Version : **2022.01**

Updated: 2022/11/22 13:43

Topic 208: HTTP Services

Contenu du Module

- Administration de Base
  - LAB #1 - Gestion de serveurs virtuels
    - Sous RHEL / CentOS 7
      - Hôte virtuel par nom
      - Hôte virtuel par adresse IP
      - Hôtes Virtuels Dynamiques avec mod_vhost_alias
    - Sous Debian 9
      - Hôte virtuel par nom
      - Hôte virtuel par adresse IP
      - Hôtes Virtuels Dynamiques avec mod_vhost_alias
  - LAB #2 - Gestion des pages personnelles avec mod_userdir
    - Sous RHEL / CentOS 7
    - Sous Debian 9
- Administration Avancée
  - LAB #3 - Gestion des pages dynamiques avec mod_php
  - LAB #4 - Gestion de l'authentification avec .htpasswd et mod_auth_basic
  - LAB #5 - Gestion de l'authentification avec MariaDB et mod_authn_dbd
  - LAB #6 - Gestion de l'authentification avec OpenLDAP et mod_authnz_ldap
  - LAB #7 - Gestion des pages web sécurisées en https avec mod_ssl
  - LAB #8 - Gestion d'un Serveur Mandataire avec mod_proxy
  - LAB #9 - Gestion du Web-based Distributed Authoring and Versioning avec mod_dav
  - LAB #10 - Gestion de la réécriture d'URL avec mod_rewrite
  - LAB #11 - Personnalisation des en-têtes de requêtes et de réponses HTTP avec mod_header
  - LAB #12 - L'exécution des scripts CGI sous l'utilisateur et le groupe spécifiés avec mod_suexec
  - LAB #13 - Améliorer l'utilisation de la Mémoire du Serveur avec mod_worker
- **Le Serveur Mandataire Squid**
  - LAB #14 - Installation et Configuration de Squid
  - LAB #15 - L'Extension squidGuard
  - LAB #16 - Dansguardian
- **Le Serveur HTTP Nginx**
  - LAB #17 - Configuration d'un Proxy Inverse
  - LAB #18 - Configuration d'un Serveur PHP
- **Ne Pas Oublier**
  - Server Name Indication

- Redirects et Alias

Le Serveur HTTP 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.

Présentation et Configuration d'Apache sous CentOS 7

Important : Demandez à votre formateur de restaurer le snapshot d'origine de votre VM CentOS 7.

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.
```

Installation à partir des dépôts

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.
```

Configuration

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 **/etc/httpd/conf.modules.d/** et **/etc/httpd/conf.d/** :

```
[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
```

/etc/httpd/conf/httpd.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
```

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.
%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 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
```

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>
```

<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
<IfModule prefork.c>
StartServers       8
MinSpareServers    5
MaxSpareServers   20
ServerLimit      256
MaxClients       256
MaxRequestsPerChild  4000
</IfModule>
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.i2tch.loc: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.i2tch.loc: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:

```
10.0.2.51       i2tch.loc
10.0.2.51       www.i2tch.loc
```

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.
```

Présentation et Configuration d'Apache sous Debian 9

Installation à partir des dépôts

Si Apache n'est pas déjà installé, utilisez **apt** pour installer le paquet **apache2**.

Configuration

Sous Debian 9 le fichier de configuration principal d'apache est **/etc/apache2/apache2.conf**. Cette configuration est complémentée par les directives se trouvant dans les fichiers contenus dans les répertoires **/etc/apache2/conf-enabled** et **/etc/apache2/mods-enabled** ainsi que par les fichiers **/etc/apache2/envvars**, **/etc/apache2/magic** et **/etc/apache2/ports.conf** :

```
root@debian9:~# ls -l /etc/apache2/
total 80
-rw-r--r-- 1 root root  7115 Mar 31 10:17 apache2.conf
drwxr-xr-x 2 root root  4096 Aug 27 11:08 conf-available
drwxr-xr-x 2 root root  4096 Aug 27 11:08 conf-enabled
-rw-r--r-- 1 root root  1782 Mar 31 10:17 envvars
-rw-r--r-- 1 root root 31063 Mar 30 16:07 magic
drwxr-xr-x 2 root root 12288 Aug 27 11:08 mods-available
drwxr-xr-x 2 root root  4096 Aug 27 11:08 mods-enabled
-rw-r--r-- 1 root root   320 Mar 30 16:07 ports.conf
drwxr-xr-x 2 root root  4096 Aug 27 11:08 sites-available
drwxr-xr-x 2 root root  4096 Aug 27 11:08 sites-enabled
root@debian9:~#
root@debian9:~# ls -lR /etc/apache2
/etc/apache2:
total 80
-rw-r--r-- 1 root root  7115 Mar 31 10:17 apache2.conf
drwxr-xr-x 2 root root  4096 Aug 27 11:08 conf-available
drwxr-xr-x 2 root root  4096 Aug 27 11:08 conf-enabled
-rw-r--r-- 1 root root  1782 Mar 31 10:17 envvars
-rw-r--r-- 1 root root 31063 Mar 30 16:07 magic
drwxr-xr-x 2 root root 12288 Aug 27 11:08 mods-available
drwxr-xr-x 2 root root  4096 Aug 27 11:08 mods-enabled
-rw-r--r-- 1 root root   320 Mar 30 16:07 ports.conf
drwxr-xr-x 2 root root  4096 Aug 27 11:08 sites-available
drwxr-xr-x 2 root root  4096 Aug 27 11:08 sites-enabled
```

```
/etc/apache2/conf-available:
total 24
-rw-r--r-- 1 root root  315 Mar 30 16:07 charset.conf
-rw-r--r-- 1 root root  127 Jul 29  2013 javascript-common.conf
-rw-r--r-- 1 root root 3224 Mar 30 16:07 localized-error-pages.conf
-rw-r--r-- 1 root root  189 Mar 30 16:07 other-vhosts-access-log.conf
-rw-r--r-- 1 root root 2190 Mar 31 10:17 security.conf
-rw-r--r-- 1 root root  455 Mar 30 16:07 serve-cgi-bin.conf

/etc/apache2/conf-enabled:
total 0
lrwxrwxrwx 1 root root 30 Aug 27 11:08 charset.conf -> ../conf-available/charset.conf
lrwxrwxrwx 1 root root 44 Aug 27 11:08 localized-error-pages.conf -> ../conf-available/localized-error-pages.conf
lrwxrwxrwx 1 root root 46 Aug 27 11:08 other-vhosts-access-log.conf -> ../conf-available/other-vhosts-access-
log.conf
lrwxrwxrwx 1 root root 31 Aug 27 11:08 security.conf -> ../conf-available/security.conf
lrwxrwxrwx 1 root root 36 Aug 27 11:08 serve-cgi-bin.conf -> ../conf-available/serve-cgi-bin.conf

/etc/apache2/mods-available:
total 528
-rw-r--r-- 1 root root  100 Mar 30 16:07 access_compat.load
-rw-r--r-- 1 root root  377 Mar 30 16:07 actions.conf
-rw-r--r-- 1 root root   66 Mar 30 16:07 actions.load
-rw-r--r-- 1 root root  843 Mar 30 16:07 alias.conf
-rw-r--r-- 1 root root   62 Mar 30 16:07 alias.load
-rw-r--r-- 1 root root   76 Mar 30 16:07 allowmethods.load
-rw-r--r-- 1 root root   76 Mar 30 16:07 asis.load
-rw-r--r-- 1 root root   94 Mar 30 16:07 auth_basic.load
-rw-r--r-- 1 root root   96 Mar 30 16:07 auth_digest.load
-rw-r--r-- 1 root root  100 Mar 30 16:07 auth_form.load
-rw-r--r-- 1 root root   72 Mar 30 16:07 authn_anon.load
-rw-r--r-- 1 root root   72 Mar 30 16:07 authn_core.load
-rw-r--r-- 1 root root   85 Mar 30 16:07 authn_dbd.load
-rw-r--r-- 1 root root   70 Mar 30 16:07 authn_dbm.load
```

```
-rw-r--r-- 1 root root   72 Mar 30 16:07 authn_file.load
-rw-r--r-- 1 root root   78 Mar 30 16:07 authn_socache.load
-rw-r--r-- 1 root root   74 Mar 30 16:07 authnz_fcgi.load
-rw-r--r-- 1 root root   90 Mar 30 16:07 authnz_ldap.load
-rw-r--r-- 1 root root   72 Mar 30 16:07 authz_core.load
-rw-r--r-- 1 root root   96 Mar 30 16:07 authz_dbd.load
-rw-r--r-- 1 root root   92 Mar 30 16:07 authz_dbm.load
-rw-r--r-- 1 root root  104 Mar 30 16:07 authz_groupfile.load
-rw-r--r-- 1 root root   94 Mar 30 16:07 authz_host.load
-rw-r--r-- 1 root root   74 Mar 30 16:07 authz_owner.load
-rw-r--r-- 1 root root   94 Mar 30 16:07 authz_user.load
-rw-r--r-- 1 root root 3374 Mar 30 16:07 autoindex.conf
-rw-r--r-- 1 root root   70 Mar 30 16:07 autoindex.load
-rw-r--r-- 1 root root   64 Mar 30 16:07 buffer.load
-rw-r--r-- 1 root root  889 Mar 30 16:07 cache_disk.conf
-rw-r--r-- 1 root root   89 Mar 30 16:07 cache_disk.load
-rw-r--r-- 1 root root   62 Mar 30 16:07 cache.load
-rw-r--r-- 1 root root   95 Mar 30 16:07 cache_socache.load
-rw-r--r-- 1 root root  115 Mar 30 16:07 cgid.conf
-rw-r--r-- 1 root root   60 Mar 30 16:07 cgid.load
-rw-r--r-- 1 root root   58 Mar 30 16:07 cgi.load
-rw-r--r-- 1 root root   76 Mar 30 16:07 charset_lite.load
-rw-r--r-- 1 root root   60 Mar 30 16:07 data.load
-rw-r--r-- 1 root root   83 Mar 30 16:07 dav_fs.conf
-rw-r--r-- 1 root root   79 Mar 30 16:07 dav_fs.load
-rw-r--r-- 1 root root   58 Mar 30 16:07 dav.load
-rw-r--r-- 1 root root   68 Mar 30 16:07 dav_lock.load
-rw-r--r-- 1 root root   58 Mar 30 16:07 dbd.load
-rw-r--r-- 1 root root  522 Mar 31 09:45 deflate.conf
-rw-r--r-- 1 root root   84 Mar 30 16:07 deflate.load
-rw-r--r-- 1 root root   64 Mar 30 16:07 dialup.load
-rw-r--r-- 1 root root  157 Mar 30 16:07 dir.conf
-rw-r--r-- 1 root root   58 Mar 30 16:07 dir.load
-rw-r--r-- 1 root root   64 Mar 30 16:07 dump_io.load
```

```
-rw-r--r-- 1 root root   60 Mar 30 16:07 echo.load
-rw-r--r-- 1 root root   58 Mar 30 16:07 env.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 expires.load
-rw-r--r-- 1 root root   72 Mar 30 16:07 ext_filter.load
-rw-r--r-- 1 root root   89 Mar 30 16:07 file_cache.load
-rw-r--r-- 1 root root   64 Mar 30 16:07 filter.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 headers.load
-rw-r--r-- 1 root root  176 Mar 30 16:07 heartbeat.load
-rw-r--r-- 1 root root  182 Mar 30 16:07 heartmonitor.load
-rw-r--r-- 1 root root   62 Mar 30 16:07 ident.load
-rw-r--r-- 1 root root   82 Mar 30 16:07 include.load
-rw-r--r-- 1 root root  402 Mar 30 16:07 info.conf
-rw-r--r-- 1 root root   60 Mar 30 16:07 info.load
-rw-r--r-- 1 root root  116 Mar 30 16:07 lbmethod_bybusyness.load
-rw-r--r-- 1 root root  116 Mar 30 16:07 lbmethod_byrequests.load
-rw-r--r-- 1 root root  114 Mar 30 16:07 lbmethod_bytraffic.load
-rw-r--r-- 1 root root  114 Mar 30 16:07 lbmethod_heartbeat.load
-rw-r--r-- 1 root root  121 Mar 30 16:07 ldap.conf
-rw-r--r-- 1 root root   60 Mar 30 16:07 ldap.load
-rw-r--r-- 1 root root   70 Mar 30 16:07 log_debug.load
-rw-r--r-- 1 root root   76 Mar 30 16:07 log_forensic.load
-rw-r--r-- 1 root root   58 Mar 30 16:07 lua.load
-rw-r--r-- 1 root root   62 Mar 30 16:07 macro.load
-rw-r--r-- 1 root root 7639 Mar 31 09:45 mime.conf
-rw-r--r-- 1 root root   60 Mar 30 16:07 mime.load
-rw-r--r-- 1 root root  120 Mar 30 16:07 mime_magic.conf
-rw-r--r-- 1 root root   72 Mar 30 16:07 mime_magic.load
-rw-r--r-- 1 root root  668 Mar 30 16:07 mpm_event.conf
-rw-r--r-- 1 root root  106 Mar 30 16:07 mpm_event.load
-rw-r--r-- 1 root root  571 Mar 30 16:07 mpm_prefork.conf
-rw-r--r-- 1 root root  108 Mar 30 16:07 mpm_prefork.load
-rw-r--r-- 1 root root  836 Mar 30 16:07 mpm_worker.conf
-rw-r--r-- 1 root root  107 Mar 30 16:07 mpm_worker.load
-rw-r--r-- 1 root root  724 Mar 30 16:07 negotiation.conf
```

```
-rw-r--r-- 1 root root   74 Mar 30 16:07 negotiation.load
-rw-r--r-- 1 root root   87 Mar 30 16:07 proxy_ajp.load
-rw-r--r-- 1 root root  347 Mar 30 16:07 proxy_balancer.conf
-rw-r--r-- 1 root root  115 Mar 30 16:07 proxy_balancer.load
-rw-r--r-- 1 root root  822 Mar 30 16:07 proxy.conf
-rw-r--r-- 1 root root   95 Mar 30 16:07 proxy_connect.load
-rw-r--r-- 1 root root   95 Mar 30 16:07 proxy_express.load
-rw-r--r-- 1 root root   89 Mar 30 16:07 proxy_fcgi.load
-rw-r--r-- 1 root root   93 Mar 30 16:07 proxy_fdpass.load
-rw-r--r-- 1 root root  189 Mar 30 16:07 proxy_ftp.conf
-rw-r--r-- 1 root root   87 Mar 30 16:07 proxy_ftp.load
-rw-r--r-- 1 root root 2511 Mar 30 16:07 proxy_html.conf
-rw-r--r-- 1 root root   89 Mar 31 10:17 proxy_html.load
-rw-r--r-- 1 root root   89 Mar 30 16:07 proxy_http.load
-rw-r--r-- 1 root root   62 Mar 30 16:07 proxy.load
-rw-r--r-- 1 root root   89 Mar 30 16:07 proxy_scgi.load
-rw-r--r-- 1 root root   97 Mar 30 16:07 proxy_wstunnel.load
-rw-r--r-- 1 root root   85 Mar 30 16:07 ratelimit.load
-rw-r--r-- 1 root root   70 Mar 30 16:07 reflector.load
-rw-r--r-- 1 root root   68 Mar 30 16:07 remoteip.load
-rw-r--r-- 1 root root 1190 Mar 30 16:07 reqtimeout.conf
-rw-r--r-- 1 root root   72 Mar 30 16:07 reqtimeout.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 request.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 rewrite.load
-rw-r--r-- 1 root root   58 Mar 30 16:07 sed.load
-rw-r--r-- 1 root root   99 Mar 30 16:07 session_cookie.load
-rw-r--r-- 1 root root   99 Mar 30 16:07 session_crypto.load
-rw-r--r-- 1 root root   93 Mar 30 16:07 session_dbd.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 session.load
-rw-r--r-- 1 root root 1280 Mar 30 16:07 setenvif.conf
-rw-r--r-- 1 root root   68 Mar 30 16:07 setenvif.load
-rw-r--r-- 1 root root   78 Mar 30 16:07 slotmem_plain.load
-rw-r--r-- 1 root root   74 Mar 30 16:07 slotmem_shm.load
-rw-r--r-- 1 root root   74 Mar 30 16:07 socache_dbm.load
```

```
-rw-r--r-- 1 root root   84 Mar 30 16:07 socache_memcache.load
-rw-r--r-- 1 root root   78 Mar 30 16:07 socache_shmcb.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 speling.load
-rw-r--r-- 1 root root 3110 Mar 30 16:07 ssl.conf
-rw-r--r-- 1 root root   97 Mar 30 16:07 ssl.load
-rw-r--r-- 1 root root  749 Mar 30 16:07 status.conf
-rw-r--r-- 1 root root   64 Mar 30 16:07 status.load
-rw-r--r-- 1 root root   72 Mar 30 16:07 substitute.load
-rw-r--r-- 1 root root   64 Mar 30 16:07 suexec.load
-rw-r--r-- 1 root root   70 Mar 30 16:07 unique_id.load
-rw-r--r-- 1 root root  423 Mar 31 10:17 userdir.conf
-rw-r--r-- 1 root root   66 Mar 30 16:07 userdir.load
-rw-r--r-- 1 root root   70 Mar 30 16:07 usertrack.load
-rw-r--r-- 1 root root   74 Mar 30 16:07 vhost_alias.load
-rw-r--r-- 1 root root   66 Mar 30 16:07 xml2enc.load

/etc/apache2/mods-enabled:
total 0
lrwxrwxrwx 1 root root 36 Aug 27 11:08 access_compat.load -> ../mods-available/access_compat.load
lrwxrwxrwx 1 root root 28 Aug 27 11:08 alias.conf -> ../mods-available/alias.conf
lrwxrwxrwx 1 root root 28 Aug 27 11:08 alias.load -> ../mods-available/alias.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 auth_basic.load -> ../mods-available/auth_basic.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 authn_core.load -> ../mods-available/authn_core.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 authn_file.load -> ../mods-available/authn_file.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 authz_core.load -> ../mods-available/authz_core.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 authz_host.load -> ../mods-available/authz_host.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 authz_user.load -> ../mods-available/authz_user.load
lrwxrwxrwx 1 root root 32 Aug 27 11:08 autoindex.conf -> ../mods-available/autoindex.conf
lrwxrwxrwx 1 root root 32 Aug 27 11:08 autoindex.load -> ../mods-available/autoindex.load
lrwxrwxrwx 1 root root 30 Aug 27 11:08 deflate.conf -> ../mods-available/deflate.conf
lrwxrwxrwx 1 root root 30 Aug 27 11:08 deflate.load -> ../mods-available/deflate.load
lrwxrwxrwx 1 root root 26 Aug 27 11:08 dir.conf -> ../mods-available/dir.conf
lrwxrwxrwx 1 root root 26 Aug 27 11:08 dir.load -> ../mods-available/dir.load
lrwxrwxrwx 1 root root 26 Aug 27 11:08 env.load -> ../mods-available/env.load
```

```
lrwxrwxrwx 1 root root 29 Aug 27 11:08 filter.load -> ../mods-available/filter.load
lrwxrwxrwx 1 root root 27 Aug 27 11:08 mime.conf -> ../mods-available/mime.conf
lrwxrwxrwx 1 root root 27 Aug 27 11:08 mime.load -> ../mods-available/mime.load
lrwxrwxrwx 1 root root 32 Aug 27 11:08 mpm_event.conf -> ../mods-available/mpm_event.conf
lrwxrwxrwx 1 root root 32 Aug 27 11:08 mpm_event.load -> ../mods-available/mpm_event.load
lrwxrwxrwx 1 root root 34 Aug 27 11:08 negotiation.conf -> ../mods-available/negotiation.conf
lrwxrwxrwx 1 root root 34 Aug 27 11:08 negotiation.load -> ../mods-available/negotiation.load
lrwxrwxrwx 1 root root 33 Aug 27 11:08 reqtimeout.conf -> ../mods-available/reqtimeout.conf
lrwxrwxrwx 1 root root 33 Aug 27 11:08 reqtimeout.load -> ../mods-available/reqtimeout.load
lrwxrwxrwx 1 root root 31 Aug 27 11:08 setenvif.conf -> ../mods-available/setenvif.conf
lrwxrwxrwx 1 root root 31 Aug 27 11:08 setenvif.load -> ../mods-available/setenvif.load
lrwxrwxrwx 1 root root 29 Aug 27 11:08 status.conf -> ../mods-available/status.conf
lrwxrwxrwx 1 root root 29 Aug 27 11:08 status.load -> ../mods-available/status.load

/etc/apache2/sites-available:
total 12
-rw-r--r-- 1 root root 1332 Mar 30 16:07 000-default.conf
-rw-r--r-- 1 root root 6437 Mar 31 10:17 default-ssl.conf

/etc/apache2/sites-enabled:
total 0
lrwxrwxrwx 1 root root 35 Aug 27 11:08 000-default.conf -> ../sites-available/000-default.conf
```

