INSTALLATION DE PRELUDE-IDS

Guillaume LEHMANN (lehmann@free.fr)

5 décembre 2003

Table des matières

1 Introduction

Nous expliquons l'installation et la configuration de Prelude-IDS et de tous les paquetages qu'il utilise. La plateforme de travail est une Debian 3.0 en stable, et nous utilisons les versions suivantes des sources de Prelude-IDS : libprelude-0.8.5, prelude-manager-0.8.7, prelude-nids-0.8.1, et prelude-lml-0.8.3 . Cette documentation a été légèrement modifiée pour être valable aussi pour les versions libprelude-0.8.8, prelude-manager-0.8.9, prelude-nids-0.8.5, et prelude-lml-0.8.6 .
Nous avons choisit de stocker les alertes reçues par le manager dans une base de donnée MySQL. L'installation et la configuration de cette dernière sera donc décrite dans ce document.
Date de publication : 05/12/2003

2 Paquetages nécessaires

Il est nécessaire de télécharger, sur le site www.prelude-ids.org, les paquetages suivants :
– libprelude-x.x.x.tar.gz (nous utiliserons ici la version 0.8.5) ;
– prelude-manager-x.x.x.tar.gz (nous utiliserons ici la version 0.8.7) ;
– prelude-nids-x.x.x.tar.gz (nous utiliserons ici la version 0.8.1) ;
– prelude-lml-x.x.x.tar.gz (nous utiliseront ici la version 0.8.3) ;

libprelude est nécessaire à prelude-nids, prelude-lml, et prelude-manager.

Décompressez les fichiers dans `/usr/local/src/` . Nous avons maintenant les nouveaux répertoire `libprelude-0.8.5`, `prelude-lml-0.8.3`, `prelude-manager-0.8.7`, et `prelude-nids-0.8.1` .

3 Installation de paquetages au préalable

Prelude-IDS nécessite pour fonctionner, des bibliothèques et autres applications que nous allons installer maintenant.

3.1 Paquetages nécessaires à Prelude-IDS

– **libpcap-dev** nécessaire pour libprelude, donc aussi à prelude-nids, prelude-lml, et prelude-manager
– **flex** nécessaire à prelude-nids
– **byacc** nécessaire pour libprelude, donc aussi pour prelude-nids, prelude-lml, et prelude-manager
– **gtk-doc-tools** nécessaire pour libprelude, donc aussi à prelude-nids, prelude-lml, et prelude-manager
– **libssl-dev** nécessaire pour libprelude, donc aussi à prelude-nids, prelude-lml, et prelude-manager
– **mysql-server** à installer sur le poste hébergeant le manager, si l'on veut stocker les alertes dans une bases MySQL
– **libmysqlclient10-dev** nécessaire à prelude-manager
– **libxml2-dev** nécessaire à prelude-manager
– **libpcre3-dev** nécessaire pour prelude-lml
– **libfam-dev** nécessaire pour prelude-lml
– **libpcap0** nécessaire pour prelude-nids et prelude-lml

3.2 Installation de ces paquetages

```
apt-get install libpcap-dev flex byacc gtk-doc-tools libssl-dev
mysql-server libmysqlclient10-dev libxml2-dev libpcre3-dev libfam-dev
```

Pendant l'installation de mysql-server, il est proposé de démarrer le serveur au démarrage de la machine. Il est conseillé de répondre `Yes`.

4 Installation

4.1 Installation de libprelude

Rentrez dans le répertoire `/usr/local/src/libprelude-0.8.5/` et tapez les commandes suivantes :

```
./configure --enable-gtk-doc --enable-openssl
make
make install
```

4.2 Installation du manager

Rentrez dans le répertoire `/usr/local/src/prelude-manager-0.8.7/` et tapez les commandes suivantes :

```
./configure --enable-gtk-doc --enable-mysql --enable-openssl
make
make install
```

4.3 Installation de la sonde réseau (nids)

Rentrez dans le répertoire `/usr/local/src/prelude-nids-0.8.1/` et tapez les commandes suivantes :

```
./configure --enable-gtk-doc
make
make install
```

4.4 Installation de la sonde hôte (lml)

Rentrez dans le répertoire `/usr/local/src/prelude-lml-0.8.3/` et tapez les commandes suivantes :

```
./configure --enable-gtk-doc --enable-fam
make
make install
```

5 Configuration

Nous allons aborder ici la configuration de tous les éléments constituant Prelude-IDS. Certaines valeurs comme les adresses IP ou encore les mots-de-passe, seront à adapter par chacun.

5.1 Configuration de MySQL

Lancer le démon mysqld si cela n'a pas encore été fait :
`/etc/init.d/mysql restart`
Rentrez dans mysql :
`mysql`

Créez la base de données `prelude`, donner les droits de création/modification de cette base de donnée à l'utilisateur `prelude`, puis resortir :

```
create database prelude;
grant all privileges on prelude.* to prelude@localhost IDENTIFIED by
'dessstri';
quit
```

Donner les droits en exécution (550 par exemple) au fichier `/usr/local/src/prelude-manager-0.8.7/prelude-manager-db-create.sh`, puis exécutez le script.

Il y a 6 phases (de 0 à 5). La première, répondre `y`. À la deuxième, répondre `mysql`. À la troisième, répondre `localhost` (choix par défaut). À la quatrième, répondre `3306` choix par défaut. À la cinquième répondre `prelude` (choix par défaut). Pour la sixième phase qui est donc la numéro 5, indiquez `root` pour l'administrateur de la base, et laisser le mot-de-passe vide car si cela n'a pas été changé, l'utilisateur `root` n'a pas de mot-de-passe par défaut (cela sera à changer ultérieurement pour améliorer la sécurité du système). L'avant-dernière phase attend la réponse `prelude` (choix par défaut), avec `dessstri` comme mot-de-passe. Enfin, pour la dernière phase, répondre `yes` si toutes les informations saisies sont correctes.

5.2 Configuration du manager

Éditez le fichier de configuration du manager `/usr/local/etc/prelude-manager/prelude-manager.conf` . Ensuite, faire apparaître les lignes suivantes (les décommenter si elles sont en commentaires, sinon, les écrire dans le fichier) :

Dans la rubrique Prelude Manager :

```
# Indiquer ici l'adresse et le port d'écoute des sondes par le serveur.
#Par défaut, c'est le port 5554 qui est utilisé.
sensors-srvr = 192.168.0.2 ;
```

Dans la rubrique MySQL :

```
# Les lignes ci-dessous sont valables même si le manager
#et les sondes ne sont pas sur la même machine.
[MySQL]
dbhost = localhost ;
dbname = prelude ;
dbuser = prelude ;
dbpass = dessstri ;
```

5.3 Configuration de la sonde réseau (nids)

Éditez le fichier de configuration de la sonde réseau `/usr/local/etc/prelude-nids/prelude-nids.conf` . Ensuite, faire apparaître les lignes suivantes (les décommenter si elles sont en commentaires, sinon, les écrire dans le fichier) :

```
manager-addr = 192.168.0.2;
user = prelude;
```
Ici, le manager se trouve sur la même machine, sinon, indiquez l'adresse IP de la machine hébergeant le manager. Au cas où le port de communication par défaut serait changé, il faudra l'indiquer à la suite de l'adresse IP, en séparant l'adresse IP et le port de communication de 2 points :
```
manager-addr = 192.168.0.2 :5554;
```

5.4 Configuration de la sonde hôte (lml)

Éditez le fichier de configuration de la sonde hôte `/usr/local/etc/prelude-lml/prelude-lml.conf` . Ensuite, faire apparaître les lignes suivantes (les décommenter si elles sont en commentaires, sinon, les écrire dans le fichier) :
```
manager-addr = 192.168.0.2;
```
Ici, le manager se trouve sur la même machine, sinon, indiquez l'adresse IP de la machine hébergeant le manager. Au cas où le port de communication par défaut serait changé, il faudra l'indiquer à la suite de l'adresse IP, en séparant l'adresse IP et le port de communication de 2 points :
```
manager-addr = 192.168.0.2 :5554;
```

6 Lancement de l'écoute

Sur le manager, tapez la commande suivante, dans un terminal, pour créer un utilisateur et avoir un mot-de-passe :
```
manager-adduser
```
Il sera donné un mot-de-passe à garder.

Sur la sonde, tapez la commande suivant, dans un terminal, pour lancer l'ajout d'un utilisateur dans le sensor :
Pour la sonde réseau, avec 192.168.0.2 pour adresse du manager :
```
sensor-adduser -s prelude-nids -m 192.168.0.2 -u 0
```

Pour la sonde hôte, avec 192.168.0.2 pour adresse du manager :
```
sensor-adduser -s prelude-lml -m 192.168.0.2 -u 0
```

Dans un cas comme dans l'autre, la suite est la même. Il est demandé de rentrer le mot-de-passe noté (lors du `manager-adduser`), puis d'indiquer le nom de l'utilisateur (`prelude`) et son mot-de-passe (`dessstri`). Ensuite on accepte de créer cet utilisateur.

On lance ensuite le manager par la commande :
```
prelude-manager
```

Nous pouvons nous affranchir du fichier de configuration en donnant les paramètres en arguments. Dans notre cas, cela va donner ceci :

```
prelude-manager --mysql --dbhost localhost --dbname prelude --dbuser prelude
 --dbpass dessstri
```

Puis on lance la sonde avec la commande pour la sonde réseau (eth0 est l'interface d'écoute du réseau) :
```
prelude-nids -i eth0 -u root
```
ou avec la commande suivante pour la sonde hôte :
```
prelude-lml -u root
```
Il est à noter qu'il faut créer un nouvel utilisateur (`manager-adduser`) pour chaque nouvelle sonde. En revanche, un manager peut écouter, en même temps, les remontées d'alertes de plusieurs sondes.

