

IfModule log_config_module indique que le pavé ne sera interprété QUE dans le cas ou le module log_config_module soit chargé.

```
<IfModule log_config_module>
```

LogFormat

La directive **LogFormat** définit un format de journal et l'associe avec un *nom*. Cette directive prend la forme :

```
LogFormat format|nom
```

```
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
    LogFormat "%h %l %u %t \"%r\" %>s %b" common
    LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %I %O" combinedio
```

L'argument **format** est une chaîne qui peut contenir des caractères littéraux, des caractères de contrôle (par exemple *\n* pour une nouvelle ligne et *\t* pour une tabulation). Les **"** littérales et les **** doivent être précédés par un caractère d'échappement.

Les significations des chaînes de formatage sont les suivantes :

Chaîne	**Description**
%b	La taille de la réponse sans les entêtes HTTP. Le caractère **-** indique 0
%h	L'hôte distant
%l	Le nom du compte de l'utilisateur distant
%r	La première ligne de la requête
%>s	Le statut de la dernière requête
%t	L'heure de la réception de la requête par le serveur
%u	Le nom du compte de l'utilisateur distant
%U	l'URL demandé
%{Referer}i	Le contenu de **Referer** dans l'entête HTTP de la requête.
%{User-agent}i	Le contenu de **User-agent** dans l'entête HTTP de la requête.
%I	Octets reçus, en-têtes et corps de requête inclus ; ne peut pas être nul.

Chaîne	Description
%O	Octets envoyés, en-têtes inclus ; ne peut pas être nul.

CustomLog

La directive **CustomLog** est utilisée pour écrire les journaux. Cette directive prend la forme :

```
CustomLog fichier|tube format
```

```
CustomLog "logs/access_log" combined
```

Le premier argument est donc soit :

- un **fichier** - un chemin complet, relatif à **ServerRoot**, vers un fichier journal, soit
- un **tube** - le caractère **|** suivi par un chemin indiquant le programme qui recevra l'information du journal sur son entrée standard. Le programme concerné est exécuté avec l'UID de l'utilisateur qui a lancé Apache. Si cette utilisateur est **root**, le programme s'exécute sous root !

Le deuxième argument peut être soit :

- Un **format** - un format de journal si celui-ci n'a pas été définit par une directive **LogFormat**, soit
- Un **nom** - un nom définit par une directive **LogFormat**

Consultez votre journal d'accès :

```
[root@centos7 ~]# cat /var/log/httpd/access_log
127.0.0.1 - - [22/Aug/2017:11:31:25 +0200] "GET /" 403 4897 "-" "-"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET / HTTP/1.1" 403 4897 "-" "Mozilla/5.0 (X11; Linux x86_64;
rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /noindex/css/bootstrap.min.css HTTP/1.1" 200 19341
"http://localhost/" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /noindex/css/open-sans.css HTTP/1.1" 200 5081 "http://localhost/"
"Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /images/apache_pb.gif HTTP/1.1" 200 2326 "http://localhost/"
"Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

```
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /images/poweredby.png HTTP/1.1" 200 3956 "http://localhost/"
"Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /noindex/css/fonts/Light/OpenSans-Light.woff HTTP/1.1" 404 241
"http://localhost/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /noindex/css/fonts/Bold/OpenSans-Bold.woff HTTP/1.1" 404 239
"http://localhost/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /noindex/css/fonts/Light/OpenSans-Light.ttf HTTP/1.1" 404 240
"http://localhost/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /noindex/css/fonts/Bold/OpenSans-Bold.ttf HTTP/1.1" 404 238
"http://localhost/noindex/css/open-sans.css" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [22/Aug/2017:15:46:32 +0200] "GET /favicon.ico HTTP/1.1" 404 209 "-" "Mozilla/5.0 (X11; Linux
x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
```

où :

Chaîne	**Valeur**
%h	127.0.0.1
%l	-
%u	-
%t	[22/Aug/2017:15:46:32 +0200]
%r	“GET /favicon.ico HTTP/1.1”
%>s	404
%b	209
%{Referer}i	-
%{User-agent}i	“Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0”

</IfModule>

Cette directive ferme le bloc **IfModule**

```
</IfModule>
```

ScriptAlias

La directive **ScriptAlias** sert ici à créer un lien pour le répertoire **cgi-bin** dans le cas où le module **alias_module** soit chargé :

```
<IfModule alias_module>
    ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
</IfModule>
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
```

TypesConfig

Cette directive indique l'emplacement du fichier mime.types qui contient les correspondances mime des fichiers à afficher dans le cas où le module **mime_module** soit chargé :

```
<IfModule mime_module>
    TypesConfig /etc/mime.types
...
</IfModule>
```

AddType

Cette directive stipule un contenu MIME-type pour une extension de fichier donnée dans le cas où le module **mime_module** soit chargé :

```
<IfModule mime_module>
    ...
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
    AddType text/html .shtml
    ...
</IfModule>
```

AddoutputFilter

La directive **AddOutputFilter** fait correspondre une extension de fichier avec un **filtre**. Les réponses du serveur aux requêtes des clients sont ensuite envoyées vers le filtre avant d'être retournées aux clients :

```
<IfModule mime_module>
    ...
    AddOutputFilter INCLUDES .shtml
</IfModule>
```

AddDefaultCharset

Cette directive spécifie un jeu de caractères par défaut de UTF-8 pour tout document du type text/plain ou text/html. L'utilisation de cette option écrase tout autre spécification basée sur le MIME-Type.

```
AddDefaultCharset UTF-8
```

MIMEMagicFile

Cette directive stipule le fichier magic. Le fichier magic est utilise pour déterminer le type mime d'un fichier.

```
<IfModule mime_magic_module>
    MIMEMagicFile conf/magic
</IfModule>
```

EnableSendfile

Cette directive définit si le programme httpd peut utiliser le support sendfile du noyau pour transmettre le contenu des fichiers aux clients. Par défaut, lorsque le traitement d'une requête ne requiert pas l'accès aux données contenues dans un fichier – par exemple, pour la transmission d'un fichier statique – Apache httpd utilise sendfile pour transmettre le contenu du fichier sans même lire ce dernier, si le système d'exploitation le permet :

```
EnableSendfile on
```

IncludeOptional

Cette directive permet d'inclure des fichiers dans les fichiers de configuration du serveur. Elle fonctionne de manière identique à la directive Include, à l'exception du fait que si l'expression avec caractères génériques wilcard ne correspond à aucun fichier ou répertoire, elle sera ignorée silencieusement au lieu de causer une erreur :

```
IncludeOptional conf.d/*.conf
```

/etc/httpd/conf.d/autoindex.conf

Les directives actives du fichier **/etc/httpd/conf.d/autoindex.conf** sont les suivantes :

```
[root@centos7 ~]# egrep -v '^(#|$)'  /etc/httpd/conf.d/autoindex.conf > /tmp/autoindex.conf
```

```
[root@centos7 ~]# cat /tmp/autoindex.conf
IndexOptions FancyIndexing HTMLTable VersionSort
Alias /icons/ "/usr/share/httpd/icons/"
<Directory "/usr/share/httpd/icons">
    Options Indexes MultiViews FollowSymlinks
    AllowOverride None
    Require all granted
</Directory>
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*
AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif /core
AddIcon /icons/bomb.gif */core.*
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^
```

```
DefaultIcon /icons/unknown.gif
ReadmeName README.html
HeaderName HEADER.html
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
```

Les Directives du fichier /etc/httpd/conf.d/autoindex.conf

IndexOptions

mod_autoindex permet la génération automatique des listes du contenu d'un répertoire quand la page d'index n'est par présente. L'option de génération est activée par la directive **Options +Indexes**. La directive **FancyIndexing** produit des colonnes ayant des liens en tête. Ces liens peuvent être utilisés pour trier l'index. La directive **VersionSort** permet une liste naturelle de fichiers ayant des numéros de versions tels foo-1.8.2 et foo-1.8.2a :

```
IndexOptions FancyIndexing HTMLTable VersionSort
```

Alias

La directive **Alias** sert ici à créer un lien pour le répertoire **icons** :

```
Alias /icons/ "/usr/share/httpd/icons/"
```

<Directory "/usr/share/httpd/icons">

Cette section définit les règles pour le répertoire **/var/www/icons** :

```
<Directory "/usr/share/httpd/icons">
    Options Indexes MultiViews FollowSymlinks
    AllowOverride None
```

```
    Require all granted
</Directory>
```

AddIconByEncoding

Cette directive indique l'icône à afficher avec **FancyIndexing** en stipulant un **chemin** complet pour le type **MIME-type** indiqué. Le format est (alttext,url) où *alttext* indique le texte à afficher pour les navigateurs texte :

```
AddIconByEncoding (CMP,/icons/compressed.gif) x-compress x-gzip
```

AddIconByType

Cette directive indique l'icône à afficher avec **FancyIndexing** en stipulant le type **MIME-type** indiqué. Le format est (alttext,MIME-type) où *alttext* indique le texte à afficher pour les navigateurs texte :

```
AddIconByType (TXT,/icons/text.gif) text/*
AddIconByType (IMG,/icons/image2.gif) image/*
AddIconByType (SND,/icons/sound2.gif) audio/*
AddIconByType (VID,/icons/movie.gif) video/*
```

AddIcon

Cette directive indique l'icône à afficher avec **FancyIndexing** en stipulant un **nom**ou un **extension**. Le format est (alttext,nom/ext) où *alttext* indique le texte à afficher pour les navigateurs texte :

```
AddIcon /icons/binary.gif .bin .exe
AddIcon /icons/binhex.gif .hqx
AddIcon /icons/tar.gif .tar
AddIcon /icons/world2.gif .wrl .wrl.gz .vrml .vrm .iv
AddIcon /icons/compressed.gif .Z .z .tgz .gz .zip
```

```
AddIcon /icons/a.gif .ps .ai .eps
AddIcon /icons/layout.gif .html .shtml .htm .pdf
AddIcon /icons/text.gif .txt
AddIcon /icons/c.gif .c
AddIcon /icons/p.gif .pl .py
AddIcon /icons/f.gif .for
AddIcon /icons/dvi.gif .dvi
AddIcon /icons/uuencoded.gif .uu
AddIcon /icons/script.gif .conf .sh .shar .csh .ksh .tcl
AddIcon /icons/tex.gif .tex
AddIcon /icons/bomb.gif /core
AddIcon /icons/bomb.gif */core.*
AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^
```

DefaultIcon

La directive **DefaultIcon** indique l'icône servie en absence d'un type de fichier connu :

```
DefaultIcon /icons/unknown.gif
```

ReadmeName

Cette directive indique le fichier qui sera ajouter à la fin de l'index. Si le nom du fichier est précédé par un **/**, Apache prend le chemin relatif à la directive **DocumentRoot**. Dans le cas contraire, Apache cherche le fichier dans le répertoire pour lequel l'index est généré :

```
ReadmeName README.html
```

HeaderName

Cette directive indique le fichier qui sera inséré en tête de l'index. Si le nom du fichier est précédé par un /, Apache prend le chemin relatif à la directive **DocumentRoot**. Dans le cas contraire, Apache cherche le fichier dans le répertoire pour lequel l'index est généré :

```
HeaderName HEADER.html
```

IndexIgnore

Cette directive stipule les types de fichiers à exclure de l'index :

```
IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t
```

/etc/httpd/conf.d/userdir.conf

Ce fichier configure la mise à disposition de pages personnelles pour chaque utilisateur ayant un compte sur le serveur Linux.

Les directives actives du fichier **/etc/httpd/conf.d/userdir.conf** sont les suivantes :

```
[root@centos7 ~]# egrep -v '^(#|$)'  /etc/httpd/conf.d/userdir.conf > /tmp/userdir.conf
[root@centos7 ~]# cat /tmp/userdir.conf
<IfModule mod_userdir.c>
    UserDir disabled
</IfModule>
<Directory "/home/*/public_html">
    AllowOverride FileInfo AuthConfig Limit Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

Les Directives du fichier /etc/httpd/conf.d/userdir.conf

<IfModule mod_userdir.c>

Cette directive vérifie si mod_userdir est active.

```
<IfModule mod_userdir.c>
```

UserDir

Le but de cette directive est d'interdire le support des répertoires des utilisateurs :

```
UserDir disable
```

/etc/httpd/conf.d/welcome.conf

Ce fichier configure l'affichage de la page par défaut du serveur Apache dans le cas où il n'existe pas de fichier index.html.

Les directives actives du fichier **/etc/httpd/conf.d/welcome.conf** sont les suivantes :

```
[root@centos7 ~]# egrep -v '^(#|$)'  /etc/httpd/conf.d/welcome.conf > /tmp/welcome.conf
[root@centos7 ~]# cat /tmp/welcome.conf
<LocationMatch "^/+$">
    Options -Indexes
    ErrorDocument 403 /.noindex.html
</LocationMatch>
<Directory /usr/share/httpd/noindex>
    AllowOverride None
    Require all granted
</Directory>
```

```
Alias /.noindex.html /usr/share/httpd/noindex/index.html
Alias /noindex/css/bootstrap.min.css /usr/share/httpd/noindex/css/bootstrap.min.css
Alias /noindex/css/open-sans.css /usr/share/httpd/noindex/css/open-sans.css
Alias /images/apache_pb.gif /usr/share/httpd/noindex/images/apache_pb.gif
Alias /images/poweredby.png /usr/share/httpd/noindex/images/poweredby.png
```

/etc/httpd/conf.modules.d/00-*.conf

Ces fichiers configurent le chargement des modules d'Apache.

Par exemple, les directives actives du fichier **/etc/httpd/conf.modules.d/00-base.conf** sont les suivantes :

```
[root@centos7 ~]# egrep -v '^(#|$)'  /etc/httpd/conf.modules.d/00-base.conf > /tmp/base.conf
[root@centos7 ~]# cat /tmp/base.conf
LoadModule access_compat_module modules/mod_access_compat.so
LoadModule actions_module modules/mod_actions.so
LoadModule alias_module modules/mod_alias.so
LoadModule allowmethods_module modules/mod_allowmethods.so
LoadModule auth_basic_module modules/mod_auth_basic.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule authn_anon_module modules/mod_authn_anon.so
LoadModule authn_core_module modules/mod_authn_core.so
LoadModule authn_dbd_module modules/mod_authn_dbd.so
LoadModule authn_dbm_module modules/mod_authn_dbm.so
LoadModule authn_file_module modules/mod_authn_file.so
LoadModule authn_socache_module modules/mod_authn_socache.so
LoadModule authz_core_module modules/mod_authz_core.so
LoadModule authz_dbd_module modules/mod_authz_dbd.so
LoadModule authz_dbm_module modules/mod_authz_dbm.so
LoadModule authz_groupfile_module modules/mod_authz_groupfile.so
LoadModule authz_host_module modules/mod_authz_host.so
LoadModule authz_owner_module modules/mod_authz_owner.so
LoadModule authz_user_module modules/mod_authz_user.so
```

```
LoadModule autoindex_module modules/mod_autoindex.so
LoadModule cache_module modules/mod_cache.so
LoadModule cache_disk_module modules/mod_cache_disk.so
LoadModule data_module modules/mod_data.so
LoadModule dbd_module modules/mod_dbd.so
LoadModule deflate_module modules/mod_deflate.so
LoadModule dir_module modules/mod_dir.so
LoadModule dumpio_module modules/mod_dumpio.so
LoadModule echo_module modules/mod_echo.so
LoadModule env_module modules/mod_env.so
LoadModule expires_module modules/mod_expires.so
LoadModule ext_filter_module modules/mod_ext_filter.so
LoadModule filter_module modules/mod_filter.so
LoadModule headers_module modules/mod_headers.so
LoadModule include_module modules/mod_include.so
LoadModule info_module modules/mod_info.so
LoadModule log_config_module modules/mod_log_config.so
LoadModule logio_module modules/mod_logio.so
LoadModule mime_magic_module modules/mod_mime_magic.so
LoadModule mime_module modules/mod_mime.so
LoadModule negotiation_module modules/mod_negotiation.so
LoadModule remoteip_module modules/mod_remoteip.so
LoadModule reqtimeout_module modules/mod_reqtimeout.so
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule setenvif_module modules/mod_setenvif.so
LoadModule slotmem_plain_module modules/mod_slotmem_plain.so
LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
LoadModule socache_dbm_module modules/mod_socache_dbm.so
LoadModule socache_memcache_module modules/mod_socache_memcache.so
LoadModule socache_shmcb_module modules/mod_socache_shmcb.so
LoadModule status_module modules/mod_status.so
LoadModule substitute_module modules/mod_substitute.so
LoadModule suexec_module modules/mod_suexec.so
LoadModule unique_id_module modules/mod_unique_id.so
```

```
LoadModule unixd_module modules/mod_unixd.so
LoadModule userdir_module modules/mod_userdir.so
LoadModule version_module modules/mod_version.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
```