/etc/apache2/apache2.conf

```
root@debian9:~# cat /etc/apache2/apache2.conf
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See http://httpd.apache.org/docs/2.4/ for detailed information about
# the directives and /usr/share/doc/apache2/README.Debian about Debian specific
# hints.
#
#
```

```
# Summary of how the Apache 2 configuration works in Debian:
# The Apache 2 web server configuration in Debian is quite different to
# upstream's suggested way to configure the web server. This is because Debian's
# default Apache2 installation attempts to make adding and removing modules,
# virtual hosts, and extra configuration directives as flexible as possible, in
# order to make automating the changes and administering the server as easy as
# possible.

# It is split into several files forming the configuration hierarchy outlined
# below, all located in the /etc/apache2/ directory:
#
#   /etc/apache2/
#   |-- apache2.conf
#   |    `--  ports.conf
#   |-- mods-enabled
#   |    |-- *.load
#   |    `-- *.conf
#   |-- conf-enabled
#   |    `-- *.conf
#   `-- sites-enabled
#        `-- *.conf
#
#
# * apache2.conf is the main configuration file (this file). It puts the pieces
#   together by including all remaining configuration files when starting up the
#   web server.
#
# * ports.conf is always included from the main configuration file. It is
#   supposed to determine listening ports for incoming connections which can be
#   customized anytime.
#
# * Configuration files in the mods-enabled/, conf-enabled/ and sites-enabled/
#   directories contain particular configuration snippets which manage modules,
#   global configuration fragments, or virtual host configurations,
```

```
#   respectively.
#
#   They are activated by symlinking available configuration files from their
#   respective *-available/ counterparts. These should be managed by using our
#   helpers a2enmod/a2dismod, a2ensite/a2dissite and a2enconf/a2disconf. See
#   their respective man pages for detailed information.
#
# * The binary is called apache2. Due to the use of environment variables, in
#   the default configuration, apache2 needs to be started/stopped with
#   /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not
#   work with the default configuration.


# Global configuration
#


#
# ServerRoot: The top of the directory tree under which the server's
# configuration, error, and log files are kept.
#
# NOTE!  If you intend to place this on an NFS (or otherwise network)
# mounted filesystem then please read the Mutex documentation (available
# at <URL:http://httpd.apache.org/docs/2.4/mod/core.html#mutex>);
# you will save yourself a lot of trouble.
#
# Do NOT add a slash at the end of the directory path.
#
#ServerRoot "/etc/apache2"

#
# The accept serialization lock file MUST BE STORED ON A LOCAL DISK.
#
Mutex file:${APACHE_LOCK_DIR} default
```

```
#
# PidFile: The file in which the server should record its process
# identification number when it starts.
# This needs to be set in /etc/apache2/envvars
#
PidFile ${APACHE_PID_FILE}

#
# Timeout: The number of seconds before receives and sends time out.
#
Timeout 300

#
# KeepAlive: Whether or not to allow persistent connections (more than
# one request per connection). Set to "Off" to deactivate.
#
KeepAlive On

#
# MaxKeepAliveRequests: The maximum number of requests to allow
# during a persistent connection. Set to 0 to allow an unlimited amount.
# We recommend you leave this number high, for maximum performance.
#
MaxKeepAliveRequests 100

#
# KeepAliveTimeout: Number of seconds to wait for the next request from the
# same client on the same connection.
#
KeepAliveTimeout 5


# These need to be set in /etc/apache2/envvars
User ${APACHE_RUN_USER}
```

```
Group ${APACHE_RUN_GROUP}

#
# HostnameLookups: Log the names of clients or just their IP addresses
# e.g., www.apache.org (on) or 204.62.129.132 (off).
# The default is off because it'd be overall better for the net if people
# had to knowingly turn this feature on, since enabling it means that
# each client request will result in AT LEAST one lookup request to the
# nameserver.
#
HostnameLookups Off

# ErrorLog: The location of the error log file.
# If you do not specify an ErrorLog directive within a <VirtualHost>
# container, error messages relating to that virtual host will be
# logged here.  If you *do* define an error logfile for a <VirtualHost>
# container, that host's errors will be logged there and not here.
#
ErrorLog ${APACHE_LOG_DIR}/error.log

#
# LogLevel: Control the severity of messages logged to the error_log.
# Available values: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the log level for particular modules, e.g.
# "LogLevel info ssl:warn"
#
LogLevel warn

# Include module configuration:
IncludeOptional mods-enabled/*.load
IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
```

```
Include ports.conf


# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
    Options FollowSymLinks
    AllowOverride None
    Require all denied
</Directory>

<Directory /usr/share>
    AllowOverride None
    Require all granted
</Directory>

<Directory /var/www/>
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>

#<Directory /srv/>
#   Options Indexes FollowSymLinks
#   AllowOverride None
#   Require all granted
#</Directory>
```

```
# AccessFileName: The name of the file to look for in each directory
# for additional configuration directives.  See also the AllowOverride
# directive.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess and .htpasswd files from being
# viewed by Web clients.
#
<FilesMatch "^\.ht">
    Require all denied
</FilesMatch>



#
# The following directives define some format nicknames for use with
# a CustomLog directive.
#
# These deviate from the Common Log Format definitions in that they use %O
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
LogFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" vhost_combined
LogFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %O" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent

# Include of directories ignores editors' and dpkg's backup files,
```

```
# see README.Debian for details.

# Include generic snippets of statements
IncludeOptional conf-enabled/*.conf

# Include the virtual host configurations:
IncludeOptional sites-enabled/*.conf

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

/etc/apache2/conf-available/charset.conf

```
root@debian9:~# cat /etc/apache2/conf-available/charset.conf
# Read the documentation before enabling AddDefaultCharset.
# In general, it is only a good idea if you know that all your files
# have this encoding. It will override any encoding given in the files
# in meta http-equiv or xml encoding tags.

#AddDefaultCharset UTF-8

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

/etc/apache2/conf-available/localized-error-pages.conf

```
root@debian9:~# cat /etc/apache2/conf-available/localized-error-pages.conf
# Customizable error responses come in three flavors:
# 1) plain text
# 2) local redirects
# 3) external redirects
#
# Some examples:
```

```
#ErrorDocument 500 "The server made a boo boo."
#ErrorDocument 404 /missing.html
#ErrorDocument 404 "/cgi-bin/missing_handler.pl"
#ErrorDocument 402 http://www.example.com/subscription_info.html
#


#
# Putting this all together, we can internationalize error responses.
#
# We use Alias to redirect any /error/HTTP_<error>.html.var response to
# our collection of by-error message multi-language collections.  We use
# includes to substitute the appropriate text.
#
# You can modify the messages' appearance without changing any of the
# default HTTP_<error>.html.var files by adding the line:
#
#Alias /error/include/ "/your/include/path/"
#
# which allows you to create your own set of files by starting with the
# /usr/share/apache2/error/include/ files and copying them to /your/include/path/,
# even on a per-VirtualHost basis.  If you include the Alias in the global server
# context, is has to come _before_ the 'Alias /error/ ...' line.
#
# The default include files will display your Apache version number and your
# ServerAdmin email address regardless of the setting of ServerSignature.
#
# WARNING: The configuration below will NOT work out of the box if you have a
#         SetHandler directive in a <Location /> context somewhere. Adding
#         the following three lines AFTER the <Location /> context should
#         make it work in most cases:
#         <Location /error/>
#            SetHandler none
#         </Location>
#
```

```
# The internationalized error documents require mod_alias, mod_include
# and mod_negotiation.  To activate them, uncomment the following 37 lines.

#<IfModule mod_negotiation.c>
#   <IfModule mod_include.c>
#       <IfModule mod_alias.c>
#
#           Alias /error/ "/usr/share/apache2/error/"
#
#           <Directory "/usr/share/apache2/error">
#               Options IncludesNoExec
#               AddOutputFilter Includes html
#               AddHandler type-map var
#               Order allow,deny
#               Allow from all
#               LanguagePriority en cs de es fr it nl sv pt-br ro
#               ForceLanguagePriority Prefer Fallback
#           </Directory>
#
#           ErrorDocument 400 /error/HTTP_BAD_REQUEST.html.var
#           ErrorDocument 401 /error/HTTP_UNAUTHORIZED.html.var
#           ErrorDocument 403 /error/HTTP_FORBIDDEN.html.var
#           ErrorDocument 404 /error/HTTP_NOT_FOUND.html.var
#           ErrorDocument 405 /error/HTTP_METHOD_NOT_ALLOWED.html.var
#           ErrorDocument 408 /error/HTTP_REQUEST_TIME_OUT.html.var
#           ErrorDocument 410 /error/HTTP_GONE.html.var
#           ErrorDocument 411 /error/HTTP_LENGTH_REQUIRED.html.var
#           ErrorDocument 412 /error/HTTP_PRECONDITION_FAILED.html.var
#           ErrorDocument 413 /error/HTTP_REQUEST_ENTITY_TOO_LARGE.html.var
#           ErrorDocument 414 /error/HTTP_REQUEST_URI_TOO_LARGE.html.var
#           ErrorDocument 415 /error/HTTP_UNSUPPORTED_MEDIA_TYPE.html.var
#           ErrorDocument 500 /error/HTTP_INTERNAL_SERVER_ERROR.html.var
#           ErrorDocument 501 /error/HTTP_NOT_IMPLEMENTED.html.var
#           ErrorDocument 502 /error/HTTP_BAD_GATEWAY.html.var
```

```
#           ErrorDocument 503 /error/HTTP_SERVICE_UNAVAILABLE.html.var
#           ErrorDocument 506 /error/HTTP_VARIANT_ALSO_VARIES.html.var
#       </IfModule>
#   </IfModule>
#</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

/etc/apache2/conf-available/other-vhosts-access-log.conf

```
root@debian9:~# cat /etc/apache2/conf-available/other-vhosts-access-log.conf
# Define an access log for VirtualHosts that don't define their own logfile
CustomLog ${APACHE_LOG_DIR}/other_vhosts_access.log vhost_combined

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

/etc/apache2/conf-available/security.conf

```
root@debian9:~# cat /etc/apache2/conf-available/security.conf
#
# Disable access to the entire file system except for the directories that
# are explicitly allowed later.
#
# This currently breaks the configurations that come with some web application
# Debian packages.
#
#<Directory />
#   AllowOverride None
#   Order Deny,Allow
#   Deny from all
#</Directory>
```

```
# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#ServerSignature Off
ServerSignature On

#
# Allow TRACE method
#
# Set to "extended" to also reflect the request body (only for testing and
# diagnostic purposes).
#
# Set to one of:  On | Off | extended
TraceEnable Off
#TraceEnable On
```

```
#
# Forbid access to version control directories
#
# If you use version control systems in your document root, you should
# probably deny access to their directories. For example, for subversion:
#
#<DirectoryMatch "/\.svn">
#   Require all denied
#</DirectoryMatch>

#
# Setting this header will prevent MSIE from interpreting files as something
# else than declared by the content type in the HTTP headers.
# Requires mod_headers to be enabled.
#
#Header set X-Content-Type-Options: "nosniff"

#
# Setting this header will prevent other sites from embedding pages from this
# site as frames. This defends against clickjacking attacks.
# Requires mod_headers to be enabled.
#
#Header set X-Frame-Options: "sameorigin"


# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

/etc/apache2/conf-available/serve-cgi-bin.conf

```
root@debian9:~# cat /etc/apache2/conf-available/serve-cgi-bin.conf
<IfModule mod_alias.c>
    <IfModule mod_cgi.c>
        Define ENABLE_USR_LIB_CGI_BIN
```

```
    </IfModule>

    <IfModule mod_cgid.c>
        Define ENABLE_USR_LIB_CGI_BIN
    </IfModule>

    <IfDefine ENABLE_USR_LIB_CGI_BIN>
        ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
        <Directory "/usr/lib/cgi-bin">
            AllowOverride None
            Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
            Require all granted
        </Directory>
    </IfDefine>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

/etc/apache2/envvars

```
root@debian9:~# cat /etc/apache2/envvars
# envvars - default environment variables for apache2ctl

# this won't be correct after changing uid
unset HOME

# for supporting multiple apache2 instances
if [ "${APACHE_CONFDIR##/etc/apache2-}" != "${APACHE_CONFDIR}" ] ; then
    SUFFIX="-${APACHE_CONFDIR##/etc/apache2-}"
else
    SUFFIX=
fi
```

```
# Since there is no sane way to get the parsed apache2 config in scripts, some
# settings are defined via environment variables and then used in apache2ctl,
# /etc/init.d/apache2, /etc/logrotate.d/apache2, etc.
export APACHE_RUN_USER=www-data
export APACHE_RUN_GROUP=www-data
# temporary state file location. This might be changed to /run in Wheezy+1
export APACHE_PID_FILE=/var/run/apache2/apache2$SUFFIX.pid
export APACHE_RUN_DIR=/var/run/apache2$SUFFIX
export APACHE_LOCK_DIR=/var/lock/apache2$SUFFIX
# Only /var/log/apache2 is handled by /etc/logrotate.d/apache2.
export APACHE_LOG_DIR=/var/log/apache2$SUFFIX

## The locale used by some modules like mod_dav
export LANG=C
## Uncomment the following line to use the system default locale instead:
#. /etc/default/locale

export LANG

## The command to get the status for 'apache2ctl status'.
## Some packages providing 'www-browser' need '--dump' instead of '-dump'.
#export APACHE_LYNX='www-browser -dump'

## If you need a higher file descriptor limit, uncomment and adjust the
## following line (default is 8192):
#APACHE_ULIMIT_MAX_FILES='ulimit -n 65536'

## If you would like to pass arguments to the web server, add them below
## to the APACHE_ARGUMENTS environment.
#export APACHE_ARGUMENTS=''

## Enable the debug mode for maintainer scripts.
## This will produce a verbose output on package installations of web server modules and web application
## installations which interact with Apache
```

```
#export APACHE2_MAINTSCRIPT_DEBUG=1
```