7 Installation et configuration du prelude-php-frontend

7.1 Installation

Étant donné que le prelude-php-frontend se base sur un serveur web, nous installerons Apache-ssl, ainsi que php4.

```
apt-get install apache-ssl php4 php4-mysql
```

Accepter l'ajout de `extension=mysql.so` qui est proposé pendant l'installation.
Ensuite se placer dans le répertoire contenant les sources compressées du prelude-php-frontend, les décompresser, et les mettre dans le répertoire du serveur Apache-ssl :

```
cd /usr/local/src/
tar -xzf prelude-php-frontend-0.8.1.tar.gz
```

Est maintenant apparu le répertoire `prelude-php-frontend` que nous copions dans le répertoire du serveur web (`/var/www/`par défaut).

```
cp -r prelude-php-frontend /var/www/
```

7.2 Configuration

Éditez le fichier de configuration d'Apache (`/etc/apache-ssl/httpd.conf`), et y écrire où décommenter les lignes suivantes (la machine a pour adresse IP 192.168.0.2) :

```
Listen 192.168.0.2
LoadModule php4_module /usr/lib/apache/1.3/libphp4.so
DirectoryIndex index.php index.html index.htm
ServerName localhost
DocumentRoot /var/www/
```

Éditez le fichier de configuration du prelude-php-frontend (`/var/www/prelude-php-frontend/config.php`), et y écrire où décommenter les lignes suivantes :

```
$server[1]['description'] = "SYSDOOR/MySQL phpfront v".VERSION;
$server[1]['dbtype'] = USE_DB_MYSQL
$server[1]['dbusername'] = "prelude"
$server[1]['dbpassword'] = "dessstri"
$server[1]['dbhostname'] = LOCAL_CONNECTION;
$server[1]['dbport'] = DEFAULT_PORT
$server[1]['dbname'] = "prelude"
```

Éditez le fichier `/var/www/prelude-php-frontend/index.php`, et y modifier la ligne `$serv = 0` en `$serv = 1`

Relancer le serveur web pour prendre en compte les changements :

```
/etc/init.d/apache-ssl restart
```

L'interface est maintenant accessible par *https ://localhost/prelude-php-frontend/*.

ATTENTION : Il y a actuellement un bogue dans le prelude-php-frontend qui fait qu'il est retourné un ligne d'erreur dans l'affichage de la page, lorsque la base de données MySQL est vide. Il suffit donc d'attendre de recevoir quelques alertes avant d'utiliser l'interface.

8 Installation et configuration du prelude-perl-frontend

8.1 Installation préalable de paquetages

Il faut biensûr que perl et quelques autres modules soient installés. Pour cela, tapez la commande suivante :
`apt-get install libdbi-perl libgd-graph-perl libdate-calc-perl apache-ssl`

8.2 Installation de prelude-perl-frontend

Télécharger les sources que www.leroutier.net/Projects/
Nous utiliserons ici les sources suivantes :
`2003-02-12-prelude-perl-web-frontend.tar.gz`
On les décompresse dans le répertoir `/var/www/frontend-perl`.

Dans le fichier de configuration d'Apache, il y a entre autres :

```
User www-data
Group www-data
```

Ils définissent le profil utilisateur d'Apache. On va changer les droits des fichiers du frontend-perl selon ces paramètres :

```
chown -R www-data.www-data /var/www/frontend-perl
chmod -R u+x /var/www/frontend-perl/
```

8.3 Configuration d'Apache

Modifez le fichier `/etc/apache-ssl/httpd.conf`, pour avoir les lignes suivantes : `Listen 192.168.0.2`

```
DirectoryIndex index.pl index.html index.htm
ServerName localhost
DocumentRoot /var/www/
```

et rajouter les lignes suivantes :

```
     <Directory "/var/www/frontend-perl/">
       Options ExecCGI
       AddHandler cgi-script .pl
     </Directory>
```

Puis transformer

```
# If the perl module is installed, this will be enabled.
<IfModule mod_perl.c>
  Alias /perl/ /var/www/perl/
  <Location /perl>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
  </Location>
</IfModule>
```

en ce qui suit

```
# If the perl module is installed, this will be enabled.
<IfModule mod_perl.c>
  Alias /perl/ /var/www/frontend-perl/
  <Location /perl/>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
  </Location>
</IfModule>
```

8.4 Configuration de prelude-perl-frontend

Éditer le fichier `/var/www/frontend-perl/Functions/config.pl` pour y faire apparaître les lignes suivantes :

```
  $conf{'dbtype'}='mysql';
  $conf{'dbname'}='prelude';
  $conf{'dbhost'}='localhost';
  $conf{'dbport'}=3306; # default mysql port is 3306
  $conf{'dblogin'}='prelude';
  $conf{'dbpasswd'}='dessstri';
```

L'interface est maintenant accessible par *https ://localhost/frontend-perl/* avec le login *prelude* et le mot-de-passe *dessstri*.

Les dernières versions de piwi permettent de supprimer les alertes dans la base de données, mais pour cela il faut se connecter à piwi sous le profil `admin`, et non `guest` comme c'est le cas par défaut. Ou bien, si on veut que `guest` puisse aussi supprimer des alertes dans la base de données, éditez le fichier `/var/www/frontend-perl/Profiles/guest.user` :

```
 # User full-name :
FullName=guest
 # IP Access mask. 255.255.255.255 means any IP :
IPAccess=255.255.255.255
 # Delete privilege : (if 'none', can't delete any alert)
priv_delete=none
 # User privilege : (if 'none', can't create/modify/delete any user profile)
priv_user=none
 # Process privilige: (if 'none', can't start processing of alerts)
priv_process=none
```

Il suffit alors de changer les valeurs des options de `none` à `all` comme c'est déjà le cas dans le fichier `/var/www/frontend-perl/Profiles/admin.user` :

```
 # User full-name :
FullName=Administrator
 # IP Access mask. 255.255.255.255 means any IP :
IPAccess=127.0.0.1
 # Delete privilege : (if 'none', can't delete any alert)
priv_delete=all
 # User privilege : (if 'none', can't create/modify/delete any user profile)
priv_user=all
 # Process privilige: (if 'none', can't start processing of alerts)
priv_process=all
```

9 Licence

10 Liens

Site officiel de Prelude-IDS : http ://www.prelude-ids.org

Dernière version de ce document : http ://lehmann.free.fr

Téléchargement des paquetages de Prelude-IDS :
http ://www.prelude-ids.org/rubrique.php3 ?id_rubrique=6

Autres documentations à propos de Prelude-IDS :
http ://www.prelude-ids.org/rubrique.php3 ?id_rubrique=1

Site officiel du frontend perl : http ://www.leroutier.net/Projects/

Site de Debian : http ://www.debian.org

Se procurer Debian sur CD : http ://ikarios.com/form/

A Liste de paquetages installés sur le système (pas à jour)