/etc/httpd/conf.d/local.conf

Afin de complémenter la configuration de base d'Apache, nous pouvons créer un fichier contenant nos directives dans le répertoire **/etc/httpd/conf.d/**. Creéz donc le fichier **/etc/httpd/conf.d/local.conf** :

```
[root@centos7 ~]# vi /etc/httpd/conf.d/local.conf
[root@centos7 ~]# cat /etc/httpd/conf.d/local.conf
ServerTokens OS
Timeout 60
KeepAlive Off
MaxKeepAliveRequests 100
KeepAliveTimeout 15
StartServers 8
MinSpareServers 5
MaxSpareServers 20
ServerLimit 256
MaxRequestWorkers 256
MaxConnectionsPerChild 4000
UseCanonicalName Off
AccessFileName .htaccess
HostnameLookups Off
ServerSignature On
AddLanguage ca .ca
AddLanguage cs .cz .cs
AddLanguage da .dk
AddLanguage de .de
AddLanguage el .el
AddLanguage en .en
```

```
AddLanguage eo .eo
AddLanguage es .es
AddLanguage et .et
AddLanguage fr .fr
AddLanguage he .he
AddLanguage hr .hr
AddLanguage it .it
AddLanguage ja .ja
AddLanguage ko .ko
AddLanguage ltz .ltz
AddLanguage nl .nl
AddLanguage nn .nn
AddLanguage no .no
AddLanguage pl .po
AddLanguage pt .pt
AddLanguage pt-BR .pt-br
AddLanguage ru .ru
AddLanguage sv .sv
AddLanguage zh-CN .zh-cn
AddLanguage zh-TW .zh-tw
AddHandler type-map var
LanguagePriority en ca cs da de el eo es et fr he hr it ja ko ltz nl nn no pl pt pt-BR ru sv zh-CN zh-TW
ForceLanguagePriority Prefer Fallback
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
```

```
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
ServerName www.homeland.net:80
ExtendedStatus On
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
</Location>
<Location /server-info>
    SetHandler server-info
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
</Location>
```

Dans ce fichier on trouve les directives suivantes :

ServerTokens

Cette directive indique le contenu de l'entête HTTP. La valeur peut être : Full | OS | Minor | Minimal | Major | Prod.

```
ServerTokens OS
```

Timeout

Cette directive indique le nombre de secondes entre une requête et le timeout :

```
Timeout 60
```

KeepAlive

Cette directive interdit plusieurs requêtes par connexion :

```
KeepAlive Off
```

MaxKeepAliveRequests

Cette directive fixe le nombre maximum de requêtes par connexion (0 = infinie) :

```
MaxKeepAliveRequests 100
```

KeepAliveTimeout

Cette directive fixe le nombre de seconds d'attente pour recevoir la requête suivante du même client sur la même connexion :

```
KeepAliveTimeout 15
```

StartServers, MinSpareServers et MaxSpareServers

Ces directives contrôlent le nombre de processus serveur fils au lancement d'Apache, au minimum et au maximum. La valeur par défaut pour prefork de **StartServers** est de 5 :

```
StartServers 8
MinSpareServers 5
MaxSpareServers 20
```

ServerLimit

Pour le module prefork, cette directive définie la valeur maximale de la directive **MaxRequestWorkers** (anciennement **MaxClients**) pour la durée de vie du processus Apache :

```
ServerLimit 256
```

MaxRequestWorkers

Pour le module prefork, la directive **MaxRequestWorkers** indique le nombre maximal de processus fils qui seront lancés pour traiter les requêtes. Sa valeur par défaut est de 256 :

```
MaxRequestWorkers 256
```

MaxConnectionsPerChild

La directive **MaxConnectionsPerChild** (anciennement **MaxRequestsPerChild**) fixe la limite du nombre de requêtes traitées par un processus fils avant que celui-ci expire. Si la valeur de **MaxRequestsPerChild** est 0, le processus n'expirera jamais :

```
MaxConnectionsPerChild 4000
```

UseCanonicalName

Cette directive indique a apache comment construire les variables SERVER_NAME et SERVER_PORT. Quand la directive est On, Apache utilise la valeur de la directive **ServerName**. Quand la directive est Off, Apache utilise les valeurs fournies par le navigateur du client :

```
UseCanonicalName Off
```

AccessFileName

Cette directive indique le nom des fichiers de permissions a utiliser avec le fichier .htpasswd.

```
AccessFileName .htaccess
```

HostnameLookups

Cette directive autorise (On) ou désactive (Off) la résolution DNS pour la trace d'accès.

```
HostnameLookups Off
```

ServerSignature

Cette directive indique si la signature du serveur sera sur les pages d'erreurs: On | Off | EMail

```
ServerSignature On
```

AddLanguage

La directive **AddLanguage** stipule l'extension du fichier à pour le code langage indiqué :

```
AddLanguage ca .ca
AddLanguage cs .cz .cs
AddLanguage da .dk
AddLanguage de .de
AddLanguage el .el
AddLanguage en .en
AddLanguage eo .eo
```

```
AddLanguage es .es
AddLanguage et .et
AddLanguage fr .fr
AddLanguage he .he
AddLanguage hr .hr
AddLanguage it .it
AddLanguage ja .ja
AddLanguage ko .ko
AddLanguage ltz .ltz
AddLanguage nl .nl
AddLanguage nn .nn
AddLanguage no .no
AddLanguage pl .po
AddLanguage pt .pt
AddLanguage pt-BR .pt-br
AddLanguage ru .ru
AddLanguage sv .sv
AddLanguage zh-CN .zh-cn
AddLanguage zh-TW .zh-tw
```

LanguagePriority

Le module **mod_negotiation** fournit la négociation de contenus et est inclus dans Apache par défaut. Il est ainsi possible d'utiliser les informations fournies par le navigateur (préférences de langues, jeu de caractères, encodage et types de médias). Apache a besoin de connaître des informations à propos de chacune des variantes. Ceci peut être fait de deux manières :

- Réaliser un fichier *.var, une **Table de Types** qui précise les fichiers définissant les variantes,
- Utiliser une recherche **MultiViews**.

Dans le cas de l'utilisation des fichiers *.var, Apache en est informé par l'utilisation de la directive **AddHandler**.

```
AddHandler type-map var
```

Pour plus d'informations concernant **mod_negociation**, veuillez consulter **cette page**

La directive **LanguagePriority** indique une liste de langues à utiliser par ordre de priorité de gauche à droite. Cette priorité joue dans le cas où Apache trouve **deux** ou **plusieurs** versions satisfaisantes du même document. En effet c'est la directive **ForceLanguagePriority**, utilisée avec la valeur **Prefer** qui indique à Apache d'utiliser le premier langue de la liste de priorité définit par **LanguagePriority**. La valeur **Fallback** indique à Apache que dans le cas où aucune version satisfaisante du document n'est trouvée, Apache doit utilisé la première version de la liste définit par **LanguagePriority** :

```
LanguagePriority en ca cs da de el eo es et fr he hr it ja ko ltz nl nn no pl pt pt-BR ru sv zh-CN zh-TW
ForceLanguagePriority Prefer Fallback
```

mod_setenvif

mod_setenvif permet de définir des variables d'environnement.

Le variable **downgrade-1.0** oblige Apache à traiter la requête comme du HTTP/1.0 même si elle a été construite sur une norme plus récente.

Le variable **force-response-1.0**, initialement implémenté pour résoudre un problème avec les serveurs mandataires d'AOL, oblige Apache à n'envoyer que des réponses en HTTP/1.0 aux clients.

Le variable **nokeepalive** désactive **Keep-Alive**, une extension à HTTP/1.0 qui permet d'envoyer de requêtes multiples sur la même connexion TCP.

Le variable **redirect-carefully** rend le serveur plus attentif quand il doit envoyer une redirection au client. Cette variable est habituellement utilisée quand un client a un problème connu pour gérer les redirections.

```
BrowserMatch "Mozilla/2" nokeepalive
BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0
BrowserMatch "RealPlayer 4\.0" force-response-1.0
BrowserMatch "Java/1\.0" force-response-1.0
BrowserMatch "JDK/1\.0" force-response-1.0
BrowserMatch "Microsoft Data Access Internet Publishing Provider" redirect-carefully
BrowserMatch "MS FrontPage" redirect-carefully
BrowserMatch "^WebDrive" redirect-carefully
```

```
BrowserMatch "^WebDAVFS/1.[0123]" redirect-carefully
BrowserMatch "^gnome-vfs/1.0" redirect-carefully
BrowserMatch "^XML Spy" redirect-carefully
BrowserMatch "^Dreamweaver-WebDAV-SCM1" redirect-carefully
```

ServerName

Cette directive indique le nom du serveur. Décommentez cette directive et modifiez-la ainsi :

```
ServerName www.homeland.net:80
```

mod-status

Ce module permet à l'administrateur d'Apache de visualiser des informations sur la charge du serveur (requêtes, processus etc.). La directive **ExtendedStatus** doit être **On** pour obtenir le maximum de renseignements. Pour activer l'utilisation de ce module, décommentez les lignes suivantes et modifiez la directive **Allow from** :

```
ExtendedStatus On

<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
</Location>
```

mod_info

Ce module permet d'obtenir une vue d'ensemble de la configuration courante du serveur dont la liste des modules installés et des directives des fichiers de configuration du serveur. Pour activer ce module décommentez les ligne suivantes et modifiez la directive **Allow from** :

```
<Location /server-info>
    SetHandler server-info
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
</Location>
```

Application de la Configuration

Editez le fichier **/etc/hosts** et ajoutez la ligne suivante:

```
10.0.2.15       www.homeland.net
```

Re-démarrez le serveur httpd :

```
[root@centos7 ~]# systemctl restart httpd
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2017-08-24 10:19:38 CEST; 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 17996 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
  Process: 21235 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 18013 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─18013 /usr/sbin/httpd -DFOREGROUND
           ├─18014 /usr/sbin/httpd -DFOREGROUND
           ├─18015 /usr/sbin/httpd -DFOREGROUND
           ├─18016 /usr/sbin/httpd -DFOREGROUND
           ├─18017 /usr/sbin/httpd -DFOREGROUND
```

```
           ├─18018 /usr/sbin/httpd -DFOREGROUND
           ├─18019 /usr/sbin/httpd -DFOREGROUND
           ├─18020 /usr/sbin/httpd -DFOREGROUND
           └─18021 /usr/sbin/httpd -DFOREGROUND

Aug 24 10:19:38 centos7.fenestros.loc systemd[1]: Starting The Apache HTTP Server...
Aug 24 10:19:38 centos7.fenestros.loc systemd[1]: Started The Apache HTTP Server.
```

Gestion de serveurs virtuels

Apache est capable de gérer de multiples sites hébergés sur la même machine. Ceci est rendu possible par un fichier de configuration spécifique appelé: **/etc/httpd/conf/vhosts.d/Vhosts.conf**. Le répertoire **/etc/httpd/conf/vhosts.d/** n'existant pas, créez-le:

```
[root@centos7 ~]# mkdir /etc/httpd/conf/vhosts.d/
```

Créez ensuite le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** :

```
[root@centos7 ~]# touch /etc/httpd/conf/vhosts.d/Vhosts.conf
```

Le contenu de fichier est inclus à l'intérieur de la configuration d'apache grâce à la directive suivante du fichier **httpd.conf**:

```
...
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.conf
Include conf/vhosts.d/*.conf
```

Ajoutez donc cette ligne au fichier **/etc/httpd/conf/httpd.conf**.

Il existe deux façons de créer des sites (hôtes) virtuels :

- Hôte Virtuel par adresse IP

- Hôte Virtuel par nom

Créez un répertoire **/www/site1** à la racine de votre arborescence pour héberger notre premier hôte virtuel :

```
[root@centos6 ~]# mkdir -p /www/site1
```

Créez ensuite le fichier **index.html** du répertoire **/www/site1**:

```
[root@centos7 ~]# vi /www/site1/index.html
```

Editez-le ainsi :

index.html

```
<html>
<head>
<title>Page de Test</title>
<body>
<center>Accueil du site 1</center>
</body>
</html>
```

Hôte virtuel par nom

Nous allons d'abord considérer les sites virtuels par nom. Editez donc le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** en suivant l'exemple ci-dessous :

Vhosts.conf

```
################## Named VirtualHosts
NameVirtualHost *:80
```

```
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
##################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
<Directory /www/site1>
Require all granted
</Directory>
</VirtualHost>
```

Important : Notez qu'apache servira toujours le **contenu da la première section** des sites virtuels par défaut, sauf précision de la part de l'internaute. Il est donc impératif d'ajouter une section **VirtualHost** pour votre site par défaut.

Redémarrez ensuite le serveur Apache :

```
[root@centos7 ~]# systemctl restart httpd
```

Avant de pouvoir consulter le site virtuel, il faut renseigner votre fichier **hosts** :

```
10.0.2.15            www.homeland.net
10.0.2.15            www.vhostnom.com
```

Sauvegardez votre fichier hosts et installez le navigateur web en mode texte **lynx** :

```
[root@centos7 ~]# yum install lynx
```

```
Loaded plugins: fastestmirror, langpacks
adobe-linux-x86_64
| 2.9 kB  00:00:00
base
| 3.6 kB  00:00:00
extras
| 3.4 kB  00:00:00
updates
| 3.4 kB  00:00:00
Loading mirror speeds from cached hostfile
 * base: centos.mirrors.ovh.net
 * extras: ftp.rezopole.net
 * updates: centos.mirrors.ovh.net
Resolving Dependencies
--> Running transaction check
---> Package lynx.x86_64 0:2.8.8-0.3.dev15.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================================
 Package                         Arch                              Version
Repository                       Size
================================================================================================================
=====================================
Installing:
 lynx                            x86_64                            2.8.8-0.3.dev15.el7
base                            1.4 M

Transaction Summary
================================================================================================================
=====================================
Install  1 Package
```

```
Total download size: 1.4 M
Installed size: 5.4 M
Is this ok [y/d/N]: y
```

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.vhostnom.com
                            Accueil du site 1


[root@centos7 ~]#
```

Afin de mieux comprendre les visites à notre site virtuel, nous avons besoin d'un fichier log ainsi qu'un fichier de log des erreurs. Ouvrez donc le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** et ajoutez les deux lignes suivantes:

```
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
```

Vous obtiendrez une fenêtre similaire à celle-ci :

Vhosts.conf

```
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
##################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
```

```
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
<Directory /www/site1>
Require all granted
</Directory>
</VirtualHost>
```

Créez ensuite le répertoire /www/logs/site1 :

```
[root@centos7 ~]# mkdir -p /www/logs/site1
```

Redémarrez le serveur Apache :

```
[root@centos7 ~]# systemctl restart httpd
```

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.vhostnom.com
                            Accueil du site 1


[root@centos7 ~]#
```

Contrôlez maintenant le contenu du répertoire **/www/logs/site1**. Vous devez y retrouver deux fichiers :

```
[root@centos7 ~]# ls -l /www/logs/site1/
total 4
-rw-r--r--. 1 root root   0 Aug 24 11:06 error.log
-rw-r--r--. 1 root root 138 Aug 24 11:06 vhostnom.log
```

Ces deux fichiers **vhostnom.log** et **error.log** sont créés automatiquement par Apache.