/etc/apache2/magic

```
root@debian9:~# more /etc/apache2/magic
# Magic data for mod_mime_magic (originally for file(1) command)
#
# The format is 4-5 columns:
#    Column #1: byte number to begin checking from, ">" indicates continuation
#    Column #2: type of data to match
#    Column #3: contents of data to match
#    Column #4: MIME type of result
#    Column #5: MIME encoding of result (optional)

#------------------------------------------------------------------------------
# Localstuff:  file(1) magic for locally observed files
# Add any locally observed files here.

# Real Audio (Magic .ra\0375)
0   belong        0x2e7261fd    audio/x-pn-realaudio
0   string        .RMF        application/vnd.rn-realmedia

#video/x-pn-realvideo
#video/vnd.rn-realvideo
#application/vnd.rn-realmedia
#   sigh, there are many mimes for that but the above are the most common.

# Taken from magic, converted to magic.mime
# mime types according to http://www.geocities.com/nevilo/mod.htm:
#   audio/it    .it
#   audio/x-zipped-it    .itz
#   audio/xm    fasttracker modules
#   audio/x-s3m    screamtracker modules
```

```
#   audio/s3m    screamtracker modules
#   audio/x-zipped-mod    mdz
#   audio/mod    mod
#   audio/x-mod    All modules (mod, s3m, 669, mtm, med, xm, it, mdz, stm, itz, xmz, s3z)

# Taken from loader code from mikmod version 2.14
# by Steve McIntyre (stevem@chiark.greenend.org.uk)
# <doj@cubic.org> added title printing on 2003-06-24
0   string    MAS_UTrack_V00
>14  string    >/0        audio/x-mod
#audio/x-tracker-module
--More--(4%)
```

/etc/apache2/ports.conf

```
root@debian9:~# cat /etc/apache2/ports.conf
# If you just change the port or add more ports here, you will likely also
# have to change the VirtualHost statement in
# /etc/apache2/sites-enabled/000-default.conf

Listen 80

<IfModule ssl_module>
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Administration de Base

LAB #1 - Gestion de serveurs virtuels

Apache est capable de gérer de multiples sites hébergés sur la même machine.

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

- Hôte Virtuel par nom
- Hôte Virtuel par adresse IP

Sous RHEL / CentOS 7

Sous **RHEL / CentOS 7** 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**.

Hôte virtuel par nom

Nous allons d'abord considérer les sites virtuels 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
[root@centos7 ~]# cat /www/site1/index.html
<html>
<head>
<title>Page de Test</title>
<body>
<center>Accueil du site 1</center>
</body>
</html>
```

Editez le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** en suivant l'exemple ci-dessous :

```
[root@centos7 ~]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 ~]# cat /etc/httpd/conf/vhosts.d/Vhosts.conf
################# Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName i2tch.loc
```

```
ServerAlias www.i2tch.loc
</VirtualHost>
##################www.rhelnom.com
<VirtualHost *:80>
ServerName www.rhelnom.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** :

```
[root@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.51   i2tch.loc
10.0.2.51   www.i2tch.loc
10.0.2.51   www.rhelnom.com
```

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

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

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.rhelnom.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/rhelnom.log combined
Errorlog /www/logs/site1/rhelnom_error.log
```

Vous obtiendrez une fenêtre similaire à celle-ci :

```
[root@centos7 ~]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 ~]# cat /etc/httpd/conf/vhosts.d/Vhosts.conf
################# Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName i2tch.loc
ServerAlias www.i2tch.loc
</VirtualHost>
##################www.rhelnom.com
<VirtualHost *:80>
ServerName www.rhelnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
```

```
Customlog /www/logs/site1/rhelnom.log combined
Errorlog /www/logs/site1/rhelnom_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.rhelnom.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 rhelnom_error.log
-rw-r--r--. 1 root root 138 Aug 24 11:06 rhelnom.log
```

Ces deux fichiers **rhelnom.log** et **rhelnom_error.log** sont créés automatiquement par Apache.

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

```
[root@centos7 ~]# cat /www/logs/site1/rhelnom.log
10.0.2.51 - - [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

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 10.0.2.51/24 brd 10.0.2.255 scope global noprefixroute eth0
[root@centos7 ~]# ip a add 192.168.1.99/24 dev eth0
[root@centos7 ~]# ip a | grep 'inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.51/24 brd 10.0.2.255 scope global noprefixroute eth0
    inet 192.168.1.99/24 scope global eth0
```

Créez maintenant le répertoire pour notre site2 :

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

Créez la page d'accueil :

```
[root@centos7 ~]# vi /www/site2/index.html
[root@centos7 ~]# cat /www/site2/index.html
<html>
<head>
<title>Page de Test</title>
<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**:

```
[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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_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 i2tch.loc
ServerAlias www.i2tch.loc
</VirtualHost>
##################www.rhelnom.com
<VirtualHost *:80>
ServerName www.rhelnom.com
```

```
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/rhelnom.log combined
Errorlog /www/logs/site1/rhelnom_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
10.0.2.51   i2tch.loc
10.0.2.51   www.i2tch.loc
10.0.2.51       www.rhelnom.com
192.168.1.99    www.rhelip.com
```

Redémarrez votre serveur Apache :

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

Testez votre configuration avec **lynx** :

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

```
total 4
-rw-r--r--. 1 root root   0 Aug 24 14:28 rhelip_error.log
-rw-r--r--. 1 root root 141 Aug 24 14:29 rhelip.log
```

Hôtes Virtuels Dynamiques avec mod_vhost_alias

Commencez par installer le paquet **dnsmasq** afin de fournir les services d'un serveur DNS :

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

Créez le fichier **/etc/dnsmasq.d/i2tch** pour indiquer à dnsmasq que le domaine i2tch.loc se trouve à l'adresse **127.0.0.1** :

```
[root@centos7 ~]# vi /etc/dnsmasq.d/i2tch
[root@centos7 ~]# cat /etc/dnsmasq.d/i2tch
listen-address=127.0.0.1
address=/.i2tch.loc/127.0.0.1
```

Re-démarrez le service dnsmasq pour prendre en compte vos modifications :

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

Pour qu'apache puisse gérer les hôtes virtuels dynamiques, il faut que les modules **mod_rewrite** et **mod_vhost_alias** soient activés dans le fichier **/etc/httpd/conf.modules.d/00-base.conf** :

```
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep rewrite
LoadModule rewrite_module modules/mod_rewrite.so
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep alias
LoadModule alias_module modules/mod_alias.so
LoadModule vhost_alias_module modules/mod_vhost_alias.so
```

Editez maintenant la section **Default Site Virtual Host** du fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** :

```
[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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
VirtualDocumentRoot /var/www/html/%-3
ServerName i2tch.loc
ServerAlias *.i2tch.loc
ServerAdmin webmaster@localhost
LogLevel info
<Directory />
Options FollowSymLinks
AllowOverride All
Require all granted
</Directory>
</VirtualHost>
##################www.rhelnom.com
<VirtualHost *:80>
ServerName www.rhelnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/rhelnom.log combined
```

```
Errorlog /www/logs/site1/rhelnom_error.log
<Directory /www/site1>
Require all granted
</Directory>
</VirtualHost>
```

Créez le fichier **/var/www/html/.htaccess** afin d'activer la ré-écriture des URLs :

```
[root@centos7 ~]# vi /var/www/html/.htaccess
[root@centos7 ~]# cat /var/www/html/.htaccess
RewriteEngine On
RewriteBase /
```

Re-démarrez le serveur httpd :

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

Creéz maintenant le répertoire **/var/www/html/_** pour contenir le site par défaut :

```
[root@centos7 ~]# mkdir /var/www/html/_
```

Créez la page d'accueil du site par défaut :

```
[root@centos7 ~]# vi /var/www/html/_/index.html
[root@centos7 ~]# cat /var/www/html/_/index.html
<html>
<body>
<center>Accueil du site par défaut</center>
</body>
</html>
```

Créez deux sites **projecta** et **projectb** :

```
[root@centos7 ~]# mkdir /var/www/html/projecta
[root@centos7 ~]# vi /var/www/html/projecta/index.html
[root@centos7 ~]# cat /var/www/html/projecta/index.html
<html>
<body>
<center>Accueil du Project A</center>
</body>
</html>
```

```
[root@centos7 ~]# mkdir /var/www/html/projectb
[root@centos7 ~]# vi /var/www/html/projectb/index.html
[root@centos7 ~]# cat /var/www/html/projectb/index.html
<html>
<body>
<center>Accueil du Project B</center>
</body>
</html>
```

Modifiez l'appartenance du répertoire **/var/www/html** et son contenu :

```
[root@centos7 ~]# chown -R apache:apache /var/www/html
```

Modifiez le fichier **/etc/resolv.conf** en y ajoutant la ligne **nameserver 127.0.0.1** :

```
[root@centos7 ~]# vi /etc/resolv.conf
[root@centos7 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search fenestros.loc
nameserver 127.0.0.1
nameserver 8.8.8.8
```

Re-démarrez le service **NetworkManager** :

```
root@debian9:~# systemctl restart NetworkManager
```

Testez que vous avez accès aux hôtes virtuels :

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


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


[root@centos7 ~]# lynx --dump http://i2tch.loc
                          Accueil du site par défaut


[root@centos7 ~]# lynx --dump http://projecta.i2tch.loc
                             Accueil du Project A


[root@centos7 ~]# lynx --dump http://projectb.i2tch.loc
                             Accueil du Project B


[root@centos7 ~]# lynx --dump http://projectc.i2tch.loc
                                  Not Found

   The requested URL / was not found on this server.
```

Sous Debian 9

Hôte virtuel par nom

Sous **Debian 9** la configuration des hôtes virtuels ne se fait pas de la même façon que sous RHEL / CentOS 7. Sous Debian, les hôtes virtuels sont configurés par des fichiers par hôte dans le répertoire **/etc/apache2/sites-available**. Ils sont activés en créant un lien symbolique dans le répertoire **/etc/apache2/sites-enabled** :

```
root@debian9:~# vi /etc/apache2/sites-available/debiannom.conf
root@debian9:~# cat /etc/apache2/sites-available/debiannom.conf
<VirtualHost *:80>
    ServerName debiannom.com
    ServerAlias www.debiannom.com

    ServerAdmin webmaster@localhost
    DocumentRoot /www/site1

    <Directory "/www/site1">
            AllowOverride None
            Require all granted
    </Directory>

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

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

```
root@debian9:~# mkdir -p /www/site1
```

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

```
root@debian9:~# vi /www/site1/index.html
root@debian9:~# cat /www/site1/index.html
<html>
```

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

Important : Notez qu'Apache servira toujours le contenu du fichier **/etc/apache2/sites-available/000-default.conf** par défaut, sauf précision de la part de l'internaute.

Modifiez l'appartenance du répertoire **/www** et son contenu :

```
root@debian9:~# chown -R www-data:www-data /www
```

Créez ensuite un lien symbolique dans le répertoire **/etc/apache2/sites-enabled** pointant vers le fichier **/etc/apache2/sites-available/debiannom.conf** :

```
root@debian9:~# cd /etc/apache2/sites-enabled/
root@debian9:/etc/apache2/sites-enabled# ln -s ../sites-available/debiannom.conf .
root@debian9:/etc/apache2/sites-enabled# ls -l
total 0
lrwxrwxrwx 1 root root 35 Aug 27 11:08 000-default.conf -> ../sites-available/000-default.conf
lrwxrwxrwx 1 root root 33 Aug 27 18:32 debiannom.conf -> ../sites-available/debiannom.conf
```

Redémarrez ensuite le serveur Apache :

```
root@debian9:/etc/apache2/sites-enabled# systemctl restart apache2
```

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

```
root@debian9:/etc/apache2/sites-enabled# vi /etc/hosts
```

```
root@debian9:/etc/apache2/sites-enabled# cat /etc/hosts
127.0.0.1   localhost
127.0.1.1   debian8.fenestros.loc    debian8

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.0.2.60   i2tch.loc
10.0.2.60   www.i2tch.loc
10.0.2.60   www.debiannom.com
```

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

```
root@debian9:/etc/apache2/sites-enabled# apt-get install lynx
```

Testez votre configuration avec **lynx** :

```
root@debian9:/etc/apache2/sites-enabled# lynx --dump http://www.debiannom.com
                             Accueil du site 1


root@debian9:/etc/apache2/sites-enabled#
```

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/apache2/sites-available/debiannom.conf** et ajoutez les deux lignes suivantes:

```
Customlog /www/logs/site1/debiannom.log combined
Errorlog /www/logs/site1/debiannom_error.log
```

Vous obtiendrez une fenêtre similaire à celle-ci :

debiannom.conf

```
<VirtualHost *:80>
    ServerName debiannom.com
    ServerAlias www.debiannom.com

    ServerAdmin webmaster@localhost
    DocumentRoot /www/site1

    Customlog /www/logs/site1/debiannom.log combined
    Errorlog /www/logs/site1/debiannom_error.log

    <Directory "/www/site1">
            AllowOverride None
            Require all granted
    </Directory>

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Créez ensuite le répertoire /www/logs/site1 :

```
root@debian9:/etc/apache2/sites-enabled# mkdir -p /www/logs/site1
```

Modifiez l'appartenance du répertoire **/www/logs** et son contenu :

```
root@debian9:/etc/apache2/sites-enabled# chown -R www-data:www-data /www/logs
```

Redémarrez le serveur Apache :

```
root@debian9:/etc/apache2/sites-enabled# systemctl restart apache2
```

Testez votre configuration avec **lynx** :

```
root@debian9:/etc/apache2/sites-enabled# lynx --dump http://www.debiannom.com
                             Accueil du site 1


root@debian9:/etc/apache2/sites-enabled#
```

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

```
root@debian9:/etc/apache2/sites-enabled# ls -l /www/logs/site1/
total 4
-rw-r--r-- 1 root root   0 Aug 27 19:34 debiannom_error.log
-rw-r--r-- 1 root root 131 Aug 27 19:35 debiannom.log
```

Ces deux fichiers **debiannom_error.log** et **debiannom.log** sont créés automatiquement par Apache.

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

```
root@debian9:/etc/apache2/sites-enabled# cat /www/logs/site1/debiannom.log
10.0.2.60 - - [27/Aug/2018:19:35:07 +0100] "GET / HTTP/1.0" 200 370 "-" "Lynx/2.8.9dev.1 libwww-FM/2.14 SSL-
MM/1.4.1 GNUTLS/3.3.8"
```

Hôte virtuel par adresse IP

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

```
root@debian9:/etc/apache2/sites-enabled# cd ~
root@debian9:~# ip a | grep 'inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.60/24 brd 10.0.2.255 scope global ens18
```

```
root@debian9:~# ip a add 192.168.1.99/24 dev ens18
root@debian9:~# ip a | grep 'inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.60/24 brd 10.0.2.255 scope global ens18
    inet 192.168.1.99/24 scope global ens18
```

Créez maintenant le répertoire pour notre site2 :

```
root@debian9:~# mkdir /www/site2
```

Créez la page d'accueil :

```
root@debian9:~# vi /www/site2/index.html
root@debian9:~# cat /www/site2/index.html
<html>
<body>
<center>Accueil du site 2</center>
</body>
</html>
```

Créez ensuite le répertoire /www/logs/site2 :

```
root@debian9:~# mkdir /www/logs/site2
```

Modifiez l'appartenance du répertoire **/www** et son contenu :

```
root@debian9:~# chown -R www-data:www-data /www
```

Copiez le fichier **/etc/apache2/sites-available/debiannom.conf** vers **/etc/apache2/sites-available/debianip.conf** :

```
root@debian9:~# cp /etc/apache2/sites-available/debiannom.conf /etc/apache2/sites-available/debianip.conf
```

Editez maintenant le fichier **/etc/apache2/sites-available/debianip.conf**:

```
root@debian9:~# vi /etc/apache2/sites-available/debianip.conf
root@debian9:~# cat /etc/apache2/sites-available/debianip.conf
<VirtualHost 192.168.1.99:80>
    ServerName debianip.com
    ServerAlias www.debianip.com

    ServerAdmin webmaster@localhost
    DocumentRoot /www/site2

    Customlog /www/logs/site2/debianip.log combined
    Errorlog /www/logs/site2/debianip_error.log

    <Directory "/www/site2">
            AllowOverride None
            Require all granted
    </Directory>

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Créez le lien symbolique pour activer le site :

```
root@debian9:~# cd /etc/apache2/sites-enabled
root@debian9:/etc/apache2/sites-enabled# ln -s ../sites-available/debianip.conf .
```

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

```
root@debian9:/etc/apache2/sites-enabled# vi /etc/hosts
root@debian9:/etc/apache2/sites-enabled# cat /etc/hosts
127.0.0.1   localhost
127.0.1.1   debian8.fenestros.loc    debian8

# The following lines are desirable for IPv6 capable hosts
```

```
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
10.0.2.60   i2tch.loc
10.0.2.60   www.i2tch.loc
10.0.2.60   www.debiannom.com
192.168.1.99    www.debianip.com
```

Redémarrez votre serveur Apache :

```
root@debian9:/etc/apache2/sites-enabled# systemctl restart httpd
```

Testez votre configuration avec **lynx** :

```
root@debian9:/etc/apache2/sites-enabled# lynx --dump http://www.debianip.com
                             Accueil du site 2


root@debian9:/etc/apache2/sites-enabled#
```

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

```
root@debian9:/etc/apache2/sites-enabled# ls -l /www/logs/site2/
total 4
-rw-r--r-- 1 root root   0 Aug 27 22:14 debianip_error.log
-rw-r--r-- 1 root root 134 Aug 27 22:17 debianip.log
root@debian9:/etc/apache2/sites-enabled# cat /www/logs/site2/debianip.log
192.168.1.99 - - [27/Aug/2018:22:17:23 +0100] "GET / HTTP/1.0" 200 311 "-" "Lynx/2.8.9dev.1 libwww-FM/2.14 SSL-
MM/1.4.1 GNUTLS/3.3.8"
```

Hôtes Virtuels Dynamiques avec mod_vhost_alias

Commencez par installer le paquet **dnsmasq** afin de fournir les services d'un serveur DNS :