Voici ce que donne l'exécution de la commande `dpkg -l` :

```
Desired=Unknown/Install/Remove/Purge/Hold
| Status=Not/Installed/Config-files/Unpacked/Failed-config/Half-installed
|/ Err?=(none)/Hold/Reinst-required/X=both-problems (Status,Err: uppercase=ba
||/ Name           Version        Description
+++-==============-==============-============================================
ii  adduser        3.49           Add and remove users and groups
ii  apache-common  1.3.26-1.1     Support files for all Apache webservers
ii  apache-ssl     1.3.26.1+1.48- Versatile, high-performance HTTP server wit
ii  apt            0.5.4          Advanced front-end for dpkg
ii  apt-utils      0.5.4          APT utility programs
ii  at             3.1.8-11       Delayed job execution and batch processing
ii  aterm          0.4.2-4        Afterstep XVT - a VT102 emulator for the X
ii  base-config    1.54           Debian base configuration package
ii  base-files     3.0.7          Debian base system miscellaneous files
ii  base-passwd    3.4.2          Debian Base System Password/Group Files
ii  bash           2.05b-3        The GNU Bourne Again SHell
ii  bc             1.06-8         The GNU bc arbitrary precision calculator la
ii  biff           0.17.pre200004 a mail notification tool
ii  bin86          0.16.3-2       16-bit assembler and loader
ii  bind9-host     9.2.1-4        Version of 'host' bundled with BIND 9.X
ii  binutils       2.13.90.0.10-1 The GNU assembler, linker and binary utilit
ii  bison          1.75-1         A parser generator that is compatible with
ii  bsdmainutils   5.20020211-7   More utilities from FreeBSD.
ii  bsdutils       2.11n-4        Basic utilities from 4.4BSD-Lite.
ii  console-common 0.7.20         Basic infrastructure for text console confi
ii  console-data   2002.12.04dbs- Keymaps, fonts, charset maps, fallback tabl
ii  console-tools  0.2.3-23.3     Linux console and font utilities.
ii  console-tools- 0.2.3-23.3     Shared libraries for Linux console and font
ii  coreutils      4.5.2-1        The GNU core utilities
ii  cpio           2.5-1          GNU cpio -- a program to manage archives of
ii  cpp            2.95.4-17      The GNU C preprocessor.
ii  cpp-2.95       2.95.4-11woody The GNU C preprocessor.
ii  cpp-3.0        3.0.4-7        The GNU C preprocessor.
ii  cron           3.0pl1-72      management of regular background processing
ii  dc             1.06-8         The GNU dc arbitrary precision reverse-poli
ii  debconf        1.2.21         Debian configuration management system
ii  debianutils    1.16.7         Miscellaneous utilities specific to Debian
ii  defoma         0.11.1         Debian Font Manager -- automatic font confi
ii  dhcp-client    2.0pl5-14      DHCP Client
ii  dialog         0.9b-20020814- Displays user-friendly dialog boxes from sh
ii  diff           2.8.1-1        File comparison utilities
ii  dnsutils       9.2.1-4        Clients provided with BIND
ii  doc-debian     3.0.2          Debian Project documentation, Debian FAQ an
ii  doc-linux-text 2003.01-1      Linux HOWTOs, mini-HOWTOs, and FAQs in ASCI
ii  docbook        4.2-2          SGML DTD for authors of technical documenta
ii  docbook-dsssl  1.77-2         Modular DocBook DSSSL stylesheets, for prin
ii  docbook-to-man 2.0.0-10       Converter from DocBook SGML into roff -man
```

```
ii  dpkg           1.10.9         Package maintenance system for Debian
ii  dpkg-dev       1.10.9         Package building tools for Debian
ii  dselect        1.10.9         a user tool to manage Debian packages
ii  e2fsprogs      1.29+1.30-WIP- The EXT2 file system utilities and librarie
ii  ed             0.2-19         The classic unix line editor
ii  emacs20        20.7-13.1      The GNU Emacs editor.
ii  emacsen-common 1.4.15         Common facilities for all emacsen.
ii  ethereal       0.9.5-2        Network traffic analyzer
ii  ethereal-commo 0.9.5-2        Network traffic analyser (common files)
ii  exim           3.36-3         An MTA (Mail Transport Agent)
ii  fdutils        5.4-20020222-3 Linux floppy utilities
ii  file           3.39-1         Determines file type using "magic" numbers
ii  fileutils      4.5.2-1        GNU file management utilities
ii  findutils      4.1.7-2        utilities for finding files--find, xargs, a
ii  finger         0.17-6         User information lookup program.
ii  flex           2.5.4a-27      A fast lexical analyzer generator.
ii  ftp            0.17-10        The FTP client.
ii  g++            2.95.4-17      The GNU C++ compiler.
ii  g++-2.95       2.95.4-11woody The GNU C++ compiler.
ii  gcc            2.95.4-17      The GNU C compiler.
ii  gcc-2.95       2.95.4-11woody The GNU C compiler.
ii  gcc-3.0        3.0.4-7        The GNU C compiler.
ii  gcc-3.0-base   3.0.4-7        The GNU Compiler Collection (base package).
ii  gdb            5.2.cvs2002040 The GNU Debugger
ii  gettext-base   0.10.40-8      GNU Internationalization utilities for the
ii  gnupg          1.2.0-1        GNU privacy guard - a free PGP replacement.
ii  gnupg-doc      2000.10.01-1   GNU privacy guard documentation.
ii  grep           2.4.2-3        GNU grep, egrep and fgrep.
ii  groff-base     1.18-7         GNU troff text-formatting system (base syst
ii  gsfonts        6.0-2.1        Fonts for the ghostscript interpreter
ii  gtk-doc-tools  1.0-4          GTK documentation tools
ii  gzip           1.3.5-1        The GNU compression utility.
ii  hermes1        1.3.2-3        The Hermes pixel-format library
ii  hostname       2.09           A utility to set/show the host name or doma
ii  iamerican      3.1.20.0-1     An American English dictionary for ispell.
ii  ibritish       3.1.20.0-1     A British English dictionary for ispell.
ii  ifupdown       0.6.4-4.4      High level tools to configure network inter
ii  info           4.2-1          Standalone GNU Info documentation browser
ii  ipchains       1.3.10-15      Network firewalling for Linux 2.2.x
ii  ipmasqadm      0.4.2-2        Utility for configuring extra masquerading
ii  iptables       1.2.7a-7       IP packet filter administration tools for 2
ii  ispell         3.1.20.0-1     International Ispell (an interactive spelli
ii  jade           1.2.1-28       James Clark's DSSSL Engine
ii  kdelibs3       2.2.2-13       KDE core libraries (runtime files)
ii  kdelibs3-bin   2.2.2-13       KDE core binaries (binary files)
ii  kdm            2.2.2-14       The K Desktop Manager
ii  klogd          1.4.1-10       Kernel Logging Daemon
ii  less           378-2          A file pager program, similar to more(1)
ii  libbz2-1.0     1.0.2-1        A high-quality block-sorting file compresso
ii  libc6          2.2.5-14.3     GNU C Library: Shared libraries and Timezon
```

```
ii  libc6-dev      2.2.5-14.3     GNU C Library: Development Libraries and He
ii  libcap1        1.10-12        support for getting/setting POSIX.1e capabi
ii  libdate-calc-p 5.0-3          Perl library for accessing dates
ii  libdb1-compat  2.1.3-7        The Berkeley database routines [glibc 2.0/2
ii  libdb2         2.7.7.0-8      The Berkeley database routines (run-time fi
ii  libdb3         3.2.9-17       Berkeley v3 Database Libraries [runtime]
ii  libdb4.0       4.0.14-1       Berkeley v4.0 Database Libraries [runtime]
ii  libdbi-perl    1.21-2         The Perl5 Database Interface by Tim Bunce
ii  libdns5        9.2.1-4        DNS Shared Library used by BIND
ii  libdps1        4.2.1-3        Display PostScript (DPS) client library
ii  libexpat1      1.95.2-9       XML parsing C library - runtime library
ii  libfam0        2.6.8-3        client library to control the FAM daemon
ii  libfreetype6   2.1.2-9        FreeType 2 font engine, shared library file
ii  libgcc1        3.2.1-0pre3    GCC support library.
ii  libgd-graph-pe 1.35-3         Graph Plotting Module for Perl 5
ii  libgd-perl     1.40-1         Perl module wrapper for libgd
ii  libgd-text-per 0.83-3         Text utilities for use with GD
ii  libgd1         1.8.4-17       GD Graphics Library
ii  libgdbmg1      1.7.3-27.1     GNU dbm database routines (runtime version)
ii  libglib1.2     1.2.10-6       The GLib library of C routines
ii  libgtk1.2      1.2.10-14      The GIMP Toolkit set of widgets for X
ii  libgtk1.2-comm 1.2.10-14      Common files for the GTK+ library
ii  libident       0.22-2         simple RFC1413 client library - runtime
ii  libisc4        9.2.1-4        ISC Shared Library used by BIND
ii  libjpeg62      6b-6           The Independent JPEG Group's JPEG runtime l
ii  liblcms        1.08-3         Color management library
ii  libldap2       2.0.23-14      OpenLDAP libraries (without TLS support).
ii  liblockfile1   1.03           NFS-safe locking library, includes dotlockf
ii  liblwres1      9.2.1-4        Lightweight Resolver Library used by BIND
ii  libmm11        1.1.3-6        Shared memory library
ii  libmng1        1.0.3-3        Multiple-image Network Graphics library
ii  libmysqlclient 3.23.52-2      mysql database client library
ii  libmysqlclient 3.23.52-2      mysql database development files
ii  libncurses5    5.2.20020112a- Shared libraries for terminal handling
ii  libnewt0       0.50.17-9.6    Not Erik's Windowing Toolkit - text mode wi
ii  libnspr4       1.0.0-0.woody. Netscape Portable Runtime Library
ii  libnss-db      2.2-6          DB Name Service Module
ii  libnss3        1.0.0-0.woody. Network Security Service Libraries - runtim
ii  libpam-modules 0.76-7         Pluggable Authentication Modules for PAM
ii  libpam-runtime 0.76-7         Runtime support for the PAM library
ii  libpam0g       0.76-7         Pluggable Authentication Modules library
ii  libpaperg      1.1.8          Library for handling paper characteristics
ii  libpcap0       0.6.2-2        System interface for user-level packet capt
ii  libpcre3       3.4-1.1        Philip Hazel's Perl Compatible Regular Expr
ii  libperl5.6     5.6.1-8.2      Shared Perl library.
ii  libpng2        1.0.12-6       PNG library - runtime
ii  libpopt0       1.6.4-2        lib for parsing cmdline parameters
ii  libqt2         2.3.1-22       Qt GUI Library (runtime version).
ii  libreadline4   4.3-4          GNU readline and history libraries, run-tim
ii  libsasl7       1.5.27-3.3     Authentication abstraction library.
```

```
ii  libsp1          1.3.4-1.2.1-28 Runtime library for James Clark's SP suite
ii  libssl-dev      0.9.6g-6       SSL development libraries, header files and
ii  libssl0.9.6     0.9.6g-6       SSL shared libraries
ii  libstdc++2.10-  2.95.4-11woody The GNU stdc++ library (development files)
ii  libstdc++2.10-  2.95.4-11woody The GNU stdc++ library
ii  libstdc++3      3.0.4-7        The GNU stdc++ library version 3
ii  libtiff3g       3.5.5-6        Tag Image File Format library
ii  libungif4g      4.1.0b1-3      shared library for GIF images (runtime lib)
ii  libwrap0        7.6-ipv6.1-3   Wietse Venema's TCP wrappers library
ii  libwraster2     0.80.1-3       Shared libraries of Window Maker rasterizer
ii  libxaw7         4.2.1-3        X Athena widget set library
ii  libxml2         2.4.24-1       GNOME XML library
ii  libxml2-dev     2.4.24-1       Development files for the GNOME XML library
ii  libxslt1        1.0.21-0.2     XSLT processing library
ii  lilo            22.3.3-2       LInux LOader - The Classic OS loader can lo
ii  locales         2.2.5-14.3     GNU C Library: National Language (locale) d
ii  login           20000902-12    System login tools
ii  logrotate       3.6.5-2        Log rotation utility
ii  lpr             2000.05.07-4.2 BSD lpr/lpd line printer spooling system
ii  lsof            4.64-1         List open files.
ii  lynx            2.8.4.1b-3.2   Text-mode WWW Browser
ii  m4              1.4-14         a macro processing language
ii  mailx           8.1.2-0.200204 A simple mail user agent.
ii  make            3.79.1-15      The GNU version of the "make" utility.
ii  makedev         2.3.1-62       Creates device files in /dev.
ii  man-db          2.4.0-10       The on-line manual pager
ii  manpages        1.48-2         Manual pages about using a GNU/Linux system
ii  manpages-dev    1.48-2         Manual pages about using GNU/Linux for deve
ii  mawk            1.3.3-9        a pattern scanning and text processing lang
ii  mbr             1.1.5-1        Master Boot Record for IBM-PC compatible co
ii  mime-support    3.20-1         MIME files 'mime.types' & 'mailcap', and su
ii  modconf         0.2.44         Device Driver Configuration
ii  modutils        2.4.19-3       Linux module utilities.
ii  mount           2.11n-4        Tools for mounting and manipulating filesys
ii  mozilla         1.0.0-0.woody. Mozilla Web Browser - dummy package
ii  mozilla-browse  1.0.0-0.woody. Mozilla Web Browser - core and browser
ii  mozilla-mailne  1.0.0-0.woody. Mozilla Web Browser - mail and news support
ii  mozilla-psm     1.0.0-0.woody. Mozilla Web Browser - Personal Security Man
ii  mpack           1.5-9          Tools for encoding/decoding MIME messages.
ii  mtools          3.9.8-10       Tools for manipulating MSDOS files
ii  mtr-tiny        0.51-1         Full screen ncurses traceroute tool
ii  mutt            1.4.0-4        Text-based mailreader supporting MIME, GPG,
ii  mysql-client    3.23.52-2      mysql database client binaries
ii  mysql-common    3.23.52-2      mysql database common files (e.g. /etc/mysq
ii  mysql-server    3.23.52-2      mysql database server binaries
ii  nano            1.1.11-1       free Pico clone with some new features
ii  ncurses-base    5.2.20020112a- Descriptions of common terminal types
ii  ncurses-bin     5.2.20020112a- Terminal-related programs and man pages
ii  ncurses-term    5.2.20020112a- Additional terminal type definitions
ii  net-tools       1.60-4         The NET-3 networking toolkit
```

```
ii  netbase        4.09           Basic TCP/IP networking system
ii  netkit-inetd   0.10-9         The Internet Superserver
ii  netkit-ping    0.10-9         The ping utility from netkit
ii  nfs-common     1.0.2-1        NFS support files common to client and serv
ii  nfs-kernel-ser 1.0.2-1        Kernel NFS server support
ii  nmap           3.00-0.1       The Network Mapper
ii  nvi            1.79-20        4.4BSD re-implementation of vi.
ii  openssl        0.9.6g-6       Secure Socket Layer (SSL) binary and relate
ii  passwd         20000902-12    Change and administer password and group da
ii  patch          2.5.4-11       Apply a diff file to an original
ii  pciutils       2.1.10-3       Linux PCI Utilities (for 2.[12345].x kernel
ii  perl           5.6.1-8.2      Larry Wall's Practical Extraction and Repor
ii  perl-base      5.6.1-8.2      The Pathologically Eclectic Rubbish Lister.
ii  perl-modules   5.6.1-8.2      Core Perl modules.
ii  php4           4.1.2-4        A server-side, HTML-embedded scripting langu
ii  php4-mysql     4.1.2-4        MySQL module for php4
ii  pidentd        3.0.12-4       TCP/IP IDENT protocol server.
ii  portmap        5-2            The RPC portmapper
ii  ppp            2.4.1.uus-4    Point-to-Point Protocol (PPP) daemon.
ii  pppconfig      2.1            A text menu based utility for configuring p
ii  pppoe          3.3-1.2        PPP over Ethernet driver
ii  pppoeconf      0.9.10.8       configures PPPoE/ADSL
ii  procmail       3.22-4         Versatile e-mail processor.
ii  procps         2.0.7-10       The /proc file system utilities.
ii  psmisc         21.2-1         Utilities that use the proc filesystem
ii  python         2.1.3-4        An interactive object-oriented scripting la
ii  python-newt    0.50.17-9.6    A newt module for Python.
ii  python2.1      2.1.3-4        An interactive object-oriented scripting la
ii  rcs            5.7-13         The GNU Revision Control System
ii  reportbug      1.50           Reports bugs in the Debian distribution.
ii  sed            3.02-8         The GNU sed stream editor.
ii  setserial      2.17-30        Controls configuration of serial ports.
ii  sgml-base      1.17           utilities to maintain SGML catalog files
ii  sgml-data      1.8            Common SGML and XML DTDs and entities
ii  sharutils      4.2.1-9        shar, unshar, uuencode, uudecode
ii  shellutils     4.5.2-1        The GNU shell programming utilities.
ii  slang1         1.4.5-1        The S-Lang programming library - runtime ve
ii  sp             1.3.4-1.2.1-28 James Clark's SGML parsing tools
ii  ssh            3.4p1-4        Secure rlogin/rsh/rcp replacement (OpenSSH)
ii  strace         4.4-1.2        A system call tracer.
ii  sysklogd       1.4.1-10       System Logging Daemon
ii  syslinux       1.75-1         Bootloader for Linux/i386 using MS-DOS flop
ii  sysvinit       2.84-3         System-V like init.
ii  t1lib1         1.3.1-1        Type 1 font rasterizer library - runtime
ii  tar            1.13.25-3      GNU tar
ii  tasksel        1.21           Tool for selecting tasks for installation o
ii  tcpd           7.6-ipv6.1-3   Wietse Venema's TCP wrapper utilities
ii  tcsh           6.11.00-2.2    TENEX C Shell, an enhanced version of Berke
ii  telnet         0.17-19        The telnet client.
ii  texinfo        4.2-1          Documentation system for on-line informatio
```

```
ii  textutils      4.5.2-1        The GNU text file processing utilities
ii  time           1.7-15         The GNU time command.
ii  util-linux     2.11n-4        Miscellaneous system utilities.
ii  util-linux-loc 2.11n-4        Locales files for util-linux
ii  vacation       3.2.5          email autoresponder
ii  wenglish       2.0-2          English dictionary words for /usr/share/dic
ii  whiptail       0.50.17-9.6    Displays user-friendly dialog boxes from sh
ii  whois          4.5.31         The GNU whois client
ii  wmaker         0.80.1-3       NeXTSTEP-like window manager for X
ii  xbase-clients  4.2.1-3        miscellaneous X clients
ii  xfonts-100dpi  4.2.1-3        100 dpi fonts for X
ii  xfonts-base    4.2.1-3        standard fonts for X
ii  xfree86-common 4.2.1-3        X Window System (XFree86) infrastructure
ii  xfs            4.2.1-3        X font server
ii  xfs-xtt        1.3.0.xf420-8  X-TrueType font server
ii  xlibmesa3      4.2.1-3        XFree86 version of Mesa 3D graphics library
ii  xlibs          4.2.1-3        X Window System client libraries
ii  xpdf           1.01-3         Portable Document Format (PDF) suite
ii  xpdf-common    1.01-3         Portable Document Format (PDF) suite -- com
ii  xpdf-reader    1.01-3         Portable Document Format (PDF) suite -- vie
ii  xpdf-utils     1.01-3         Portable Document Format (PDF) suite -- uti
ii  xserver-common 4.2.1-3        files and utilities common to all X servers
ii  xserver-xfree8 4.2.1-3        the XFree86 X server
ii  xsltproc       1.0.21-0.2     XSLT command line processor
ii  xterm          4.2.1-3        X terminal emulator
ii  xutils         4.2.1-3        X Window System utility programs
ii  zlib1g         1.1.4-6        compression library - runtime
ii  zlib1g-dev     1.1.4-6        compression library - development
```