En contrôlant le contenu du fichier **/www/logs/site1/vhostnom.log** nous constatons que le log a été généré :

```
[root@centos7 ~]# cat /www/logs/site1/vhostnom.log
10.0.2.15 - - [24/Aug/2017:11:06:47 +0200] "GET / HTTP/1.0" 200 100 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14 SSL-
MM/1.4.1 OpenSSL/1.0.1e-fips"
```

Hôte virtuel par adresse IP

Commencez par créer une adresse IP fixe :

```
[root@centos7 ~]# nmcli connection add con-name ip_fixe ifname enp0s3 type ethernet ip4 10.0.2.16/24 gw4 10.0.2.2
[root@centos7 ~]# nmcli connection up ip_fixe
[root@centos7 ~]# nmcli connection mod ip_fixe ipv4.dns 8.8.8.8
[root@centos7 ~]# systemctl restart NetworkManager
[root@centos7 ~]# nslookup www.free.fr
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name:   www.free.fr
Address: 212.27.48.10
```

Vous allez maintenant procéder à la création d'un site (hôte) virtuel par adresse IP. Normalement, votre serveur serait muni de deux cartes réseaux permettant ainsi d'attribuer un site ou hôte virtuel par numéro IP. Cependant, dans le cas suivant vous allez tout simplement affecté deux numéros IP à la même carte afin de procéder aux tests. Pour faire ceci, vous devez associer une deuxième adresse IP à votre carte réseau eth0. Saisissez donc la commande suivante dans une fenêtre de console en tant que root :

```
[root@centos7 ~]# ip a | grep 'inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.16/24 brd 10.0.2.255 scope global enp0s3
[root@centos7 ~]# ip a add 192.168.1.99/24 dev enp0s3
[root@centos7 ~]# ip a | grep 'inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.16/24 brd 10.0.2.255 scope global enp0s3
```

```
    inet 192.168.1.99/24 scope global enp0s3
```

Créez maintenant le répertoire pour notre site2 :

```
[root@centos7 ~]# mkdir /www/site2
```

Créez la page d'accueil :

```
[root@centos7 ~]# vi /www/site2/index.html
```

Editez la page d'accueil :

index.html

```
<html>
<body>
<center>Accueil du site 2</center>
</body>
</html>
```

Créez ensuite le répertoire /www/logs/site2 :

```
[root@centos7 ~]# mkdir /www/logs/site2
```

Editez maintenant le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf**:

Vhosts.conf

```
################## IP-based Virtual Hosts
<VirtualHost 192.168.1.99>
DocumentRoot /www/site2
ServerName www.vhostip.com
```

```
DirectoryIndex index.html
Customlog /www/logs/site2/vhostip.log combined
Errorlog /www/logs/site2/error.log
<Directory /www/site2>
Require all granted
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
###################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
###################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
<Directory /www/site1>
Require all granted
</Directory>
</VirtualHost>
```

Éditez ensuite le fichier **/etc/hosts** :

```
[root@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.16   centos7.fenestros.loc
```

```
10.0.2.16   www.homeland.net
10.0.2.16       www.vhostnom.com
192.168.1.99    www.vhostip.com
```

Redémarrez votre serveur Apache :

```
[root@centos7 ~]# systemctl restart httpd
```

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.vhostip.com
                            Accueil du site 2


[root@centos7 ~]#
```

Consultez maintenant le répertoire **/www/logs/site2**. Vous constaterez l'apparition d'un fichier log pour le site www.vhostip.com :

```
[root@centos7 ~]# ls -l /www/logs/site2/
total 4
-rw-r--r--. 1 root root   0 Aug 24 14:28 error.log
-rw-r--r--. 1 root root 141 Aug 24 14:29 vhostip.log
```

Modules Additionnels

mod_userdir

Gestion des pages personnelles

Pour qu'apache puisse gérer les pages personnelles des utilisateurs enregistrées du système, il faut que le module **mod_userdir** soit activé dans le

fichier **/etc/httpd/conf/httpd.conf** :

```
LoadModule userdir_module modules/mod_userdir.so
```

Afin de pouvoir tester les pages perso, ajoutez un nouveau utilisateur dénommé homepage :

```
[root@centos6 ~]# groupadd homepage && useradd homepage -c homepage -g homepage -d /home/homepage -s /bin/bash
```

Créez le répertoire /home/homepage/public_html :

```
[root@centos6 ~]# mkdir /home/homepage/public_html
```

Modifiez l'appartenance du répertoire /home/homepage :

```
[root@centos6 ~]# chown -R homepage:homepage /home/homepage
```

Ouvrez le fichier **/etc/httpd/conf/httpd.conf** et recherchez la chaîne **IfModule mod_userdir.c**.

Le but de cette section est de configurer le support des répertoires des utilisateurs dans le cas où le module **mod_userdir.c** est chargé :

```
...
<IfModule mod_userdir.c>
    #
    # UserDir is disabled by default since it can confirm the presence
    # of a username on the system (depending on home directory
    # permissions).
    #
    UserDir disable

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disable" line above, and uncomment
    # the following line instead:
    #
```

```
    #UserDir public_html

</IfModule>

#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
#<Directory /home/*/public_html>
#    AllowOverride FileInfo AuthConfig Limit
#    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
#    <Limit GET POST OPTIONS>
#        Order allow,deny
#        Allow from all
#    </Limit>
#    <LimitExcept GET POST OPTIONS>
#        Order deny,allow
#        Deny from all
#    </LimitExcept>
#</Directory>
...
```

Modifiez cette section ainsi :

```
...
<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>
#
# Control access to UserDir directories.  The following is an example
# for a site where these directories are restricted to read-only.
#
<Directory /home/*/public_html>
    AllowOverride FileInfo AuthConfig Limit
```

```
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    <Limit GET POST OPTIONS>
        Order allow,deny
        Allow from all
    </Limit>
    <LimitExcept GET POST OPTIONS>
        Order deny,allow
        Deny from all
    </LimitExcept>
</Directory>
...
```

Redémarrez le service apache :

```
[root@centos6 ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Creéz maintenant une page d'accueil dans le répertoire **/home/homepage/public_html/**:

```
[root@centos6 ~]# vi /home/homepage/public_html/index.html
```

Ce fichier est vide. Il faut donc l'éditer afin de pouvoir afficher quelque chose aux visiteurs. Saisissez donc le texte suivant dans le fichier concerné :

index.html

```
<html>
<head>
<title>Page de Test</title>
<body>
<center>La Page de l'utilisateur Homepage</center>
</body>
</html>
```

Modifiez les permissions sur le répertoire **/home/homepage** afin que l'utilisateur **apache** puisse avoir accès à son contenu :

```
[root@centos6 ~]# chmod 755 /home/homepage
```

Le site personnel de l'utilisateur est maintenant en ligne. Pour le tester, il suffit de taper l'adresse **http://localhost/~homepage/** dans la barre d'adresses du navigateur de votre choix.

Testez donc la configuartion avec **lynx** :

```
[root@centos6 ~]# lynx --dump http://localhost/~homepage/
                      La Page de l'utilisateur Homepage
```

mod_auth_basic

La sécurité sous Apache se gère grâce à deux fichiers :

- **.htaccess**
  - Ce fichier contient les droits d'accès au répertoire dans lequel est situé le fichier
- **.htpasswd**
  - Ce fichier contient les noms d'utilisateurs et les mots de passe des personnes autorisées à accéder au répertoire protégé par le fichier .htaccess.

Pour activer la sécurité sous apache 2.2, les trois modules **mod_auth_basic**, **mod_authn_file** et **mod_authz_host** doivent être chargées. Vérifiez donc que les trois lignes suivantes ne sont **pas** en commentaires dans le fichier **httpd.conf**:

```
[root@centos6 ~]# cat /etc/httpd/conf/httpd.conf | grep auth_basic
LoadModule auth_basic_module modules/mod_auth_basic.so
[root@centos6 ~]# cat /etc/httpd/conf/httpd.conf | grep authn_file
LoadModule authn_file_module modules/mod_authn_file.so
[root@centos6 ~]# cat /etc/httpd/conf/httpd.conf | grep authz_host_module
LoadModule authz_host_module modules/mod_authz_host.so
```

Configuration de la sécurité avec .htaccess

Dans le cas de notre serveur, nous souhaitons mettre en place un répertoire privé appelé ***secret***. Ce répertoire ne doit être accessible qu'au **webmaster**. Pour le faire, procédez ainsi :

Créez le répertoire secret dans le répertoire **/www/site1** :

```
[root@centos6 ~]# mkdir /www/site1/secret/
```

Créez le fichier **/www/site1/secret/.htaccess**:

```
[root@centos6 ~]# vi /www/site1/secret/.htaccess
```

Editez-le en suivant l'exemple ci-dessous :

.htaccess

```
AuthUserFile /www/passwords/site1/.htpasswd
AuthName "Secret du Site1"
AuthType Basic
<Limit GET>
require valid-user
</Limit>
```

Sauvegardez votre fichier.

Mise en place d'un fichier de mots de passe

Ensuite créez maintenant le répertoire /www/passwords/site1 :

```
[root@centos6 ~]# mkdir -p /www/passwords/site1
```

Créez maintenant le fichier **.htpasswd** avec une entrée pour le **webmaster** grâce à la commande **htpasswd** :

```
[root@centos6 ~]# htpasswd -c /www/passwords/site1/.htpasswd webmaster
New password: fenestros
Re-type new password: fenestros
Adding password for user webmaster
```

Vérifiez le contenu du fichier **/www/passwords/site1/.htpasswd** grâce à la commande **cat** :

```
[root@centos6 ~]# cat /www/passwords/site1/.htpasswd
webmaster:Xa2SvtJUBz.g.
```

Créez maintenant une page html dans le répertoire secret :

```
[root@centos6 ~]# vi /www/site1/secret/index.html
```

Maintenant, éditez-le ainsi :

index.html

```
<html>
<body>
<center>Si vous voyez ce message, vous avez decouvert mon secret !</center>
</body>
</html>
```

Finalement, pour que la sécurité par **.htaccess** soit prise en compte pour le répertoire secret, il faut rajouter une directive à la section de l'hôte virtuel par nom dans le fichier **Vhosts.conf** :

Vhosts.conf

```
################## IP-based Virtual Hosts
<VirtualHost 192.168.1.99>
DocumentRoot /www/site2
ServerName www.vhostip.com
DirectoryIndex index.html
Customlog /www/logs/site2/vhostip.log combined
Errorlog /www/logs/site2/error.log
<Directory /www/site2>
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
###################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
###################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
<Directory /www/site1>
Order allow,deny
Allow from all
</Directory>
<Directory /www/site1/secret>
AllowOverride AuthConfig
</Directory>
```

```
</VirtualHost>
```

Sauvegardez votre fichier et puis redémarrez votre serveur Apache :

```
[root@centos6 ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Testez ensuite votre section privée en tapant http://www.vhostnom.com/secret/index.html dans la barre d'adresses de votre navigateur. Vous constaterez qu'une boîte de dialogue apparaît en vous demandant de renseigner le nom d'utilisateur ainsi que le mot de passe pour pouvoir avoir accès à la section « Secret du Site1 ».

mod_auth_mysql

Vous devez utiliser **mod_auth_mysql** pour protéger l'accès à un répertoire **secret2** dans votre site virtuel www.vhostnom.com.

Installation

Installez le module **mod_auth_mysql** et le serveur mysql :

```
[root@centos6 ~]# yum install mysql-server mod_auth_mysql
```

Configuration de MySQL

Il est maintenant nécessaire de préparer une base de données MySQL pour être compatible avec **mod_auth_mysql**. Démarrez donc le service **mysqld** :

```
[root@centos6 ~]# service mysqld start
Initialisation de la base de données MySQL :  WARNING: The host 'centos.fenestros.loc' could not be looked up
```

```
with resolveip.
This probably means that your libc libraries are not 100 % compatible
with this binary MySQL version. The MySQL daemon, mysqld, should work
normally with the exception that host name resolving will not work.
This means that you should use IP addresses instead of hostnames
when specifying MySQL privileges !
Installing MySQL system tables...
130715 10:56:43 [Note] libgovernor.so not found
OK
Filling help tables...
130715 10:56:43 [Note] libgovernor.so not found
OK

To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h centos.fenestros.loc password 'new-password'

Alternatively you can run:
/usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &
```

```
You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!

                                                          [  OK  ]
Démarrage de mysqld :
```

Connectez-vous à mysql :

```
[root@centos6 ~]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
Server version: 5.5.32-cll-lve MySQL Community Server (GPL) by Atomicorp

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Puis saisissez les commandes MySQL suivantes :

```
CREATE DATABASE auth;

USE auth;

CREATE TABLE users (
user_name CHAR(30) NOT NULL,
user_passwd CHAR(20) NOT NULL,
```

```
PRIMARY KEY (user_name)
);

GRANT SELECT
ON auth.users
TO authuser@localhost
IDENTIFIED BY 'PaSsW0Rd';

INSERT INTO users VALUES ('testuser', ENCRYPT('testpass'));
```

Configuration d'Apache

Quittez mysql :

```
mysql> exit;
Bye
[root@centos6 ~]#
```

Créez ensuite le répertoire **/www/site1/secret2** :

```
[root@centos6 ~]# mkdir /www/site1/secret2
```

Créez maintenant une page **index.html** dans le répertoire **secret2** et éditez-le ainsi :

index.html

```
<html>
<body>
<center>Si vous voyez ce message, vous connaissez mon secret MySQL !</center>
</body>
</html>
```

Ouvrez ensuite le fichier de configuration de mod_auth_mysql **/etc/httpd/conf.d/auth_mysql.conf** et ôtez les **#** devant chacunes des lignes suivantes :

```
<Directory /var/www>
    AuthName "MySQL authenticated zone"
    AuthType Basic

    AuthMYSQLEnable on
    AuthMySQLUser authuser
    AuthMySQLPassword PaSsW0Rd
    AuthMySQLDB auth
    AuthMySQLUserTable users
    AuthMySQLNameField user_name
    AuthMySQLPasswordField user_passwd

    require valid-user
</Directory>
```

Modifiez ensuite la ligne suivante :

```
<Directory /var/www>
```

en

```
<Directory /www/site1/secret2>
```

Afin que les modifications soient prises en charge par apache, redémarrez le service :

```
[root@centos6 ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

En utilisant votre navigateur, ouvrez le site http://www.vhostnom.com/secret2/index.html, renseignez l'utilisateur **testuser** et le mot de passe **testpass** puis cliquez sur le bouton **OK**.

Vous devrez découvert le secret MySQL !

mod_authnz_ldap

Vous devez maintenant utiliser **mod_authnz_ldap** pour protéger l'accès à votre site principal. Pour activer l'authentification en utilisant OpenLDAP sous apache 2.2, les deux modules **mod_ldap** et **mod_authnz_ldap** doivent être chargées. Vérifiez donc que les deux lignes suivantes ne sont **pas** en commentaires dans le fichier **httpd.conf**:

```
...
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
...
```

Pour installer le serveur OpenLDAP sous GNU/Linux ou Unix vous pouvez soit utiliser la version binaire fournie par les dépôts de paquets de votre distribution GNU/Linux ou Unix soit télécharger la dernière version à compiler du site d'OpenLDAP.

Dans notre cas, nous allons installer OpenLDAP à partir des dépôts sur un système CentOS. Commencez par installer OpenLDAP :

```
[root@centos6 ~]# yum install openldap-servers openldap-clients openldap
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * atomic: mir01.syntis.net
 * base: centos.quelquesmots.fr
 * epel: mirror.1000mbps.com
 * extras: centos.quelquesmots.fr
 * rpmforge: mirror.ate.info
 * updates: centos.quelquesmots.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package openldap.i686 0:2.4.23-32.el6_4.1 will be updated
---> Package openldap.i686 0:2.4.23-34.el6_5.1 will be an update
---> Package openldap-clients.i686 0:2.4.23-34.el6_5.1 will be installed
```

```
---> Package openldap-servers.i686 0:2.4.23-34.el6_5.1 will be installed
--> Processing Dependency: libcrypto.so.10(libcrypto.so.10) for package: openldap-servers-2.4.23-34.el6_5.1.i686
--> Running transaction check
---> Package openssl.i686 0:1.0.0-27.el6_4.2 will be updated
---> Package openssl.i686 0:1.0.1e-16.el6_5.7 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                 Arch                            Version
Repository                            Size
================================================================================================================
================================================
Installing:
 openldap-clients                        i686                            2.4.23-34.el6_5.1
updates                               160 k
 openldap-servers                        i686                            2.4.23-34.el6_5.1
updates                               2.0 M
Updating:
 openldap                                i686                            2.4.23-34.el6_5.1
updates                               267 k
Updating for dependencies:
 openssl                                 i686                            1.0.1e-16.el6_5.7
updates                               1.5 M

Transaction Summary
================================================================================================================
================================================
Install       2 Package(s)
Upgrade       2 Package(s)

Total download size: 3.9 M
```

```
Is this ok [y/N]: y
```

Sous CentOS le service OpenLDAP s'appelle **slapd**. Une vérification de son état démontre qi'il n'est démarré dans aucun niveau d'exécution :

```
[root@centos6 ~]# chkconfig --list slapd
slapd           0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
```

Il convient donc d'activer le service :

