SER201 - Gestion de Base du Serveur Web Apache 2.4

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,

- **mpm_netware** - un serveur web basé exclusivement sur les threads et optimisé pour Novell NetWare™,
- **mpmt_os2** - un serveur hybride multi-processus, multi-thread pour OS/2,
- **prefork** - module propre à Unix et Linux qui implémente un serveur mono-tâche à duplication,
- **worker** - module propre à Unix et Linux qui implémente un serveur hybride multi-tâche et multitraitement,
- **event** - module propre à Unix et Linux conçu pour permettre le traitement d'un nombre accru de requêtes simultanées en déléguant certaines tâches aux threads d'écoute, libérant par là-même les threads de travail et leur permettant de traiter les nouvelles requêtes.

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
    Require ip 127.0.0.1
</Location>
<Location /server-info>
    SetHandler server-info
    Require ip 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, ajoutez les lignes suivantes :

```
ExtendedStatus On

<Location /server-status>
    SetHandler server-status
    Require ip 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 ajoutez les lignes suivantes :

```
<Location /server-info>
    SetHandler server-info
    Require ip 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@centos7 ~]# 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 **/etc/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 enp0s3. 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.modules.d/00-base.conf** :

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

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

```
[root@centos7 ~]# groupadd homepage && useradd homepage -c homepage -g homepage -d /home/homepage -s /bin/bash
```

Créez le répertoire /home/homepage/public_html :

```
[root@centos7 ~]# mkdir /home/homepage/public_html
```

Modifiez l'appartenance du répertoire /home/homepage :

```
[root@centos7 ~]# chown -R homepage:homepage /home/homepage
```

Ouvrez le fichier **/etc/httpd/conf.d/userdir.conf**. Le but de de fichier est de configurer le support des répertoires des utilisateurs dans le cas où le module **mod_userdir.c** est chargé :

```
[root@centos7 ~]# cat /etc/httpd/conf.d/userdir.conf
#
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
<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 disabled

    #
    # To enable requests to /~user/ to serve the user's public_html
    # directory, remove the "UserDir disabled" 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 Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

Modifiez ce fichier ainsi :

```
[root@centos7 ~]# vi /etc/httpd/conf.d/userdir.conf
[root@centos7 ~]# cat /etc/httpd/conf.d/userdir.conf
#
# UserDir: The name of the directory that is appended onto a user's home
# directory if a ~user request is received.
#
# The path to the end user account 'public_html' directory must be
# accessible to the webserver userid.  This usually means that ~userid
# must have permissions of 711, ~userid/public_html must have permissions
# of 755, and documents contained therein must be world-readable.
# Otherwise, the client will only receive a "403 Forbidden" message.
#
<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 Indexes
    Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
    Require method GET POST OPTIONS
</Directory>
```

Redémarrez le service apache :

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

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

```
[root@centos7 ~]# vi /home/homepage/public_html/index.html
[root@centos7 ~]# cat /home/homepage/public_html/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@centos7 ~]# chmod 711 /home/homepage
[root@centos7 ~]# chmod 755 /home/homepage/public_html/
[root@centos7 ~]# chmod 666 /home/homepage/public_html/index.html
```

Le site personnel de l'utilisateur est maintenant en ligne. Pour le tester utilisez **lynx** :

```
[root@centos7 ~]# lynx --dump http://localhost/~homepage/
                      La Page de l'utilisateur Homepage
```

```
[root@centos7 ~]#
```

mod_php

Introduction

PHP existe en plusieurs versions :

- La version 5
- La version 7

Installation

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

```
[root@centos7 ~]# yum install php php-mysql
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.crazyfrogs.org
 * extras: centos.crazyfrogs.org
 * updates: centos.crazyfrogs.org
Resolving Dependencies
--> Running transaction check
---> Package php.x86_64 0:5.4.16-42.el7 will be installed
--> Processing Dependency: php-common(x86-64) = 5.4.16-42.el7 for package: php-5.4.16-42.el7.x86_64
--> Processing Dependency: php-cli(x86-64) = 5.4.16-42.el7 for package: php-5.4.16-42.el7.x86_64
---> Package php-mysql.x86_64 0:5.4.16-42.el7 will be installed
--> Processing Dependency: php-pdo(x86-64) = 5.4.16-42.el7 for package: php-mysql-5.4.16-42.el7.x86_64
--> Running transaction check
---> Package php-cli.x86_64 0:5.4.16-42.el7 will be installed
```

```
---> Package php-common.x86_64 0:5.4.16-42.el7 will be installed
--> Processing Dependency: libzip.so.2()(64bit) for package: php-common-5.4.16-42.el7.x86_64
---> Package php-pdo.x86_64 0:5.4.16-42.el7 will be installed
--> Running transaction check
---> Package libzip.x86_64 0:0.10.1-8.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================
 Package                          Arch                          Version                                Repository
Size
================================================================================================================
=====================
Installing:
 php                              x86_64                        5.4.16-42.el7                          base
1.4 M
 php-mysql                        x86_64                        5.4.16-42.el7                          base
101 k
Installing for dependencies:
 libzip                           x86_64                        0.10.1-8.el7                           base
48 k
 php-cli                          x86_64                        5.4.16-42.el7                          base
2.7 M
 php-common                       x86_64                        5.4.16-42.el7                          base
564 k
 php-pdo                          x86_64                        5.4.16-42.el7                          base
98 k

Transaction Summary
================================================================================================================
=====================
Install  2 Packages (+4 Dependent packages)
```

```
Total download size: 4.9 M
Installed size: 18 M
Is this ok [y/d/N]: y
```

Tester PHP

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

```
[root@centos7 ~]# vi /var/www/html/php.php
[root@centos7 ~]# cat /var/www/html/php.php
<html>
<head>
<title>Ma page de test en PHP</title>
</head>
<body>
<?PHP
phpinfo();
?>
</body>
</html>
```

Redémarrez Apache :

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

Si vous vous êtes connecté à votre machine virtuelle via ssh, passez la VM CentOS 7 en démarrage en mode graphique :

```
[root@centos7 ~]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx. 1 root root 41 May  9 15:18 /etc/systemd/system/default.target -> /usr/lib/systemd/system/multi-
user.target
[root@centos7 ~]# rm -rf /etc/systemd/system/default.target
[root@centos7 ~]# ln -s /lib/systemd/system/graphical.target /etc/systemd/system/default.target
```

```
[root@centos7 ~]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx 1 root root 36 Nov  5 08:02 /etc/systemd/system/default.target -> /lib/systemd/system/graphical.target
[root@centos7 ~]# shutdown -r now
```

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_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 2.4, 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@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep auth_basic
LoadModule auth_basic_module modules/mod_auth_basic.so
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep authn_file
LoadModule authn_file_module modules/mod_authn_file.so
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.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@centos7 ~]# 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@centos7 ~]# mkdir -p /www/passwords/site1
```