B Fichier httpd.conf

```
##
## httpd.conf -- Apache HTTP server configuration file
##

#
# Based upon the NCSA server configuration files originally by Rob McCool.
#
# This is the main Apache server configuration file.  It contains the
# configuration directives that give the server its instructions.
# See <URL:http://www.apache.org/docs/> for detailed information about
# the directives.
#
# Do NOT simply read the instructions in here without understanding
# what they do.  They're here only as hints or reminders.  If you are unsure
# consult the online docs. You have been warned.
#
# After this file is processed, the server will look for and process
```

```
# /etc/apache-ssl/srm.conf and then /etc/apache-ssl/access.conf
# unless you have overridden these with ResourceConfig and/or
# AccessConfig directives here.
#
# The configuration directives are grouped into three basic sections:
#  1. Directives that control the operation of the Apache server process as a
#     whole (the 'global environment').
#  2. Directives that define the parameters of the 'main' or 'default' server
#     which responds to requests that aren't handled by a virtual host.
#     These directives also provide default values for the settings
#     of all virtual hosts.
#  3. Settings for virtual hosts, which allow Web requests to be sent to
#     different IP addresses or hostnames and have them handled by the
#     same Apache server process.
#
# Configuration and logfile names: If the filenames you specify for many
# of the server's control files begin with "/" (or "drive:/" for Win32), the
# server will use that explicit path.  If the filenames do *not* begin
# with "/", the value of ServerRoot is prepended -- so "logs/foo.log"
# with ServerRoot set to "/usr/local/apache" will be interpreted by the
# server as "/usr/local/apache/logs/foo.log".
#

### Section 1: Global Environment
#
# The directives in this section affect the overall operation of Apache,
# such as the number of concurrent requests it can handle or where it
# can find its configuration files.
#

#
# ServerType is either inetd, or standalone.  Inetd mode is only supported on
# Unix platforms.
# SSL Servers MUST be standalone, currently.
#
ServerType standalone

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

```
#
# The LockFile directive sets the path to the lockfile used when Apache
# is compiled with either USE_FCNTL_SERIALIZED_ACCEPT or
# USE_FLOCK_SERIALIZED_ACCEPT. This directive should normally be left at
# its default value. The main reason for changing it is if the logs
# directory is NFS mounted, since the lockfile MUST BE STORED ON A LOCAL
# DISK. The PID of the main server process is automatically appended to
# the filename.
#
LockFile /var/lock/apache.lock

#
# PidFile: The file in which the server should record its process
# identification number when it starts.
#
PidFile /var/run/apache-ssl.pid

#
# ScoreBoardFile: File used to store internal server process information.
# Not all architectures require this.  But if yours does (you'll know because
# this file will be  created when you run Apache) then you *must* ensure that
# no two invocations of Apache share the same scoreboard file.
#
ScoreBoardFile /var/run/apache-ssl.scoreboard

#
# In the standard configuration, the server will process this file,
# srm.conf, and access.conf in that order.  The latter two files are
# now distributed empty, as it is recommended that all directives
# be kept in a single file for simplicity.  The commented-out values
# below are the built-in defaults.  You can have the server ignore
# these files altogether by using "/dev/null" (for Unix) or
# "nul" (for Win32) for the arguments to the directives.
#
#ResourceConfig /etc/apache-ssl/srm.conf
#AccessConfig /etc/apache-ssl/access.conf

#
# 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 15

#
# Server-pool size regulation.  Rather than making you guess how many
# server processes you need, Apache dynamically adapts to the load it
# sees --- that is, it tries to maintain enough server processes to
# handle the current load, plus a few spare servers to handle transient
# load spikes (e.g., multiple simultaneous requests from a single
# Netscape browser).
#
# It does this by periodically checking how many servers are waiting
# for a request.  If there are fewer than MinSpareServers, it creates
# a new spare.  If there are more than MaxSpareServers, some of the
# spares die off.  The default values are probably OK for most sites.
#
MinSpareServers 5
MaxSpareServers 10