```
[root@centos6 ~]# chkconfig slapd on
[root@centos6 ~]# chkconfig --list slapd
slapd           0:arrêt    1:arrêt    2:marche    3:marche    4:marche    5:marche    6:arrêt
```

Créez le répertoire **/var/lib/ldap/fenestros** pour contenir un nouveau base de données :

```
[root@centos6 ~]# mkdir /var/lib/ldap/fenestros
```

Nettoyez les anciens fichiers de configuration et fichiers de données :

```
[root@centos6 ~]# rm -Rf /etc/openldap/slapd.d/*
[root@centos6 ~]# rm -f /var/lib/ldap/alock
[root@centos6 ~]# rm -f /var/lib/ldap/__db.00?
```

Créez le fichier **/etc/openldap/slapd.conf** :

```
[root@centos6 ~]# touch /etc/openldap/slapd.conf
```

Editez le fichier **/etc/openldap/slapd.conf** ainsi :

/etc/openldap/slapd.conf

```
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
```

```
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema

allow bind_v2

pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args

TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password

database config
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none

database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Admin,o=fenestros" read
        by * none

########################################

database    bdb
```

```
suffix      "o=fenestros"
checkpoint      1024 15
rootdn      "cn=Admin,o=fenestros"
rootpw
directory   /var/lib/ldap/fenestros
lastmod         on
index           cn,sn,st        eq,pres,sub
```

Créez un mot de passe crypté pour l'admistrateur LDAP :

```
[root@centos6 ~]# slappasswd -s fenestros
{SSHA}C7ieZyzD/uvgaIOca3iukkwYUfl3TRB2
```

Editez ensuite la section **database** du fichier **/etc/openldap/slapd.conf** :

```
...
database        bdb
suffix          "o=fenestros"
checkpoint      1024 15
rootdn          "cn=Admin,o=fenestros"
rootpw          {SSHA}C7ieZyzD/uvgaIOca3iukkwYUfl3TRB2
directory       /var/lib/ldap/fenestros
lastmod         on
index           cn,sn,st                eq,pres,sub
```

Copiez le fichier /usr/share/openldap-servers/DB_CONFIG.example vers **/var/lib/ldap/DB_CONFIG** :

```
[root@centos6 ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/fenestros/DB_CONFIG
```

Initialisez la première base de données :

```
[root@centos6 ~]# echo “” | slapadd -f /etc/openldap/slapd.conf
```

```
The first database does not allow slapadd; using the first available one (2)
str2entry: entry -1 has no dn
slapadd: could not parse entry (line=1)
```

Initialisez ensuite l'arborescence dans **/etc/openldap/slapd.d** :

```
[root@centos6 ~]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
```

Vérifiez que l'arborescence initiale soit créée :

```
[root@centos6 ~]# ls -l /etc/openldap/slapd.d
total 8
drwxr-x---. 3 root root 4096  8 sept. 18:25 cn=config
-rw-------. 1 root root 1127  8 sept. 18:25 cn=config.ldif
```

Modifiez le propriétaire, le groupe ainsi que le droits du répertoire **/etc/openldap/slapd.d** :

```
[root@centos6 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos6 ~]# chmod -R u+rwX /etc/openldap/slapd.d
```

Modifiez le propriétaire et le groupe répertoire **/var/lib/ldap/fenestros** ainsi que le fichier **/etc/openldap/slapd.conf** :

```
[root@centos6 ~]# chown -R ldap:ldap /var/lib/ldap/fenestros /etc/openldap/slapd.conf
```

Démarrez ensuite le service slapd :

```
[root@centos6 ~]# service slapd start
Démarrage de slapd :                                       [  OK  ]
```

Créez le fichier **fenestros.ldif** :

```
dn: o=fenestros
```

```
objectClass: top
objectClass: organization
o: fenestros
description: LDAP Authentification

dn: cn=Admin,o=fenestros
objectClass: organizationalRole
cn: Admin
description: Administrateur LDAP

dn: ou=GroupA,o=fenestros
ou: GroupA
objectClass: top
objectClass: organizationalUnit
description: Membres de GroupA

dn: ou=GroupB,o=fenestros
ou: GroupB
objectClass: top
objectClass: organizationalUnit
description: Membres de GroupB

dn: ou=group,o=fenestros
ou: group
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: fenestros

dn: cn=users,ou=group,o=fenestros
cn: users
objectClass: top
objectClass: posixGroup
gidNumber: 100
memberUid: jean
```

```
memberUid: jacques

dn: cn=Jean Legrand,ou=GroupA,o=fenestros
ou: GroupA
o: fenestros
cn: Jean Legrand
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jean.legrand@fenestros.loc
givenname: Jean
sn: Legrand
uid: jean
uidNumber: 1001
gidNumber: 100
gecos: Jean Legrand
loginShell: /bin/bash
homeDirectory: /home/jean
shadowLastChange: 14368
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
userPassword: secret1
homePostalAddress: 99 avenue de Linux, 75000 Paris
postalAddress: 99 avenue de Linux.
l: Paris
st: 75
postalcode: 75000
telephoneNumber: 01.10.20.30.40
homePhone: 01.50.60.70.80
facsimileTelephoneNumber: 01.99.99.99.99
```

```
title: Ingénieur

dn: cn=Jacques Lebeau,ou=GroupA,o=fenestros
ou: GroupA
o: fenestros
cn: Jacques Lebeau
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jacques.lebeau@fenestros.loc
givenname: Jacques
sn: Lebeau
uid: jacques
uidNumber: 1002
gidNumber: 100
gecos: Jacques Lebeau
loginShell: /bin/bash
homeDirectory: /home/jacques
shadowLastChange: 14365
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
userPassword: secret2
initials: JL
homePostalAddress: 99 route d'Unix, 75000 Paris
postalAddress: 99 route d'Unix.
l: Paris
st: 75
postalcode: 75000
pager: 01.04.04.04.04
homePhone: 01.05.05.05.05
```

```
telephoneNumber: 01.06.06.06.06
mobile: 06.01.02.03.04
title: Technicienne
facsimileTelephoneNumber: 01.04.09.09.09
manager: cn=Jean Legrand,ou=GroupA,o=fenestros
```

Injectez le fichier fenestros.ldif dans OpenLDAP :

```
[root@centos6 ~]# ldapadd -f fenestros.ldif -xv -D "cn=Admin,o=fenestros" -h 127.0.0.1 -w fenestros
ldap_initialize( ldap://127.0.0.1 )
add objectClass:
    top
    organization
add o:
    fenestros
add description:
    LDAP Authentification
adding new entry "o=fenestros"
modify complete

add objectClass:
    organizationalRole
add cn:
    Admin
add description:
    Administrateur LDAP
adding new entry "cn=Admin,o=fenestros"
modify complete

add ou:
    GroupA
add objectClass:
    top
    organizationalUnit
```

```
add description:
    Membres de GroupA
adding new entry "ou=GroupA,o=fenestros"
modify complete

add ou:
    GroupB
add objectClass:
    top
    organizationalUnit
add description:
    Membres de GroupB
adding new entry "ou=GroupB,o=fenestros"
modify complete

add ou:
    group
add objectclass:
    organizationalUnit
    domainRelatedObject
add associatedDomain:
    fenestros
adding new entry "ou=group,o=fenestros"
modify complete

add cn:
    users
add objectClass:
    top
    posixGroup
add gidNumber:
    100
add memberUid:
    jean
```

```
    jacques
adding new entry "cn=users,ou=group,o=fenestros"
modify complete

add ou:
    GroupA
add o:
    fenestros
add cn:
    Jean Legrand
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jean.legrand@fenestros.loc
add givenname:
    Jean
add sn:
    Legrand
add uid:
    jean
add uidNumber:
    1001
add gidNumber:
    100
add gecos:
    Jean Legrand
add loginShell:
    /bin/bash
add homeDirectory:
```

```
    /home/jean
add shadowLastChange:
    14368
add shadowMin:
    0
add shadowMax:
    999999
add shadowWarning:
    7
add userPassword:
    secret1
add homePostalAddress:
    99 avenue de Linux, 75000 Paris
add postalAddress:
    99 avenue de Linux.
add l:
    Paris
add st:
    75
add postalcode:
    75000
add telephoneNumber:
    01.10.20.30.40
add homePhone:
    01.50.60.70.80
add facsimileTelephoneNumber:
    01.99.99.99.99
add title:
    NOT ASCII (10 bytes)
adding new entry "cn=Jean Legrand,ou=GroupA,o=fenestros"
modify complete

add ou:
    GroupA
```

```
add o:
    fenestros
add cn:
    Jacques Lebeau
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jacques.lebeau@fenestros.loc
add givenname:
    Jacques
add sn:
    Lebeau
add uid:
    jacques
add uidNumber:
    1002
add gidNumber:
    100
add gecos:
    Jacques Lebeau
add loginShell:
    /bin/bash
add homeDirectory:
    /home/jacques
add shadowLastChange:
    14365
add shadowMin:
    0
add shadowMax:
```

```
    999999
add shadowWarning:
    7
add userPassword:
    secret2
add initials:
    JL
add homePostalAddress:
    99 route d'Unix, 75000 Paris
add postalAddress:
    99 route d'Unix.
add l:
    Paris
add st:
    75
add postalcode:
    75000
add pager:
    01.04.04.04.04
add homePhone:
    01.05.05.05.05
add telephoneNumber:
    01.06.06.06.06
add mobile:
    06.01.02.03.04
add title:
    Technicienne
add facsimileTelephoneNumber:
    01.04.09.09.09
add manager:
    cn=Jean Legrand,ou=GroupA,o=fenestros
adding new entry "cn=Jacques Lebeau,ou=GroupA,o=fenestros"
modify complete
```

Arrêtez le serveur Apache :

```
[root@centos6 ~]# service httpd stop
Arrêt de httpd :                                           [  OK  ]
```

Remplacez la section **<Directory ”/var/www/html“>** du fichier **/etc/httpd/conf/httpd.conf** avec les lignes suivantes :

```
...
<Directory "/var/www/html">
   AuthType Basic
   AuthName "Bienvenue : Connectez-vous avec votre nom d'utilisateur"
   AuthBasicProvider ldap
   AuthzLDAPAuthoritative on
   AuthLDAPURL ldap://localhost:389/o=fenestros?uid?sub
   AuthLDAPBindDN "cn=Admin,o=fenestros"
   AuthLDAPBindPassword fenestros
   require ldap-user jean jacques
   AllowOverride None
   Options Indexes FollowSymLinks
</Directory>
...
```

Démarrez le serveur apache :

```
[root@centos6 ~]# service httpd start
Démarrage de httpd :                                       [  OK  ]
```

Connectez-vous à http://localhost en utilisant le compte de jean puis le compte de jacques.

mod_php

Introduction

PHP existe en plusieurs versions :

- La version 3
- La version 4
- La version 5

Installation

Afin de faire fonctionner Apache avec PHP, vous avez besoin des paquetages adéquats. Si ce n'est pas déjà le cas, procédez à l'installation du paquet en utilisant **yum** :

```
[root@centos6 ~]# yum install php php-mysql
```

Tester PHP

Afin de tester que PHP fonctionne, créez un fichier de test en php:

```
[root@centos6 ~]# vi /var/www/html/php.php
```

Editez ensuite le fichier ainsi :

php.php

```
<html>
<head>
<title>Ma page de test en PHP</title>
</head>
<body>
<?PHP
```

```
phpinfo();
?>
</body>
</html>
```

Redémarrez Apache :

```
[root@centos6 ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Pour vérifier qu'Apache fonctionne correctement avec php, lancez votre navigateur et saisissez l'adresse http://localhost/php.php dans la barre d'adresses.

mod_proxy

Sous RHEL / CentOS le support pour mod_proxy est installé par défaut.

Editez donc le fichier de configuration **/etc/httpd/conf/httpd.conf** et enlever les **#** devant les lignes suivantes :

```
#<IfModule mod_proxy.c>
#ProxyRequests On
#
#<Proxy *>
#    Order deny,allow
#    Deny from all
#    Allow from .example.com
#</Proxy>
```

Modifiez ensuite la section ainsi :

```
<IfModule mod_proxy.c>
ProxyRequests On
listen 0.0.0.0:8081

<Proxy *>
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1 10.0.2.0/24
</Proxy>
```

Sauvegardez le fichier rechargez la configuration du serveur apache :

```
[root@centos6 ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Configurez votre navigateur pour utiliser le serveur mandataire (proxy):

localhost
port: 8081

Testez ensuite votre serveur proxy apache en rechargeant cette page. Consultez votre fichier de log **access**. Vous constaterez un résultat similaire à celui-ci :

```
[root@centos6 ~]# tail /var/log/httpd/access_log
127.0.0.1 - - [15/Jul/2013:11:17:46 +0200] "GET http://fonts.googleapis.com/css?family=Nobile HTTP/1.1" 200 239
"http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:46 +0200] "GET
http://www.linuxelearning.com/wp-content/plugins/wpachievements/css/style.css?ver=3.5.2 HTTP/1.1" 200 2175
"http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:46 +0200] "GET
http://www.linuxelearning.com/wp-content/plugins/sfwd-lms/wp-pro-quiz/css/wpProQuiz_front.min.css?ver=0.23
```

```
HTTP/1.1" 304 - "http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like
Gecko) Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:46 +0200] "GET
http://www.linuxelearning.com/wp-content/plugins/contact-form-plugin/css/style.css?ver=3.5.2 HTTP/1.1" 304 -
"http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:46 +0200] "GET
http://www.linuxelearning.com/wp-content/plugins/wpachievements/js/jquery.gritter.js?ver=3.5.2 HTTP/1.1" 200 3919
"http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:46 +0200] "GET
http://www.linuxelearning.com/wp-content/plugins/popover/popover-load-js.php?ver=3.5.2 HTTP/1.1" 200 1491
"http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:48 +0200] "GET
http://www.linuxelearning.com/wp-content/themes/studio/library/styles/colour-images/greybutton.png HTTP/1.1" 200
132 "http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:50 +0200] "GET
http://www.linuxelearning.com/wp-content/themes/studio/library/styles/colour-images/greybutton_on.png HTTP/1.1"
200 132 "http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:48 +0200] "GET
http://www.linuxelearning.com/wp-admin/admin-ajax.php?callback=po_onsuccess&action=popover_selective_ajax&thefrom
=http%3A%2F%2Fwww.linuxelearning.com%2F&thereferrer=&active_popover=0&_=1373879868755 HTTP/1.1" 200 52
"http://www.linuxelearning.com/" "Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.31 (KHTML, like Gecko)
Chrome/26.0.1410.63 Safari/537.31"
127.0.0.1 - - [15/Jul/2013:11:17:48 +0200] "GET
http://www.linuxelearning.com/wp-content/themes/studio/favicon.ico HTTP/1.1" 404 3906 "-" "Mozilla/5.0 (X11;
Linux i686) AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.63 Safari/537.31"
```

mod_disk_cache

Afin de mettre en place un serveur manadataire avec cache disque en utilisant apache, il convient d'activer les modules suivants :

```
LoadModule cache_module             modules/mod_cache.so
LoadModule disk_cache_module        modules/mod_disk_cache.so
```

Modifiez ensuite la section suivante du fichier httpd.conf en enlevant les **#** devant les lignes :

```
#<IfModule mod_disk_cache.c>
#   CacheEnable disk /
#   CacheRoot "/var/cache/mod_proxy"
#</IfModule>
```

Modifiez cette section ainsi :

```
<IfModule mod_disk_cache.c>
   CacheEnable disk /
   CacheRoot "/var/cache/mod_proxy"
   CacheDisable microsoft.com
   CacheMaxExpire 86400
   CacheDefaultExpire 3600
   CacheIgnoreNoLastMod Off
   CacheIgnoreCacheControl Off
   CacheStorePrivate Off
   CacheStoreNoStore Off
   CacheIgnoreHeaders None
   CacheLastModifiedFactor 0.1
   CacheDirLevels 5
   CacheDirLength 3
   CacheMinFileSize 1
   CacheMaxFileSize 1000000
</IfModule>
```

Passez en revue les **directives** contenues dans cette section en utilisant le **Manuel en ligne d'Apache**.

Sauvegardez votre fichier puis re-chargez la configuration du serveur apache.

Nettoyez le cache de votre navigateur. Testez ensuite votre serveur cache apache en rechargeant cette page. Consultez votre répertoire de cache disque **/var/cache/mod_proxy**. Vous constaterez un résultat similaire à celui-ci :