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

```
[root@centos7 ~]# 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@centos7 ~]# cat /www/passwords/site1/.htpasswd
webmaster:$apr1$jnlskgOH$a/SaUQCeDHobz.PM2pDun.
```

Créez maintenant une page html dans le répertoire secret :

```
[root@centos7 ~]# 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>
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>
<Directory /www/site1/secret>
AllowOverride AuthConfig
</Directory>
</VirtualHost>
```

Sauvegardez votre fichier et puis redémarrez votre serveur Apache :

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

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 serveur MariaDB ainsi que **apr-util-mysql** :

```
[root@centos7 ~]# yum install mariadb mariadb-server apr-util-mysql
```

Vérifiez que le module **mod_authn_dbd** est activé :

```
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep authn_dbd
LoadModule authn_dbd_module modules/mod_authn_dbd.so
```

Copiez le module **/usr/lib64/apr-util-1/apr_dbd_mysql.so** dans le répertoire **/usr/lib64/httpd/modules/** :

```
[root@centos7 ~]# updatedb
[root@centos7 ~]# locate apr_dbd_mysql.so
/usr/lib64/apr-util-1/apr_dbd_mysql.so
[root@centos7 ~]# cp /usr/lib64/apr-util-1/apr_dbd_mysql.so /usr/lib64/httpd/modules/
```

Configuration de MariaDB

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

```
[root@centos7 ~]# systemctl enable mariadb
[root@centos7 ~]# systemctl start mariadb
[root@centos7 ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2017-11-05 08:04:45 CET; 1h 41min ago
 Main PID: 1293 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─1293 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─1964 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-
dir=/usr/lib64/mysql/plugin --log-error=/var...

Nov 05 08:04:24 centos7.fenestros.loc systemd[1]: Starting MariaDB database server...
Nov 05 08:04:31 centos7.fenestros.loc mariadb-prepare-db-dir[687]: Database MariaDB is probably initialized in
/var/lib/mysql a...one.
Nov 05 08:04:36 centos7.fenestros.loc mysqld_safe[1293]: 171105 08:04:36 mysqld_safe Logging to
'/var/log/mariadb/mariadb.log'.
Nov 05 08:04:37 centos7.fenestros.loc mysqld_safe[1293]: 171105 08:04:37 mysqld_safe Starting mysqld daemon with
databases fro...mysql
Nov 05 08:04:45 centos7.fenestros.loc systemd[1]: Started MariaDB database server.
Hint: Some lines were ellipsized, use -l to show in full.
```

Définissez le mot de passe fenestros pour root avec la commande suivante :

```
[root@centos7 ~]# mysqladmin -u root password fenestros
```

Connectez-vous à MariaDB :

```
[root@centos7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 4
Server version: 5.5.56-MariaDB MariaDB Server
```

```
Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

Puis saisissez les requêtes et commandes suivantes :

```
MariaDB [(none)]> CREATE DATABASE auth;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> USE auth;
Database changed
MariaDB [auth]> CREATE TABLE users (
    -> user_name VARCHAR(50) NOT NULL,
    -> user_passwd VARCHAR(50) NOT NULL,
    -> PRIMARY KEY (user_name)
    -> );
Query OK, 0 rows affected (0.42 sec)

MariaDB [auth]> GRANT SELECT
    -> ON auth.users
    -> TO apache@localhost
    -> IDENTIFIED BY 'PaSsW0Rd';
Query OK, 0 rows affected (0.32 sec)

MariaDB [auth]> exit
Bye
[root@centos7 ~]# mysql -u root -p -e "INSERT INTO users (user_name, user_passwd) VALUES (\"apache\",\"$(htpasswd
-nb apache password |cut -d ':' -f 2)\")" auth
Enter password:
[root@centos7 ~]# mysql -u root -p -e "SELECT * FROM auth.users;"
Enter password:
+-----------+-------------------------------------+
```

```
| user_name | user_passwd                                |
+-----------+--------------------------------------------+
| apache    | $apr1$isUDg5bK$8oh0oMFUDfL41h84M9vYu1 |
+-----------+--------------------------------------------+
[root@centos7 ~]#
```

Configuration d'Apache

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

```
[root@centos7 ~]# mkdir /www/site1/secret2
```

Créez maintenant une page **index.html** dans le répertoire **secret2** :

```
[root@centos7 ~]# vi /www/site1/secret2/index.html
[root@centos7 ~]# cat /www/site1/secret2/index.html
<html>
<body>
<center>Si vous voyez ce message, vous connaissez mon secret MariaDB !</center>
</body>
</html>
```

Ouvrez ensuite le fichier de configuration **/etc/httpd/conf/vhosts.d/Vhosts.conf** et modifiez-le ainsi :

```
[root@centos7 vhosts.d]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 vhosts.d]# cat /etc/httpd/conf/vhosts.d/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
DBDriver mysql
DBDParams "dbname=auth user=apache pass=PaSsW0Rd"
DBDMin  4
DBDKeep 8
DBDMax  20
DBDExptime 300
<Directory /www/site1>
Require all granted
</Directory>
<Directory /www/site1/secret>
AllowOverride AuthConfig
</Directory>
<Directory /www/site1/secret2>
 AuthType Basic
 AuthName "MariaDB Secret"
```

```
 AuthBasicProvider dbd
 Require valid-user
 AuthDBDUserPWQuery "SELECT user_passwd FROM users WHERE user_name = %s"
</Directory>
</VirtualHost>
```

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

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

En utilisant le navigateur web graphique de votre VM, ouvrez le site http://www.vhostnom.com/secret2/index.html, renseignez l'utilisateur **apache** et le mot de passe **password** 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 2.4, le module **mod_ldap** doit être installée :

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

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. Commencez par installer OpenLDAP :

```
[root@centos7 ~]# yum install openldap-servers openldap-clients openldap
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.ate.info
 * extras: distrib-coffee.ipsl.jussieu.fr
 * updates: mirror.guru
```

```
Resolving Dependencies
--> Running transaction check
---> Package openldap.x86_64 0:2.4.40-13.el7 will be updated
---> Package openldap.x86_64 0:2.4.44-5.el7 will be an update
---> Package openldap-clients.x86_64 0:2.4.44-5.el7 will be installed
---> Package openldap-servers.x86_64 0:2.4.44-5.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
 Package                                Arch                           Version                              Repository
Size
================================================================================================================
Installing:
 openldap-clients                       x86_64                         2.4.44-5.el7                         base
188 k
 openldap-servers                       x86_64                         2.4.44-5.el7                         base
2.2 M
Updating:
 openldap                               x86_64                         2.4.44-5.el7                         base
354 k

Transaction Summary
================================================================================================================
Install  2 Packages
Upgrade  1 Package

Total download size: 2.7 M
Is this ok [y/d/N]:  y
```

Sous CentOS le service OpenLDAP s'appelle **slapd** :