#
# Number of servers to start initially --- should be a reasonable ballpark
# figure.
#
StartServers 5

#
# Limit on total number of servers running, i.e., limit on the number
# of clients who can simultaneously connect --- if this limit is ever
# reached, clients will be LOCKED OUT, so it should NOT BE SET TOO LOW.
# It is intended mainly as a brake to keep a runaway server from taking
# the system with it as it spirals down...
#
MaxClients 150

#
# MaxRequestsPerChild: the number of requests each child process is
# allowed to process before the child dies.  The child will exit so
# as to avoid problems after prolonged use when Apache (and maybe the
# libraries it uses) leak memory or other resources.  On most systems, this
# isn’t really needed, but a few (such as Solaris) do have notable leaks
```

```
# in the libraries. For these platforms, set to something like 10000
# or so; a setting of 0 means unlimited.
#
# NOTE: This value does not include keepalive requests after the initial
#       request per connection. For example, if a child process handles
#       an initial request and 10 subsequent "keptalive" requests, it
#       would only count as 1 request towards this limit.
#
MaxRequestsPerChild 100

#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, in addition to the default. See also the <VirtualHost>
# directive.
#
#Listen 3000
Listen 192.168.0.2

#
# BindAddress: You can support virtual hosts with this option. This directive
# is used to tell the server which IP address to listen to. It can either
# contain "*", an IP address, or a fully qualified Internet domain name.
# See also the <VirtualHost> and Listen directives.
#
#BindAddress *

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO yo
# have to place corresponding ‘LoadModule’ lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Please read the file README.DSO in the Apache 1.3 distribution for more
# details about the DSO mechanism and run ‘apache -l’ for the list of already
# built-in (statically linked and thus always available) modules in your apac
# binary.
#
# Please keep this LoadModule: line here, it is needed for installation.
# LoadModule vhost_alias_module /usr/lib/apache/1.3/mod_vhost_alias.so
# LoadModule env_module /usr/lib/apache/1.3/mod_env.so
LoadModule config_log_module /usr/lib/apache/1.3/mod_log_config_ssl.so
LoadModule mime_magic_module /usr/lib/apache/1.3/mod_mime_magic.so
LoadModule mime_module /usr/lib/apache/1.3/mod_mime_ssl.so
LoadModule negotiation_module /usr/lib/apache/1.3/mod_negotiation.so
LoadModule status_module /usr/lib/apache/1.3/mod_status.so
# LoadModule info_module /usr/lib/apache/1.3/mod_info.so
# LoadModule includes_module /usr/lib/apache/1.3/mod_include.so
LoadModule autoindex_module /usr/lib/apache/1.3/mod_autoindex.so
LoadModule dir_module /usr/lib/apache/1.3/mod_dir.so
LoadModule cgi_module /usr/lib/apache/1.3/mod_cgi.so
```

```
# LoadModule asis_module /usr/lib/apache/1.3/mod_asis.so
# LoadModule imap_module /usr/lib/apache/1.3/mod_imap.so
# LoadModule action_module /usr/lib/apache/1.3/mod_actions.so
# LoadModule speling_module /usr/lib/apache/1.3/mod_speling.so
LoadModule userdir_module /usr/lib/apache/1.3/mod_userdir.so
LoadModule alias_module /usr/lib/apache/1.3/mod_alias.so
LoadModule rewrite_module /usr/lib/apache/1.3/mod_rewrite.so
LoadModule access_module /usr/lib/apache/1.3/mod_access.so
LoadModule auth_module /usr/lib/apache/1.3/mod_auth_ssl.so
# LoadModule anon_auth_module /usr/lib/apache/1.3/mod_auth_anon.so
# LoadModule dbm_auth_module /usr/lib/apache/1.3/mod_auth_dbm.so
# LoadModule db_auth_module /usr/lib/apache/1.3/mod_auth_db.so
# LoadModule proxy_module /usr/lib/apache/1.3/libproxy.so
# LoadModule digest_module /usr/lib/apache/1.3/mod_digest.so
# LoadModule cern_meta_module /usr/lib/apache/1.3/mod_cern_meta.so
LoadModule expires_module /usr/lib/apache/1.3/mod_expires.so
# LoadModule headers_module /usr/lib/apache/1.3/mod_headers.so
# LoadModule usertrack_module /usr/lib/apache/1.3/mod_usertrack.so
LoadModule unique_id_module /usr/lib/apache/1.3/mod_unique_id.so
LoadModule setenvif_module /usr/lib/apache/1.3/mod_setenvif.so
# LoadModule sys_auth_module /usr/lib/apache/1.3/mod_auth_sys.so
# LoadModule put_module /usr/lib/apache/1.3/mod_put.so
# LoadModule throttle_module /usr/lib/apache/1.3/mod_throttle.so
LoadModule apache_ssl_module /usr/lib/apache/1.3/libssl.so
# LoadModule allowdev_module /usr/lib/apache/1.3/mod_allowdev.so
# LoadModule eaccess_module /usr/lib/apache/1.3/mod_eaccess.so
# LoadModule roaming_module /usr/lib/apache/1.3/mod_roaming.so
LoadModule php4_module /usr/lib/apache/1.3/libphp4.so


#
# ExtendedStatus: controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information (ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On

### Section 2: 'Main' server configuration
#
# The directives in this section set up the values used by the 'main'
# server, which responds to any requests that aren't handled by a
# <VirtualHost> definition.  These values also provide defaults for
# any <VirtualHost> containers you may define later in the file.
#
# All of these directives may appear inside <VirtualHost> containers,
# in which case these default settings will be overridden for the
# virtual host being defined.
#

#
```

```
# If your ServerType directive (set earlier in the 'Global Environment'
# section) is set to "inetd", the next few directives don't have any
# effect since their settings are defined by the inetd configuration.
# Skip ahead to the ServerAdmin directive.
#

#
# Port: The port to which the standalone server listens. For
# ports < 1023, you will need apache to be run as root initially.
#
# The default port for SSL is 443...

Port 443

#
# If you wish apache to run as a different user or group, you must run
# apacheas root initially and it will switch.
#
# User/Group: The name (or #number) of the user/group to run apache as.
#  . On SCO (ODT 3) use "User nouser" and "Group nogroup".
#  . On HPUX you may not be able to use shared memory as nobody, and the
#    suggested workaround is to create a user www and use that user.
#  NOTE that some kernels refuse to setgid(Group) or semctl(IPC_SET)
#  when the value of (unsigned)Group is above 60000;
#  don't use Group nobody on these systems!
#
User www-data
Group www-data

#
# ServerAdmin: Your address, where problems with the server should be
# e-mailed.  This address appears on some server-generated pages, such
# as error documents.
#
ServerAdmin webmaster@manager

#
# ServerName: allows you to set a host name which is sent back to clients for
# your server if it's different than the one the program would get (i.e., use
# "www" instead of the host's real name).
#
# Note: You cannot just invent host names and hope they work. The name you
# define here must be a valid DNS name for your host. If you don't understand
# this, ask your network administrator.
# If your host doesn't have a registered DNS name, enter its IP address here.
# You will have to access it by its address (e.g., http://123.45.67.89/)
# anyway, and this will make redirections work in a sensible way.
#
ServerName localhost
```

```
#
# DocumentRoot: The directory out of which you will serve your
# documents. By default, all requests are taken from this directory, but
# symbolic links and aliases may be used to point to other locations.
#
DocumentRoot /var/www

#
# Each directory to which Apache has access, can be configured with respect
# to which services and features are allowed and/or disabled in that
# directory (and its subdirectories).
#
# First, we configure the "default" to be a very restrictive set of
# permissions.
#
<Directory />
    Options SymLinksIfOwnerMatch
    AllowOverride None
</Directory>

#
# Note that from this point forward you must specifically allow
# particular features to be enabled - so if something's not working as
# you might expect, make sure that you have specifically enabled it
# below.
#

#
# This should be changed to whatever you set DocumentRoot to.
#
<Directory /var/www/>

#
# This may also be "None", "All", or any combination of "Indexes",
# "Includes", "FollowSymLinks", "ExecCGI", or "MultiViews".
#
# Note that "MultiViews" must be named *explicitly* --- "Options All"
# doesn't give it to you.
#
    Options Indexes Includes FollowSymLinks MultiViews

#
# This controls which options the .htaccess files in directories can
# override. Can also be "All", or any combination of "Options", "FileInfo",
# "AuthConfig", and "Limit"
#
    AllowOverride None

#
# Controls who can get stuff from this server.
```

```
#
    Order allow,deny
    Allow from all
</Directory>

#
# UserDir: The name of the directory which is appended onto a user's home
# directory if a ~user request is received.
#
<IfModule mod_userdir.c>
    UserDir public_html
</IfModule>

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

#
# DirectoryIndex: Name of the file or files to use as a pre-written HTML
# directory index.  Separate multiple entries with spaces.
#
<IfModule mod_dir.c>
    DirectoryIndex index.pl index.php index.html index.htm index.shtml index.
</IfModule>

#
# AccessFileName: The name of the file to look for in each directory
# for access control information.
#
AccessFileName .htaccess

#
# The following lines prevent .htaccess files from being viewed by
# Web clients.  Since .htaccess files often contain authorization
# information, access is disallowed for security reasons.  Comment
# these lines out if you want Web visitors to see the contents of
# .htaccess files.  If you change the AccessFileName directive above,
```

```
# be sure to make the corresponding changes here.
#
# Also, folks tend to use names such as .htpasswd for password
# files, so this will protect those as well.
#
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>

#
# CacheNegotiatedDocs: By default, Apache sends "Pragma: no-cache" with each
# document that was negotiated on the basis of content. This asks proxy
# servers not to cache the document. Uncommenting the following line disables
# this behavior, and proxies will be allowed to cache the documents.
#
#CacheNegotiatedDocs

#
# UseCanonicalName:  (new for 1.3)  With this setting turned on, whenever
# Apache needs to construct a self-referencing URL (a URL that refers back
# to the server the response is coming from) it will use ServerName and
# Port to form a "canonical" name.  With this setting off, Apache will
# use the hostname:port that the client supplied, when possible.  This
# also affects SERVER_NAME and SERVER_PORT in CGI scripts.
#
UseCanonicalName On

#
# TypesConfig describes where the mime.types file (or equivalent) is
# to be found.
#
TypesConfig /etc/mime.types

#
# DefaultType is the default MIME type the server will use for a document
# if it cannot otherwise determine one, such as from filename extensions.
# If your server contains mostly text or HTML documents, "text/plain" is
# a good value.  If most of your content is binary, such as applications
# or images, you may want to use "application/octet-stream" instead to
# keep browsers from trying to display binary files as though they are
# text.
#
DefaultType text/plain

#
# The mod_mime_magic module allows the server to use various hints from the
# contents of the file itself to determine its type.  The MIMEMagicFile
# directive tells the module where the hint definitions are located.
# mod_mime_magic is not part of the default server (you have to add
```

```
# it yourself with a LoadModule [see the DSO paragraph in the 'Global
# Environment' section], or recompile the server and include mod_mime_magic
# as part of the configuration), so it's enclosed in an <IfModule> container.
# This means that the MIMEMagicFile directive will only be processed if the
# module is part of the server.
#
<IfModule mod_mime_magic.c>
    MIMEMagicFile share/magic
</IfModule>

#
# 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

# Note that Log files are now rotated by logrotate, not by apache itself.
# This means that apache no longer attempts to magically determine
# where your log files are kept; you have to fill out stanzas in
# /etc/logrotate.d/apache-ssl yourself.