```
[root@centos6 ~]# ls /var/cache/mod_proxy
1Cu  1SM  bsp  Dv@  gHh  hhD  H_N  hzr  iyG  MS3  pTT  QaO  QD_  QNm  QuO  s2z  sEY  sOF  Svr  w28  W9I  xwm  z4E
```

mod_dav

Introduction

WebDAV (Web-based Distributed Authoring and Versioning) est une extension du protocole HTTP. Le protocole WebDAV :

- est décrit dans la **RFC 2518**,
- permet de simplifier la gestion de fichiers avec des serveurs distants
- permet de récupérer, déposer, synchroniser et publier des fichiers et dossiers,
- permet, grâce à un mécanisme de verrouillage et de déverrouillage de protéger contre l'écrasement,
- gère les métadonnées : titre, sujet, créateur, etc,
- gère les attributs de fichiers : copier, renommer, déplacer et supprimer des fichiers,

Installation

Pour activer WebDAV, il faut que les deux modules suivants soient activés dans le fichier httpd.conf :

```
[root@centos6 ~]# cat /etc/httpd/conf/httpd.conf | grep mod_dav.so
```

```
LoadModule dav_module modules/mod_dav.so
[root@centos6 ~]# cat /etc/httpd/conf/httpd.conf | grep mod_dav_fs.so
LoadModule dav_fs_module modules/mod_dav_fs.so
```

Configuration

Afin de mettre en place un hôte virtuel pour contenir un site WebDAV, créez son répertoire racine :

```
[root@centos6 ~]# mkdir /www/dav
```

Créez ensuite le fichier /www/dav/dav.test contenant le mot **test** :

```
[root@centos6 ~]# echo test > /www/dav/dav.test
```

Ensuite éditez le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** en y ajoutant la section suivante à la fin :

```
##################dav.homeland.net
<VirtualHost *:80>
ServerName dav.homeland.net
DocumentRoot /www/dav
<Directory /www/dav>
Order allow,deny
Allow from all
</Directory>
<Location />
Dav On
AuthType Basic
AuthName "Accès WebDAV"
AuthUserFile /www/passwords/dav/.davusers
<LimitExcept GET HEAD OPTIONS>
Require valid-user
</LimitExcept>
```

```
</Location>
</VirtualHost>
```

Créez maintenant le répertoire pour contenir le fichier des mots de passe :

```
[root@centos6 ~]# mkdir /www/passwords/dav
```

Créez le fichier **.davusers** avec un mot de passe pour **webmaster** :

```
[root@centos6 ~]# htpasswd -c /www/passwords/dav/.davusers webmaster
New password: fenestros
Re-type new password: fenestros
Adding password for user webmaster
```

Ajoutez le site **dav.homeland.net** au fichier **/etc/hosts** :

hosts

```
10.0.2.15   centos.fenestros.loc
127.0.0.1   localhost.localdomain    localhost
::1 centos    localhost6.localdomain6    localhost6
10.0.2.15       www.homeland.net
10.0.2.15       www.vhostnom.com
192.168.1.99    www.vhostip.com
10.0.2.15   dav.homeland.net
```

Rechargez les fichiers de configuration d'apache :

```
[root@centos6 ~]# service httpd reload
Rechargement de httpd :
```

Pour tester la configuration, il convient d'utiliser le client WebDAV en ligne de commande, **cadaver**.

Téléchargez et installez Cadaver :

```
[root@centos6 ~]# wget http://www.webdav.org/cadaver/cadaver-0.23.3.tar.gz
[root@centos6 ~]# tar xvf cadaver-0.23.3.tar.gz
[root@centos6 ~]# cd cadaver-0.23.3
[root@centos6 cadaver-0.23.3]# ./configure
[root@centos6 cadaver-0.23.3]# make
[root@centos6 cadaver-0.23.3]# make install
```

Connectez-vous au site **http://dav.homeland.net** avec **cadaver** et saisissez votre mot de passe. Vous obtiendrez un résultat similaire à celui-ci :

```
[root@centos6 cadaver-0.23.3]# cadaver http://dav.homeland.net
Authentication required for Accès WebDAV on server `dav.homeland.net':
Username: webmaster
Password:
dav:/> ls
Listing collection `/': succeeded.
        dav.test                                5  juil. 15 11:47
dav:/> cat dav.test
Displaying `/dav.test':
test
dav:/> exit
Connection to `dav.homeland.net' closed.
```

mod_rewrite

Introduction

Le module **mod_rewrite** permet la réécriture d'URL en temps réel en utilisant des **expressions régulières**.

Activer mod_rewrite

Pour activer **mod_rewrite**, il convient de vérifier que la ligne suivante de votre fichier **httpd.conf** ne soit pas en commentaire :

```
LoadModule rewrite_module modules/mod_rewrite.so
```

LABS

Mettre un site en maintenance

Dans cet exemple, vous allez rediriger votre site principal vers une page nommée maintenance.html.

Créez donc une page **maintenance.html** dans le répertoire **/var/www/html** et éditez-la ainsi :

maintenance.html

```
<html>
<head>
<title>Site en Maintenance</title>
</head>
<body>
Notre site est actuellement en maintenance. Merci de revenir plus tard.
</body>
</html>
```

Editez ensuite le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** ainsi :

```
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
```

```
RewriteEngine on
RewriteRule ^/$ /maintenance.html [R]
</VirtualHost>
```

La directive **RewriteEngine on** active mod_rewrite pour le serveur virtuel principal.

La directive **RewriteRule ^/$ /maintenance.html [R]** permet de rediriger toute requête pour le site vers la page maintenance.html.

Sauvegardez votre fichier puis rechargez la configuration d'apache :

```
[root@centos6 ~]# service httpd reload
Rechargement de httpd :
```

Testez ensuite votre configuration avec lynx :

```
[root@centos6 ~]# lynx --dump http://www.homeland.net

   Notre site est actuellement en maintenance. Merci de revenir plus tard.
```

Interdire l'accès pour une adresse IP spécifique

Dans ce cas, vous avez constaté qu'un pirate vous crée problèmes et vous avez pu relever son adresse IP. Le but ici est donc de renvoyer ce pirate vers une page **aurevoir.html** créer spécialement pour l'acceuillir.

Commencez par créer la page **aurevoir.html** dans le répertoire **/var/www/html** :

aurevoir.html

```
<html>
<head>
<title>Aurevoir</title>
</head>
<body>
```

```
<center>Aurevoir Pirate ! Ha! Ha! Ha!</center>
</body>
</html>
```

Editez ensuite le fichier **Vhosts.conf** afin de renvoyer toute requête d'une adresse IP spécifique vers la page **aurevoir.html** en y ajoutant les lignes suivantes :

```
RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.15$
RewriteCond %{REQUEST_URI} !^aurevoir\.html
RewriteRule .* /aurevoir.html
```

Vous obtiendrez le résultat suivant :

```
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.15$
RewriteCond %{REQUEST_URI} !^aurevoir\.html
RewriteRule .* /aurevoir.html
</VirtualHost>
```

Notez bien que la règle precédente a été mise en commentaire.

Sauvegardez votre fichier puis rechargez la configuration d'apache :

```
[root@centos6 ~]# service httpd reload
Rechargement de httpd :
```

Testez ensuite votre configuration avec lynx, vous devez obtenir une fenêtre similaire à celle-ci :

```
[root@centos6 vhosts.d]# lynx --dump http://www.homeland.net

                        Aurevoir Pirate ! Ha! Ha! Ha!
```

Indiquer un déplacement permenant

Dans ce cas, votre but est de rediriger les internautes de l'**anciennepage.html** vers la **nouvellepage.html**, tout en indiquant aux moteurs de recherche que le déplacement de l'**anciennepage.html** est définitif.

Commencez par créer vos deux fichiers **anciennepage.html** et **nouvellepage.html** dans **/var/www/html**.

Le fichier **anciennepage.html** est vide car son contenu a été déplacé à la **nouvellepage.html** :

```
Fichier vide
```

Le fichier **nouvellepage.html** contient donc le nouveau contenu :

nouvellepage.html

```
<html>
<head>
<title>Page déplacée</title>
<body>
<center>Exemple de DEPLACEMENT PERMENANT</center>
</body>
</html>
```

Editez ensuite le fichier **Vhosts.conf** en y ajoutant la ligne suivante :

```
RewriteRule ^/anciennepage\.html /nouvellepage.html [R=301,L]
```

Vous obtiendrez le résultat suivant :

```
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.15$
#RewriteCond %{REQUEST_URI} !^aurevoir\.html
#RewriteRule .* /aurevoir.html
RewriteRule ^/anciennepage\.html /nouvellepage.html [R=301,L]
</VirtualHost>
```

Notez bien que les règles précédentes ont été mises en commentaires.

Sauvegardez votre fichier puis rechargez la configuration d'apache :

```
[root@centos6 ~]# service httpd reload
Rechargement de httpd :
```

Testez ensuite votre configuration avec lynx, vous devez obtenir un résultat similaire à celui-ci :

```
[root@centos6 ~]# lynx --dump http://www.homeland.net/anciennepage.html

                      Exemple de DEPLACEMENT PERMENANT
```

Expliquez ensuite l'utilisation de **[R=301,L]**.

Indiquer qu'une ressource est indisponible

Au bout d'une certaine période, on peux considérer que les moteurs de recherche soient mis à jours avec notre changement vers la **nouvellepage.html**.

Dans ce cas, nous allons donc tout simplement indiquer que l'**anciennepage.html** n'existe plus.

Editez ensuite le fichier **Vhosts.com** en y ajoutant la ligne suivante :

```
RewriteRule ^/anciennepage\.html - [G]
```

Vous obtiendrez le résultat suivant :

```
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.15$
#RewriteCond %{REQUEST_URI} !^aurevoir\.html
#RewriteRule .* /aurevoir.html
#RewriteRule ^/anciennepage\.html /nouvellepage.html [R=301,L]
RewriteRule ^/anciennepage\.html - [G]
</VirtualHost>
```

Notez bien que les règles précédentes ont été mises en commentaires.

Sauvegardez votre fichier puis rechargez la configuration d'apache :

```
[root@centos6 ~]# service httpd reload
```

```
Rechargement de httpd :
```

Testez ensuite votre configuration avec lynx, vous devez obtenir un résultat similaire à celui-ci :

```
[root@centos6 ~]# lynx --dump http://www.homeland.net/anciennepage.html
                                    Gone

   The requested resource
   /anciennepage.html
   is no longer available on this server and there is no forwarding
   address. Please remove all references to this resource.
     ____________________________________________________________


    Apache/2.2.15 (CentOS) Server at www.homeland.net Port 80
```

Expliquez ensuite l'utilisation de **[G]**.

Directives de mod_rewrite

RewriteEngine

RewriteEngine on|off

Cette directive active ou désactive le moteur de réécriture.

RewriteOptions

RewriteOptions options

Cette directive définit deux options :

- Inherit
  - La configuration courante hérite de la configuration parente. Ceci peut être appliquer à un hôte virtuel ou un répertoire.
- MaxRedirects=nombre
  - *nombre* dont la valeur par défaut est de 10, permet de sortir d'une règle mal écrite au bout de *nombre* boucles. Dans ce cas le serveur sert une page HTTP 500 - Internal Server Error.

RewriteLog

RewriteLog fichier

Cette directive consigne les activités de réécriture dans le fichier passé en argument.

RewriteLogLevel

RewriteLogLevel niveau

Cette directive définit le niveau de verbosité de 0 à 9 où 0 ne consigne rien et 9 consigne tout. En production la valeur ne devrait pas dépasser **2**, sauf en cas de débogage.

RewriteLock

RewriteLock fichier

Cette directive désigne le fichier-verrou utilisé par mod_rewrite pour éviter des accès concurrentiels à des programmes et scripts définis par la directive **RewriteMap**.

RewriteMap

RewriteMap table txt|dbm|prg:fichier

Cette directive définit une table externe utilisée pour des réécritures. La règle de réécriture est écrite comme suit :

```
$ { table : clef : ValeurParDéfaut }
```

Lors de l'utilisation de cette règle, la *table* est consultée et la *clef* recherchée. Dans le cas où la *clef* est trouvée, la fonction retourne la **ValeurDeSubstitution** trouvée dans la *table*. Dans le cas contraire, la fonction retourne la **ValeurParDéfaut** stipulée dans la règle de réécriture

La *table* peut être au format **texte brut**, au format **DBM** ou être un **binaire** ou un **script** :

- **txt:fichier**
  - La table contient une paire par ligne au format *clef ValeurDeSubstitution*
- **dbm:fichier**
  - La table contient une paire par ligne au format *clef ValeurDeSubstitution*. La différence entre DBM et txt réside dans le fait que les fichiers binaires DBM sont optimisés pour la vitesse.
- **prg:fichier**
  - prg est un binaire ou un script. prg reçoit sur stdin la clef et retourne sur stdout la ValeurDeSubstitution. Si aucune correspondance n'est trouvée, prg retourne la chaîne *NULL* sur stdout.

RewriteBase

RewriteBase urlrélatif

Cette directive indique l'URL de base pour les règles de réécriture incluses dans un fichier **.htaccess**. Dans ce cas, l'action des règles est localisée dans le sens où la partie du chemin d'accès de l'url contenant le fichier .htaccess est enlevée. Après traitement des règles, l'URL au complet doit être réinjecter dans le serveur en utilisant la valeur de la directive **RewriteBase**.

RewriteCond

RewriteCond chaineatester motif [drapeau1,drapeau2,...]

La directive **RewriteCond** définit une condition d'application pour la ou les règle(s) de réécriture qui suit(vent). Plusieurs conditions d'application peuvent se suivre. Cependant notez que la ou les règle(s) de réécriture qui suivent ne seront interprétées **que** dans le cas où **toutes** les conditions d'applications soient remplies.

L'argument **chaineatester** est une chaîne de caractères sur laquelle sera appliquer le motif. Cet argument peut contenir des variables :

- *La variable $N allant de **1** à **9** faisant référence à la règle de réécriture*.
  - Cette variable permet de récupérer la valeur d'un sous-motif, après l'application du **motif** sur la **RewriteRule** qui suit le bloc **RewriteCond**actuel à condition que les sous-motifs soient entourés de parenthèses.
- *La variable %N allant de **1** à **9** faisant référence à la dernière condition remplie*.
  - Cette variable permet de récupérer la valeur d'un sous-motif du **motif** de la dernière **RewriteCond** remplie du bloc actuel à condition que les sous-motifs soient entourés de parenthèses.
- *Une variable serveur :*
  - En-têtes HTTP
    - HTTP_USER_AGENT
    - HTTP_REFERER
    - HTTP_COOKIE
    - HTTP_FORWARDED
    - HTTP_HOST
    - HTTP_PROXY_CONNECTION
    - HTTP_ACCEPT
  - Connexions et requêtes
    - REMOTE_ADDR
    - REMOTE_HOST
    - REMOTE_USER
    - REMOTE_IDENT
    - REQUEST_METHOD
    - SCRIPT_FILENAME
    - PATH_INFO
    - QUERY_STRING

        - AUTH_TYPE
    - Variables internes
        - DOCUMENT_ROOT
        - SERVER_ADMIN
        - SERVER_NAME
        - SERVER_PORT
        - SERVER_PROTOCAL
        - SERVER_SOFTWARE
        - SERVER_VERSION
    - Variables système
        - TIME_YEAR
        - TIME_MON
        - TIME_DAY
        - TIME_HOUR
        - TIME_MIN
        - TIME_SEC
        - TIME_WDAY
        - TIME
    - Variables spéciales
        - API_VERSION
        - THE_REQUEST
        - REQUEST_URI
        - REQUEST_FILE
        - NAME
        - IS_SUBREQ

Passez en revue les **variables serveur** en utilisant le **Manuel en ligne d'Apache**.

Le **motif** est soit une expression régulière :

Caractère spécial	Description
^	Trouver la chaîne au début de la ligne
$	Trouver la chaîne à la fin de la ligne
.	Trouver n'importe quel caractère
*	Trouver 0 ou plus du caractère qui précède
+	Trouver 1 ou plus du caractère qui précède
\	Annuler l'effet spécial du caractère suivant
[ ]	Trouver n'importe quel des caractères entre les crochets
[^]	Exclure les caractères entre crochets
{a}	Trouver a occurrences de ce qui précède
|	Trouver soit ce qui se trouve avant, soit ce qui se trouve après
( )	Limiter la portée d'une alternative

soit une expression :

Expression	Description
<chaine	Vrai si chaineatester est lexicographiquement inférieur à chaine
>chaine	Vrai si chaineatester est lexicographiquement supérieur à chaine
=chaine	Vrai si chaineatester est lexicographiquement égal à chaine
-d	Vrai si chaineatester est un répertoire qui existe
-f	Vrai si chaineatester est un fichier normal qui existe
-s	Vrai si chaineatester est un fichier normal non-vide qui existe
-l	Vrai si chaineatester est un lien symbolique qui existe
-F	Vrai si chaineatester est un fichier existant et accessible selon la configuration du serveur
-F	Vrai si chaineatester est un URL existant et accessible selon la configuration du serveur

Les **drapeaux** sont une liste de commutateurs séparés par des virgules et entourés de crochets. Voici une liste de commutateurs les plus utilisés :

Drapeaux	Description
[NC]	Insensible à la casse
[OR]	Permet de lier deux conditions **RewriteCond** par un **OU**

RewriteRule

RewriteRule motif substitution [drapeau1,drapeau2,...]

Cette directive définit la **règle de réécriture**.

Le **motif** est une expression régulière qui sera appliquée à l'URL courante. L'URL courante n'est pas nécessairement l'URL d'origine.

La **substitution** est une chaîne qui remplacera l'URL qui correspond au **motif**.

Cette chaîne peut contenir des variables :

- *La variable $N allant de **1** à **9** faisant référence à la règle de réécriture*.
  - Cette variable permet de récupérer la valeur d'un sous-motif du **motif** de la règle courante à condition que les sous-motifs soient entourés de parenthèses.
- *La variable %N allant de **1** à **9** faisant référence à la drective **RewriteCond** précédente*.
  - Cette variable permet de récupérer la valeur d'un sous-motif du **motif** de la dernière **RewriteCond** à condition que les sous-motifs soient entourés de parenthèses.
- *Une variable serveur :*
  - En-têtes HTTP
    - HTTP_USER_AGENT
    - HTTP_REFERER
    - HTTP_COOKIE
    - HTTP_FORWARDED
    - HTTP_HOST
    - HTTP_PROXY_CONNECTION
    - HTTP_ACCEPT
  - Connexions et requêtes
    - REMOTE_ADDR
    - REMOTE_HOST
    - REMOTE_USER
    - REMOTE_IDENT
    - REQUEST_METHOD
    - SCRIPT_FILENAME

        - PATH_INFO
        - QUERY_STRING
        - AUTH_TYPE
    - Variables internes
        - DOCUMENT_ROOT
        - SERVER_ADMIN
        - SERVER_NAME
        - SERVER_PORT
        - SERVER_PROTOCAL
        - SERVER_SOFTWARE
        - SERVER_VERSION
    - Variables système
        - TIME_YEAR
        - TIME_MON
        - TIME_DAY
        - TIME_HOUR
        - TIME_MIN
        - TIME_SEC
        - TIME_WDAY
        - TIME
    - Variables spéciales
        - API_VERSION
        - THE_REQUEST
        - REQUEST_URI
        - REQUEST_FILE
        - NAME
        - IS_SUBREQ
- Des appels à des fonctions **RewriteMap**.

Les **drapeaux** sont une liste de commutateurs séparés par des virgules et entourés de crochets. Voici une liste de commutateurs les plus utilisés :

Drapeaux	**Description**
[R[=code]]	Force la redirection
[F]	L'URL sera interdit (Erreur 403)

Drapeaux	Description
[G]	L'URL sera marqué comme déménagé (Erreur 410)
[P]	Force la redirection à passer par le proxy d'apache
[L]	Arrête le traitement de réécriture
[C]	Force un chaînage avec la règle suivante
[N]	Force un traitement en boucle de la règle de réécriture
[NC]	Insensible à la casse

Dernièrement il existe une expression de substitution spéciale définie par **-**. Dans ce cas, il n'y a **pas** de substitution.

Consultez la **Liste des codes HTTP** sur Wikipédia et notez la signification des codes **301** et **410**.

mod_header

HSTS ou **HTTP Strict Transport Security** est une caractéristique de sécurité qui permet à un site web d'informer les navigateurs qui le site web n'accepte que des connexions sécurisées.

Pour mettre en place cette notification, il convient d'éditer le fichier **/etc/httpd/conf.d/ssl.conf** en faisant appel à **mod_header** afin que l'en-tête soit modifié :