```
root@debian9:/etc/apache2/sites-enabled# cd ~
root@debian9:~# apt-get install dnsmasq
```

Créez le fichier **/etc/dnsmasq.d/i2tch** pour indiquer à dnsmasq que le domaine i2tch.loc se trouve à l'adresse **127.0.0.1** :

```
root@debian9:~# vi /etc/dnsmasq.d/i2tch
root@debian9:~# cat /etc/dnsmasq.d/i2tch
listen-address=127.0.0.1
address=/.i2tch.loc/127.0.0.1
```

Re-démarrez le service dnsmasq pour prendre en compte vos modifications :

```
root@debian9:~# systemctl restart dnsmasq
```

Pour qu'apache puisse gérer les hôtes virtuels dynamiques, il faut que les modules **mod_rewrite** et **mod_vhost_alias** soient activés :

```
root@debian9:~# a2enmod vhost_alias
Enabling module vhost_alias.
To activate the new configuration, you need to run:
  service apache2 restart
root@debian9:~#
root@debian9:~# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  service apache2 restart
```

Editez maintenant le fichier **/etc/apache2/sites-available/000-default.conf** :

```
root@debian9:~# vi /etc/apache2/sites-available/000-default.conf
root@debian9:~# cat /etc/apache2/sites-available/000-default.conf
<VirtualHost *:80>
```

```
    ServerName i2tch.loc
    ServerAlias *.i2tch.loc

    ServerAdmin webmaster@localhost
    VirtualDocumentRoot /var/www/html/%-3

    LogLevel info

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

    <Directory />
        Options FollowSymLinks
        AllowOverride All
    </Directory>

</VirtualHost>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Créez le fichier **/var/www/html/.htaccess** afin d'activer la ré-écriture des URLs :

```
root@debian9:~# vi /var/www/html/.htaccess
root@debian9:~# cat /var/www/html/.htaccess
RewriteEngine On
RewriteBase /
```

Re-démarrez le serveur apache2 :

```
root@debian9:~# systemctl restart apache2
```

Creéz maintenant le répertoire **/var/www/html/_** pour contenir le site par défaut :

```
root@debian9:~# mkdir /var/www/html/_
```

Créez la page d'accueil du site par défaut :

```
root@debian9:~# vi /var/www/html/_/index.html
root@debian9:~# cat /var/www/html/_/index.html
<html>
<body>
<center>Accueil du site par défaut</center>
</body>
</html>
```

Créez deux sites **projecta** et **projectb** :

```
root@debian9:~# mkdir /var/www/html/projecta
root@debian9:~# vi /var/www/html/projecta/index.html
root@debian9:~# cat /var/www/html/projecta/index.html
<html>
<body>
<center>Accueil du Project A</center>
</body>
</html>
```

```
root@debian9:~# mkdir /var/www/html/projectb
root@debian9:~# vi /var/www/html/projectb/index.html
root@debian9:~# cat /var/www/html/projectb/index.html
<html>
<body>
<center>Accueil du Project B</center>
</body>
</html>
```

Modifiez l'appartenance du répertoire **/var/www/html** et son contenu :

```
root@debian9:~# chown -R www-data:www-data /var/www/html
```

Modifiez le fichier **/etc/resolv.conf** en y ajoutant la ligne **nameserver 127.0.0.1** :

```
root@debian9:~# vi /etc/resolv.conf
root@debian9:~# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 127.0.0.1
nameserver 8.8.8.8
```

Re-démarrez le service **NetworkManager** :

```
root@debian9:~# systemctl restart NetworkManager
```

Testez que vous avez accès aux hôtes virtuels :

```
root@debian9:~# lynx --dump http://www.debiannom.com
                             Accueil du site 1

root@debian9:~# lynx --dump http://www.debianip.com
                             Accueil du site 2

root@debian9:~# lynx --dump http://i2tch.loc
                         Accueil du site par défaut

root@debian9:~# lynx --dump http://projecta.i2tch.loc/
                            Accueil du Project A

root@debian9:~# lynx --dump http://projectb.i2tch.loc/
                            Accueil du Project B
```

LAB #2 - Gestion des pages personnelles avec mod_userdir

Sous RHEL / CentOS 7

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 ~]#
```

Sous Debian 9

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

```
root@debian9:~# apachectl -M | grep userdir
root@debian9:~# a2enmod userdir
Enabling module userdir.
To activate the new configuration, you need to run:
  service apache2 restart
root@debian9:~# apachectl -M | grep userdir
 userdir_module (shared)
```

```
root@debian9:~# systemctl restart apache2
```

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

```
root@debian9:~# groupadd homepage
root@debian9:~# useradd homepage -m -c homepage -g homepage -d /home/homepage -s /bin/bash
```

Créez le répertoire /home/homepage/public_html :

```
root@debian9:~# mkdir /home/homepage/public_html
```

Modifiez l'appartenance du répertoire /home/homepage :

```
root@debian9:~# chown -R homepage:homepage /home/homepage
```

Consultez le fichier **/etc/apache2/mods-available/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 :

```
<code>
root@debian9:~# cat  /etc/apache2/mods-available/userdir.conf
<IfModule mod_userdir.c>
        UserDir public_html
        UserDir disabled root

        <Directory /home/*/public_html>
                AllowOverride FileInfo AuthConfig Limit Indexes
                Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
                Require method GET POST OPTIONS
        </Directory>
</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

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

```
root@debian9:~# vi /home/homepage/public_html/index.html
root@debian9:~# 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 **www-data** puisse avoir accès à son contenu :

```
root@debian9:~# chmod 711 /home/homepage
root@debian9:~# chmod 755 /home/homepage/public_html/
root@debian9:~# chmod 666 /home/homepage/public_html/index.html
```

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

```
root@debian9:~# lynx --dump http://localhost/~homepage/
                     La Page de l'utilisateur Homepage


root@debian9:~#
```

Administration Avancée

Important - La suite de ce cours est basée sur l'utilisation de la distribution RHEL / CentOS 7.

LAB #3 - Gestion des pages dynamiques avec mod_php

Introduction

PHP existe en plusieurs versions dont les deux versions courrament utilisées sont :

- La version 5.6
- La version 7.x

Mise en place

Dans ce LAB, vous allez apprendre comment faire co-habiter les deux versions.

Commencez par installer le dépôt EPEL :

```
[root@centos7 ~]# yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

Continuez en installant le dépôt REMI qui contient les différentes versions de PHP dont nous aurons besoin :

```
[root@centos7 ~]# yum install http://rpms.remirepo.net/enterprise/remi-release-7.rpm
```

Installez maintenant les versions 5.6 et 7.2 de PHP :

```
[root@centos7 ~]# yum install yum-utils php56 php72 php56-php-fpm php72-php-fpm -y
```

Par défaut, les deux serveurs FPM écoutent sur le port **9000**. Modifiez le port pour chaque version de PHP :

```
[root@centos7 ~]# sed -i 's/:9000/:9056/' /etc/opt/remi/php56/php-fpm.d/www.conf
[root@centos7 ~]# sed -i 's/:9000/:9072/' /etc/opt/remi/php72/php-fpm.d/www.conf
```

Démarrez les deux serveurs FPM :

```
[root@centos7 ~]# systemctl start php56-php-fpm
[root@centos7 ~]# systemctl status php56-php-fpm
● php56-php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php56-php-fpm.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2018-09-02 16:12:39 CEST; 7s ago
 Main PID: 25889 (php-fpm)
   Status: "Ready to handle connections"
   CGroup: /system.slice/php56-php-fpm.service
           ├─25889 php-fpm: master process (/opt/remi/php56/root/etc/php-fpm.conf)
           ├─25890 php-fpm: pool www
           ├─25891 php-fpm: pool www
           ├─25892 php-fpm: pool www
           ├─25893 php-fpm: pool www
           └─25894 php-fpm: pool www

Sep 02 16:12:39 centos7.fenestros.loc systemd[1]: Starting The PHP FastCGI Process Manager...
Sep 02 16:12:39 centos7.fenestros.loc systemd[1]: Started The PHP FastCGI Process Manager.
[root@centos7 ~]#
[root@centos7 ~]# systemctl start php72-php-fpm
[root@centos7 ~]# systemctl status php72-php-fpm
● php72-php-fpm.service - The PHP FastCGI Process Manager
   Loaded: loaded (/usr/lib/systemd/system/php72-php-fpm.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2018-09-02 16:13:03 CEST; 1s ago
 Main PID: 26083 (php-fpm)
   Status: "Ready to handle connections"
   CGroup: /system.slice/php72-php-fpm.service
           ├─26083 php-fpm: master process (/etc/opt/remi/php72/php-fpm.conf)
           ├─26084 php-fpm: pool www
           ├─26085 php-fpm: pool www
           ├─26086 php-fpm: pool www
           ├─26087 php-fpm: pool www
           └─26088 php-fpm: pool www

Sep 02 16:13:03 centos7.fenestros.loc systemd[1]: Starting The PHP FastCGI Process Manager...
```

```
Sep 02 16:13:03 centos7.fenestros.loc systemd[1]: Started The PHP FastCGI Process Manager.
```

Créez deux scripts CGI pour appeler **php56-cgi** et **php72-cgi** :

```
[root@centos7 ~]# cat > /var/www/cgi-bin/php56.fcgi << EOF
> #!/bin/bash
> exec /bin/php56-cgi
> EOF
[root@centos7 ~]# cat > /var/www/cgi-bin/php72.fcgi << EOF
> #!/bin/bash
> exec /bin/php72-cgi
> EOF
```

Rendez les deux scripts CGI exécutables :

```
[root@centos7 ~]# chmod 755 /var/www/cgi-bin/php56.fcgi
[root@centos7 ~]# chmod 755 /var/www/cgi-bin/php72.fcgi
```

Créez maintenant la configuration php :

```
[root@centos7 ~]# vi /etc/httpd/conf.d/php.conf
[root@centos7 ~]# cat /etc/httpd/conf.d/php.conf
ScriptAlias /cgi-bin/ "/var/www/cgi-bin/"
AddHandler php56-fcgi .php
Action php56-fcgi /cgi-bin/php56.fcgi
Action php72-fcgi /cgi-bin/php72.fcgi

<Directory /var/www/html/_/php56>
    DirectoryIndex index.php
    AllowOverride all
    Require all granted
</Directory>
<Directory /var/www/html/_/php72>
    DirectoryIndex index.php
```

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

Important : Notez que la configuration par défaut exécute le handler **php56-fcgi**.

Créez les pages de test PHP :

```
[root@centos7 ~]# mkdir -p /var/www/html/_/php56
[root@centos7 ~]# mkdir -p /var/www/html/_/php72
[root@centos7 ~]# echo "<?php phpinfo(); ?>" > /var/www/html/_/php56/index.php
[root@centos7 ~]# echo "<?php phpinfo(); ?>" > /var/www/html/_/php72/index.php
```

Indiquez que le handler **php72-fcgi** doit être utilisé dans le répertoire **php72** :

```
[root@centos7 ~]# echo "AddHandler php72-fcgi .php" > /var/www/html/_/php72/.htaccess
```

Re-démarrez le service httpd :

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

Testez maintenant les versions de PHP :

```
[root@centos7 ~]# lynx http://i2tch.loc/php56
phpinfo() (p1 of 20)
   PHP logo

PHP Version 5.6.37

   System Linux centos7.fenestros.loc 3.10.0-693.21.1.el7.x86_64 #1 SMP Wed Mar 7 19:03:37 UTC 2018 x86_64
   Build Date Jul 19 2018 19:35:58
```

```
   Server API CGI/FastCGI
   Virtual Directory Support disabled
   Configuration File (php.ini) Path /opt/remi/php56/root/etc
   Loaded Configuration File /opt/remi/php56/root/etc/php.ini
   Scan this dir for additional .ini files /opt/remi/php56/root/etc/php.d
   Additional .ini files parsed /opt/remi/php56/root/etc/php.d/20-bz2.ini, /opt/remi/php56/root/etc/php.d/20-
calendar.ini,
   /opt/remi/php56/root/etc/php.d/20-ctype.ini, /opt/remi/php56/root/etc/php.d/20-curl.ini,
/opt/remi/php56/root/etc/php.d/20-dom.ini,
   /opt/remi/php56/root/etc/php.d/20-exif.ini, /opt/remi/php56/root/etc/php.d/20-fileinfo.ini,
/opt/remi/php56/root/etc/php.d/20-ftp.ini,
   /opt/remi/php56/root/etc/php.d/20-gettext.ini, /opt/remi/php56/root/etc/php.d/20-iconv.ini,
/opt/remi/php56/root/etc/php.d/20-phar.ini,
   /opt/remi/php56/root/etc/php.d/20-posix.ini, /opt/remi/php56/root/etc/php.d/20-shmop.ini,
/opt/remi/php56/root/etc/php.d/20-simplexml.ini,
   /opt/remi/php56/root/etc/php.d/20-sockets.ini, /opt/remi/php56/root/etc/php.d/20-sysvmsg.ini,
/opt/remi/php56/root/etc/php.d/20-sysvsem.ini,
   /opt/remi/php56/root/etc/php.d/20-sysvshm.ini, /opt/remi/php56/root/etc/php.d/20-tokenizer.ini,
/opt/remi/php56/root/etc/php.d/20-xml.ini,
   /opt/remi/php56/root/etc/php.d/20-xmlwriter.ini, /opt/remi/php56/root/etc/php.d/20-xsl.ini,
/opt/remi/php56/root/etc/php.d/30-wddx.ini,
   /opt/remi/php56/root/etc/php.d/30-xmlreader.ini, /opt/remi/php56/root/etc/php.d/40-json.ini,
/opt/remi/php56/root/etc/php.d/40-zip.ini
   PHP API 20131106
   PHP Extension 20131226
   Zend Extension 220131226
   Zend Extension Build API220131226,NTS
   PHP Extension Build API20131226,NTS
   Debug Build no
   Thread Safety disabled
   Zend Signal Handling disabled
   Zend Memory Manager enabled
   Zend Multibyte Support disabled
   IPv6 Support enabled
```

```
   DTrace Support available, disabled
   Registered PHP Streams https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar, zip
   Registered Stream Socket Transports tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
   Registered Stream Filters zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*,
consumed, dechunk, bzip2.*, convert.iconv.*
   Zend logo This program makes use of the Zend Scripting Language Engine:
...
```

```
[root@centos7 ~]# lynx http://i2tch.loc/php72
phpinfo() (p1 of 18)
   PHP logo

PHP Version 7.2.9

   System Linux centos7.fenestros.loc 3.10.0-693.21.1.el7.x86_64 #1 SMP Wed Mar 7 19:03:37 UTC 2018 x86_64
   Build Date Aug 15 2018 08:05:24
   Server API CGI/FastCGI
   Virtual Directory Support disabled
   Configuration File (php.ini) Path /etc/opt/remi/php72
   Loaded Configuration File /etc/opt/remi/php72/php.ini
   Scan this dir for additional .ini files /etc/opt/remi/php72/php.d
   Additional .ini files parsed /etc/opt/remi/php72/php.d/20-bz2.ini, /etc/opt/remi/php72/php.d/20-calendar.ini,
/etc/opt/remi/php72/php.d/20-ctype.ini,
   /etc/opt/remi/php72/php.d/20-curl.ini, /etc/opt/remi/php72/php.d/20-exif.ini, /etc/opt/remi/php72/php.d/20-
fileinfo.ini, /etc/opt/remi/php72/php.d/20-ftp.ini,
   /etc/opt/remi/php72/php.d/20-gettext.ini, /etc/opt/remi/php72/php.d/20-iconv.ini,
/etc/opt/remi/php72/php.d/20-json.ini, /etc/opt/remi/php72/php.d/20-phar.ini,
   /etc/opt/remi/php72/php.d/20-sockets.ini, /etc/opt/remi/php72/php.d/20-tokenizer.ini
   PHP API 20170718
   PHP Extension 20170718
   Zend Extension 320170718
   Zend Extension Build API320170718,NTS
   PHP Extension Build API20170718,NTS
   Debug Build no
```

```
   Thread Safety disabled
   Zend Signal Handling enabled
   Zend Memory Manager enabled
   Zend Multibyte Support disabled
   IPv6 Support enabled
   DTrace Support available, disabled
   Registered PHP Streams https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
   Registered Stream Socket Transports tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
   Registered Stream Filters zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*,
consumed, dechunk, bzip2.*, convert.iconv.*
   Zend logo This program makes use of the Zend Scripting Language Engine:
   Zend Engine v3.2.0, Copyright (c) 1998-2018 Zend Technologies
________________________________________________________________________________________________________________
_____________________________________________

Configuration
...
```

LAB #4 - Gestion de l'authentification avec .htpasswd et 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@centos7 ~]# vi /www/site1/secret/.htaccess
[root@centos7 ~]# cat /www/site1/secret/.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
[root@centos7 ~]# cat /www/site1/secret/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.rhelip.com
```

```
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
###################Default Site Virtual Host
<VirtualHost *:80>
VirtualDocumentRoot /var/www/html/%-3
ServerName i2tch.loc
ServerAlias *.i2tch.loc
ServerAdmin webmaster@localhost
LogLevel info
<Directory />
Options FollowSymLinks
AllowOverride All
Require all granted
</Directory>
</VirtualHost>
###################www.rhelnom.com
<VirtualHost *:80>
ServerName www.rhelnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/rhelnom.log combined
Errorlog /www/logs/site1/rhelnom_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 :

```
[root@centos7 ~]# curl http://www.rhelnom.com/secret/index.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
[root@centos7 ~]#
[root@centos7 ~]# curl -u webmaster:fenestros http://www.rhelnom.com/secret/index.html
<html>
<body>
<center>Si vous voyez ce message, vous avez decouvert mon secret !</center>
</body>
</html>
```