#
# 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 /var/log/apache-ssl/error.log

#
# LogLevel: Control the number of messages logged to the error_log.
# Possible values include: debug, info, notice, warn, error, crit,
# alert, emerg.
#
LogLevel warn

#
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %T %v
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\" %P %T
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" comb
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
```

```
LogFormat "%{User-agent}i" agent

#
# The location and format of the access logfile (Common Logfile Format).
# If you do not define any access logfiles within a <VirtualHost>
# container, they will be logged here.  Contrariwise, if you *do*
# define per-<VirtualHost> access logfiles, transactions will be
# logged therein and *not* in this file.
#
#CustomLog /var/log/apache-ssl/access.log common

#
# If you would like to have agent and referer logfiles, uncomment the
# following directives.
#
#CustomLog /var/log/apache-ssl/referer.log referer
#CustomLog /var/log/apache-ssl/agent.log agent

#
# If you prefer a single logfile with access, agent, and referer information
# (Combined Logfile Format) you can use the following directive.
#
CustomLog /var/log/apache-ssl/access.log combined

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

#
# Aliases: Add here as many aliases as you need (with no limit). The format i
# Alias fakename realname
#
# Note that if you include a trailing / on fakename then the server will
# require it to be present in the URL.  So "/icons" isn't aliased in this
# example, only "/icons/"..
#

Alias /icons/ /usr/share/apache/icons/

<Directory /usr/share/apache/icons>
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
</Directory>
```

```
#
# ScriptAlias: This controls which directories contain server scripts.
# ScriptAliases are essentially the same as Aliases, except that
# documents in the realname directory are treated as applications and
# run by the server when requested rather than as documents sent to the clien
# The same rules about trailing "/" apply to ScriptAlias directives as to
# Alias.
#
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/

#
# "/usr/lib/cgi-bin" could be changed to whatever your ScriptAliased
# CGI directory exists, if you have that configured.
#
<Directory /usr/lib/cgi-bin/>
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>

#
# Redirect allows you to tell clients about documents which used to exist in
# your server's namespace, but do not anymore. This allows you to tell the
# clients where to look for the relocated document.
# Format: Redirect old-URI new-URL
#

#
# Directives controlling the display of server-generated directory listings.
#

<IfModule mod_autoindex.c>

    #
    # FancyIndexing: whether you want fancy directory indexing or standard
    #
    IndexOptions FancyIndexing NameWidth=*

    #
    # AddIcon* directives tell the server which icon to show for different
    # files or filename extensions.  These are only displayed for
    # FancyIndexed directories.
    #
    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/deb.gif .deb

AddIcon /icons/back.gif ..
AddIcon /icons/hand.right.gif README
AddIcon /icons/folder.gif ^^DIRECTORY^^
AddIcon /icons/blank.gif ^^BLANKICON^^

#
# DefaultIcon: which icon to show for files which do not have an icon
# explicitly set.
#
DefaultIcon /icons/unknown.gif

#
# AddDescription: allows you to place a short description after a file in
# server-generated indexes.  These are only displayed for FancyIndexed
# directories.
# Format: AddDescription "description" filename
#
#AddDescription "GZIP compressed document" .gz
#AddDescription "tar archive" .tar
#AddDescription "GZIP compressed tar archive" .tgz

#
# ReadmeName: the name of the README file the server will look for by
# default, and append to directory listings.
#
# HeaderName: the name of a file which should be prepended to
# directory indexes.
#
# The server will first look for name.html and include it if found.
# If name.html doesn’t exist, the server will then look for name.txt
```

```
    # and include it as plaintext if found.
    #
    ReadmeName README
    HeaderName HEADER

    #
    # IndexIgnore: a set of filenames which directory indexing should ignore
    # and not include in the listing.  Shell-style wildcarding is permitted.
    #
    IndexIgnore .??* *~ *# HEADER* README* RCS CVS *,v *,t

</IfModule>

#
# Document types.
#
<IfModule mod_mime.c>

    # AddEncoding allows you to have certain browsers (Mosaic/X 2.1+)
    # uncompress information on the fly. Note: Not all browsers support
    # this.  Despite the name similarity, the following Add* directives
    # have nothing to do with the FancyIndexing customization
    # directives above.

    AddEncoding x-compress Z
    AddEncoding x-gzip gz tgz

    #
    # AddLanguage: allows you to specify the language of a document. You can
    # then use content negotiation to give a browser a file in a language
    # it can understand.
    #
    # Note 1: The suffix does not have to be the same as the language
    # keyword --- those with documents in Polish (whose net-standard
    # language code is pl) may wish to use "AddLanguage pl .po" to
    # avoid the ambiguity with the common suffix for perl scripts.
    #
    # Note 2: The example entries below illustrate that in quite
    # some cases the two character 'Language' abbriviation is not
    # identical to the two character 'Country' code for its country,
    # E.g. 'Danmark/dk' versus 'Danish/da'.
    #
    # Note 3: In the case of 'ltz' we violate the RFC by using a three char
    # specifier. But there is 'work in progress' to fix this and get
    # the reference data for rfc1766 cleaned up.
    #
    # Danish (da) - Dutch (nl) - English (en) - Estonian (ee)
    # French (fr) - German (de) - Greek-Modern (el)
    # Italian (it) - Portugese (pt) - Luxembourgeois* (ltz)
    # Spanish (es) - Swedish (sv) - Catalan (ca) - Czech(cz)
```

```
# Polish (pl) - Brazilian Portuguese (pt-br) - Japanese (ja)
#
AddLanguage da .dk
AddLanguage nl .nl
AddLanguage en .en
AddLanguage et .ee
AddLanguage fr .fr
AddLanguage de .de
AddLanguage el .el
AddLanguage it .it
AddLanguage ja .ja
AddCharset ISO-2022-JP .jis
AddLanguage pl .po
AddCharset ISO-8859-2 .iso-pl
AddLanguage pt .pt
AddLanguage pt-br .pt-br
AddLanguage ltz .lu
AddLanguage ca .ca
AddLanguage es .es
AddLanguage sv .se
AddLanguage cz .cz

# LanguagePriority: allows you to give precedence to some languages
# in case of a tie during content negotiation.
#
# Just list the languages in decreasing order of preference. We have
# more or less alphabetized them here. You probably want to change
# this.
#
<IfModule mod_negotiation.c>
    LanguagePriority en da nl et fr de el it ja pl pt pt-br ltz ca es sv
</IfModule>

#
# AddType allows you to tweak mime.types without actually editing
# it, or to make certain files to be certain types.
#
# For example, the PHP 3.x module (not part of the Apache
# distribution - see http://www.php.net) will typically use:
#
#AddType application/x-httpd-php3 .php3
#AddType application/x-httpd-php3-source .phps
#
# And for PHP 4.x, use:
#
#AddType application/x-httpd-php .php
#AddType application/x-httpd-php-source .phps

AddType application/x-tar .tgz
AddType image/bmp .bmp
```

```
    # hdml
    AddType text/x-hdml .hdml

    #
    # AddHandler allows you to map certain file extensions to "handlers",
    # actions unrelated to filetype. These can be either built into
    # the server or added with the Action command (see below).
    #
    # If you want to use server side includes, or CGI outside
    # ScriptAliased directories, uncomment the following lines.
    #
    # To use CGI scripts:
    #
    #AddHandler cgi-script .cgi .sh .pl

    #
    # To use server-parsed HTML files
    #
    #AddType text/html .shtml
    #AddHandler server-parsed .shtml

    #
    # Uncomment the following line to enable Apache's send-asis HTTP
    # file feature.
    #
    #AddHandler send-as-is asis

    #
    # If you wish to use server-parsed imagemap files, use
    #
    #AddHandler imap-file map

    #
    # To enable type maps, you might want to use
    #
    #AddHandler type-map var

</IfModule>
# End of document types.

# Default charset to iso-8859-1 (ttp://www.apache.org/info/css-security/).

AddDefaultCharset on

#
# Action: lets you define media types that will execute a script whenever
# a matching file is called. This eliminates the need for repeated URL
# pathnames for oft-used CGI file processors.
# Format: Action media/type /cgi-script/location
```

```
# Format: Action handler-name /cgi-script/location
#

#
# MetaDir: specifies the name of the directory in which Apache can find
# meta information files. These files contain additional HTTP headers
# to include when sending the document
#
#MetaDir .web

#
# MetaSuffix: specifies the file name suffix for the file containing the
# meta information.
#
#MetaSuffix .meta

#
# Customizable error response (Apache style)
#  these come in three flavors
#
#    1) plain text
#ErrorDocument 500 "The server made a boo boo.
#  n.b.  the (") marks it as text, it does not get output
#
#    2) local redirects
#ErrorDocument 404 /missing.html
#  to redirect to local URL /missing.html
#ErrorDocument 404 /cgi-bin/missing_handler.pl
#  N.B.: You can redirect to a script or a document using server-side-include
#
#    3) external redirects
#ErrorDocument 402 http://some.other_server.com/subscription_info.html
#  N.B.: Many of the environment variables associated with the original
#  request will *not* be available to such a script.