```
[root@centos7 ~]# systemctl status slapd.service
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
[root@centos7 ~]# systemctl enable slapd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to
/usr/lib/systemd/system/slapd.service.
[root@centos7 ~]# systemctl start slapd.service
[root@centos7 ~]# systemctl status slapd.service
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2017-11-05 12:39:40 CET; 6s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
  Process: 28650 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited,
status=0/SUCCESS)
  Process: 28632 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 28653 (slapd)
   CGroup: /system.slice/slapd.service
           └─28653 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

Nov 05 12:39:39 centos7.fenestros.loc systemd[1]: Starting OpenLDAP Server Daemon...
Nov 05 12:39:39 centos7.fenestros.loc runuser[28637]: pam_unix(runuser:session): session opened for user ldap by
(uid=0)
```

```
Nov 05 12:39:39 centos7.fenestros.loc slapcat[28643]: DIGEST-MD5 common mech free
Nov 05 12:39:40 centos7.fenestros.loc slapd[28650]: @(#) $OpenLDAP: slapd 2.4.44 (Aug  4 2017 14:23:27) $
mockbuild@c1bm.rdu2.centos.org:/builddir/build/BUILD/openldap-2.4.../slapd
Nov 05 12:39:40 centos7.fenestros.loc slapd[28653]: hdb_db_open: warning - no DB_CONFIG file found in directory
/var/lib/ldap: (2).
                                                    Expect poor performance for suffix "dc=my-domain,dc=com".
Nov 05 12:39:40 centos7.fenestros.loc slapd[28653]: slapd starting
Nov 05 12:39:40 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Daemon.
Hint: Some lines were ellipsized, use -l to show in full.
```

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

```
[root@centos7 ~]# mkdir /var/lib/ldap/ittraining
```

Nettoyez les anciens fichiers de configuration et fichiers de données :

```
[root@centos7 ~]# rm -Rf /etc/openldap/slapd.d/*
[root@centos7 ~]# rm -f /var/lib/ldap/alock
[root@centos7 ~]# rm -f /var/lib/ldap/__db.00?
```

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

```
[root@centos7 ~]# vi /etc/openldap/slapd.conf
[root@centos7 ~]# cat /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=ittraining"
checkpoint      1024 15
rootdn      "cn=Admin,o=ittraining"
rootpw
directory   /var/lib/ldap/ittraining
lastmod         on
index           cn,sn,st        eq,pres,sub
```

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

```
[root@centos7 ~]# slappasswd -s fenestros
{SSHA}B4p7daRzJZPbf7AjuuYzohaW9nS7hGXi
```

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

```
...
database        bdb
suffix          "o=ittraining"
checkpoint      1024 15
rootdn          "cn=Admin,o=ittraining"
rootpw          {SSHA}B4p7daRzJZPbf7AjuuYzohaW9nS7hGXi
directory       /var/lib/ldap/ittraining
lastmod         on
index           cn,sn,st                eq,pres,sub
```

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

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

Initialisez la première base de données :

```
[root@centos7 ~]# echo “” | slapadd -f /etc/openldap/slapd.conf
59ff01da The first database does not allow slapadd; using the first available one (2)
59ff01da str2entry: entry -1 has no dn
slapadd: could not parse entry (line=1)
```

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

```
[root@centos7 ~]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
```

Vérifiez que l'arborescence initiale soit créée :

```
[root@centos7 ~]# ls -l /etc/openldap/slapd.d
total 8
drwxr-x--- 3 root root 4096 Nov  5 13:20 cn=config
-rw------- 1 root root 1258 Nov  5 13:20 cn=config.ldif
```

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

```
[root@centos7 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos7 ~]# chmod -R u+rwX /etc/openldap/slapd.d
```

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

```
[root@centos7 ~]# chown -R ldap:ldap /var/lib/ldap/ittraining /etc/openldap/slapd.conf
```

Démarrez ensuite le service slapd :

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

Créez le fichier **ittraining.ldif** :

```
[root@centos7 ~]# vi ittraining.ldif
[root@centos7 ~]# cat ittraining.ldif
dn: o=ittraining
objectClass: top
objectClass: organization
o: ittraining
description: LDAP Authentification

dn: cn=Admin,o=ittraining
objectClass: organizationalRole
cn: Admin
```

```
description: Administrateur LDAP

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

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

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

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

dn: cn=Jean Legrand,ou=GroupA,o=ittraining
ou: GroupA
o: ittraining
cn: Jean Legrand
objectClass: person
objectClass: organizationalPerson
```

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jean.legrand@ittraining.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=ittraining
ou: GroupA
o: ittraining
cn: Jacques Lebeau
objectClass: person
objectClass: organizationalPerson
```

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jacques.lebeau@ittraining.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=ittraining
```

Injectez le fichier ittraining.ldif dans OpenLDAP :

```
[root@centos7 ~]# ldapadd -f ittraining.ldif -xv -D "cn=Admin,o=ittraining" -h 127.0.0.1 -w fenestros
ldap_initialize( ldap://127.0.0.1 )
add objectClass:
    top
    organization
add o:
    ittraining
add description:
    LDAP Authentification
adding new entry "o=ittraining"
modify complete

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

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

add ou:
    GroupB
add objectClass:
```

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

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

add cn:
    users
add objectClass:
    top
    posixGroup
add gidNumber:
    100
add memberUid:
    jean
    jacques
adding new entry "cn=users,ou=group,o=ittraining"
modify complete

add ou:
    GroupA
add o:
    ittraining
```

```
add cn:
    Jean Legrand
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jean.legrand@ittraining.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=ittraining"
modify complete

add ou:
    GroupA
add o:
    ittraining
add cn:
    Jacques Lebeau
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
```

```
    posixAccount
    shadowAccount
    top
add mail:
    jacques.lebeau@ittraining.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=ittraining
adding new entry "cn=Jacques Lebeau,ou=GroupA,o=ittraining"
modify complete
```

Arrêtez le serveur Apache :

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

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

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

```
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    # Options Indexes FollowSymLinks
    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    # AllowOverride None
    #
    # Controls who can get stuff from this server.
    #
    # Require all granted
# </Directory>

<Directory "/var/www/html">
   AuthType Basic
   AuthName "LDAP Authentifaction"
   AuthBasicProvider ldap
   AuthLDAPURL ldap://localhost:389/o=ittraining?uid?sub
   AuthLDAPBindDN "cn=Admin,o=ittraining"
   AuthLDAPBindPassword fenestros
   require ldap-user jean jacques
   AllowOverride None
```

```
   Options Indexes FollowSymLinks
</Directory>
...
```

AuthzLDAPAuthoritative

Re-démarrez le serveur apache :

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

Connectez-vous à http://localhost en utilisant le compte de jean et le mot de passe secret1.