LAB #5 - Gestion de l'authentification avec MariaDB et mod_authn_dbd

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

Installation

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

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

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 :

```
CREATE DATABASE auth;
```

```
USE auth;
```

```
CREATE TABLE users (
    user_name VARCHAR(50) NOT NULL,
    user_passwd VARCHAR(50) NOT NULL,
    PRIMARY KEY (user_name)
    );
```

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

Par exemple :

```
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: fenestros
[root@centos7 ~]# mysql -u root -p -e "SELECT * FROM auth.users;"
Enter password: fenestros
+-----------+-------------------------------------+
| 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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
VirtualDocumentRoot /var/www/html/%-3
ServerName i2tch.loc
ServerAlias *.i2tch.loc
ServerAdmin webmaster@localhost
LogLevel info
<Directory />
Options FollowSymLinks
AllowOverride All
Require all granted
</Directory>
</VirtualHost>
##################www.rhelnom.com
```

```
<VirtualHost *:80>
ServerName www.rhelnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/rhelnom.log combined
Errorlog /www/logs/site1/rhelnom_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
```

Testez ensuite votre section privée :

```
[root@centos7 ~]# curl -u webmaster:fenestros http://www.rhelnom.com/secret/index.html
```

```
<html>
<body>
<center>Si vous voyez ce message, vous avez decouvert mon secret !</center>
</body>
</html>
[root@centos7 ~]# curl -u webmaster:fenestros http://www.rhelnom.com/secret2/index.html
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
[root@centos7 ~]# curl -u apache:password http://www.rhelnom.com/secret2/index.html
<html>
<body>
<center>Si vous voyez ce message, vous connaissez mon secret MariaDB !</center>
</body>
</html>
```

LAB #6 - Gestion de l'authentification avec OpenLDAP et 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
```

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.
```

Configuration d'OpenLDAP

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}RRo5UcZ9zzb2nYZuE5ZH+74u/Y2cyco2
```

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}RRo5UcZ9zzb2nYZuE5ZH+74u/Y2cyco2
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@centos7 ~]# 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
```

Configuration d'Apache

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>
...
```

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 :

```
[root@centos7 ~]# curl http://localhost
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
browser doesn't understand how to supply
the credentials required.</p>
</body></html>
```

```
[root@centos7 ~]#
[root@centos7 ~]# curl -u jean:secret1 http://localhost
<html>
<body>
<center>Accueil du site par défaut</center>
</body>
</html>
```

Préparer la Suite de la Formation

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
```

LAB #7 - Gestion des pages web sécurisées en https avec 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 :

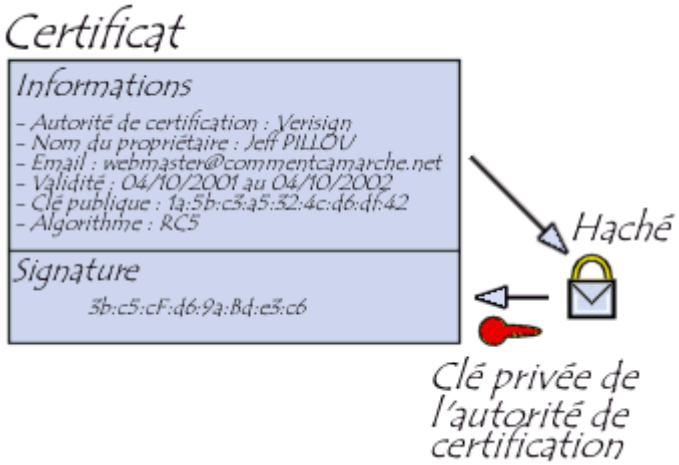
- La partie contenant les informations
- La partie contenant la signature de l'autorité de certification

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

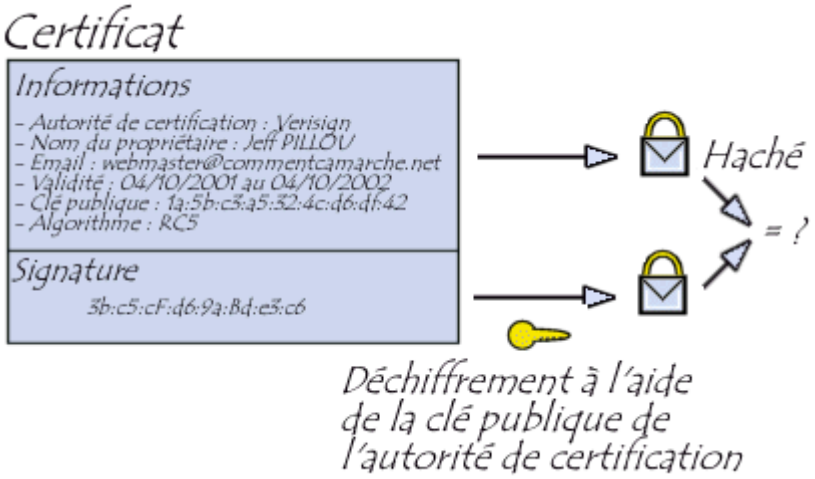
Elle contient :

- 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
```

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.i2tch.loc.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.i2tch.loc.key -out www.i2tch.loc.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) []:www.i2tch.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.i2tch.loc.csr -signkey www.i2tch.loc.key -out
www.i2tch.loc.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.i2tch.loc.key /etc/pki/tls/private/
[root@centos7 ~]# cp /root/www.i2tch.loc.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.i2tch.loc.crt
SSLCertificateKeyFile /etc/pki/tls/private/www.i2tch.loc.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.i2tch.loc: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 curl :

```
[root@centos7 ~]# curl -k https://www.i2tch.loc
<html>
```

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

Avec Apache 2.2.12 et OpenSSL v0.9.8j et versions ultérieurs, il est possible d'utiliser **TLS Extension Server Name Indication (SNI)** afin d'utiliser des certificats différents pour chaque hôte virtuel.

Par exemple :

```
NameVirtualHost *:443

<VirtualHost *:443>
 ServerName www.yoursite.com
 DocumentRoot /var/www/site
 SSLEngine on
 SSLCertificateFile /path/to/www_yoursite_com.crt
 SSLCertificateKeyFile /path/to/www_yoursite_com.key
 SSLCertificateChainFile /path/to/DigiCertCA.crt
</VirtualHost>

<VirtualHost *:443>
 ServerName www.yoursite2.com
 DocumentRoot /var/www/site2
 SSLEngine on
 SSLCertificateFile /path/to/www_yoursite2_com.crt
 SSLCertificateKeyFile /path/to/www_yoursite2_com.key
 SSLCertificateChainFile /path/to/DigiCertCA.crt
</VirtualHost>
```

LAB #8 - Gestion d'un Serveur Mandataire avec mod_proxy

Sous RHEL / CentOS 7 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
    Require ip 10.0.2.0/24
</Proxy>
</IfModule>
```

Sauvegardez le fichier et 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 :

```
[root@centos7 ~]# curl --proxy http://127.0.0.1 http://www.redhat.com
curl: (7) Failed connect to 127.0.0.1:1080; Connection refused
[root@centos7 ~]# curl --proxy http://127.0.0.1:8081 http://www.redhat.com
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>301 Moved Permanently</title>
</head><body>
<h1>Moved Permanently</h1>
<p>The document has moved <a href="https://www.redhat.com/">here</a>.</p>
</body></html>
[root@centos7 ~]# curl --proxy http://127.0.0.1:8081 http://www.microsoft.com
<html><head><title>Microsoft Corporation</title><meta http-equiv="X-UA-Compatible"
content="IE=EmulateIE7"></meta><meta http-equiv="Content-Type" content="text/html; charset=utf-8"></meta><meta
name="SearchTitle" content="Microsoft.com" scheme=""></meta><meta name="Description" content="Get product
information, support, and news from Microsoft." scheme=""></meta><meta name="Title" content="Microsoft.com Home
Page" scheme=""></meta><meta name="Keywords" content="Microsoft, product, support, help, training, Office,
Windows, software, download, trial, preview, demo,  business, security, update, free, computer, PC, server,
search, download, install, news" scheme=""></meta><meta name="SearchDescription" content="Microsoft.com Homepage"
scheme=""></meta></head><body><p>Your current User-Agent string appears to be from an automated process, if this
is incorrect, please click this link:<a href="http://www.microsoft.com/en/us/default.aspx?redir=true">United
States English Microsoft Homepage</a></p></body></html>
```

Consultez votre fichier de log **access**. Vous constaterez un résultat similaire à celui-ci :

```
[root@centos7 ~]# tail /var/log/httpd/access_log
10.0.2.51 - - [02/Sep/2018:17:21:00 +0200] "GET /php72/ HTTP/1.0" 200 886 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14
SSL-MM/1.4.1 OpenSSL/1.0.1e-fips"
```

```
10.0.2.51 - - [02/Sep/2018:17:25:29 +0200] "GET /php72 HTTP/1.0" 301 231 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14
SSL-MM/1.4.1 OpenSSL/1.0.1e-fips"
10.0.2.51 - - [02/Sep/2018:17:25:31 +0200] "GET /php72/ HTTP/1.0" 200 64036 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14
SSL-MM/1.4.1 OpenSSL/1.0.1e-fips"
10.0.2.51 - - [02/Sep/2018:17:28:21 +0200] "GET /php56 HTTP/1.0" 301 231 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14
SSL-MM/1.4.1 OpenSSL/1.0.1e-fips"
10.0.2.51 - - [02/Sep/2018:17:28:23 +0200] "GET /php56/ HTTP/1.0" 200 68473 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14
SSL-MM/1.4.1 OpenSSL/1.0.1e-fips"
127.0.0.1 - jean [02/Sep/2018:18:15:32 +0200] "GET / HTTP/1.1" 200 75 "-" "curl/7.29.0"
127.0.0.1 - - [02/Sep/2018:18:15:49 +0200] "GET / HTTP/1.1" 401 381 "-" "curl/7.29.0"
127.0.0.1 - - [02/Sep/2018:18:28:31 +0200] "GET / HTTP/1.1" 200 75 "-" "curl/7.29.0"
127.0.0.1 - - [02/Sep/2018:22:27:20 +0200] "GET http://www.redhat.com/ HTTP/1.1" 301 231 "-" "curl/7.29.0"
127.0.0.1 - - [02/Sep/2018:22:27:33 +0200] "GET http://www.microsoft.com/ HTTP/1.1" 200 1020 "-" "curl/7.29.0"
```

LAB #9 - Gestion du Web-based Distributed Authoring and Versioning avec 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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
VirtualDocumentRoot /var/www/html/%-3
ServerName i2tch.loc
ServerAlias *.i2tch.loc
ServerAdmin webmaster@localhost
LogLevel info
<Directory />
Options FollowSymLinks
AllowOverride All
Require all granted
</Directory>
</VirtualHost>
##################www.rhelnom.com
```

```
<VirtualHost *:80>
ServerName www.rhelnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/rhelnom.log combined
Errorlog /www/logs/site1/rhelnom_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
10.0.2.51   i2tch.com
10.0.2.51   *.i2tch.loc
10.0.2.51       www.rhelnom.com
192.168.1.99    www.rhelip.com
10.0.2.51   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**.

Installez Cadaver :

```
[root@centos7 ~]yum install cadaver
```

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  Sep  2 23:37
dav:/> cat dav.test
Displaying `/dav.test':
test
dav:/> exit
Connection to `dav.homeland.net' closed.
[root@centos7 ~]#
```

LAB #10 - Gestion de la réécriture d'URL avec 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
```

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 **/www/site2/** et éditez-la ainsi :

```
[root@centos7 ~]# vi /www/site2/maintenance.html
[root@centos7 ~]# cat /www/site2/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 :

```
[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.rhelip.com
```

```
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
AllowOverride All
</Directory>
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.rhelip.com
   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 **/www/site2/** :

```
[root@centos7 ~]# vi /www/site2/bye.html
[root@centos7 ~]# cat /www/site2/bye.html
<html>
<head>
<title>Aurevoir</title>
</head>
<body>
<center>Bye bye Pirate ! Ha! Ha! Ha!</center>
</body>
</html>
```

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

```
[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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
AllowOverride All
</Directory>
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
RewriteCond %{REMOTE_ADDR} ^192\.168\.1\.99$
RewriteCond %{REQUEST_URI} !^bye\.html
RewriteRule .* /bye.html
```

```
</VirtualHost>
...
```

Important - 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.rhelip.com
                       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 **/www/site2/**.

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

```
[root@centos7 ~]# touch /www/site2/oldpage.html
[root@centos7 ~]# vi /www/site2/newpage.html
[root@centos7 ~]# cat /www/site2/newpage.html
<html>
```

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

Editez ensuite le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** en y ajoutant la ligne suivante :

```
[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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
AllowOverride All
</Directory>
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^192\.168\.1\.99$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
</VirtualHost>
...
```

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.rhelip.com/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 **/etc/httpd/conf/vhosts.d/Vhosts.conf** en y ajoutant la ligne suivante :

```
[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.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
AllowOverride All
</Directory>
```

```
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^192\.168\.1\.99$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
#RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
RewriteRule ^/oldpage\.html - [G]
</VirtualHost>
...
```

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.rhelip.com/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.
```

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.

Par exemple, nous souhaitons rediriger les URLs de format suivant **www.exampledomain.com/en/product1234/product_detail.php** vers les URLs de format suivant **www.exampledomain.com/en/travelbox_12/product_detail.php**.

On commence par créer une table de correspondance :

```
vi /etc/apache2/conf.d/productrewrites.txt

cat /etc/apache2/conf.d/productrewrites.txt
product1234 travelbox_12
product1235 travelbox_13
product2310 case_07
product3126 case_12
product9320 anotheritem_54
...
```

On crée une base de données avec l'utilitaire **httxt2dbm** :

```
httxt2dbm -f db -i /etc/apache2/conf.d/productrewrites.txt -o /etc/apache2/conf.d/productrewrites.db
```

puis on utilise les règles suivantes :

```
RewriteEngine On
RewriteMap rewrites dbm=db:/etc/apache2/conf.d/productrewrites.db
RewriteCond {rewrites:$1} !=""
RewriteRule ^/(.*)/(.*)/(.*)$ http://www.exampledomain.com/(.*)/${rewrites:$1}/$2? [R=permanent,L]
```

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

A Faire - 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

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

soit une expression :

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

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

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

RewriteRule

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

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

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

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

Cette chaîne peut contenir des variables :

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

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

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

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

Drapeaux	Description
[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**.

HERE

LAB #11 - Personnalisation des en-têtes de requêtes et de réponses HTTP avec 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** :

```
[root@centos7 ~]# vi /etc/httpd/conf.d/ssl.conf
[root@centos7 ~]# 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"

##
```

```
...
```

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>
VirtualDocumentRoot /var/www/html/%-3
ServerName i2tch.loc
ServerAlias *.i2tch.loc
ServerAdmin webmaster@localhost
LogLevel info
<Directory />
Options FollowSymLinks
AllowOverride All
Require all granted
</Directory>
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
##################www.rhelnom.com
...
```

Rechargez la configuration d'apache :

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

Testez ensuite avec un navigateur le lien **http://i2tch.loc** :

```
[root@centos7 ~]# lynx --dump http://i2tch.loc

Looking up i2tch.loc
Making HTTP connection to i2tch.loc
Sending HTTP request.
HTTP request sent; waiting for response.
HTTP/1.1 302 Found
Data transfer complete
HTTP/1.1 302 Found
Using https://i2tch.loc/
Looking up i2tch.loc
Making HTTPS connection to i2tch.loc
SSL callback:self signed certificate, preverify_ok=0, ssl_okay=0
Retrying connection without TLS.
Looking up i2tch.loc
Making HTTPS connection to i2tch.loc
Alert!: Unable to make secure connection to remote host.

lynx: Can't access startfile http://i2tch.loc/
```

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 ~]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 ~]# cat /etc/httpd/conf/vhosts.d/Vhosts.conf | more
################## IP-based Virtual Hosts
<VirtualHost 192.168.1.99>
DocumentRoot /www/site2
ServerName www.rhelip.com
DirectoryIndex index.html
Customlog /www/logs/site2/rhelip.log combined
Errorlog /www/logs/site2/rhelip_error.log
<Directory /www/site2>
Require all granted
AllowOverride All
</Directory>
RewriteEngine on
#RewriteRule ^/$ /maintenance.html [R]
#RewriteCond %{REMOTE_ADDR} ^192\.168\.1\.99$
#RewriteCond %{REQUEST_URI} !^bye\.html
#RewriteRule .* /bye.html
#RewriteRule ^/oldpage\.html /newpage.html [R=301,L]
RewriteRule ^/oldpage\.html - [G]
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
VirtualDocumentRoot /var/www/html/%-3
ServerName i2tch.loc
ServerAlias *.i2tch.loc
ServerAdmin webmaster@localhost
LogLevel info
<Directory />
Options FollowSymLinks
AllowOverride All
Require all granted
```

```
</Directory>
#RewriteEngine on
#RewriteCond %{HTTPS} off
#RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}
</VirtualHost>
##################www.rhelnom.com
<VirtualHost *:80>
--More--
```

Dernièrement, re-démarrez apache :

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

LAB #12 - L'exécution des scripts CGI sous l'utilisateur et le groupe spécifiés avec 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 :

