Configuration du serveur web apache2 sous Ubunto

Fichier ou répertoire	Description
/etc/apache2/apache2.conf	Le fichier de configuration principal
/etc/apache2/ports.conf	contient la liste des ports en écoute
/etc/apache2/mods-available	contient les modules installés
/etc/apache2/mods-enabled	contient les modules activés. Les modules activés sont des liens symboliques vers les modules installés.
/etc/apache2/sites-available	contient les sites web disponibles
/etc/apache2/sites-enabled	Contient les sites activés

Un exemple de fichier de configuration d'une application web nommée site-exemple

(ce fichier est situé dans /etc/apache2/sites-available)

```
NameVirtualHost 10.0.0.1:80
<VirtualHost 10.0.0.1:80>
ServerName site-exemple.org
DocumentRoot /var/www/site-exemple
<Directory /var/www/site-exemple>
        Options Indexes FollowSymLinks ExecCGI
#Indexes : autorise l'affichage du contenu d'un répertoire (si un fichier par défaut n'y est pas trouvé).
#FollowSymLinks: le serveur est autorisé à suivre les liens symboliques dans ce répertoire.
#ExecCGI : l'exécution de scripts CGI est autorisé.
#AllowOverride None : permet de désactiver l'utilisation des fichiers .htaccess (valeur par #défaut=none)
#AllowOverride AuthConfig : active l'utilisation des fichiers .htaccess
        Order allow,deny
        allow from all
</Directory>
#### contrôler l'accès au répertoire intranet##############################################
<Directory /var/www/site-exemple/intranet>
    Options Indexes FollowSymLinks ExecCGI
    # définit l'ordre les règles de restriction (On refuse puis on alloue l'accès à quelques  adresses)
```

```
        Order deny,allow
        deny from all
        allow from 192.168.1
 #autoriser l'accès aux machines du réseau d'adresse 192.168.1.0/24 et l'interdire à tous les autres.
</Directory>
####Authentifier l'accès au répertoire intranet/RH########################################
<Directory /var/www/site-exemple/intranet/RH>
        # définit le mode d'authentification et d'encryptage , dans ce cas c'est le  mode  “basic”
        AuthType Basic
        #définit ce qui sera affiché au client pour lui demander de s'authentifier
        AuthName "Veuillez-vous identifier pour accéder! espace protégé!!"
        #définit le fichier qui contient la liste des noms d'utilisateurs et des mots de passe
        AuthUserFile /etc/apache2/.fileForPassword
        <Limit GET POST>
                require valid-user
        </Limit>
</Directory>
</VirtualHost>
```

Quelques directives du fichier /etc/apache2.conf

```
KeepAlive on
#Autorise les connexions persistantes (plusieurs requêtes par connexion)
MaxKeepAliveRequests 100
#Nombre Maximum de requêtes allouées durant une connexion persistante.  0 = non limité
MinSpareServer 5
MaxSpareServer 10
#Ces valeurs servent à l'autorégulation de charge du serveur.
#En fait apache contrôle lui-même sa charge, suivant le nombre de clients qu'il sert et le nombre de
#requêtes envoyées par chaque client. Il fait en sorte que tout le monde puisse être servi et ajoute
#tout seul un certain nombre d'instances apaches pour servir de nouveaux clients qui se connecte
#raient. Les valeurs par défaut conviennent à la plupart des sites.
MaxClients 150
# Fixe la limite maximale de requêtes simultanées que le serveur peut prendre en charge
```