```
#
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
Listen 443
Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"
```

Dans ce cas, l'expiration de la notification est dans deux ans (63 072 000 secondes). Un navigateur visitant le site aujourd'hui verra donc l'expiration de deux ans. Si le navigateur reviens demain, celui-ci verra encore deux ans mais à partir de la date de demain.

Pour forcer les navigateurs à connecter en https, il convient d'inclure une règle de ré-ecriture dans la section du site principal de la balise **VirtualHost** qui se trouve dans notre cas dans le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** :

```
...
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
<IfModule mod_rewrite.c>
  RewriteEngine On
  RewriteCond %{HTTPS} off
  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</IfModule>
</VirtualHost>
...
```

Modifiez vos fichiers de configuration et re-démarrez le service **httpd**. Testez ensuite avec un navigateur le lien **http://www.homeland.net**.

mod_security

ModSecurity est un **WAF** (*Web Application Firewall*)) qui est chargé en tant que module dans un serveur web pour fournir de la protection contre des attaques. ModSecurity surveille le trafic HTTP et l'analyse en temps réel. Le produit est développé par la société *Breach Security* et est disponible pour Apache, Nginx and IIS.

Installez mod_security ainsi que le jeu de règles de base :

```
[root@centos6 ~]# yum install mod_security mod_security_crs --nogpgcheck
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * atomic: www7.atomicorp.com
```

```
 * base: centos.mirror.fr.planethoster.net
 * epel: fedora.mirrors.romtelecom.ro
 * extras: ftp.rezopole.net
 * rpmforge: mirror.nl.leaseweb.net
 * updates: mir01.syntis.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package mod_security.i686 1:2.8.0-24.el6.art will be installed
---> Package mod_security_crs.noarch 0:2.2.6-3.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                    Arch                           Version
Repository                          Size
================================================================================================================
================================================
Installing:
 mod_security                               i686                           1:2.8.0-24.el6.art
atomic                             214 k
 mod_security_crs                           noarch                         2.2.6-3.el6
epel                                92 k

Transaction Summary
================================================================================================================
================================================
Install       2 Package(s)

Total size: 306 k
Total download size: 92 k
Installed size: 1.1 M
```

```
Is this ok [y/N]: y
```

L'installation créé un répertoire supplémentaire dans **/etc/httpd** :

```
[root@centos6 ~]# ls -l /etc/httpd/modsecurity.d/
total 20
drwxr-xr-x. 2 root root  4096  9 sept. 12:06 activated_rules
-rw-r--r--. 1 root root 13544 15 nov.   2012 modsecurity_crs_10_config.conf
-rw-r--r--. 1 root root     0  9 sept. 12:06 tortix_waf.conf
```

Le répertoire **/etc/httpd/modsecurity.d/** contient, entre autre, le fichier **modsecurity_crs_10_config.conf**. Ce fichier contient les *policies* appliquées aux règles :

```
[root@centos6 ~]# cat /etc/httpd/modsecurity.d/modsecurity_crs_10_config.conf
# ------------------------------------------------------------
# Core ModSecurity Rule Set ver.2.2.6
# Copyright (C) 2006-2012 Trustwave All rights reserved.
#
# The OWASP ModSecurity Core Rule Set is distributed under
# Apache Software License (ASL) version 2
# Please see the enclosed LICENCE file for full details.
# ------------------------------------------------------------



#
# -- [[ Recommended Base Configuration ]] ------------------------------------------------
#
# The configuration directives/settings in this file are used to control
# the OWASP ModSecurity CRS. These settings do **NOT** configure the main
# ModSecurity settings such as:
#
# - SecRuleEngine
# - SecRequestBodyAccess
# - SecAuditEngine
```

```
# - SecDebugLog
#
# You should use the modsecurity.conf-recommended file that comes with the
# ModSecurity source code archive.
#
# Ref: http://mod-security.svn.sourceforge.net/viewvc/mod-security/m2/trunk/modsecurity.conf-recommended
#



#
# -- [[ Rule Version ]] ------------------------------------------------------------
#
# Rule version data is added to the "Producer" line of Section H of the Audit log:
#
# - Producer: ModSecurity for Apache/2.7.0-rc1 (http://www.modsecurity.org/); OWASP_CRS/2.2.4.
#
# Ref: https://sourceforge.net/apps/mediawiki/mod-security/index.php?title=Reference_Manual#SecComponentSignature
#
SecComponentSignature "OWASP_CRS/2.2.6"



#
# -- [[ Modes of Operation: Self-Contained vs. Collaborative Detection ]] -----------------
#
# Each detection rule uses the "block" action which will inherit the SecDefaultAction
# specified below.  Your settings here will determine which mode of operation you use.
#
# -- [[ Self-Contained Mode ]] --
# Rules inherit the "deny" disruptive action.  The first rule that matches will block.
#
# -- [[ Collaborative Detection Mode ]] --
# This is a "delayed blocking" mode of operation where each matching rule will inherit
# the "pass" action and will only contribute to anomaly scores.  Transactional blocking
# can be applied
```

```
#
# -- [[ Alert Logging Control ]] --
# You have three options -
#
# - To log to both the Apache error_log and ModSecurity audit_log file use: "log"
# - To log *only* to the ModSecurity audit_log file use: "nolog,auditlog"
# - To log *only* to the Apache error_log file use: "log,noauditlog"
#
# Ref:
http://blog.spiderlabs.com/2010/11/advanced-topic-of-the-week-traditional-vs-anomaly-scoring-detection-modes.html
# Ref: https://sourceforge.net/apps/mediawiki/mod-security/index.php?title=Reference_Manual#SecDefaultAction
#
SecDefaultAction "phase:1,deny,log"



#
# -- [[ Collaborative Detection Severity Levels ]] ------------------------------------------
#
# These are the default scoring points for each severity level.  You may
# adjust these to you liking.  These settings will be used in macro expansion
# in the rules to increment the anomaly scores when rules match.
#
# These are the default Severity ratings (with anomaly scores) of the individual rules -
#
#    - 2: Critical - Anomaly Score of 5.
#         Is the highest severity level possible without correlation.  It is
#         normally generated by the web attack rules (40 level files).
#    - 3: Error - Anomaly Score of 4.
#         Is generated mostly from outbound leakage rules (50 level files).
#    - 4: Warning - Anomaly Score of 3.
#         Is generated by malicious client rules (35 level files).
#    - 5: Notice - Anomaly Score of 2.
#         Is generated by the Protocol policy and anomaly files.
#
```

```
SecAction \
  "id:'900001', \
  phase:1, \
  t:none, \
  setvar:tx.critical_anomaly_score=5, \
  setvar:tx.error_anomaly_score=4, \
  setvar:tx.warning_anomaly_score=3, \
  setvar:tx.notice_anomaly_score=2, \
  nolog, \
  pass"


#
# -- [[ Collaborative Detection Scoring Threshold Levels ]] ------------------------------
#
# These variables are used in macro expansion in the 49 inbound blocking and 59
# outbound blocking files.
#
# **MUST HAVE** ModSecurity v2.5.12 or higher to use macro expansion in numeric
# operators.  If you have an earlier version, edit the 49/59 files directly to
# set the appropriate anomaly score levels.
#
# You should set the score to the proper threshold you would prefer. If set to "5"
# it will work similarly to previous Mod CRS rules and will create an event in the error_log
# file if there are any rules that match.  If you would like to lessen the number of events
# generated in the error_log file, you should increase the anomaly score threshold to
# something like "20".  This would only generate an event in the error_log file if
# there are multiple lower severity rule matches or if any 1 higher severity item matches.
#
SecAction \
  "id:'900002', \
  phase:1, \
  t:none, \
  setvar:tx.inbound_anomaly_score_level=5, \
```

```
  nolog, \
  pass"


SecAction \
  "id:'900003', \
  phase:1, \
  t:none, \
  setvar:tx.outbound_anomaly_score_level=4, \
  nolog, \
  pass"


#
# -- [[ Collaborative Detection Blocking ]] ------------------------------------------------
#
# This is a collaborative detection mode where each rule will increment an overall
# anomaly score for the transaction. The scores are then evaluated in the following files:
#
# Inbound anomaly score - checked in the modsecurity_crs_49_inbound_blocking.conf file
# Outbound anomaly score - checked in the modsecurity_crs_59_outbound_blocking.conf file
#
# If you want to use anomaly scoring mode, then uncomment this line.
#
#SecAction \
  "id:'900004', \
  phase:1, \
  t:none, \
  setvar:tx.anomaly_score_blocking=on, \
  nolog, \
  pass"


#
```

```
# -- [[ GeoIP Database ]] ------------------------------------------------------------
#
# There are some rulesets that need to inspect the GEO data of the REMOTE_ADDR data.
#
# You must first download the MaxMind GeoIP Lite City DB -
#
#       http://geolite.maxmind.com/download/geoip/database/GeoLiteCity.dat.gz
#
# You then need to define the proper path for the SecGeoLookupDb directive
#
# Ref: http://blog.spiderlabs.com/2010/10/detecting-malice-with-modsecurity-geolocation-data.html
# Ref: http://blog.spiderlabs.com/2010/11/detecting-malice-with-modsecurity-ip-forensics.html
#
#SecGeoLookupDb /opt/modsecurity/lib/GeoLiteCity.dat

#
# -- [[ Regression Testing Mode ]] ---------------------------------------------------
#
# If you are going to run the regression testing mode, you should uncomment the
# following rule. It will enable DetectionOnly mode for the SecRuleEngine and
# will enable Response Header tagging so that the client testing script can see
# which rule IDs have matched.
#
# You must specify the your source IP address where you will be running the tests
# from.
#
#SecRule REMOTE_ADDR "@ipMatch 192.168.1.100" \
  "id:'900005', \
  phase:1, \
  t:none, \
  ctl:ruleEngine=DetectionOnly, \
  setvar:tx.regression_testing=1, \
  nolog, \
  pass"
```

```
#
# -- [[ HTTP Policy Settings ]] ------------------------------------------------
#
# Set the following policy settings here and they will be propagated to the 23 rules
# file (modsecurity_common_23_request_limits.conf) by using macro expansion.
# If you run into false positives, you can adjust the settings here.
#
# Only the max number of args is uncommented by default as there are a high rate
# of false positives.  Uncomment the items you wish to set.
#
#
# -- Maximum number of arguments in request limited
SecAction \
  "id:'900006', \
  phase:1, \
  t:none, \
  setvar:tx.max_num_args=255, \
  nolog, \
  pass"

#
# -- Limit argument name length
#SecAction \
  "id:'900007', \
  phase:1, \
  t:none, \
  setvar:tx.arg_name_length=100, \
  nolog, \
  pass"

#
# -- Limit value name length
#SecAction \
  "id:'900008', \
```

```
  phase:1, \
  t:none, \
  setvar:tx.arg_length=400, \
  nolog, \
  pass"

#
# -- Limit arguments total length
#SecAction \
  "id:'900009', \
  phase:1, \
  t:none, \
  setvar:tx.total_arg_length=64000, \
  nolog, \
  pass"

#
# -- Individual file size is limited
#SecAction \
  "id:'900010', \
  phase:1, \
  t:none, \
  setvar:tx.max_file_size=1048576, \
  nolog, \
  pass"

#
# -- Combined file size is limited
#SecAction \
  "id:'900011', \
  phase:1, \
  t:none, \
  setvar:tx.combined_file_sizes=1048576, \
  nolog, \
```

```
  pass"