Editez de nouveau le fichier **/etc/httpd/conf/httpd.conf** en supprimant la section <Directory> de la configuration LDAP :

```
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks
    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None
```

```
    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
...
```

Re-démarrez le serveur apache :

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

mod_ssl

Présentation de SSL

SSL (*Secure Sockets Layers*) est utilisé pour sécuriser des transactions effectuées sur le Web et a été mis au point par :

- Netscape
- MasterCard
- Bank of America
- MCI
- Silicon Graphics

SSL est indépendant du protocole utilisé et agit en tant que couche supplémentaire entre la couche Application et la couche Transport. Il peut être utilisé avec :

- HTTP

- FTP
- POP
- IMAP

Fonctionnement de SSL

Le fonctionnement de SSL suit la procédure suivante :

- Le navigateur demande une page web sécurisée en https,
- Le serveur web émet sa clé publique et son certificat,
- Le navigateur vérifie que le certificat a été émis par une autorité fiable, qu'il est valide et qu'il fait référence au site consulté,
- Le navigateur utilise la clé publique du serveur pour chiffrer une clé symétrique aléatoire, une clé de session, et l'envoie au serveur avec l'URL demandé ainsi que des données HTTP chiffrées,
- Le serveur déchiffre la clé symétrique avec sa clé privée et l'utilise pour récupérer l'URL demandé et les données HTTP,
- Le serveur renvoie le document référencé par l'URL ainsi que les données HTTP chiffrées avec la clé symétrique,
- Le navigateur déchiffre le tout avec la clé symétrique et affiche les informations.

Quand on parle de **SSL**, on parle de **cryptologie**.

PKI

On appelle **PKI** (Public Key Infrastucture, ou en français **infrastructure à clé publique (ICP)**, parfois **infrastructure de gestion de clés (IGC)**) l'ensemble des solutions techniques basées sur la cryptographie à clé publique.

Les cryptosystèmes à clés publiques permettent de s'affranchir de la nécessité d'avoir recours systématiquement à un canal sécurisé pour s'échanger les clés. En revanche, la publication de la clé publique à grande échelle doit se faire en toute confiance pour assurer que :

- La clé publique est bien celle de son propriétaire ;
- Le propriétaire de la clé est digne de confiance ;
- La clé est toujours valide.

Ainsi, il est nécessaire d'associer au bi-clé (ensemble clé publique / clé privée) un certificat délivré par un **tiers de confiance** : l'infrastructure de

gestion de clés.

Le tiers de confiance est une entité appelée communément autorité de certification (ou en anglais Certification authority, abrégé CA) chargée d'assurer la véracité des informations contenues dans le certificat de clé publique et de sa validité.

Pour ce faire, l'autorité signe le certificat de clé publique à l'aide de sa propre clé en utilisant le principe de signature numérique.

Le rôle de l'infrastructure de clés publiques est multiple et couvre notamment les champs suivants :

- enregistrer des demandes de clés en vérifiant l'identité des demandeurs ;
- générer les paires de clés (clé privée / clé publique) ;
- garantir la confidentialité des clés privées correspondant aux clés publiques ;
- certifier l'association entre chaque utilisateurs et sa clé publique ;
- révoquer des clés (en cas de perte par son propriétaire, d'expiration de sa date de validité ou de compromission).

Une infrastructure à clé publique est en règle générale composée de trois entités distinctes :

- L'autorité d'enregistrement (AE ou RA pour Recording authority), chargée des formalité administratives telles que la vérification de l'identité des demandeurs, le suivi et la gestion des demandes, etc.) ;
- L'autorité de certification (AC ou CA pour Certification Authority), chargée des tâches techniques de création de certificats. L'autorité de certification est ainsi chargée de la signature des demandes de certificat (CSR pour Certificate Signing Request, parfois appelées PKCS#10, nom du format correspondant). L'autorité de certification a également pour mission la signature des listes de révocations (CRL pour Certificate Revocation List) ;
- L'Autorité de dépôt (Repository) dont la mission est de conserver en sécurité les certificats.

Certificats X509

Pour palier aux problèmes liés à des clefs publiques piratées, un système de certificats a été mis en place.

Le certificat permet d’associer la clef publique à une entité ou une personne. Les certificats sont délivrés par des Organismes de Certification.

Les certificats sont des fichiers divisés en deux parties :

- La partie contenant les informations

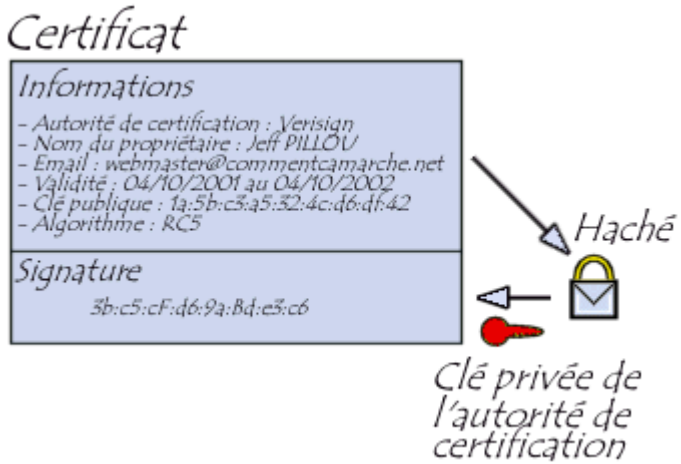
- La partie contenant la signature de l'autorité de certification

La structure des certificats est normalisée par le standard **X.509** de l'**Union internationale des télécommunications**.

Elle contient :

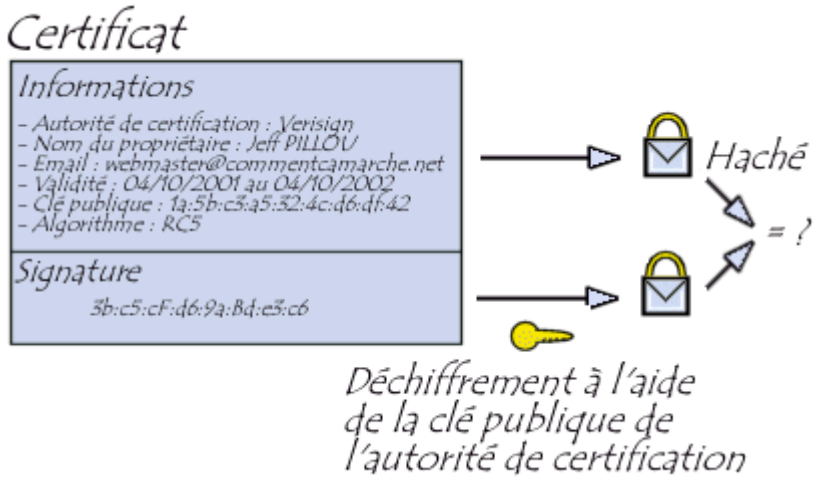
- Le nom de l'autorité de certification
- Le nom du propriétaire du certificat
- La date de validité du certificat
- L'algorithme de chiffrement utilisé
- La clé publique du propriétaire

Le Certificat est signé par l'autorité de certification:



;#; ;#;

La vérification se passe ainsi:



;#; ;#;