```
[root@centos7 cgi-bin]# tail /var/log/httpd/error_log
[Mon Sep 03 00:51:39.292823 2018] [mpm_prefork:notice] [pid 1136] AH00170: caught SIGWINCH, shutting down
gracefully
[Mon Sep 03 00:51:40.387480 2018] [core:notice] [pid 3484] SELinux policy enabled; httpd running as context
system_u:system_r:httpd_t:s0
[Mon Sep 03 00:51:40.388881 2018] [suexec:notice] [pid 3484] AH01232: suEXEC mechanism enabled (wrapper:
/usr/sbin/suexec)
[Mon Sep 03 00:51:40.412024 2018] [alias:warn] [pid 3484] AH00671: The ScriptAlias directive in
/etc/httpd/conf.d/php.conf at line 1 will probably never match because it overlaps an earlier ScriptAlias.
[Mon Sep 03 00:51:40.413924 2018] [auth_digest:notice] [pid 3484] AH01757: generating secret for digest
```

```
authentication ...
[Mon Sep 03 00:51:40.414925 2018] [lbmethod_heartbeat:notice] [pid 3484] AH02282: No slotmem from
mod_heartmonitor
[Mon Sep 03 00:51:40.420110 2018] [mpm_prefork:notice] [pid 3484] AH00163: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-
fips configured -- resuming normal operations
[Mon Sep 03 00:51:40.420256 2018] [core:notice] [pid 3484] AH00094: Command line: '/usr/sbin/httpd -D FOREGROUND'
[Mon Sep 03 01:00:45.867408 2018] [cgi:error] [pid 3489] [client 127.0.0.1:57982] AH01215: (13)Permission denied:
exec of '/var/www/cgi-bin/whoami.cgi' failed
[Mon Sep 03 01:00:45.867459 2018] [cgi:error] [pid 3489] [client 127.0.0.1:57982] End of script output before
headers: whoami.cgi
```

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

```
[root@centos7 cgi-bin]# ls -l
total 12
-rwxr-xr-x. 1 root root 32 Sep  2 16:14 php56.fcgi
-rwxr-xr-x. 1 root root 32 Sep  2 16:14 php72.fcgi
-rwxr--r--. 1 root root 87 Sep  3 01:00 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

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

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 Sep  3 01:00 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 dans le fichier **/etc/httpd/conf/httpd.conf** :

```
...
```

```
#
# "/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
[Mon Sep 03 01:09:02.891762 2018] [alias:warn] [pid 11365] AH00671: The ScriptAlias directive in
/etc/httpd/conf.d/php.conf at line 1 will probably never match because it overlaps an earlier ScriptAlias.
AH00548: NameVirtualHost has no effect and will be removed in the next release
/etc/httpd/conf/vhosts.d/Vhosts.conf:21
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

[root@centos7 scripts]#
```

LAB #13 - Améliorer l'utilisation de la Mémoire du Serveur avec mod_worker

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

Ajoutez la section suivante au fichier **/etc/httpd/conf.d/local.conf** pour pouvoir gérer **800** connexions simultanées :

```
[root@centos7 ~]# vi /etc/httpd/conf.d/local.conf
[root@centos7 ~]# more /etc/httpd/conf.d/local.conf
ServerTokens OS
Timeout 60
KeepAlive Off
MaxKeepAliveRequests 100
KeepAliveTimeout 15
<IfModule prefork.c>
StartServers       8
MinSpareServers    5
MaxSpareServers   20
ServerLimit      256
MaxClients       256
MaxRequestsPerChild  4000
</IfModule>
<IfModule worker.c>
ServerLimit              25
```

```
StartServers              10
MinSpareThreads           75
MaxSpareThreads     250
ThreadLimit               64
ThreadsPerChild           32
MaxClients          800
MaxRequestsPerChild   10000
</IfModule>
--More--(22%)
```

A faire - Voir la page **https://httpd.apache.org/docs/2.4/fr/mod/worker.html** pour une description des directives.

Ouvrez maintenant le fichier **/etc/httpd/conf.modules.d/00-mpm.conf**, commentez la directive **LoadModule mpm_prefork_module modules/mod_mpm_prefork.so** et décommentez la directive **LoadModule mpm_worker_module modules/mod_mpm_worker.so** :

```
[root@centos7 ~]# vi /etc/httpd/conf.modules.d/00-mpm.conf
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-mpm.conf
# Select the MPM module which should be used by uncommenting exactly
# one of the following LoadModule lines:

# prefork MPM: Implements a non-threaded, pre-forking web server
# See: http://httpd.apache.org/docs/2.4/mod/prefork.html
#LoadModule mpm_prefork_module modules/mod_mpm_prefork.so

# worker MPM: Multi-Processing Module implementing a hybrid
# multi-threaded multi-process web server
# See: http://httpd.apache.org/docs/2.4/mod/worker.html
#
LoadModule mpm_worker_module modules/mod_mpm_worker.so

# event MPM: A variant of the worker MPM with the goal of consuming
```

```
# threads only for connections with active processing
# See: http://httpd.apache.org/docs/2.4/mod/event.html
#
#LoadModule mpm_event_module modules/mod_mpm_event.so
```

Important - Le MPM Worker n'est pas comptible avec PHP.

Redémarrez ensuite apache :

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

Consultez les adresses http://127.0.0.1/server-status et http://127.0.0.1/server-info pour vérifier que votre apache utilise le MPM worker :

```
[root@centos7 ~]# lynx http://127.0.0.1/server-status
Apache Status (p1 of 2)
                                                    Apache Server Status for 127.0.0.1 (via 127.0.0.1)

   Server Version: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
   Server MPM: worker
   Server Built: Jun 27 2018 13:48:59
_____________________________________________________________________________________________________
_____________________________________

   Current Time: Monday, 03-Sep-2018 01:16:18 CEST
   Restart Time: Monday, 03-Sep-2018 01:15:56 CEST
   Parent Server Config. Generation: 1
   Parent Server MPM Generation: 0
   Server uptime: 22 seconds
   Server load: 0.00 0.02 0.07
   Total accesses: 0 - Total Traffic: 0 kB
   CPU Usage: u0 s0 cu0 cs0
```

```
   0 requests/sec - 0 B/second -
   1 requests currently being processed, 223 idle workers

.............................._____________________________________
______________________________________________________________________
_____________________________________________________W_____________
.....................................................................
_____________________________________________________________________
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
..............................

   Scoreboard Key:
   "_" Waiting for Connection, "S" Starting up, "R" Reading Request,
   "W" Sending Reply, "K" Keepalive (read), "D" DNS Lookup,
   "C" Closing connection, "L" Logging, "G" Gracefully finishing,
...
```

```
[root@centos7 ~]# lynx http://127.0.0.1/server-info
Server Information (p1 of 59)
                                                                Apache Server Information

   Subpages:
          Configuration Files, Server Settings, Module List, Active Hooks, Available Providers
_____________________________________________________________________________________________________________
_____________________________________

   Sections:
          Loaded Modules, Server Settings, Startup Hooks, Request Hooks, Other Hooks, Providers
```

```
_____________________________________________________

Loaded Modules

   core.c, http_core.c, mod_access_compat.c, mod_actions.c, mod_alias.c, mod_allowmethods.c, mod_auth_basic.c,
mod_auth_digest.c, mod_authn_anon.c,
          mod_authn_core.c, mod_authn_dbd.c, mod_authn_dbm.c, mod_authn_file.c, mod_authn_socache.c,
mod_authnz_ldap.c, mod_authz_core.c, mod_authz_dbd.c,
          mod_authz_dbm.c, mod_authz_groupfile.c, mod_authz_host.c, mod_authz_owner.c, mod_authz_user.c,
mod_autoindex.c, mod_cache.c, mod_cache_disk.c,
          mod_cgid.c, mod_data.c, mod_dav.c, mod_dav_fs.c, mod_dav_lock.c, mod_dbd.c, mod_deflate.c, mod_dir.c,
mod_dumpio.c, mod_echo.c, mod_env.c, mod_expires.c,
          mod_ext_filter.c, mod_filter.c, mod_headers.c, mod_include.c, mod_info.c, mod_lbmethod_bybusyness.c,
mod_lbmethod_byrequests.c, mod_lbmethod_bytraffic.c,
          mod_lbmethod_heartbeat.c, mod_log_config.c, mod_logio.c, mod_lua.c, mod_mime.c, mod_mime_magic.c,
mod_negotiation.c, mod_proxy.c, mod_proxy_ajp.c,
          mod_proxy_balancer.c, mod_proxy_connect.c, mod_proxy_express.c, mod_proxy_fcgi.c, mod_proxy_fdpass.c,
mod_proxy_ftp.c, mod_proxy_http.c,
          mod_proxy_scgi.c, mod_proxy_wstunnel.c, mod_remoteip.c, mod_reqtimeout.c, mod_rewrite.c,
mod_setenvif.c, mod_slotmem_plain.c, mod_slotmem_shm.c,
          mod_so.c, mod_socache_dbm.c, mod_socache_memcache.c, mod_socache_shmcb.c, mod_ssl.c, mod_status.c,
mod_substitute.c, mod_suexec.c, mod_systemd.c,
          mod_unique_id.c, mod_unixd.c, mod_userdir.c, mod_version.c, mod_vhost_alias.c, util_ldap.c, worker.c,
_____________________________________________________

Server Settings

   Server Version: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips
   Server Built: Jun 27 2018 13:48:59
   Server loaded APR Version: 1.4.8
   Compiled with APR Version: 1.4.8
   Server loaded APU Version: 1.5.2
```

```
   Compiled with APU Version: 1.5.2
   Module Magic Number: 20120211:24
   Hostname/port: 127.0.0.1:80
   Timeouts: connection: 60    keep-alive: 15
   MPM Name: worker
...
```

Le Serveur Mandataire Squid

Squid est un serveur mandataire (proxy cache) sous Linux. Squid permet d'accélérer l'accès à Internet en stockant des fichiers reçus des sites visités en mémoire cache. Notez, cependant que Squid n'est pas un serveur proxy pour les protocoles POP, SMTP et NNTP car il ne peut traiter que les protocoles HTTP et FTP et d'une manière limitée les protocoles TLS, SSL, Internet Gopher et HTTPS.

Il est utile de noter ici qu'un serveur proxy utilise beaucoup d'espace disque pour le cache et pour ses logs. Dans la mesure du possible donc, il faut prévoir une partition à part, d'une taille importante pour le cache et éventuellement une autre partition pour les fichiers logs.

LAB #14 - Installation et Configuration de Squid

Utilisez yum :

```
# yum install squid [Entrée]
```

```
[root@centos6 ~]# yum install squid
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
```

```
--> Running transaction check
---> Package squid.i686 7:3.1.10-1.el6_2.4 set to be updated
--> Processing Dependency: perl(DBI) for package: 7:squid-3.1.10-1.el6_2.4.i686
--> Running transaction check
---> Package perl-DBI.i686 0:1.609-4.el6 set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                 Arch                                 Version
Repository                              Size
================================================================================
================================================================================
Installing:
 squid                                   i686                                 7:3.1.10-1.el6_2.4
updates                                1.7 M
Installing for dependencies:
 perl-DBI                                i686                                 1.609-4.el6
base                                   705 k

Transaction Summary
================================================================================
================================================================================
Install       2 Package(s)
Upgrade       0 Package(s)

Total download size: 2.4 M
Installed size: 7.3 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): perl-DBI-1.609-4.el6.i686.rpm
| 705 kB     00:00
```

```
(2/2): squid-3.1.10-1.el6_2.4.i686.rpm
| 1.7 MB     00:01
--------------------------------------------------------------------------------------------------------------
--------------------------------------------------
Total
1.2 MB/s | 2.4 MB     00:01
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : perl-DBI-1.609-4.el6.i686
1/2
  Installing     : 7:squid-3.1.10-1.el6_2.4.i686
2/2

Installed:
  squid.i686 7:3.1.10-1.el6_2.4

Dependency Installed:
  perl-DBI.i686 0:1.609-4.el6

Complete!
```

Configurez ensuite le service squid pour un démarrage automatique à chaque démarrage du système :

```
[root@centos6 ~]# chkconfig --level 345 squid on
[root@centos6 ~]# chkconfig --list squid
squid           0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Les options de cette commande sont :

```
[root@centos6 squidguard]# squid -h
Usage: squid [-cdhvzCFNRVYX] [-s | -l facility] [-f config-file] [-[au] port] [-k signal]
       -a port   Specify HTTP port number (default: 3128).
```

```
       -d level  Write debugging to stderr also.
       -f file   Use given config-file instead of
                 /etc/squid/squid.conf
       -h        Print help message.
       -k reconfigure|rotate|shutdown|interrupt|kill|debug|check|parse
                 Parse configuration file, then send signal to
                 running copy (except -k parse) and exit.
       -s | -l facility
                 Enable logging to syslog.
       -u port   Specify ICP port number (default: 3130), disable with 0.
       -v        Print version.
       -z        Create swap directories
       -C        Do not catch fatal signals.
       -D        OBSOLETE. Scheduled for removal.
       -F        Don't serve any requests until store is rebuilt.
       -N        No daemon mode.
       -R        Do not set REUSEADDR on port.
       -S        Double-check swap during rebuild.
       -X        Force full debugging.
       -Y        Only return UDP_HIT or UDP_MISS_NOFETCH during fast reload.
```

Créez maintenant un fichier squid.conf sans commentaires :

```
[root@centos6 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/squid/squid.conf > squid.conf
```

Ouvrez le fichier **/tmp/squid.conf** avec l'éditeur de votre choix. Ajoutez les directives ci-dessous.

Cette directive stipule la taille en Mo, ici 124 MB, du cache en mémoire :

```
cache_mem 124 MB
```

Cette directive spécifie l'endroit et la taille, ici 3 641 Mo, du cache sur disque :

```
cache_dir ufs /var/spool/squid 3641 16 256
```

Cette directive correspond à la règle nécessaire pour que les machines du réseau local puissent se connecter à Squid :

```
acl mynetwork src 10.0.2.0/24
```

Cette directive spécifie l'emplacement du fichier log qui contiendra une entrée pour chaque requête d'un client :

```
cache_access_log /var/log/squid/access.log
```

Cette directive spécifie l'emplacement du fichier log général :

```
cache_log /var/log/squid/cache.log
```

Cette directive accorde l'accès au proxy à partir de votre réseau :

```
http_access allow mynetwork
```

Cette directive définit le nom d'hôte du serveur squid :

```
visible_hostname proxy.fenestros.loc
```

Sauvegardez votre fichier et déplacez-le à /etc/squid :

```
[root@centos6 tmp]# mv /tmp/squid.conf /etc/squid/
mv : voulez-vous écraser « /etc/squid/squid.conf » ? o
```

Vous devez maintenant vérifier le syntaxe de votre fichier de configuration à l'aide de la commande :

```
[root@centos6 tmp]# squid -k parse
2012/06/01 09:00:41| Processing Configuration File: /etc/squid/squid.conf (depth 0)
2012/06/01 09:00:41| Initializing https proxy context
```

En cas d'erreur, consultez la ligne indiquée et corrigez l'erreur.

Voici le fichier édité :

squid.conf

```
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1
acl localnet src 10.0.0.0/8 # RFC1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines
acl SSL_ports port 443
acl Safe_ports port 80      # http
acl Safe_ports port 21      # ftp
acl Safe_ports port 443     # https
acl Safe_ports port 70      # gopher
acl Safe_ports port 210     # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280     # http-mgmt
acl Safe_ports port 488     # gss-http
acl Safe_ports port 591     # filemaker
acl Safe_ports port 777     # multiling http
acl CONNECT method CONNECT
http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localnet
http_access allow localhost
http_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
coredump_dir /var/spool/squid
```

```
refresh_pattern ^ftp:       1440    20%    10080
refresh_pattern ^gopher:    1440    0%    1440
refresh_pattern -i (/cgi-bin/|?) 0  0%    0
refresh_pattern .       0    20%    4320
cache_mem 124 MB
cache_dir ufs /var/spool/squid 3641 16 256
acl mynetwork src 10.0.2.0/24
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
http_access allow mynetwork
visible_hostname proxy.fenestros.loc
```

Si squid doit passer par le proxy de votre société, ajoutez la ligne suivante à votre fichier de configuration squid.conf en modifiant les variables :

cache_peer $PROXY_HOST parent $PROXY_PORT 0 no-query default proxy-only login=$PROXY_USER:$PROXY_PASSWORD

Important - Attention à l'ordre des directives dans le fichier ci-dessus. En cas de règles contradictoires, c'est la première règle troiuvée qui est appliquée.

Sous CentOS 6, SELinux est en mode **enforcing** :

```
[root@centos6 tmp]# getenforce
Enforcing
```

Afin de poursuivre, il faut changer le mode de SELinux en **permissive** :

```
[root@centos6 tmp]# setenforce permissive
[root@centos6 tmp]# getenforce
Permissive
```

Démarrez le service squid :

```
[root@centos6 tmp]# service squid start
init_cache_dir /var/spool/squid... Démarrage de squid : .  [  OK  ]
```

Si vous obtenez une sortie similaire à celle ci-dessous, vous avez oubliez de passer SELinux en mode **permissive** :

```
[root@centos6 tmp]# service squid start
Démarrage de squid :                                       [ÉCHOUÉ]
2012/11/09 14:46:33| Processing Configuration File: /etc/squid/squid.conf (depth 0)
FATAL: Unable to open configuration file: /etc/squid/squid.conf: (13) Permission denied
Squid Cache (Version 3.1.10): Terminated abnormally.
CPU Usage: 0.011 seconds = 0.007 user + 0.004 sys
Maximum Resident Size: 18928 KB
Page faults with physical i/o: 0
```

LAB #15 - L'Extension squidGuard

squidGuard est une **extension** pour le serveur proxy **Squid**. **squidGuard** est un **redirecteur** qui permet de filtrer l'accès à des sites suivant des règles en affichant à leur place une ou plusieurs pages html définies par root.

squidGuard se trouve dans les dépôts **rpm-forge**.Installez donc ce dépôt ainsi :

```
[root@centos6 tmp]# rpm -Uhv
http://apt.sw.be/redhat/el6/en/i386/rpmforge/RPMS/rpmforge-release-0.5.2-2.el6.rf.i686.rpm
```

Installez ensuite squidGuard et ses **blacklists** :

```
[root@centos6 tmp]# yum install squidguard squidguard-blacklists
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package squidguard.i686 0:1.3-2.el6.rf set to be updated
---> Package squidguard-blacklists.noarch 1:1.3-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                Arch                           Version
Repository                          Size
================================================================================
================================================================================
Installing:
 squidguard                             i686                           1.3-2.el6.rf
rpmforge                            90 k
 squidguard-blacklists                  noarch                         1:1.3-1.el6.rf
rpmforge                            19 M

Transaction Summary
================================================================================
================================================================================
Install       2 Package(s)
Upgrade       0 Package(s)
```

```
Total download size: 19 M
Installed size: 74 M
Is this ok [y/N]: y
Downloading Packages:
(1/2): squidguard-1.3-2.el6.rf.i686.rpm
|  90 kB     00:00
(2/2): squidguard-blacklists-1.3-1.el6.rf.noarch.rpm
|  19 MB     00:14
--------------------------------------------------------------------------------------------------------------------
--------------------------------------------------
Total
1.3 MB/s |  19 MB     00:14
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : squidguard-1.3-2.el6.rf.i686
1/2
  Installing     : 1:squidguard-blacklists-1.3-1.el6.rf.noarch
2/2

Installed:
  squidguard.i686 0:1.3-2.el6.rf                                                squidguard-blacklists.noarch
1:1.3-1.el6.rf

Complete!
```

Vous devez maintenant indiquer à **squid** que vous allez utiliser squidGuard.

Ajoutez les lignes suivantes au fichier **/etc/squid/squid.conf** :

```
redirect_program /usr/bin/squidGuard -c /etc/squid/squidguard.conf
redirect_children 4
```

Consultez le fichier **/etc/squid/squidguard.conf**.