#
# Set the following policy settings here and they will be propagated to the 30 rules
# file (modsecurity_crs_30_http_policy.conf) by using macro expansion.
# If you run into false positves, you can adjust the settings here.
#
SecAction \
  "id:'900012', \
  phase:1, \
  t:none, \
  setvar:'tx.allowed_methods=GET HEAD POST OPTIONS', \
  setvar:'tx.allowed_request_content_type=application/x-www-form-urlencoded|multipart/form-
data|text/xml|application/xml|application/x-amf', \
  setvar:'tx.allowed_http_versions=HTTP/0.9 HTTP/1.0 HTTP/1.1', \
  setvar:'tx.restricted_extensions=.asa/ .asax/ .ascx/ .axd/ .backup/ .bak/ .bat/ .cdx/ .cer/ .cfg/ .cmd/ .com/
.config/ .conf/ .cs/ .csproj/ .csr/ .dat/ .db/ .dbf/ .dll/ .dos/ .htr/ .htw/ .ida/ .idc/ .idq/ .inc/ .ini/ .key/
.licx/ .lnk/ .log/ .mdb/ .old/ .pass/ .pdb/ .pol/ .printer/ .pwd/ .resources/ .resx/ .sql/ .sys/ .vb/ .vbs/
.vbproj/ .vsdisco/ .webinfo/ .xsd/ .xsx/', \
  setvar:'tx.restricted_headers=/Proxy-Connection/ /Lock-Token/ /Content-Range/ /Translate/ /via/ /if/', \
  nolog, \
  pass"


#
# -- [[ Content Security Policy (CSP) Settings ]] ---------------------------------------
#
# The purpose of these settings is to send CSP response headers to
# Mozilla FireFox users so that you can enforce how dynamic content
# is used. CSP usage helps to prevent XSS attacks against your users.
#
# Reference Link:
#
```

```
#   https://developer.mozilla.org/en/Security/CSP
#
# Uncomment this SecAction line if you want use CSP enforcement.
# You need to set the appropriate directives and settings for your site/domain and
# and activate the CSP file in the experimental_rules directory.
#
# Ref:
http://blog.spiderlabs.com/2011/04/modsecurity-advanced-topic-of-the-week-integrating-content-security-policy-csp
.html
#
#SecAction \
  "id:'900013', \
  phase:1, \
  t:none, \
  setvar:tx.csp_report_only=1, \
  setvar:tx.csp_report_uri=/csp_violation_report, \
  setenv:'csp_policy=allow \'self\'; img-src *.yoursite.com; media-src *.yoursite.com; style-src *.yoursite.com;
frame-ancestors *.yoursite.com; script-src *.yoursite.com; report-uri %{tx.csp_report_uri}', \
  nolog, \
  pass"



#
# -- [[ Brute Force Protection ]] ----------------------------------------------------------
#
# If you are using the Brute Force Protection rule set, then uncomment the following
# lines and set the following variables:
# - Protected URLs: resources to protect (e.g. login pages) - set to your login page
# - Burst Time Slice Interval: time interval window to monitor for bursts
# - Request Threshold: request # threshold to trigger a burst
# - Block Period: temporary block timeout
#
#SecAction \
  "id:'900014', \
```

```
  phase:1, \
  t:none, \
  setvar:'tx.brute_force_protected_urls=/login.jsp /partner_login.php', \
  setvar:'tx.brute_force_burst_time_slice=60', \
  setvar:'tx.brute_force_counter_threshold=10', \
  setvar:'tx.brute_force_block_timeout=300', \
  nolog, \
  pass"


#
# -- [[ DoS Protection ]] ------------------------------------------------------------
#
# If you are using the DoS Protection rule set, then uncomment the following
# lines and set the following variables:
# - Burst Time Slice Interval: time interval window to monitor for bursts
# - Request Threshold: request # threshold to trigger a burst
# - Block Period: temporary block timeout
#
#SecAction \
  "id:'900015', \
  phase:1, \
  t:none, \
  setvar:'tx.dos_burst_time_slice=60', \
  setvar:'tx.dos_counter_threshold=100', \
  setvar:'tx.dos_block_timeout=600', \
  nolog, \
  pass"


#
# -- [[ Check UTF enconding ]] -------------------------------------------------------
#
# We only want to apply this check if UTF-8 encoding is actually used by the site, otherwise
```

```
# it will result in false positives.
#
# Uncomment this line if your site uses UTF8 encoding
#SecAction \
  "id:'900016', \
  phase:1, \
  t:none, \
  setvar:tx.crs_validate_utf8_encoding=1, \
  nolog, \
  pass"



#
# -- [[ Enable XML Body Parsing ]] ---------------------------------------------------------
#
# The rules in this file will trigger the XML parser upon an XML request
#
# Initiate XML Processor in case of xml content-type
#
SecRule REQUEST_HEADERS:Content-Type "text/xml" \
  "id:'900017', \
  phase:1, \
  t:none,t:lowercase, \
  nolog, \
  pass, \
  chain"
    SecRule REQBODY_PROCESSOR "!@streq XML" \
      "ctl:requestBodyProcessor=XML"



#
# -- [[ Global and IP Collections ]] -------------------------------------------------------
#
# Create both Global and IP collections for rules to use
```

```
# There are some CRS rules that assume that these two collections
# have already been initiated.
#
SecRule REQUEST_HEADERS:User-Agent "^(.*)$" \
  "id:'900018', \
  phase:1, \
  t:none,t:sha1,t:hexEncode, \
  setvar:tx.ua_hash=%{matched_var}, \
  nolog, \
  pass"


SecRule REQUEST_HEADERS:x-forwarded-for "^\b(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\b" \
  "id:'900019', \
  phase:1, \
  t:none, \
  capture, \
  setvar:tx.real_ip=%{tx.1}, \
  nolog, \
  pass"


SecRule &TX:REAL_IP "!@eq 0" \
  "id:'900020', \
  phase:1, \
  t:none, \
  initcol:global=global, \
  initcol:ip=%{tx.real_ip}_%{tx.ua_hash}, \
  nolog, \
  pass"


SecRule &TX:REAL_IP "@eq 0" \
  "id:'900021', \
```

```
  phase:1, \
  t:none, \
  initcol:global=global, \
  initcol:ip=%{remote_addr}_%{tx.ua_hash}, \
  nolog, \
  pass"
```

Les règles activées sont contenues dans le répertoire **/etc/httpd/modsecurity.d/activated_rules/**. On constate que les fichiers ici ne sont que des liens symboliques vers des fichiers se trouvant dans le répertoire **/usr/lib/modsecurity.d/base_rules** :

```
[root@centos6 ~]# ls -l /etc/httpd/modsecurity.d/activated_rules/
total 88
lrwxrwxrwx. 1 root root 64  9 sept. 12:06 modsecurity_35_bad_robots.data ->
/usr/lib/modsecurity.d/base_rules/modsecurity_35_bad_robots.data
lrwxrwxrwx. 1 root root 62  9 sept. 12:06 modsecurity_35_scanners.data ->
/usr/lib/modsecurity.d/base_rules/modsecurity_35_scanners.data
lrwxrwxrwx. 1 root root 69  9 sept. 12:06 modsecurity_40_generic_attacks.data ->
/usr/lib/modsecurity.d/base_rules/modsecurity_40_generic_attacks.data
lrwxrwxrwx. 1 root root 75  9 sept. 12:06 modsecurity_41_sql_injection_attacks.data ->
/usr/lib/modsecurity.d/base_rules/modsecurity_41_sql_injection_attacks.data
lrwxrwxrwx. 1 root root 62  9 sept. 12:06 modsecurity_50_outbound.data ->
/usr/lib/modsecurity.d/base_rules/modsecurity_50_outbound.data
lrwxrwxrwx. 1 root root 70  9 sept. 12:06 modsecurity_50_outbound_malware.data ->
/usr/lib/modsecurity.d/base_rules/modsecurity_50_outbound_malware.data
lrwxrwxrwx. 1 root root 77  9 sept. 12:06 modsecurity_crs_20_protocol_violations.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_20_protocol_violations.conf
lrwxrwxrwx. 1 root root 76  9 sept. 12:06 modsecurity_crs_21_protocol_anomalies.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_21_protocol_anomalies.conf
lrwxrwxrwx. 1 root root 72  9 sept. 12:06 modsecurity_crs_23_request_limits.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_23_request_limits.conf
lrwxrwxrwx. 1 root root 69  9 sept. 12:06 modsecurity_crs_30_http_policy.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_30_http_policy.conf
lrwxrwxrwx. 1 root root 68  9 sept. 12:06 modsecurity_crs_35_bad_robots.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_35_bad_robots.conf
```

```
lrwxrwxrwx. 1 root root 73  9 sept. 12:06 modsecurity_crs_40_generic_attacks.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_40_generic_attacks.conf
lrwxrwxrwx. 1 root root 79  9 sept. 12:06 modsecurity_crs_41_sql_injection_attacks.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_41_sql_injection_attacks.conf
lrwxrwxrwx. 1 root root 69  9 sept. 12:06 modsecurity_crs_41_xss_attacks.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_41_xss_attacks.conf
lrwxrwxrwx. 1 root root 72  9 sept. 12:06 modsecurity_crs_42_tight_security.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_42_tight_security.conf
lrwxrwxrwx. 1 root root 65  9 sept. 12:06 modsecurity_crs_45_trojans.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_45_trojans.conf
lrwxrwxrwx. 1 root root 75  9 sept. 12:06 modsecurity_crs_47_common_exceptions.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_47_common_exceptions.conf
lrwxrwxrwx. 1 root root 82  9 sept. 12:06 modsecurity_crs_48_local_exceptions.conf.example ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_48_local_exceptions.conf.example
lrwxrwxrwx. 1 root root 74  9 sept. 12:06 modsecurity_crs_49_inbound_blocking.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_49_inbound_blocking.conf
lrwxrwxrwx. 1 root root 66  9 sept. 12:06 modsecurity_crs_50_outbound.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_50_outbound.conf
lrwxrwxrwx. 1 root root 75  9 sept. 12:06 modsecurity_crs_59_outbound_blocking.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_59_outbound_blocking.conf
lrwxrwxrwx. 1 root root 69  9 sept. 12:06 modsecurity_crs_60_correlation.conf ->
/usr/lib/modsecurity.d/base_rules/modsecurity_crs_60_correlation.conf
```

```
[root@centos6 ~]# ls -l /usr/lib/modsecurity.d/base_rules
total 332
-rw-r--r--. 1 root root  1980 15 nov.   2012 modsecurity_35_bad_robots.data
-rw-r--r--. 1 root root   386 15 nov.   2012 modsecurity_35_scanners.data
-rw-r--r--. 1 root root  3928 15 nov.   2012 modsecurity_40_generic_attacks.data
-rw-r--r--. 1 root root  2610 15 nov.   2012 modsecurity_41_sql_injection_attacks.data
-rw-r--r--. 1 root root  2224 15 nov.   2012 modsecurity_50_outbound.data
-rw-r--r--. 1 root root 56714 15 nov.   2012 modsecurity_50_outbound_malware.data
-rw-r--r--. 1 root root 22861 15 nov.   2012 modsecurity_crs_20_protocol_violations.conf
-rw-r--r--. 1 root root  6915 15 nov.   2012 modsecurity_crs_21_protocol_anomalies.conf
-rw-r--r--. 1 root root  3792 15 nov.   2012 modsecurity_crs_23_request_limits.conf
```

```
-rw-r--r--. 1 root root  6933 15 nov.   2012 modsecurity_crs_30_http_policy.conf
-rw-r--r--. 1 root root  5394 15 nov.   2012 modsecurity_crs_35_bad_robots.conf
-rw-r--r--. 1 root root 19157 15 nov.   2012 modsecurity_crs_40_generic_attacks.conf
-rw-r--r--. 1 root root 43961 15 nov.   2012 modsecurity_crs_41_sql_injection_attacks.conf
-rw-r--r--. 1 root root 87470 15 nov.   2012 modsecurity_crs_41_xss_attacks.conf
-rw-r--r--. 1 root root  1795 15 nov.   2012 modsecurity_crs_42_tight_security.conf
-rw-r--r--. 1 root root  3660 15 nov.   2012 modsecurity_crs_45_trojans.conf
-rw-r--r--. 1 root root  2253 15 nov.   2012 modsecurity_crs_47_common_exceptions.conf
-rw-r--r--. 1 root root  2787 15 nov.   2012 modsecurity_crs_48_local_exceptions.conf.example
-rw-r--r--. 1 root root  1835 15 nov.   2012 modsecurity_crs_49_inbound_blocking.conf
-rw-r--r--. 1 root root 22314 15 nov.   2012 modsecurity_crs_50_outbound.conf
-rw-r--r--. 1 root root  1448 15 nov.   2012 modsecurity_crs_59_outbound_blocking.conf
-rw-r--r--. 1 root root  2674 15 nov.   2012 modsecurity_crs_60_correlation.conf
```

Dans le répertoire **/usr/lib/modsecurity.d/base_rules** se trouvent des fichiers ayant une extension **.data**. Un exemple est le fichier **modsecurity_35_bad_robots.data**. Ce fichier contient la liste des noms des robots considérés d'être néfastes :

```
[root@centos6 ~]# cat /usr/lib/modsecurity.d/base_rules/modsecurity_35_bad_robots.data
webmole
wisenutbot
prowebwalker
hanzoweb
email
toata dragostea mea pentru diavola
gameBoy, powered by nintendo
missigua
poe-component-client
emailsiphon
adsarobot
under the rainbow 2.
nessus
floodgate
email extractor
webaltbot
```

```
contactbot/
butch__2.1.1
pe 1.4
indy library
autoemailspider
mozilla/3.mozilla/2.01
fantombrowser
digout4uagent
panscient.com
telesoft
; widows
converacrawler
www.weblogs.com
murzillo compatible
isc systems irc search 2.1
emailmagnet
microsoft url control
datacha0s
emailwolf
production bot
sitesnagger
webbandit
web by mail
faxobot
grub crawler
jakarta
eirgrabber
webemailextrac
extractorpro
attache
educate search vxb
8484 boston project
franklin locator
nokia-waptoolkit
```

```
mailto:craftbot@yahoo.com
full web bot
pcbrowser
psurf
user-Agent
pleasecrawl/1.
kenjin spider
gecko/25
no browser
webster pro
wep Search 00
grub-client
fastlwspider
this is an exploit
contentsmartz
teleport pro
dts agent
nikto
morzilla
via
atomic_email_hunter
program shareware 1.0.
ecollector
emailcollect
china local browse 2.
backdoor
stress test
foobar/
emailreaper
xmlrpc exploit
compatible ; msie
s.t.a.l.k.e.r.
compatible-
webvulnscan
```

```
nameofagent
copyrightcheck
advanced email extractor
surveybot
compatible ;.
searchbot admin@google
wordpress/4.01
webemailextract
larbin@unspecified
turing machine
zeus
windows-update-agent
morfeus fucking scanner
user-agent:
voideye
mosiac 1
chinaclaw
newt activeX; win32
web downloader
safexplorer tl
agdm79@mail.ru
cheesebot
hhjhj@yahoo
fiddler
psycheclone
microsoft internet explorer/5.0
core-project/1
atspider
copyguard
neuralbot/0.2
wordpress hash grabber
amiga-aweb/3.4
packrat
rsync
```

```
crescent internet toolpak
security scan
vadixbot
concealed defense
a href=
bwh3_user_agent
internet ninja
microsoft url
emailharvest
shai
wisebot
internet exploiter sux
wells search ii
webroot
digimarc webreader
botversion
black hole
windows xp 5
w3mir
pmafind
athens
hl_ftien_spider
 injection
takeout
eo browse
cherrypicker
internet-exprorer
```

Le même répertoire contient aussi des fichiers ayant une extention **.conf**, tel **modsecurity_crs_35_bad_robots.conf**. Ce fichier détecte les mauvais robots :

```
[root@centos6 ~]# cat /usr/lib/modsecurity.d/base_rules/modsecurity_crs_35_bad_robots.conf
# ------------------------------------------------------------
# Core ModSecurity Rule Set ver.2.2.6
```

```
# Copyright (C) 2006-2012 Trustwave All rights reserved.
#
# The OWASP ModSecurity Core Rule Set is distributed under
# Apache Software License (ASL) version 2
# Please see the enclosed LICENCE file for full details.
# ------------------------------------------------------------



#
# NOTE Bad robots detection is based on checking elements easily
#      controlled by the client. As such a determined attacked can bypass
#      those checks. Therefore bad robots detection should not be viewed as
#      a security mechanism against targeted attacks but rather as a nuisance
#      reduction, eliminating most of the random attacks against your web
#      site.