Installation de ssl

Afin de pouvoir configurer le serveur apache en mode ssl, il est necessaire d'installer les paquets **mod_ssl** et **openssl**. Le paquet **openssl** étant déjà installé, installez donc **mod_ssl** :

```
[root@centos7 ~]# yum install mod_ssl
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: distrib-coffee.ipsl.jussieu.fr
 * updates: mirror.guru
```

```
Resolving Dependencies
--> Running transaction check
---> Package mod_ssl.x86_64 1:2.4.6-67.el7.centos.6 will be installed
--> Processing Dependency: libcrypto.so.10(OPENSSL_1.0.2)(64bit) for package:
1:mod_ssl-2.4.6-67.el7.centos.6.x86_64
--> Running transaction check
---> Package openssl-libs.x86_64 1:1.0.1e-60.el7_3.1 will be updated
--> Processing Dependency: openssl-libs(x86-64) = 1:1.0.1e-60.el7_3.1 for package:
1:openssl-1.0.1e-60.el7_3.1.x86_64
---> Package openssl-libs.x86_64 1:1.0.2k-8.el7 will be an update
--> Running transaction check
---> Package openssl.x86_64 1:1.0.1e-60.el7_3.1 will be updated
---> Package openssl.x86_64 1:1.0.2k-8.el7 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================
 Package                         Arch                     Version                                  Repository
Size
================================================================================================================
=====================
Installing:
 mod_ssl                         x86_64                   1:2.4.6-67.el7.centos.6                  updates
109 k
Updating for dependencies:
 openssl                         x86_64                   1:1.0.2k-8.el7                           base
492 k
 openssl-libs                    x86_64                   1:1.0.2k-8.el7                           base
1.2 M

Transaction Summary
================================================================================================================
```

```
====================
Install  1 Package
Upgrade             ( 2 Dependent packages)

Total download size: 1.8 M
Is this ok [y/d/N]: y
```

Configuration de SSL

Dans le cas où vous souhaitez générer vos propres clés, vous devez d'abord générer une clé privée, nécessaire pour la création d'un **Certificate Signing Request**. Le CSR doit alors être envoyé à une des sociétés faisant autorité en la matière afin que celle-ci puisse vous retourner votre certificat définitif. Ce service est payant. C'est ce certificat définitif qui est utilisé pour des connexions sécurisées.

Saisissez donc la commande suivante pour générer votre clé privée :

```
[root@centos7 ~]# openssl genrsa -out www.homeland.net.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.................................++++++
e is 65537 (0x10001)
```

Générer maintenant votre CSR :

```
[root@centos7 ~]# openssl req -new -key www.homeland.net.key -out www.homeland.net.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:GB
State or Province Name (full name) []:SURREY
```

```
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LIMITED
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []:centos7.fenestros.loc
Email Address []:infos@i2tch.co.uk

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

et répondez aux questions qui vous sont posées. Notez bien la réponse à la question **Common Name**. Si vous ne donnez pas votre FQDN, certains navigateurs ne gèreront pas votre certificat correctement. Vous pouvez maintenant envoyé votre CSR à la société que vous avez choisie. Quand votre clé **.crt** vous est retournée, copiez-la, ainsi que votre clé privée dans le répertoire **/etc/pki/tls/certs/**.

Sans passer par un prestataire externe, vous pouvez signer votre CSR avec votre propre clé afin de générer votre certificat :

```
[root@centos7 ~]# openssl x509 -req -days 365 -in www.homeland.net.csr -signkey www.homeland.net.key -out
www.homeland.net.crt
Signature ok
subject=/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
Getting Private key
```

Cette procédure va générer trois fichiers dont votre clé privée et un certificat – une clé ayant une extension **.crt**.

Il convient ensuite de copier ces deux fichiers dans l'arborescence **/etc/pki/tls** :

```
[root@centos7 ~]# cp /root/www.homeland.net.key /etc/pki/tls/private/
[root@centos7 ~]# cp /root/www.homeland.net.crt /etc/pki/tls/certs/
```

Mise en place des paramètres de sécurité SSL

Créez maintenant le répertoire qui va contenir le site sécurisé :

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

Créez le fichier **index.html** pour notre site sécurisé :

```
[root@centos7 ~]# vi /www/ssl/index.html
[root@centos7 ~]# cat /www/ssl/index.html
<html>
<body>
<center>Accueil du site SSL</center>
</body>
</html>
```

En consultant le contenu du répertoire **/etc/httpd/conf.d**, vous constaterez un fichier **ssl.conf** :

```
[root@centos7 ~]# ls /etc/httpd/conf.d
autoindex.conf  README  ssl.conf  userdir.conf  welcome.conf
```

Ouvrez ce fichier et modifiez la ligne suivante :

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

en :

```
DocumentRoot "/www/ssl"
```

Cette directive indique que la racine du site sécurisé sera **/www/ssl**.

Définissez ensuite les droits d'accès à ce site en ajoutant la section suivante à l'emplacement indiqué :

```
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
```

```
</Files>
# Ajoutez la section suivante
<Directory "/www/ssl">
Require all granted
</Directory>
# Fin
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
</Directory>
```

Dernièrement modifiez les deux lignes suivantes :

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

en :

```
SSLCertificateFile /etc/pki/tls/certs/www.homeland.net.crt
SSLCertificateKeyFile /etc/pki/tls/private/www.homeland.net.key
```

respectivement.

Sauvegardez votre fichier et redémarrez votre serveur apache :

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

A Faire - Passez en revue les **directives** contenues dans le fichier **ssl.conf** en utilisant le **Manuel en ligne d'Apache**.

Tester Votre Configuration

Pour tester votre serveur apache en mode SSL saisissez la commande suivante :

```
[root@centos7 ~]# openssl s_client -connect www.homeland.net:443
CONNECTED(00000003)
depth=0 C = GB, ST = SURREY, L = ADDLESTONE, O = I2TCH LIMITED, OU = TRAINING, CN = centos7.fenestros.loc,
emailAddress = infos@i2tch.co.uk
verify error:num=18:self signed certificate
verify return:1
depth=0 C = GB, ST = SURREY, L = ADDLESTONE, O = I2TCH LIMITED, OU = TRAINING, CN = centos7.fenestros.loc,
emailAddress = infos@i2tch.co.uk
verify return:1
---
Certificate chain
 0 s:/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
   i:/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICuTCCAiICCQDauUN3s4rA2zANBgkqhkiG9w0BAQsFADCBoDELMAkGA1UEBhMC
R0IxDzANBgNVBAgMBlNVUlJFWTETMBEGA1UEBwwKQURETEVTVE9ORTEWMBQGA1UE
CgwNSTJUQ0ggTElNSVRFRDERMA8GA1UECwwIVFJBSU5JTkcxHjAcBgNVBAMMFWNl
bnRvczcuZmVuZXN0cm9zLmxvYzEgMB4GCSqGSIb3DQEJARYRaW5mb3NAaTJ0Y2gu
Y28udWswHhcNMTcxMTA1MTI1NDM4WhcNMTgxMTA1MTI1NDM4WjCBoDELMAkGA1UE
BhMCR0IxDzANBgNVBAgMBlNVUlJFWTETMBEGA1UEBwwKQURETEVTVE9ORTEWMBQG
A1UECgwNSTJUQ0ggTElNSVRFRDERMA8GA1UECwwIVFJBSU5JTkcxHjAcBgNVBAMM
FWNlbnRvczcuZmVuZXN0cm9zLmxvYzEgMB4GCSqGSIb3DQEJARYRaW5mb3NAaTJ0
Y2guY28udWswgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALTR07YEuayyb23D
2TXd6Zh4ZZg1cHLKURQN1sjxkJTKwmscKFHExqtQKEmQV+CKAAMj51DL5M1j55dp
G9/72AEAniMVlXT6mOCihRcpEoiiESRz9i71EJtLAIT7c7/ptaxLdTMScDIAUqZN
```