```
[root@centos6 tmp]# cat /etc/squid/squidguard.conf
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard
logdir /var/log/squidguard

#
# TIME RULES:
# abbrev for weekdays:
# s = sun, m = mon, t =tue, w = wed, h = thu, f = fri, a = sat

time workhours {
    weekly mtwhf 08:00 - 16:30
    date *-*-01  08:00 - 16:30
}

#
# REWRITE RULES:
#

rew dmz {
    s@://admin/@://admin.foo.bar.de/@i
    s@://foo.bar.de/@://www.foo.bar.de/@i
}

#
# SOURCE ADDRESSES:
#

src admin {
```

```
    ip        1.2.3.4 1.2.3.5
    user        root foo bar
    within         workhours
}

src foo-clients {
    ip        172.16.2.32-172.16.2.100 172.16.2.100 172.16.2.200
}

src bar-clients {
    ip        172.16.4.0/26
}

#
# DESTINATION CLASSES:
#

dest good {
}

dest local {
}

dest adult {
    domainlist    dest/adult/domains
    urllist        dest/adult/urls
    expressionlist    dest/adult/expressions
    redirect
http://admin.foo.bar.de/cgi/blocked?clientaddr=%a+clientname=%n+clientuser=%i+clientgroup=%s+targetgroup=%t+url=%
u
}


acl {
```

```
    admin {
        pass     any
    }

    foo-clients within workhours {
        pass     good !in-addr !adult any
    } else {
        pass any
    }

    bar-clients {
        pass    local none
    }

    default {
        pass     local none
        rewrite     dmz
        redirect
http://admin.foo.bar.de/cgi/blocked?clientaddr=%a+clientname=%n+clientuser=%i+clientgroup=%s+targetgroup=%t+url=%
u
    }
}
```

Remplacez ce fichier par le suivant :

squidguard.conf

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard
logdir /var/log/squidguard
```

```
time workhours {
        weekly s 09:30-12:00 13:00-19:00
        weekly m 09:00-12:00 13:00-19:00
        weekly t 09:00-11:00 12:00-19:00
        weekly w 09:00-12:00 12:00-18:00
        weekly h 09:00-13:00 13:00-18:00
        weekly f 09:00-12:00 13:30-18:00
        weekly a 08:20-13:00 13:30-19:00
}

#
# SOURCE ADDRESSES:
#

src privilegedsource {
        iplist  privilegedsource/ips
}

src bannedsource {
        iplist  bannedsource/ips
}

src lansource {
        iplist lansource/lan
}

#
# DESTINATION CLASSES:
#

dest porn {
        domainlist porn/domains
        urllist porn/urls
}
```

```
dest adult {
        domainlist adult/domains
        urllist adult/urls
        expressionlist  adult/expressions
}

dest audio-video {
        domainlist audio-video/domains
        urllist audio-video/urls
}

dest forums {
        domainlist forums/domains
        urllist forums/urls
        expressionlist  forums/expressions
}

dest hacking {
        domainlist hacking/domains
        urllist hacking/urls
}

dest redirector {
        domainlist redirector/domains
        urllist redirector/urls
}

dest warez {
        domainlist warez/domains
         urllist warez/urls
}

dest ads {
```

```
         domainlist ads/domains
         urllist ads/urls
}

dest aggressive {
        domainlist aggressive/domains
        urllist aggressive/urls
}

dest drugs {
         domainlist drugs/domains
         urllist drugs/urls
}

dest gambling {
         domainlist gambling/domains
         urllist gambling/urls
}

dest violence {
        domainlist violence/domains
        urllist violence/urls
        expressionlist  violence/expressions
}

#
# ACLs
#
acl {
        privilegedsource {
                pass !ads all
                redirect http://localhost/access-denied.html?url=%u

        }
```

```
        bannedsource {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }

        lansource {
                pass !porn !adult !audio-video !forums !hacking !redirector !warez !ads !aggressive !drugs
!gambling !violence all
                redirect http://localhost/access-denied.html?url=%u
        }


        default {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }
}
```

Ce fichier contient des sections dont :

Nom de la Section	***Qui déclare***
CONFIGURATION DIRECTORIES	Les **Chemins** des fichiers db et des logs
TIME RULES	Les **Plages Horaires** de connexion
SOURCE ADDRESES	Les **Clients** se connectant au proxy
DESTINATION RULES	Les règles gouvernant les **URLs** de Destination
ACL	Les Règles de Contrôle d'Accès (ACL)

Le fichier de configuration de squidGuard contient des directives de chargement des bases de données. Ces directives contiennent uniquement les noms des fichiers sans extension, par exemple, **domains**.

squidGuard utilise des bases de données de type **Berkeley**.

Ces fichiers sont stockés dans **/var/lib/squidguard/** et sont au format db ou au format texte.

squidGuard utilise une base de données divisée en catégories telles **local**, **clients** etc.

Chaque catégorie peut être composée de listes de **domaines**, d'**URL**s ou d'**expressions régulières**.

```
[root@centos6 tmp]# ls /var/lib/squidguard/
ads  adult  aggressive  audio-video  drugs  forums  gambling  hacking  local  mail  proxy  violence  warez
```

Lors de son lancement squidGuard essaie dans un premier temps de localiser le fichier **.db**. S'il ne parvient pas, il charge la version texte de la liste et construit les **B-arbres** en mémoire.

Cette construction de B-arbres peut ralentir le démarrage de **Squid** sensiblement.

Afin de palier à cet éventuel problème, les fichiers texte peuvent être transformés en base de données pré-construites à l'aide de la commande :

```
squidGuard -C chemin_et_nom_du_fichier_texte [Entrée]
```

Installez maintenant la mise à jour de la liste **blacklist**.

Premièrement téléchargez la liste suivante :

```
[root@centos6 tmp]# wget http://www.shallalist.de/Downloads/shallalist.tar.gz
--2012-06-01 09:20:46--  http://www.shallalist.de/Downloads/shallalist.tar.gz
Résolution de www.shallalist.de... 78.47.242.85
Connexion vers www.shallalist.de|78.47.242.85|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 9907814 (9,4M) [application/x-tar]
Sauvegarde en : «shallalist.tar.gz»
```

```
100%[=======================================================================================================
==================>] 9 907 814    804K/s   ds 11s

2012-06-01 09:20:57 (873 KB/s) - «shallalist.tar.gz» sauvegardé [9907814/9907814]
```

Désarchivez blacklists.tar.gz :

```
[root@centos6 tmp]# tar xvf shallalist.tar.gz
BL/
BL/porn/
BL/porn/domains
BL/porn/urls
BL/gamble/
BL/gamble/domains
BL/gamble/urls
BL/chat/
BL/chat/domains
BL/chat/urls
BL/automobile/
BL/automobile/cars/
BL/automobile/cars/domains
BL/automobile/cars/urls
BL/automobile/bikes/
BL/automobile/bikes/domains
BL/automobile/bikes/urls
BL/automobile/boats/
BL/automobile/boats/domains
BL/automobile/boats/urls
BL/automobile/planes/
...
```

Créez ensuite les répertoires et fichiers pour les ACL des adresses IP :

```
[root@centos6 tmp]# cd /var/lib/squidguard
```

```
[root@centos6 squidguard]# mkdir privilegedsource bannedsource lansource
[root@centos6 squidguard]# touch privilegedsource/ips bannedsource/ips lansource/lan
```

Éditez le fichier **/var/lib/squidguard/lansource/lan** :

lan

```
127.0.0.0/8
10.0.2.0/24
```

De cette façon, vous autorisez votre propre machine ainsi que les machines de votre réseau à utiliser le serveur proxy.

Copiez les fichiers du répertoire **/tmp/BL** vers **/var/lib/squidguard/** :

```
[root@centos6 squidguard]# cp -pfR /tmp/BL/* /var/lib/squidguard/
cp : voulez-vous écraser « /var/lib/squidguard/aggressive/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/aggressive/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/drugs/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/drugs/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/hacking/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/hacking/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/violence/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/violence/urls » ? o
cp : voulez-vous écraser « /var/lib/squidguard/warez/domains » ? o
cp : voulez-vous écraser « /var/lib/squidguard/warez/urls » ? o
```

Pré-générez maintenant les B-arbres des listes et mettez-les à jour :

```
[root@centos6 squidguard]# squidGuard -C all
Processing file and database /var/lib/squidguard/porn/domains
    [================================================] 100 % done
Processing file and database /var/lib/squidguard/porn/urls
    [================================================] 100 % done
```

```
Processing file and database /var/lib/squidguard/adult/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/adult/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/audio-video/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/audio-video/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/forums/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/forums/urls

Processing file and database /var/lib/squidguard/hacking/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/hacking/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/redirector/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/redirector/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/warez/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/warez/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/ads/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/ads/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/aggressive/domains
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/aggressive/urls
    [==================================================] 100 % done
Processing file and database /var/lib/squidguard/drugs/domains
    [==================================================] 100 % done
```

```
Processing file and database /var/lib/squidguard/drugs/urls
    [================================================] 100 % done
Processing file and database /var/lib/squidguard/gambling/domains
    [================================================] 100 % done
Processing file and database /var/lib/squidguard/gambling/urls
    [================================================] 100 % done
Processing file and database /var/lib/squidguard/violence/domains
    [================================================] 100 % done
Processing file and database /var/lib/squidguard/violence/urls
    [================================================] 100 % done
```

La commande suivante permet de mettre à jour les listes :

```
[root@centos6 squidguard]# squidGuard -u
```

Assurez-vous que /var/lib/squidguard appartient à l'utilisateur **squid** du groupe **squid**:

```
[root@centos6 squidguard]# chown -R squid:squid /var/lib/squidguard
```

Pour que **squid** prenne en compte la modification des listes, il faut utiliser la commande :

```
[root@centos6 squidguard]# squid -k reconfigure
```

Étudiez le contenu de /var/lib/squidguard/. Vous y trouverez d'autres répertoires contenant des listes selon des catégories. Notez que les fichiers à extension **.diff** sont des fichiers de **modification** de listes. Ces fichiers de modifications contiennent des instructions du type :

```
+nouvelle_entrée_à_ajouter
-ancienne_entrée_à_retirer
```

Consultez maintenant le fichier **/var/log/squidguard/squidGuard.log** et vérifiez que les fichiers ont été mis à jour correctement :

```
[root@centos6 squidguard]# cat /var/log/squidguard/squidGuard.log
2012-06-01 09:26:24 [7426] New setting: dbhome: /var/lib/squidguard
```

```
2012-06-01 09:26:24 [7426] New setting: logdir: /var/log/squidguard
2012-06-01 09:26:24 [7426] init iplist /var/lib/squidguard/privilegedsource/ips
2012-06-01 09:26:24 [7426] sourceblock privilegedsource missing active content, set inactive
2012-06-01 09:26:24 [7426] init iplist /var/lib/squidguard/bannedsource/ips
2012-06-01 09:26:24 [7426] sourceblock bannedsource missing active content, set inactive
2012-06-01 09:26:24 [7426] init iplist /var/lib/squidguard/lansource/lan
2012-06-01 09:26:24 [7426] init domainlist /var/lib/squidguard/porn/domains
2012-06-01 09:28:09 [7426] create new dbfile /var/lib/squidguard/porn/domains.db
2012-06-01 09:28:09 [7426] init urllist /var/lib/squidguard/porn/urls
2012-06-01 09:28:15 [7426] create new dbfile /var/lib/squidguard/porn/urls.db
2012-06-01 09:28:15 [7426] init domainlist /var/lib/squidguard/adult/domains
2012-06-01 09:30:28 [7426] create new dbfile /var/lib/squidguard/adult/domains.db
2012-06-01 09:30:28 [7426] init urllist /var/lib/squidguard/adult/urls
2012-06-01 09:30:41 [7426] create new dbfile /var/lib/squidguard/adult/urls.db
2012-06-01 09:30:41 [7426] init expressionlist /var/lib/squidguard/adult/expressions
2012-06-01 09:30:41 [7426] init domainlist /var/lib/squidguard/audio-video/domains
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/audio-video/domains.db
2012-06-01 09:30:42 [7426] init urllist /var/lib/squidguard/audio-video/urls
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/audio-video/urls.db
2012-06-01 09:30:42 [7426] init domainlist /var/lib/squidguard/forums/domains
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/forums/domains.db
2012-06-01 09:30:42 [7426] init urllist /var/lib/squidguard/forums/urls
2012-06-01 09:30:42 [7426] urllist empty, removed from memory
2012-06-01 09:30:42 [7426] init expressionlist /var/lib/squidguard/forums/expressions
2012-06-01 09:30:42 [7426] init domainlist /var/lib/squidguard/hacking/domains
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/hacking/domains.db
2012-06-01 09:30:42 [7426] init urllist /var/lib/squidguard/hacking/urls
2012-06-01 09:30:42 [7426] create new dbfile /var/lib/squidguard/hacking/urls.db
2012-06-01 09:30:42 [7426] init domainlist /var/lib/squidguard/redirector/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/redirector/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/redirector/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/redirector/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/warez/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/warez/domains.db
```

```
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/warez/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/warez/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/ads/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/ads/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/ads/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/ads/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/aggressive/domains
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/aggressive/domains.db
2012-06-01 09:30:50 [7426] init urllist /var/lib/squidguard/aggressive/urls
2012-06-01 09:30:50 [7426] create new dbfile /var/lib/squidguard/aggressive/urls.db
2012-06-01 09:30:50 [7426] init domainlist /var/lib/squidguard/drugs/domains
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/drugs/domains.db
2012-06-01 09:30:55 [7426] init urllist /var/lib/squidguard/drugs/urls
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/drugs/urls.db
2012-06-01 09:30:55 [7426] init domainlist /var/lib/squidguard/gambling/domains
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/gambling/domains.db
2012-06-01 09:30:55 [7426] init urllist /var/lib/squidguard/gambling/urls
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/gambling/urls.db
2012-06-01 09:30:55 [7426] init domainlist /var/lib/squidguard/violence/domains
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/violence/domains.db
2012-06-01 09:30:55 [7426] init urllist /var/lib/squidguard/violence/urls
2012-06-01 09:30:55 [7426] create new dbfile /var/lib/squidguard/violence/urls.db
2012-06-01 09:30:55 [7426] init expressionlist /var/lib/squidguard/violence/expressions
2012-06-01 09:30:55 [7426] squidGuard 1.3 started (1338535584.022)
2012-06-01 09:30:55 [7426] db update done
2012-06-01 09:30:55 [7426] squidGuard stopped (1338535855.695)
2012-06-01 09:37:59 [7519] New setting: dbhome: /var/lib/squidguard
2012-06-01 09:37:59 [7519] New setting: logdir: /var/log/squidguard
2012-06-01 09:37:59 [7519] init iplist /var/lib/squidguard/privilegedsource/ips
2012-06-01 09:37:59 [7519] sourceblock privilegedsource missing active content, set inactive
2012-06-01 09:37:59 [7519] init iplist /var/lib/squidguard/bannedsource/ips
2012-06-01 09:37:59 [7519] sourceblock bannedsource missing active content, set inactive
2012-06-01 09:37:59 [7519] init iplist /var/lib/squidguard/lansource/lan
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/porn/domains
```

```
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/porn/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/porn/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/porn/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/adult/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/adult/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/adult/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/adult/urls.db
2012-06-01 09:37:59 [7519] init expressionlist /var/lib/squidguard/adult/expressions
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/audio-video/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/audio-video/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/audio-video/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/audio-video/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/forums/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/forums/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/forums/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/forums/urls.db
2012-06-01 09:37:59 [7519] init expressionlist /var/lib/squidguard/forums/expressions
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/hacking/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/hacking/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/hacking/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/hacking/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/redirector/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/redirector/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/redirector/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/redirector/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/warez/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/warez/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/warez/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/warez/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/ads/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/ads/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/ads/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/ads/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/aggressive/domains
```

```
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/aggressive/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/aggressive/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/aggressive/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/drugs/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/drugs/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/drugs/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/drugs/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/gambling/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/gambling/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/gambling/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/gambling/urls.db
2012-06-01 09:37:59 [7519] init domainlist /var/lib/squidguard/violence/domains
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/violence/domains.db
2012-06-01 09:37:59 [7519] init urllist /var/lib/squidguard/violence/urls
2012-06-01 09:37:59 [7519] loading dbfile /var/lib/squidguard/violence/urls.db
2012-06-01 09:37:59 [7519] init expressionlist /var/lib/squidguard/violence/expressions
2012-06-01 09:37:59 [7519] squidGuard 1.3 started (1338536279.458)
2012-06-01 09:37:59 [7519] db update done
2012-06-01 09:37:59 [7519] squidGuard stopped (1338536279.467)
```

Redémarrez le service squid pour que toutes vos modifications soient prises en compte :

```
[root@centos6 squidguard]# service squid restart
Arrêt de squid : .................                          [  OK  ]
Démarrage de squid : .                                     [  OK  ]
```

Créez maintenant la page **/var/www/html/access-denied.html** :

access-denied.html

```
<html>
<head>
<title>Acc&egrave;s Interdit</title>
</head>
```

```
<body>
<br>
<br>
<br>
<center>ACCES INTERDIT !!</center>
</body>
</html>
```

Puisque le serveur apache va servir la page **access-denied.html**, il convient de démarrer le service **httpd**.