SecRule REQUEST_HEADERS:User-Agent "@pmFromFile modsecurity_35_scanners.data" \
        "phase:2,rev:'2',ver:'OWASP_CRS/2.2.6',maturity:'9',accuracy:'9',t:none,t:lowercase,block,msg:'Request
Indicates a Security Scanner Scanned the
Site',logdata:'%{matched_var}',id:'990002',tag:'OWASP_CRS/AUTOMATION/SECURITY_SCANNER',tag:'WASCTC/WASC-21',tag:'
OWASP_TOP_10/A7',tag:'PCI/6.5.10',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.critical
_anomaly_score},setvar:tx.%{rule.id}-OWASP_CRS/AUTOMATION/SECURITY_SCANNER-%{matched_var_name}=%{matched_var}"
SecRule REQUEST_HEADERS_NAMES "\bacunetix-product\b" \
        "phase:2,rev:'2',ver:'OWASP_CRS/2.2.6',maturity:'9',accuracy:'9',t:none,t:lowercase,block,msg:'Request
Indicates a Security Scanner Scanned the
Site',logdata:'%{matched_var}',id:'990901',tag:'OWASP_CRS/AUTOMATION/SECURITY_SCANNER',tag:'WASCTC/WASC-21',tag:'
OWASP_TOP_10/A7',tag:'PCI/6.5.10',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.critical
_anomaly_score},setvar:tx.%{rule.id}-OWASP_CRS/AUTOMATION/SECURITY_SCANNER-%{matched_var_name}=%{matched_var}"
SecRule REQUEST_FILENAME "^/nessustest" \
        "phase:2,rev:'2',ver:'OWASP_CRS/2.2.6',maturity:'9',accuracy:'9',t:none,t:lowercase,block,msg:'Request
Indicates a Security Scanner Scanned the
Site',logdata:'%{matched_var}',id:'990902',tag:'OWASP_CRS/AUTOMATION/SECURITY_SCANNER',tag:'WASCTC/WASC-21',tag:'
OWASP_TOP_10/A7',tag:'PCI/6.5.10',severity:'2',setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.critical
_anomaly_score},setvar:tx.%{rule.id}-OWASP_CRS/AUTOMATION/SECURITY_SCANNER-%{matched_var_name}=%{matched_var}"
```

```
SecRule REQUEST_HEADERS:User-Agent "@pmFromFile modsecurity_35_bad_robots.data" \
        "chain,phase:2,rev:'2',ver:'OWASP_CRS/2.2.6',maturity:'9',accuracy:'9',t:none,block,msg:'Rogue web site
crawler',id:'990012',tag:'OWASP_CRS/AUTOMATION/MALICIOUS',tag:'WASCTC/WASC-21',tag:'OWASP_TOP_10/A7',tag:'PCI/6.5
.10',severity:'4',capture,logdata:'%{TX.0}'"
    SecRule REQUEST_HEADERS:User-Agent "(?i:(?:c(?:o(?:n(?:t(?:entsmartz|actbot/)|cealed
defense|veracrawler)|mpatible(?: ;(?: msie|\.)|-)|py(?:rightcheck|guard)|re-project/1.0)|h(?:ina(?: local browse
2\.|claw)|e(?:rrypicker|esebot))|rescent internet toolpak)|w(?:e(?:b(?: (?:downloader|by
mail)|(?:(?:altb|ro)o|bandi)t|emailextract?|vulnscan|mole)|lls search ii|p Search 00)|i(?:ndows(?:-update-agent|
xp 5)|se(?:nut)?bot)|ordpress(?: hash grabber|\/4\.01)|3mir)|m(?:o(?:r(?:feus fucking
scanner|zilla)|zilla\/3\.mozilla\/2\.01$|siac 1.)|i(?:crosoft (?:internet explorer\/5\.0$|url
control)|ssigua)|ailto:craftbot\@yahoo\.com|urzillo compatible)|p(?:ro(?:gram shareware 1\.0\.|duction
bot|webwalker)|a(?:nscient\.com|ckrat)|oe-component-client|s(?:ycheclone|urf)|leasecrawl\/1\.|cbrowser|e
1\.4|mafind)|e(?:mail(?:(?:collec|harves|magne)t|(?:
extracto|reape)r|(siphon|spider)|siphon|wolf)|(?:collecto|irgrabbe)r|ducate search vxb|xtractorpro|o
browse)|t(?:(?: ?h ?a ?t ?' ?s g ?o ?t ?t ?a ? h ?u ?r ?|his is an exploi|akeou)t|oata dragostea mea pentru
diavola|ele(?:port pro|soft)|uring machine)|a(?:t(?:(?:omic_email_hunt|spid)er|tache|hens)|d(?:vanced email
extractor|sarobot)|gdm79\@mail\.ru|miga-aweb\/3\.4|utoemailspider| href=)|^(?:(google|i?explorer?\.exe|(ms)?ie(
[0-9.]+)?\ ?(compatible( browser)?)?)$|www\.weblogs\.com|(?:jakart|vi)a|microsoft url|user-Agent)|s(?:e(?:archbot
admin@google.com|curity scan)|(?:tress tes|urveybo)t|\.t\.a\.l\.k\.e\.r\.|afexplorer
tl|itesnagger|hai)|n(?:o(?:kia-waptoolkit.* googlebot.*googlebot| browser)|e(?:(?:wt activeX;
win3|uralbot\/0\.)2|ssus)|ameofagent|ikto)|f(?:a(?:(?:ntombrows|stlwspid)er|xobot)|(?:ranklin locato|iddle)r|ull
web bot|loodgate|oobar/)|i(?:n(?:ternet(?: (?:exploiter sux|ninja)|-exprorer)|dy library)|sc systems irc search
2\.1)|g(?:ameBoy, powered by nintendo|rub(?: crawler|-client)|ecko\/25)|(myie2|libwen-us|murzillo
compatible|webaltbot|wisenutbot)|b(?:wh3_user_agent|utch__2\.1\.1|lack hole|ackdoor)|d(?:ig(?:imarc
webreader|out4uagent)|ts agent)|(?:(script|sql) inject|$botname/$botvers)ion|(msie .+; .*windows xp|compatible \;
msie)|h(?:l_ftien_spider|hjhj@yahoo|anzoweb)|(?:8484 boston projec|xmlrpc exploi)t|u(?:nder the rainbow 2\.|ser-
agent:)|(sogou develop spider|sohu agent)|(?:(?:d|e)browse|demo bot)|zeus(?: .*webster pro)?|[a-
z]surf[0-9][0-9]|v(?:adixbot|oideye)|larbin@unspecified|\bdatacha0s\b|kenjin spider|; widows|rsync|\\\r))"
"capture,setvar:'tx.msg=%{rule.msg}',setvar:tx.anomaly_score=+%{tx.warning_anomaly_score},setvar:tx.%{rule.id}-
OWASP_CRS/AUTOMATION/MALICIOUS-%{matched_var_name}=%{matched_var}"
SecMarker END_ROBOT_CHECK
```

Le fichier principal de configuration de mod_security est :

```
[root@centos6 ~]# cat /etc/httpd/conf.d/00_mod_security.conf
#
# ASL Free trial ruleset is available at: https://atomicorp.com/amember/signup/cart/
#
#
LoadModule security2_module modules/mod_security2.so
LoadModule unique_id_module modules/mod_unique_id.so
#
<IfModule mod_security2.c>
    # Basic configuration goes in here
    Include modsecurity.d/tortix_waf.conf
    # Rule management is handled by ASL
    Include modsecurity.d/00*exclude.conf
    Include modsecurity.d/*asl*.conf
    Include modsecurity.d/99*exclude.conf

</IfModule>
```

Pour activer mod_security, ajoutez la directive **SecRuleEngine On** :

```
[root@centos6 ~]# cat /etc/httpd/conf.d/00_mod_security.conf
#
# ASL Free trial ruleset is available at: https://atomicorp.com/amember/signup/cart/
#
#
LoadModule security2_module modules/mod_security2.so
LoadModule unique_id_module modules/mod_unique_id.so
#
<IfModule mod_security2.c>
        SecRuleEngine On
    # Basic configuration goes in here
    Include modsecurity.d/tortix_waf.conf
    # Rule management is handled by ASL
    Include modsecurity.d/00*exclude.conf
```

```
    Include modsecurity.d/*asl*.conf
    Include modsecurity.d/99*exclude.conf

</IfModule>
```

Redémarrez le serveur Apache :

```
[root@centos6 ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Consultez la fin du fichier **/var/log/httpd/error_log** :

```
[root@centos6 ~]# tail /var/log/httpd/error_log
[Tue Sep 09 14:19:36 2014] [notice] SELinux policy enabled; httpd running as context
unconfined_u:system_r:httpd_t:s0
[Tue Sep 09 14:19:36 2014] [notice] suEXEC mechanism enabled (wrapper: /usr/sbin/suexec)
[Tue Sep 09 14:19:37 2014] [notice] ModSecurity for Apache/2.7.7 (http://www.modsecurity.org/) configured.
[Tue Sep 09 14:19:37 2014] [notice] ModSecurity: APR compiled version="1.3.9"; loaded version="1.3.9"
[Tue Sep 09 14:19:37 2014] [notice] ModSecurity: PCRE compiled version="7.8 "; loaded version="7.8 2008-09-05"
[Tue Sep 09 14:19:37 2014] [notice] ModSecurity: LUA compiled version="Lua 5.1"
[Tue Sep 09 14:19:37 2014] [notice] ModSecurity: LIBXML compiled version="2.7.6"
[Tue Sep 09 14:19:37 2014] [notice] Digest: generating secret for digest authentication ...
[Tue Sep 09 14:19:37 2014] [notice] Digest: done
[Tue Sep 09 14:19:38 2014] [notice] Apache/2.2.15 (Unix) DAV/2 configured -- resuming normal operations
```

Vous consterez que ModSecurity fonctionne.

mod_suexec

Le mod_suexec introduit un contrôle plus sévère en ce qui concerne quels comptes peuvent exécuter de CGI.

Naviguez au répertoire **/var/www/cgi-bin/** :

```
[root@centos6 ~]# cd /var/www/cgi-bin/
```

Créez un script bash appelé **whoami.cgi** :

/var/www/cgi-bin/whoami.cgi

```
#!/bin/bash
echo "Content-type: text/plain"
echo ""
echo "Nom de connexion :" `whoami`
```

Le but de ce script est de montrer qui exécute le CGI en question.

Rendez le script exécutable :

```
[root@centos6 cgi-bin]# chmod u+x whoami.cgi
```

Appelez le script CGI :

```
[root@centos6 cgi-bin]# lynx --dump http://localhost/cgi-bin/whoami.cgi
                            Internal Server Error

   The server encountered an internal error or misconfiguration and was
   unable to complete your request.

   Please contact the server administrator, root@localhost and inform them
   of the time the error occurred, and anything you might have done that
   may have caused the error.

   More information about this error may be available in the server error
   log.
     ____________________________________________________________________
```

```
    Apache/2.2.15 (CentOS) Server at localhost Port 80
```

Notez que l'appel génère une erreur “Internal Server Error”.

Avant de continuer, expliquez pourquoi l'erreur s'est produite.

Regardez dans le fichier de journalisation **/var/log/httpd/error_log**. Vous verrez deux lignes similaires à celles-ci :

```
...
[Wed Sep 10 10:53:37 2014] [error] [client ::1] (13)Permission denied: exec of '/var/www/cgi-bin/whoami.cgi'
failed
[Wed Sep 10 10:53:37 2014] [error] [client ::1] Premature end of script headers: whoami.cgi
...
```

En effet, le fichier whoami.cgi apprtient à root :

```
[root@centos6 cgi-bin]# ls -l
total 4
-rwxr--r--. 1 root root 87 10 sept. 10:46 whoami.cgi
```

Modifiez donc le propriétaire et le groupe à **apache** :

```
[root@centos6 cgi-bin]# chown apache:apache whoami.cgi
```

Appelez le script CGI :

```
[root@centos6 cgi-bin]# lynx --dump http://localhost/cgi-bin/whoami.cgi
```

```
Nom de connexion : apache
```

Vous allez maintenant créer un utilisateur spécifique pour l'exécution des scripts :

```
[root@centos6 cgi-bin]# useradd scripts
```

Créez le répertoire **/var/www/scripts** :

```
[root@centos6 cgi-bin]# mkdir /var/www/scripts
```

Modifiez le propriétaire, le groupe et les permissions du répertoire nouvellement créé :

```
[root@centos6 cgi-bin]# chown scripts:scripts /var/www/scripts/
[root@centos6 cgi-bin]# chmod 2755 /var/www/scripts/
```

Déplacez le script vers **/var/www/scripts** :

```
[root@centos6 cgi-bin]# mv whoami.cgi /var/www/scripts
[root@centos6 cgi-bin]# cd !$
cd /var/www/scripts
[root@centos6 scripts]# ls -l
total 4
-rwxr--r--. 1 apache apache 87 10 sept. 10:46 whoami.cgi
```

Editez le fichier **/etc/httpd/conf/httpd.conf** en ajoutant la directive **SuexecUserGroup** :

```
...
ServerRoot "/etc/httpd"
SuexecUserGroup scripts scripts
...
```

Vérifiez que la ligne suivante existe dans la section des modules :

```
...
LoadModule suexec_module modules/mod_suexec.so
...
```

Ajoutez l'alias **scripts** et définissez les options pour le répertoire /var/www/scripts :

```
...
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    Allow from all
</Directory>
Alias /scripts/ "/var/www/scripts/"
<Directory "/var/www/scripts/">
        Options +ExecCGI
        SetHandler cgi-script
</Directory>
...
```

Sauvegardez et vérifiez votre fichier de configuration :

```
[root@centos6 scripts]# httpd -t
Syntax OK
```

Appelez le script dans le répertoire **scripts** :

```
[root@centos6 scripts]# lynx --dump http://localhost/scripts/whoami.cgi
                            Internal Server Error

   The server encountered an internal error or misconfiguration and was
   unable to complete your request.
```

```
   Please contact the server administrator, root@localhost and inform them
   of the time the error occurred, and anything you might have done that
   may have caused the error.

   More information about this error may be available in the server error
   log.
     ---------------------------------------------------------------------------


    Apache/2.2.15 (CentOS) Server at localhost Port 80
```

Notez la présence de l'erreur. Ouvrez le fichier **/var/log/httpd/error_log** :

```
[root@centos6 scripts]# tail /var/log/httpd/error_log
[Wed Sep 10 10:56:38 2014] [notice] ModSecurity: PCRE compiled version="7.8 "; loaded version="7.8 2008-09-05"
[Wed Sep 10 10:56:38 2014] [notice] ModSecurity: LUA compiled version="Lua 5.1"
[Wed Sep 10 10:56:38 2014] [notice] ModSecurity: LIBXML compiled version="2.7.6"
[Wed Sep 10 10:56:38 2014] [notice] Digest: generating secret for digest authentication ...
[Wed Sep 10 10:56:38 2014] [notice] Digest: done
[Wed Sep 10 10:56:39 2014] [notice] Apache/2.2.15 (Unix) DAV/2 configured -- resuming normal operations
[Wed Sep 10 11:02:15 2014] [error] [client ::1] suexec policy violation: see suexec log for more details
[Wed Sep 10 11:02:15 2014] [error] [client ::1] Premature end of script headers: whoami.cgi
[Wed Sep 10 11:06:42 2014] [error] [client ::1] suexec policy violation: see suexec log for more details
[Wed Sep 10 11:06:42 2014] [error] [client ::1] Premature end of script headers: whoami.cgi
```

Notez cette-fois ci la présence d'une **suexec policy violation**.

Consultez donc le fichier **/var/log/httpd/suexec.log** :

```
[root@centos6 scripts]# cat /var/log/httpd/suexec.log
[2014-09-10 08:05:09]: uid: (501/scripts) gid: (502/scripts) cmd: whoami.cgi
```

```
[2014-09-10 08:05:09]: target uid/gid (501/502) mismatch with directory (501/502) or program (48/48)
[2014-09-10 11:02:15]: uid: (501/scripts) gid: (502/scripts) cmd: whoami.cgi
[2014-09-10 11:02:15]: target uid/gid (501/502) mismatch with directory (0/0) or program (48/48)
[2014-09-10 11:06:42]: uid: (501/scripts) gid: (502/scripts) cmd: whoami.cgi
[2014-09-10 11:06:42]: target uid/gid (501/502) mismatch with directory (501/502) or program (48/48)
```

Modifiez donc le propriétaire et groupe du script :

```
[root@centos6 scripts]# chown scripts:scripts whoami.cgi
```

Appelez le script dans le répertoire **scripts** :

```
[root@centos6 scripts]# lynx --dump http://localhost/scripts/whoami.cgi
Nom de connexion : scripts
```

> Non seulement suexec apporte une clarté au niveau de la raison des erreurs éventuelles mais le module permet de faire exécuter des CGI par un autre utilisateur qu'apache.