```
PcX6yTdDDyb4MqBjaHfaHTxS/JgzAgMBAAEwDQYJKoZIhvcNAQELBQADgYEAaNKp
eBmvUNVmsYzK6N5WgVtdVgKARVlPRwrWAPp2KDTRBNNz7lkgyYt9zmjHFBYifcQW
iLFSb+cl6EtDrty+zWBztKA3CRVdNejI3Q9YQ56ztOAYrGlrRMtUINNxnZcHBe05
bTSecVYeyRu6aChGIyISwL5LjNyMKpXiSjSi5u0=
-----END CERTIFICATE-----
subject=/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
issuer=/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 1264 bytes and written 415 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: AF724406B1B2C2F3E8B33EEC51E51364F8E2B62374CCC16054217FBE866C4D09
    Session-ID-ctx:
    Master-Key: A6BF30C3757101E375F74A3075E1F68FCEF2C6450D18DD3AF12F42F65162B53FBCC4B27C80BE5C3F27A104BFC40CEF15
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
```

```
    0000 - a8 28 11 9b 9f 2b 09 f9-ac 4c 20 5f 0c b7 ae 87   .(...+...L _....
    0010 - 7d 3b 12 4b b2 d1 f5 6f-ce 2e a8 74 9f 2d 59 a9   };.K...o...t.-Y.
    0020 - 6a d6 53 c9 54 f9 3e cc-0b c3 e6 92 58 8d 45 9c   j.S.T.>.....X.E.
    0030 - 41 ab a7 a4 b5 24 7c 2a-f2 4f 67 48 d5 35 68 29   A....$|*.OgH.5h)
    0040 - 3b 24 b6 2b 16 99 2d 6e-aa ea 4c c8 7e df 59 08   ;$.+..-n..L.~.Y.
    0050 - 42 06 1b 88 fa 5b c1 0b-4b 7c 01 d3 1a 28 6b 61   B....[..K|...(ka
    0060 - 70 c9 7b d0 74 93 f7 1e-c1 a6 58 54 b7 e6 4c 83   p.{.t.....XT..L.
    0070 - 5a d4 53 ff 61 71 46 f1-14 55 26 8f 83 29 11 69   Z.S.aqF..U&..).i
    0080 - e2 ee 08 dc 4e 7e 95 23-f7 54 c6 79 2e 88 7f 1d   ....N~.#.T.y....
    0090 - 5a a7 72 be 80 84 e3 4f-77 aa 63 28 06 a5 58 d1   Z.r....Ow.c(..X.
    00a0 - fa a8 28 9c 0d 22 ba 62-51 dc 33 d6 0c 56 57 c1   ..(.."bQ.3..VW.
    00b0 - b7 8c e3 eb da 54 82 d0-df e1 63 66 2b 10 85 cd   .....T....cf+...

    Start Time: 1509887084
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
^C
```

Procédez maintenant au test en utilisant le navigateur web de votre VM en saisissant l'adresse **https://www.homeland.net**.

Important - Il est normal que la vérification échoue car dans ce cas il s'agit du certificat de test auto-signé.

mod_proxy

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

```
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-proxy.conf | grep mod_proxy
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
```

```
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_express_module modules/mod_proxy_express.so
LoadModule proxy_fcgi_module modules/mod_proxy_fcgi.so
LoadModule proxy_fdpass_module modules/mod_proxy_fdpass.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
LoadModule proxy_wstunnel_module modules/mod_proxy_wstunnel.so
</proxy>

Créez le fichier de configuration **/etc/httpd/conf.d/proxy.conf** :

<code>
[root@centos7 ~]# vi /etc/httpd/conf.d/proxy.conf
[root@centos7 ~]# cat /etc/httpd/conf.d/proxy.conf
<IfModule mod_proxy.c>
ProxyRequests On
listen 0.0.0.0:8081

<Proxy *>
    Require all denied
    Require ip 127.0.0.1 10.0.2.0/24
</Proxy>
</IfModule>
```

Sauvegardez le fichier rechargez la configuration du serveur apache :

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

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@centos7 ~]# tail /var/log/httpd/access_log
127.0.0.1 - - [05/Nov/2017:15:15:04 +0100] "GET
http://edugroupe.ittraining.center/www/themes/efront2013/images/css_images/32x32map.png HTTP/1.1" 304 -
"http://edugroupe.ittraining.center/www/themes/efront2013/css/css_global.css?build=18025" "Mozilla/5.0 (X11;
Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [05/Nov/2017:15:15:04 +0100] "GET
http://edugroupe.ittraining.center/www/themes/efront2013/images/css_images/16x16map.png HTTP/1.1" 304 -
"http://edugroupe.ittraining.center/www/themes/efront2013/css/css_global.css?build=18025" "Mozilla/5.0 (X11;
Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0"
127.0.0.1 - - [05/Nov/2017:15:15:04 +0100] "GET
http://edugroupe.ittraining.center/www/themes/default/images/16x16/error_delete.png HTTP/1.1" 304 -
"http://edugroupe.ittraining.center/www/index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0"
127.0.0.1 - - [05/Nov/2017:15:15:04 +0100] "GET
http://edugroupe.ittraining.center/www/themes/default/images/16x16/help.png HTTP/1.1" 304 -
"http://edugroupe.ittraining.center/www/index.php" "Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101
Firefox/52.0"
...
```

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@centos7 ~]# cat /etc/httpd/conf.modules.d/00-dav.conf
LoadModule dav_module modules/mod_dav.so
LoadModule dav_fs_module modules/mod_dav_fs.so
LoadModule dav_lock_module modules/mod_dav_lock.so
```

Configuration

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

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

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

```
[root@centos7 ~]# 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>
Require all granted
</Directory>
```

```
<Location />
Dav On
AuthType Basic
AuthName "Accès WebDAV"
AuthUserFile /www/passwords/dav/.davusers
<LimitExcept GET HEAD OPTIONS>
Require valid-user
</LimitExcept>
</Location>
</VirtualHost>
```

Vous obtiendrez :