Modifiez le propriétaire et le groupe du fichier **/var/www/html/access-denied.html** :

```
[root@centos6 squidguard]# chown apache:apache /var/www/html/access-denied.html
```

Les options de cette commande sont :

```
[root@centos6 squidguard]# squidguard --help
squidguard: invalid option -- '-'
Usage: squidGuard [-u] [-C block] [-t time] [-c file] [-v] [-d]
Options:
  -v          : show version number
  -d          : all errors to stderr
  -c file     : load alternate configfile
  -t time     : specify startup time in the format: yyyy-mm-ddTHH:MM:SS
  -u          : update .db files from .diff files
  -C file|all : create new .db files from urls/domain files
                specified in "file".
```

Créer une whitelist

Trouver le site de google.de dans les fichiers de squidGuard est une tâche fastidieuse, d'autant plus qu'il est fort probable que d'autres sites peuvent se trouver dans une des bases par erreur.

La façon la plus simple de remédier à ceci est de créer votre propre base de données de sites où vous accordez l'accès et de faire analyser cette base avant les autres.

Ouvrez donc le fichier **squidguard.conf** et ajoutez la section suivante :

DESTINATION CLASSES:

```
dest ok { domainlist ok/domains
          urllist ok/urls
}
```

Modifiez ensuite l'**ACL lansource** comme indiqué ci-après :

```
lansource {pass ok !porn !adult !audio-video ! ..... }
```

Votre fichier de configuration ressemblera à :

squidguard.conf

```
#
# CONFIG FILE FOR SQUIDGUARD
#

dbhome /var/lib/squidguard
logdir /var/log/squidguard

time workhours {
        weekly s 09:30-12:00 13:00-19:00
```

```
        weekly m 09:00-12:00 13:00-19:00
        weekly t 09:00-11:00 12:00-19:00
        weekly w 09:00-12:00 12:00-18:00
        weekly h 09:00-13:00 13:00-18:00
        weekly f 09:00-12:00 13:30-18:00
        weekly a 08:20-13:00 13:30-19:00
}

#
# SOURCE ADDRESSES:
#

src privilegedsource {
        iplist  privilegedsource/ips
}

src bannedsource {
        iplist  bannedsource/ips
}

src lansource {
        iplist lansource/lan
}

#
# DESTINATION CLASSES:
#

dest porn {
        domainlist porn/domains
        urllist porn/urls
}

dest adult {
```

```
        domainlist adult/domains
        urllist adult/urls
        expressionlist  adult/expressions
}

dest audio-video {
        domainlist audio-video/domains
        urllist audio-video/urls
}

dest forums {
        domainlist forums/domains
        urllist forums/urls
        expressionlist  forums/expressions
}

dest hacking {
        domainlist hacking/domains
        urllist hacking/urls
}

dest redirector {
        domainlist redirector/domains
        urllist redirector/urls
}

dest warez {
        domainlist warez/domains
         urllist warez/urls
}

dest ads {
         domainlist ads/domains
         urllist ads/urls
```

```
}

dest aggressive {
        domainlist aggressive/domains
        urllist aggressive/urls
}

dest drugs {
         domainlist drugs/domains
         urllist drugs/urls
}

dest gambling {
         domainlist gambling/domains
         urllist gambling/urls
}

dest violence {
        domainlist violence/domains
        urllist violence/urls
        expressionlist  violence/expressions
}

dest ok { domainlist ok/domains
          urllist ok/urls
}

#
# ACLs
#
acl {
        privilegedsource {
                pass !ads all
                redirect http://localhost/access-denied.html?url=%u
```

```
        }

        bannedsource {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }

        lansource {
                pass ok !porn !adult !audio-video !forums !hacking !redirector !warez !ads !aggressive
!drugs !gambling !violence all
                redirect http://localhost/access-denied.html?url=%u
        }


        default {
                pass none
                redirect http://localhost/access-denied.html?url=%u

        }
}
```

Créez maintenant le répertoire **ok** :

```
[root@centos6 squidguard]# mkdir /var/lib/squidguard/ok
```

Et ensuite les fichiers domains et urls :

```
[root@centos6 squidguard]# touch /var/lib/squidguard/ok/domains
[root@centos6 squidguard]# touch /var/lib/squidguard/ok/urls
```

Editez ensuite le fichier **domains** en y insérant les adresses IP du site auquel vous voulez avoir accès :

domains

```
XXX.XXX.XXX.XXX
```

Editez ensuite le fichier **urls** en y insérant l'URL du site auquel vous voulez avoir accès :

urls

```
www.site.ext
site.ext
```

Pré-générez maintenant les B-arbres des listes et mettez-les à jour :

```
[root@centos6 squidguard]# squidGuard -C ok/domains
Processing file and database /var/lib/squidguard/ok/domains
    [================================================] 100 % done
Processing file and database /var/lib/squidguard/ok/urls
    [================================================] 100 % done
[root@centos6 squidguard]# squidGuard -u
Processing file and database /var/lib/squidguard/ok/urls
    [================================================] 100 % done
[root@centos6 squidguard]# squid -k reconfigure
```

Assurez-vous que les repertoires et les fichiers que vous venez de créer appartiennent à l'utilisateur **squid** du groupe **squid** :

```
[root@centos6 squidguard]# chown -R squid:squid /var/lib/squidguard/
```

Ensuite redémarrez squid :

```
[root@centos6 squidguard]# service squid restart
Arrêt de squid : ..............                            [  OK  ]
```

```
Démarrage de squid : .                                     [  OK  ]
```

LAB #16 - Dansguardian

Squid ne peut pas contrôler le *contenu* des pages web. Pour faire ceci, il faut utiliser un logiciel de filtrage du contenu tel **Dansguardian** :

```
[root@centos6 squidguard]# yum install dansguardian
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package dansguardian.i686 0:2.10.1.1-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                 Arch                              Version
Repository                               Size
================================================================================================================
================================================
Installing:
 dansguardian                            i686                              2.10.1.1-1.el6.rf
rpmforge                                454 k

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

```
============================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 454 k
Installed size: 1.4 M
Is this ok [y/N]: y
Downloading Packages:
dansguardian-2.10.1.1-1.el6.rf.i686.rpm
| 454 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : dansguardian-2.10.1.1-1.el6.rf.i686
1/1

Installed:
  dansguardian.i686 0:2.10.1.1-1.el6.rf

Complete!
[root@centos6 squidguard]# chkconfig --level 345 dansguardian on
[root@centos6 squidguard]# chkconfig --list dansguardian
dansguardian    0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Dansguardian se configure grâce au fichier **/etc/dansguardian/dansguardian.conf**.

Notez que Dansguardian est un logiciel *complémentaire* à squid. En effet, Dansguardian n'est pas un proxy mais seulement un filtre.

Démarrez votre service dansguardian :

```
[root@centos6 squidguard]# service dansguardian start
Démarrage de Web Content Filter (dansguardian) :           [  OK  ]
```

Configurez votre navigateur afin d'utiliser le proxy 127.0.0.1 port 8080. Testez maintenant votre accès à Internet.

Le Serveur HTTP Nginx

Présentation et Configuration de Nginx sous Debian 11

Commencez par vous connectez à votre VM Debian 11 au 10.0.2.46.

Présentation

Nginx est un logiciel libre de serveur Web ainsi qu'un proxy inverse écrit par Igor Sysoev, dont le développement a débuté en 2002 pour les besoins d'un site russe à très fort trafic (Rambler). La documentation est disponible dans plusieurs langues.

NGINX Inc a été racheté par F5 Networks le 11 mars 2019, pour 670 millions de dollars.

Ses sources sont disponibles sous une licence de type BSD.

LAB #17 - Configuration d'un Proxy Inverse

Installez nginx et gunicorn :

```
root@debian11:~# apt install nginx gunicorn curl -y
```

Important : Gunicorn est un Python WSGI server.

Créez le fichier **/etc/nginx/sites-available/reverse-proxy.loc** :

```
root@debian11:~# vi /etc/nginx/sites-available/reverse-proxy.loc
root@debian11:~# cat /etc/nginx/sites-available/reverse-proxy.loc
server {
    listen 80;
    listen [::]:80;

    server_name reverse-proxy.loc www.reverse-proxy.loc;
    location / {
        proxy_pass http://127.0.0.1:8000;
        include proxy_params;
    }
}
```

Important : La directive **proxy-pass** indique l'URL de Gunicorn.

Consultez le contenu du fichier **/etc/nginx/proxy_params** :

```
root@debian11:~# cat /etc/nginx/proxy_params
proxy_set_header Host $http_host;
proxy_set_header X-Real-IP $remote_addr;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_set_header X-Forwarded-Proto $scheme;
```

Vérifiez la syntaxe de votre fichier **/etc/nginx/nginx.conf** :

```
root@debian11:~# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
```

Créez le lien symbolique pour **reverse-proxy.loc** dans le répertoire **/etc/nginx/sites-enabled/** :

```
root@debian11:~# ln -s /etc/nginx/sites-available/reverse-proxy.loc /etc/nginx/sites-enabled/
```

Editez le fichier **/etc/hosts** :

```
root@debian11:~# vi /etc/hosts
root@debian11:~# cat /etc/hosts
127.0.0.1       localhost
10.0.2.46       debian11.ittraining.loc debian11
10.0.2.46       reverse-proxy.loc

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Redémarrez le serveur nginx :

```
root@debian11:~# systemctl restart nginx
root@debian11:~# systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabl>
     Active: active (running) since Tue 2022-11-22 13:03:56 CET; 14s ago
       Docs: man:nginx(8)
    Process: 1927 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on;>
    Process: 1928 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=ex>
   Main PID: 1929 (nginx)
      Tasks: 9 (limit: 19150)
     Memory: 7.7M
        CPU: 30ms
     CGroup: /system.slice/nginx.service
             ├─1929 nginx: master process /usr/sbin/nginx -g daemon on; master_proces>
             ├─1930 nginx: worker process
             ├─1931 nginx: worker process
             ├─1932 nginx: worker process
```

```
             ├─1933 nginx: worker process
             ├─1934 nginx: worker process
             ├─1935 nginx: worker process
             ├─1936 nginx: worker process
             └─1937 nginx: worker process

Nov 22 13:03:56 debian11 systemd[1]: nginx.service: Succeeded.
Nov 22 13:03:56 debian11 systemd[1]: Stopped A high performance web server and a reve>
lines 1-23
```

Créez le fichier une fonction Python qui retournera **Hello World!** en tant que réponse HTTP :

```
root@debian11:~# vi test.py
root@debian11:~# cat test.py
def app(environ, start_response):
    start_response("200 OK", [])
    return iter([b"Hello, World!"])
```

Lancez Gunicorn :

```
root@debian11:~# gunicorn --workers=2 test:app &
[1] 1944
root@debian11:~# [2022-11-22 13:05:38 +0100] [1944] [INFO] Starting gunicorn 20.1.0
[2022-11-22 13:05:38 +0100] [1944] [INFO] Listening at: http://127.0.0.1:8000 (1944)
[2022-11-22 13:05:38 +0100] [1944] [INFO] Using worker: sync
[2022-11-22 13:05:38 +0100] [1945] [INFO] Booting worker with pid: 1945
[2022-11-22 13:05:39 +0100] [1946] [INFO] Booting worker with pid: 1946
[Enter]
root@debian11:~#
```

Consultez le site **reverse-proxy.loc** :

```
root@debian11:~# curl http://reverse-proxy.loc
Hello, World!root@debian11:~#
```

```
root@debian11:~#
```

LAB #18 - Configuration d'un Serveur PHP

Commencez par installe **php** et **php-fpm** :

```
root@debian11:~# apt install php php-fpm -y
```

Vérifiez la version de PHP installée :

```
root@debian11:~# php -version
PHP 7.4.33 (cli) (built: Nov  8 2022 11:40:37) ( NTS )
Copyright (c) The PHP Group
Zend Engine v3.4.0, Copyright (c) Zend Technologies
    with Zend OPcache v7.4.33, Copyright (c), by Zend Technologies
```

Modifiez maintenant le fichier **/etc/nginx/sites-available/reverse-proxy.loc**

```
root@debian11:~# vi /etc/nginx/sites-available/reverse-proxy.loc
root@debian11:~# cat /etc/nginx/sites-available/reverse-proxy.loc
server {
    listen 80;
    server_name reverse-proxy.loc;
    root /var/www/html;

    index index.html index.htm index.php;

    location / {
        try_files $uri $uri/ =404;
    }

    location ~ \.php$ {
```

```
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
     }

    location ~ /\.ht {
        deny all;
    }

}
```

Important : Notez que la directive **root** définit le chemin vers les pages du contenu du site et que la directive **listen** spécifie le port d'écoute du serveur.

Créez le fichier **/var/www/html/info.php** :

```
root@debian11:~# vi /var/www/html/info.php
root@debian11:~# cat /var/www/html/info.php
<?php
phpinfo();
?>
```

Redémarrez le serveur nginx pour une pris en compte directe des modifications :

```
root@debian11:~# systemctl restart nginx
root@debian11:~# systemctl status  nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabl>
     Active: active (running) since Tue 2022-11-22 13:43:30 CET; 9s ago
       Docs: man:nginx(8)
    Process: 9799 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on;>
    Process: 9800 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=ex>
```

```
   Main PID: 9801 (nginx)
      Tasks: 9 (limit: 19150)
     Memory: 7.9M
        CPU: 33ms
     CGroup: /system.slice/nginx.service
             ├─9801 nginx: master process /usr/sbin/nginx -g daemon on; master_proces>
             ├─9802 nginx: worker process
             ├─9803 nginx: worker process
             ├─9804 nginx: worker process
             ├─9805 nginx: worker process
             ├─9806 nginx: worker process
             ├─9807 nginx: worker process
             ├─9808 nginx: worker process
             └─9809 nginx: worker process

Nov 22 13:43:30 debian11 systemd[1]: Starting A high performance web server and a rev>
Nov 22 13:43:30 debian11 systemd[1]: Started A high performance web server and a reve>
root@debian11:~#
```

Consultez ensuite la page **info.php** :

```
root@debian11:~# curl http://reverse-proxy.loc/info.php | more
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 65721    0 65721    0     0   567<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "DTD/xhtml1-
transitiona
k      0l.dtd">
 --:--:-- --:--:-- --:--:--  567k
<html xmlns="http://www.w3.org/1999/xhtml"><head>
<style type="text/css">
body {background-color: #fff; color: #222; font-family: sans-serif;}
pre {margin: 0; font-family: monospace;}
a:link {color: #009; text-decoration: none; background-color: #fff;}
a:hover {text-decoration: underline;}
```

```
table {border-collapse: collapse; border: 0; width: 934px; box-shadow: 1px 2px 3px #cc
c;}
.center {text-align: center;}
.center table {margin: 1em auto; text-align: left;}
.center th {text-align: center !important;}
td, th {border: 1px solid #666; font-size: 75%; vertical-align: baseline; padding: 4px
 5px;}
th {position: sticky; top: 0; background: inherit;}
h1 {font-size: 150%;}
h2 {font-size: 125%;}
.p {text-align: left;}
.e {background-color: #ccf; width: 300px; font-weight: bold;}
.h {background-color: #99c; font-weight: bold;}
.v {background-color: #ddd; max-width: 300px; overflow-x: auto; word-wrap: break-word;
}
--More--
[q]
```

Ne Pas Oublier

Server Name Indication

Selon **Wikipédia** :

Server Name Indication (SNI), qui peut se traduire par « indication du nom du serveur », est une extension du protocole TLS1. Avec le protocole SNI, le client indique le nom de l'hôte (hostname) avec lequel il tente de démarrer une négociation TLS. Cela permet au serveur de présenter plusieurs certificats pour la même adresse IP (mais des noms d'hôte différents), et donc de mutualiser des hébergements pour des sites sécurisés en https.

Les navigateurs web modernes prennent en charge le SNI2. Lorsque le navigateur ne gère pas le SNI, le serveur fournit le certificat par défaut, et un avertissement au sujet du certificat se produit donc le plus souvent.

Redirects et Alias

Veuillez noter que :

- Les **Redirects** sont traités du côté du **client**,
- Les **Alias** sont traités du côté du **serveur**.