<IfModule mod_setenvif.c>
    #
    # The following directives modify normal HTTP response behavior.
    # The first directive disables keepalive for Netscape 2.x and browsers tha
    # spoof it. There are known problems with these browser implementations.
    # The second directive is for Microsoft Internet Explorer 4.0b2
    # which has a broken HTTP/1.1 implementation and does not properly
    # support keepalive when it is used on 301 or 302 (redirect) responses.
    #
    BrowserMatch "Mozilla/2" nokeepalive
    BrowserMatch "MSIE 4\.0b2;" nokeepalive downgrade-1.0 force-response-1.0

    #
    # The following directive disables HTTP/1.1 responses to browsers which
    # are in violation of the HTTP/1.0 spec by not being able to grok a
```

```
    # basic 1.1 response.
    #
    BrowserMatch "RealPlayer 4\.0" force-response-1.0
    BrowserMatch "Java/1\.0" force-response-1.0
    BrowserMatch "JDK/1\.0" force-response-1.0
</IfModule>


# If the perl module is installed, this will be enabled.
<IfModule mod_perl.c>
  Alias /perl/ /var/www/frontend-perl/
  <Location /perl/>
    SetHandler perl-script
    PerlHandler Apache::Registry
    Options +ExecCGI
  </Location>
</IfModule>

# PerlModule Apache::DBI

#     <Files *.pl>
#       SetHandler perl-script
#       PerlHandler Apache::PerlRun
#       PerlSendHeader On
#     </Files>


     <Directory "/var/www/frontend-perl/">
       Options ExecCGI
       AddHandler cgi-script .pl
     </Directory>



#
# Allow http put (such as Netscape Gold's publish feature)
# Use htpasswd to generate /etc/apache/passwd.
# You must unremark these two lines at the top of this file as well:
#LoadModule put_module modules/mod_put.so
#
#Alias /upload /tmp
#<Location /upload>
#    EnablePut On
#    AuthType Basic
#    AuthName Temporary
#    AuthUserFile /etc/apache/passwd
#    EnableDelete Off
#    umask 007
#    <Limit PUT>
# require valid-user
```

```
#    </Limit>
#</Location>

#
# Allow server status reports, with the URL of http://servername/server-statu
# Change the ".your_domain.com" to match your domain to enable.
#
#<Location /server-status>
#    SetHandler server-status
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>

#
# Allow remote server configuration reports, with the URL of
#  http://servername/server-info (requires that mod_info.c be loaded).
# Change the ".your_domain.com" to match your domain to enable.
#
#<Location /server-info>
#    SetHandler server-info
#    Order deny,allow
#    Deny from all
#    Allow from .your_domain.com
#</Location>

# Allow access to local system documentation from localhost.
# (Debian Policy assumes /usr/share/doc is "/doc/", at least from the localho
Alias /doc/ /usr/share/doc/

<Location /doc>
  order deny,allow
  deny from all
  allow from 127.0.0.0/255.0.0.0
  Options Indexes FollowSymLinks MultiViews
</Location>

#
# There have been reports of people trying to abuse an old bug from pre-1.1
# days.  This bug involved a CGI script distributed as a part of Apache.
# By uncommenting these lines you can redirect these attacks to a logging
# script on phf.apache.org.  Or, you can record them yourself, using the scri
# support/phf_abuse_log.cgi.
#
#<Location /cgi-bin/phf*>
#    Deny from all
#    ErrorDocument 403 http://phf.apache.org/phf_abuse_log.cgi
#</Location>

<IfModule mod_proxy.c>
```

```
    #
    # Proxy Server directives. Uncomment the following lines to
    # enable the proxy server:
    #
    #<IfModule mod_proxy.c>
    #ProxyRequests On
    #
    #<Directory proxy:*>
    #    Order deny,allow
    #    Deny from all
    #    Allow from .your_domain.com
    #</Directory>
</IfModule>

#
# Enable/disable the handling of HTTP/1.1 "Via:" headers.
# ("Full" adds the server version; "Block" removes all outgoing Via: headers)
# Set to one of: Off | On | Full | Block
#
#ProxyVia On

#
# To enable the cache as well, edit and uncomment the following lines:
# (no cacheing without CacheRoot)
#
#CacheRoot "/var/cache/apache"
#CacheSize 5
#CacheGcInterval 4
#CacheMaxExpire 24
#CacheLastModifiedFactor 0.1
#CacheDefaultExpire 1
#NoCache a_domain.com another_domain.edu joes.garage_sale.com

#</IfModule>
# End of proxy directives.

### Section 3: Virtual Hosts
#
# VirtualHost: If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them.
# Please see the documentation at <URL:http://www.apache.org/docs/vhosts/>
# for further details before you try to setup virtual hosts.
# You may use the command line option '-S' to verify your virtual host
# configuration.

#
# If you want to use name-based virtual hosts you need to define at
# least one IP address (and port number) for them.
#
#NameVirtualHost 12.34.56.78:80
```

```
#NameVirtualHost 12.34.56.78



#
# VirtualHost example:
# Almost any Apache directive may go into a VirtualHost container.
#
#<VirtualHost ip.address.of.host.some_domain.com>
#    ServerAdmin webmaster@host.some_domain.com
#    DocumentRoot /www/docs/host.some_domain.com
#    ServerName host.some_domain.com
#    ErrorLog logs/host.some_domain.com-error.log
#    CustomLog logs/host.some_domain.com-access.log common
#</VirtualHost>

#<VirtualHost _default_:*>
#</VirtualHost>

# ------------------------------SSL-----------------------------------
# This is an example configuration file for Apache-SSL.
# Copyright (C) 1995,6,7 Ben Laurie

# By popular demand, this file now illustrates the way to create two websites
# one secured (on port 8887), the other not (on port 8888).

# You may need one of thse
#User webuser
#User ben
#Group group

# SSL Servers MUST be standalone, currently.
#ServerType standalone

# The default port for SSL is 443...
#Port 8887
#Listen ServerPort
Listen 443

# My test document root
#DocumentRoot /u/ben/www/1/docs
#DocumentRoot /u/ben/apache/apache_1.3.0-ssl/htdocs

#<Directory /u/ben/apache/apache_1.3.0-ssl/htdocs/manual>
# This directive forbids access except when SSL is in use. Very handy for
# defending against configuration errors that expose stuff that should be
# protected
#SSLRequireSSL
#</Directory>
```

```
# Watch what’s going on
#TransferLog /var/log/apache-ssl/transfer.log

# Note that all SSL options can apply to virtual hosts.

# Disable SSL. Useful in combination with virtual hosts. Note that SSLEnable
# now also supported.
SSLEnable

# Set the path for the global cache server executable.
# If this facility gives you trouble, you can disable it by setting
# CACHE_SESSIONS to FALSE in apache_ssl.c
SSLCacheServerPath /usr/lib/apache-ssl/gcache

# Set the global cache server port number, or path. If it is a path, a Unix
# domain socket is used. If a number, a TCP socket.
SSLCacheServerPort /var/run/gcache_port
#SSLCacheServerPort 1234

# Set the session cache timeout, in seconds (set to 15 for testing, use a
# higher value in real life)
SSLSessionCacheTimeout 15

# Set the CA certificate verification path (must be PEM encoded).
# (in addition to getenv("SSL_CERT_DIR"), I think).
#SSLCACertificatePath /u/ben/apache/apache_1.2.5-ssl/SSLconf/conf
SSLCACertificatePath /etc/apache-ssl

# Set the CA certificate verification file (must be PEM encoded).
# (in addition to getenv("SSL_CERT_FILE"), I think).
#SSLCACertificateFile /some/where/somefile
#SSLCACertificateFile /u/ben/apache/apache_1.2.5-ssl/SSLconf/conf/httpsd.pem

# Point SSLCertificateFile at a PEM encoded certificate.
# If the certificate is encrypted, then you will be prompted for a pass phras
# Note that a kill -1 will prompt again.
# A test certificate can be generated with "make certificate".
SSLCertificateFile /etc/apache-ssl/apache.pem
#SSLCertificateFile /u/ben/apache/apache_1.2.6-ssl/SSLconf/conf/t1.pem


# If the key is not combined with the certificate, use this directive to
# point at the key file. If this starts with a ’/’ it specifies an absolute
# path, otherwise it is relative to the default certificate area. That is, it
# means "<default>/private/<keyfile>".
#SSLCertificateKeyFile /some/place/with/your.key

# Set SSLVerifyClient to:
# 0 if no certicate is required
```

```
# 1 if the client may present a valid certificate
# 2 if the client must present a valid certificate
# 3 if the client may present a valid certificate but it is not required to
#   have a valid CA
SSLVerifyClient 0
# How deeply to verify before deciding they don't have a valid certificate
SSLVerifyDepth 10

# Translate the client X509 into a Basic authorisation. This means that the
# standard Auth/DBMAuth methods can be used for access control. The user name
# is the "one line" version of the client's X509 certificate. Note that no
# password is obtained from the user. Every entry in the user file needs this
# password: xxj31ZMTZzkVA. See the code for further explanation.
SSLFakeBasicAuth

# List the ciphers that the client is permitted to negotiate. See the source
# for a definitive list. For example:
#SSLRequiredCiphers RC4-MD5:RC4-SHA:IDEA-CBC-MD5:DES-CBC3-SHA

# These two can be used per-directory to require or ban ciphers. Note that (a
# least in the current version) Apache-SSL will not attempt to renegotiate if
# cipher is banned (or not required).
#SSLRequireCipher
#SSLBanCipher

# A home for miscellaneous rubbish generated by SSL. Much of it is duplicated
# in the error log file. Put this somewhere where it cannot be used for symli
# attacks on a real server (i.e. somewhere where only root can write).
#SSLLogFile /var/log/ssl.log