```
[root@centos7 ~]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 ~]# cat /etc/httpd/conf/vhosts.d/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
DBDriver mysql
DBDParams "dbname=auth user=apache pass=PaSsW0Rd"
DBDMin  4
DBDKeep 8
DBDMax  20
DBDExptime 300
<Directory /www/site1>
Require all granted
</Directory>
<Directory /www/site1/secret>
AllowOverride AuthConfig
</Directory>
<Directory /www/site1/secret2>
 AuthType Basic
 AuthName "MariaDB Secret"
 AuthBasicProvider dbd
 Require valid-user
 AuthDBDUserPWQuery "SELECT user_passwd FROM users WHERE user_name = %s"
</Directory>
</VirtualHost>
##################dav.homeland.net
<VirtualHost *:80>
ServerName dav.homeland.net
DocumentRoot /www/dav
<Directory /www/dav>
Require all granted
</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@centos7 ~]# mkdir /www/passwords/dav
```

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

```
[root@centos7 ~]# 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** :

```
[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
10.0.2.16   dav.homeland.net
```

Rechargez les fichiers de configuration d'apache :

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

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

Téléchargez et installez Cadaver à partir du dépôt EPEL :

```
[root@centos7 ~]# wget http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-11.noarch.rpm
--2017-11-05 16:11:09--  http://dl.fedoraproject.org/pub/epel/7/x86_64/Packages/e/epel-release-7-11.noarch.rpm
Resolving dl.fedoraproject.org (dl.fedoraproject.org)... 209.132.181.23, 209.132.181.25, 209.132.181.24
Connecting to dl.fedoraproject.org (dl.fedoraproject.org)|209.132.181.23|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15080 (15K) [application/x-rpm]
Saving to: ‘epel-release-7-11.noarch.rpm’

100%[======================================================================================>] 15,080
52.1KB/s   in 0.3s

2017-11-05 16:11:10 (52.1 KB/s) - ‘epel-release-7-11.noarch.rpm’ saved [15080/15080]

[root@centos7 ~]# rpm -Uvh epel-release*rpm
warning: epel-release-7-11.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 352c64e5: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:epel-release-7-11                ################################# [100%]
^C[root@centos7 ~]yum install cadaver
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.ate.info
 * epel: mirror.kinamo.be
 * extras: distrib-coffee.ipsl.jussieu.fr
 * updates: mirror.guru
Resolving Dependencies
--> Running transaction check
---> Package cadaver.x86_64 0:0.23.3-9.el7 will be installed
```

```
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================
 Package                         Arch                            Version                                 Repository
Size
================================================================================================================
=====================
Installing:
 cadaver                         x86_64                          0.23.3-9.el7                            epel
96 k

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

Total download size: 96 k
Installed size: 283 k
Is this ok [y/d/N]: y
Downloading packages:
warning: /var/cache/yum/x86_64/7/epel/packages/cadaver-0.23.3-9.el7.x86_64.rpm: Header V3 RSA/SHA256 Signature,
key ID 352c64e5: NOKEY
Public key for cadaver-0.23.3-9.el7.x86_64.rpm is not installed
cadaver-0.23.3-9.el7.x86_64.rpm                                                                             |
96 kB  00:00:02
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
Importing GPG key 0x352C64E5:
 Userid     : "Fedora EPEL (7) <epel@fedoraproject.org>"
 Fingerprint: 91e9 7d7c 4a5e 96f1 7f3e 888f 6a2f aea2 352c 64e5
 Package    : epel-release-7-11.noarch (installed)
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-7
```

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

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@centos7 ~]# 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  Nov  5 15:58
dav:/> cat dav.test
Displaying `/dav.test':
test
dav:/> exit
Connection to `dav.homeland.net' closed.
[root@centos7 ~]#
```

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 :

```
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep mod_rewrite
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 :

```
[root@centos7 ~]# vi /var/www/html/maintenance.html
[root@centos7 ~]# cat /var/www/html/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@centos7 ~]# systemctl reload httpd
```

Testez ensuite votre configuration avec lynx :

```
[root@centos7 ~]# lynx --dump http://www.homeland.net
   Notre site est actuellement en maintenance. Merci de revenir plus tard.


[root@centos7 ~]#
```

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** :

```
[root@centos7 ~]# vi /var/www/html/bye.html
[root@centos7 ~]# cat /var/www/html/bye.html
<html>
<head>
<title>Aurevoir</title>
</head>
<body>
<center>Bye bye 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 :

```
#RewriteRule ^/$ /maintenance.html [R]
RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.16$
RewriteCond %{REQUEST_URI} !^bye\.html
RewriteRule .* /bye.html
```

Vous obtiendrez le résultat suivant :

```
...
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.16$
RewriteCond %{REQUEST_URI} !^bye\.html
RewriteRule .* /bye.html
</VirtualHost>
##################www.vhostnom.com
...
```

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

Sauvegardez votre fichier puis rechargez la configuration d'apache :

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

Testez ensuite votre configuration avec lynx :

```
[root@centos7 ~]# lynx --dump http://www.homeland.net
                       Bye bye Pirate ! Ha! Ha! Ha!


[root@centos7 ~]#
```

Indiquer un déplacement permenant

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

Commencez par créer vos deux fichiers **oldpage.html** et **newpage.html** dans **/var/www/html**.

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

```
[root@centos7 ~]# touch /var/www/html/oldpage.html
[root@centos7 ~]# vi /var/www/html/newpage.html
[root@centos7 ~]# cat /var/www/html/newpage.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 ^/oldpage\.html /newpage.html [R=301,L]
```

Vous obtiendrez le résultat suivant :

```
...
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.16$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
</VirtualHost>
##################www.vhostnom.com
...
```

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

Sauvegardez votre fichier puis rechargez la configuration d'apache :

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

Testez ensuite votre configuration avec lynx :

```
[root@centos7 ~]# lynx --dump http://www.homeland.net/oldpage.html
                     Exemple de DEPLACEMENT PERMENANT


[root@centos7 ~]#
```

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 **newpage.html**.

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

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

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

Vous obtiendrez le résultat suivant :

```
...
################# Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.16$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
#RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
RewriteRule ^/oldpage\.html - [G]
</VirtualHost>
##################www.vhostnom.com
...
```

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

Sauvegardez votre fichier puis rechargez la configuration d'apache :

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

Testez ensuite votre configuration avec lynx :

```
[root@centos7 ~]# lynx --dump http://www.homeland.net/oldpage.html
                                    Gone

   The requested resource
   /oldpage.html
   is no longer available on this server and there is no forwarding
   address. Please remove all references to this resource.
[root@centos7 ~]#
```

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

Caractère spécial	Description
{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 directive **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)
[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 en faisant appel à **mod_headers** afin que l'en-tête soit modifié

```
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep mod_headers
LoadModule headers_module modules/mod_headers.so
```

Pour mettre en place cette notification, il convient d'éditer le fichier **/etc/httpd/conf.d/ssl.conf** :