# Custom logging
CustomLog /var/log/apache-ssl/ssl.log "%t %{version}c %{cipher}c %{clientcert

#<VirtualHost scuzzy:8888>
#SSLDisable
#SSLEnable
#</VirtualHost>

# If you want, you can disable SSL globally, and enable it in a virtual host.
#<VirtualHost scuzzy:8887>
#SSLEnable
# and the rest of the SSL stuf...
#</VirtualHost>

# Experiment with authorization...
#<Directory /u/ben/www/1/docs>
#AuthType Basic
#AuthName Experimental
#AuthGroupFile /dev/null
#AuthUserFile /u/ben/www/1/users
```

```
#<Limit PUT GET>
#allow from all
#require valid-user
#</Limit>
#</Directory>

#ScriptAlias /scripts /u/ben/www/scripts

#<VirtualHost ServerName:443>
#SSLEnable
#</VirtualHost>
```

C Fichier prelude-manager.conf

```
[Prelude Manager]

# Address where the sensors serber is listening on.
# if value is 127.0.0.1 (or is resolved as being 127.0.0.1),
# it mean the Manager server will be listening via a local (UNIX)
# socket.
#
# format : address:port
#
sensors-srvr = 192.168.0.2;


# Address where the administrative server is listening on.
# if value is "unix", it mean the report server is listening
# on the same machine via a local (UNIX) socket.
#
# format : address:port
#
# admin-srvr = 0.0.0.0:5555;


# If you want the message caught by this manager to be relayed.
# You can use boolean AND and OR to make the rule.
#
# relay-manager = x.x.x.x || y.y.y.y && z.z.z.z
#
# This mean the emission should occur on x.x.x.x or, if it fail,
# on y.y.y.y and z.z.z.z (if one of the two host in the AND fail,
# the emission will be considered as failed involving saving the
# message locally).


#####################################
# Here start plugins configuration #
#####################################
```

```
# [MySQL]

# Host the database is listening on.
dbhost = localhost;

# Name of the database.
dbname = prelude;

# Username to be used to connect the database.
dbuser = prelude;

# Password used to connect the database.
dbpass = dessstri;



#
# The Textmod plugin allow to report alert as text
# in a file. Or to dump theses alert to stderr.
#
# The default logfile for this plugin is /var/log/prelude.log
#

[TextMod]
#
# Tell Textmod to output to stderr
# stderr;
#

logfile = /var/log/prelude.log;



#
# The Xmlmod plugin allow to report alert as IDMEF XML
# in a file. Or to dump theses alert to stderr.
#
# The default logfile for this plugin is /var/log/prelude-xml.log
#

[XmlMod]
#
# Tell Xmlmod to output to stderr
# stderr;
#
# Tell Xmlmod to check generated XML against IDMEF DTD
# check-dtd;
#
```

```
logfile = /var/log/prelude-xml.log;



# [Debug]
#
# Print the value of each element.
# verbose;
#
# Be aggressive, print strings even if consistency checks fail
# (may lead to crash).
# aggressive;
#
# Use wide format for lists.
# wide-format;
```

D Fichier prelude-nids.conf

```
################################################
# Configuration for the Prelude NIDS Sensor  #
################################################

[Prelude NIDS]

# Address where the Prelude Manager Server is listening on.
# if value is "127.0.0.1", the connection will occur throught
# an UNIX socket.
#
# This entry is disabled. The default is to use the entry
# located in sensors-default.conf... You may overwrite the
# default address for this sensor by uncommenting this entry.
#
 manager-addr = 192.168.0.2:5554;


# Set this entry if you want Prelude NIDS to use a specific user.
#
# user = prelude;



#[Tcp-Reasm]

#
# TCP stream reassembly option
#
# Only analyse TCP packet that are part of a stream,
```

```
# this defeat stick/snot against TCP signatures.
#
# statefull-only;

#
# Only reassemble TCP data sent by the client (default).
#
# client-only;

#
# Only reassemble TCP data sent by the server.
#
# server-only;

#
# Reassemble TCP data sent by client and server.
#
# both;

#
# Don't reassemble data until we queued a minimum of byte (default is 8192).
#
# min-length = 8192;

#
# Only reassemble data to specific port (default is to reassemble everything)
#
# If this option is used with the statefull-only option, packet that are not
# going to theses specified port will be analyzed anyway.
#
# port-list = 1 2 3 4;


####################################
# Here start plugins configuration #
####################################

[SnortRules]

ruleset=/usr/local/etc/prelude-nids/ruleset/prelude.rules;


[ScanDetect]

# Number of connection attempt to get from the same
# host and targeted on different port before the scan
# detection plugin issue an alert.
#
high-port-cnx-count = 50;
low-port-cnx-count = 5;
```

```
# Window of time without getting any activity the scan
# detection plugin should wait before issuing an alert
# for a given host.
#
cnx-ttl = 60;



# [Shellcode]
#
# This plugin allow for polymorphic shellcode detection.
# It may consume a lot of CPU time, so it's disabled by
# default. Uncomment the section name to enable it, or
# specify --shellcode on the command line.

nops_raise_alert = 60;

#
# If a port-list is specified, the Shellcode plugin
# will only analyse data going to theses port (when
# the protocol used have have dst port).
#
# port-list = 1 2 3 4;



# [Debug]
#
# This plugin issue an alert for each packet.
# Carefull to the loging activity it generate.


[HttpMod]
#
# Normalize HTTP request.
# The "codepage-file" option contains the name of the file containing
# Unicode to ASCII convertion tables for WIN32 machines.
#
# The "codepage-number" option is the codepage number your WIN32 servers use.
#
#
# end-on-param:
# Stop parsing the URL when we meet a parameter.
#
# double-encode:
# Check for encoded '%' character.
#
# max-whitespace:
```

```
# Maximum number of whitespace allowed before URL begin.
#
# flip-backslash:
# Change '\' to '/' when parsing URL.
#

double-encode;
flip-backslash;
max-whitespace = 10;
codepage-file = /usr/local/etc/prelude-nids/unitable.txt;
codepage-number = 437;


port-list = 80 8080;


[RpcMod]
#
# Decode RPC traffic, Also provide the RPC rule key.
#
port-list = 111;


[TelnetMod]
#
# Normalize telnet negotiation character
#
port-list = 23 21;


[ArpSpoof]
#
# Search anomaly in ARP request.
#
# The "directed" option will result in a warn each time an ARP
# request is sent to an address other than the broadcast address.
#
# directed;
# arpwatch=<ip> <macaddr>;
```

E Fichier prelude-lml.conf

```
##############################################
# Configuration for the Prelude LML Sensor   #
##############################################

[Prelude LML]
```

```
# Address where the Prelude Manager Server is listening on.
# if value is "127.0.0.1", the connection will occur throught
# an UNIX socket.
#
# This entry is disabled. The default is to use the entry
# located in sensors-default.conf... You may overwrite the
# default address for this sensor by uncommenting this entry.
#
 manager-addr = 192.168.0.2;


# Configuration for the UDP message receiver.
# commented out by default since most people only want to
# monitor files.
#
# [Udp-Srvr]
#
# port = 514
# addr = 0.0.0.0



#
# Files to monitor
#
file = /var/log/auth.log
file = /var/log/messages


#####################################
# Here start plugins configuration #
#####################################

[SimpleMod]

ruleset=/usr/local/etc/prelude-lml/ruleset/simple.rules;


# [Debug]
#
# This plugin issue an alert for each packet.
# Carefull to the loging activity it generate.
```

F Fichier config.pl

```
sub LoadConfig()
```

```
{
    # Database :
  $conf{'dbtype'}='mysql';
  $conf{'dbname'}='prelude';
  $conf{'dbhost'}='localhost';
  $conf{'dbport'}=3306; # default mysql port is 3306
#  $conf{'dboptions'}='mysql_compression=1';
  $conf{'dblogin'}='prelude';
  $conf{'dbpasswd'}='dessstri';

    # Other :
  $conf{'debug'}=1; # Debug perl code onscreen (0 or 1)
  $conf{'extension'}='.pl'; # scripts file extension (.pl)

  $conf{'refresh'}=600; # AlertList refresh in seconds (600)

  $conf{'ettercap_fp_db'}='./generated/DB/etter.passive.os.fp';
  $conf{'ettercap_mac_db'}='./generated/DB/mac-fingerprints';

  $conf{'HostName_Lookup'}=1; # Host Name Resolution (0 or 1)

  $conf{'GD_transparent'}=0; # Are graphs transparent ?
}

1;
```

G Fichier config.php

```
<?
/*
 *
 * Copyright (C) 2002 Vergoz Michael <descript@sysdoor.net>
 * All Rights Reserved
 *
 * This file is part of the Prelude program.
 *
 * This program is free software; you can redistribute it and/or modify
 * it under the terms of the GNU General Public License as published by
 * the Free Software Foundation; either version 2, or (at your option)
 * any later version.
 *
 * This program is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
 * GNU General Public License for more details.
 *
 * You should have received a copy of the GNU General Public License
```

```
 * along with this program; see the file COPYING.  If not, write to
 * the Free Software Foundation, 675 Mass Ave, Cambridge, MA 02139, USA.
 *
 */
?>

<?

$server[0]['description'] = "SYSDOOR/PostGreSQL phpfront v".VERSION;
$server[0]['dbtype'] = USE_DB_PGSQL;
$server[0]['dbusername'] = "";
$server[0]['dbpassword'] = "";
$server[0]['dbhostname'] = LOCAL_CONNECTION;
$server[0]['dbport'] = DEFAULT_PORT;
$server[0]['dbname'] = "prelude";

$server[1]['description']      =      "SYSDOOR/MySQL phpfront v".VERSION;
$server[1]['dbtype']           =      USE_DB_MYSQL;
$server[1]['dbusername']       =      "prelude";
$server[1]['dbpassword']       =      "dessstri";
$server[1]['dbhostname']       =      LOCAL_CONNECTION;
$server[1]['dbport']           =      DEFAULT_PORT;
$server[1]['dbname']           =      "prelude";


/*
 * Local variables:
 * tab-width: 4
 * c-basic-offset: 4
 * End:
 * vim600: noet sw=4 ts=4 fdm=marker
 * vim<600: noet sw=4 ts=4
 */
?>
```