```
#
# 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** :

```
...
################ Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
```

```
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.16$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
#RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
#RewriteRule ^/oldpage\.html - [G]
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
##################www.vhostnom.com
...
```

Rechargez la configuration d'apache :

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

Testez ensuite avec un navigateur le lien **http://www.homeland.net** :

```
[root@centos7 ~]# lynx --dump http://www.homeland.net

Looking up www.homeland.net
Making HTTP connection to www.homeland.net
Sending HTTP request.
HTTP request sent; waiting for response.
HTTP/1.1 302 Found
Data transfer complete
HTTP/1.1 302 Found
Using https://www.homeland.net/
Looking up www.homeland.net
Making HTTPS connection to www.homeland.net
```

```
SSL callback:self signed certificate, preverify_ok=0, ssl_okay=0
Retrying connection without TLS.
Looking up www.homeland.net
Making HTTPS connection to www.homeland.net
SSL callback:self signed certificate, preverify_ok=0, ssl_okay=0
Alert!: Unable to make secure connection to remote host.

lynx: Can't access startfile http://www.homeland.net/
```

Revenez à la configuration d'origine en mettant en commentaires les lignes ajoutées :

```
[root@centos7 cgi-bin]# vi /etc/httpd/conf.d/ssl.conf
[root@centos7 cgi-bin]# cat /etc/httpd/conf.d/ssl.conf
#
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
Listen 443 https
# Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"
...
```

```
[root@centos7 cgi-bin]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 cgi-bin]# cat /etc/httpd/conf/vhosts.d/Vhosts.conf | more
################## 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
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^10\.0\.2\.16$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
#RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
#RewriteRule ^/oldpage\.html - [G]
#RewriteCond %{HTTPS} off
#RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</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
DBDriver mysql
--More--
```

Dernièrement, re-démarrez apache :

```
[root@centos7 cgi-bin]# systemctl restart httpd
```

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@centos7 ~]# cd /var/www/cgi-bin/
```

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

```
[root@centos7 cgi-bin]# vi /var/www/cgi-bin/whoami.cgi
[root@centos7 cgi-bin]# cat /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@centos7 cgi-bin]# chmod u+x whoami.cgi
```

Appelez le script CGI :

```
[root@centos7 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 at root@localhost to inform
   them of the time this error occurred, and the actions you performed
   just before this error.

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

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

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

```
...
[Sun Nov 05 17:42:13.905639 2017] [cgi:error] [pid 20358] [client 127.0.0.1:47466] AH01215: (13)Permission
denied: exec of '/var/www/cgi-bin/whoami.cgi' failed
[Sun Nov 05 17:42:13.905817 2017] [cgi:error] [pid 20358] [client 127.0.0.1:47466] End of script output before
headers: whoami.cgi
```

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

```
[root@centos7 cgi-bin]# ls -l
total 4
-rwxr--r-- 1 root root 87 Nov  5 17:33 whoami.cgi
```

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

```
[root@centos7 cgi-bin]# chown apache:apache whoami.cgi
```

Appelez le script CGI :

```
[root@centos7 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@centos7 cgi-bin]# useradd scripts
```

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

```
[root@centos7 cgi-bin]# mkdir /var/www/scripts
```

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

```
[root@centos7 cgi-bin]# chown scripts:scripts /var/www/scripts/
[root@centos7 cgi-bin]# chmod 2755 /var/www/scripts/
```

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

```
[root@centos7 cgi-bin]# mv whoami.cgi /var/www/scripts
[root@centos7 cgi-bin]# cd !$
cd /var/www/scripts
[root@centos7 scripts]# ls -l
total 4
-rwxr--r-- 1 apache apache 87 Nov  5 17:33 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 le fichier **/etc/httpd/conf.modules.d/00-base.conf** :

```
[root@centos7 scripts]# cat /etc/httpd/conf.modules.d/00-base.conf | grep mod_suexec
LoadModule suexec_module modules/mod_suexec.so
```

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

```
...
#
# "/var/www/cgi-bin" should be changed to whatever your ScriptAliased
```

```
# CGI directory exists, if you have that configured.
#
<Directory "/var/www/cgi-bin">
    AllowOverride None
    Options None
    Require all granted
</Directory>
Alias /scripts/ "/var/www/scripts/"
<Directory "/var/www/scripts/">
        Options +ExecCGI
        SetHandler cgi-script
</Directory>

<IfModule mime_module>
...
```

Sauvegardez et vérifiez votre fichier de configuration :

```
[root@centos7 scripts]# httpd -t
AH00548: NameVirtualHost has no effect and will be removed in the next release
/etc/httpd/conf/vhosts.d/Vhosts.conf:13
Syntax OK
```

Re-démarrez le serveur apache :

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

Modifiez donc le propriétaire et groupe du script :

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

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

```
[root@centos7 scripts]# lynx --dump http://localhost/scripts/whoami.cgi
```

```
Nom de connexion : scripts
```

Améliorer l'utilisation de la Mémoire du Serveur

Passer Apache en Mode Worker

Le module MPM worker utilise moins de mémoire que le module prefork pour le même nombre de connexions.

Editez le fichier **/etc/httpd/conf/httpd.conf** pour pouvoir gérer **800** connexions simultanées :

```
...
<IfModule worker.c>
ServerLimit              25
StartServers             10
MinSpareThreads          75
MaxSpareThreads     250
ThreadLimit              64
ThreadsPerChild          32
MaxClients          800
MaxRequestsPerChild   10000
</IfModule>
...
```

Voir la page **http://httpd.apache.org/docs/2.2/mod/worker.html** pour une description des directives.

Ouvrez maintenant le fichier **/etc/sysconfig/httpd** et décommentez la directive **HTTPD=/usr/sbin/httpd.worker** :

```
[root@mail ~]# vi /etc/sysconfig/httpd
```

/etc/sysconfig/httpd

```
# Configuration file for the httpd service.

#
# The default processing model (MPM) is the process-based
# 'prefork' model.  A thread-based model, 'worker', is also
# available, but does not work with some modules (such as PHP).
# The service must be stopped before changing this variable.
#
HTTPD=/usr/sbin/httpd.worker

#
# To pass additional options (for instance, -D definitions) to the
# httpd binary at startup, set OPTIONS here.
#
#OPTIONS=

#
# By default, the httpd process is started in the C locale; to
# change the locale in which the server runs, the HTTPD_LANG
# variable can be set.
#
#HTTPD_LANG=C

#
# By default, the httpd process will create the file
# /var/run/httpd/httpd.pid in which it records its process
# identification number when it starts.  If an alternate location is
# specified in httpd.conf (via the PidFile directive), the new
# location needs to be reported in the PIDFILE.
#
#PIDFILE=/var/run/httpd/httpd.pid
```

Redémarrez ensuite apache :

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

Consultez les adresses http://localhost/server-status et http://localhost/server-status pour vérifier que votre apache utilise le MPM worker.
