Configuration des services sous Linux

Yann-Érick proy yeproy@quartz.fr
Quartz Informatique (Argonay)

Configuration des services sous Linux

Quels réseaux ?

Service web : Apache

Présention

Configuration

Sécurisation

Extension

Quels réseaux ?

Service ⇒ serveur

Où le placer ?

- sur le LAN
  services internes, privés (Intranet)
  accès éventuel via un VPN

- sur l'Internet
  services publics (authentification éventuelle)

Quels réseaux ?

Sur l'Internet

Quelle connectivité ?

- Sur site : connexion ADSL
  - IP dynamique (dyndns ?)
  - IP fixe

    en option (Orange) ou systématique (Nerim)
    liée au dégroupage, ou au triple-play

Points faibles : fiabilité, débit, upload

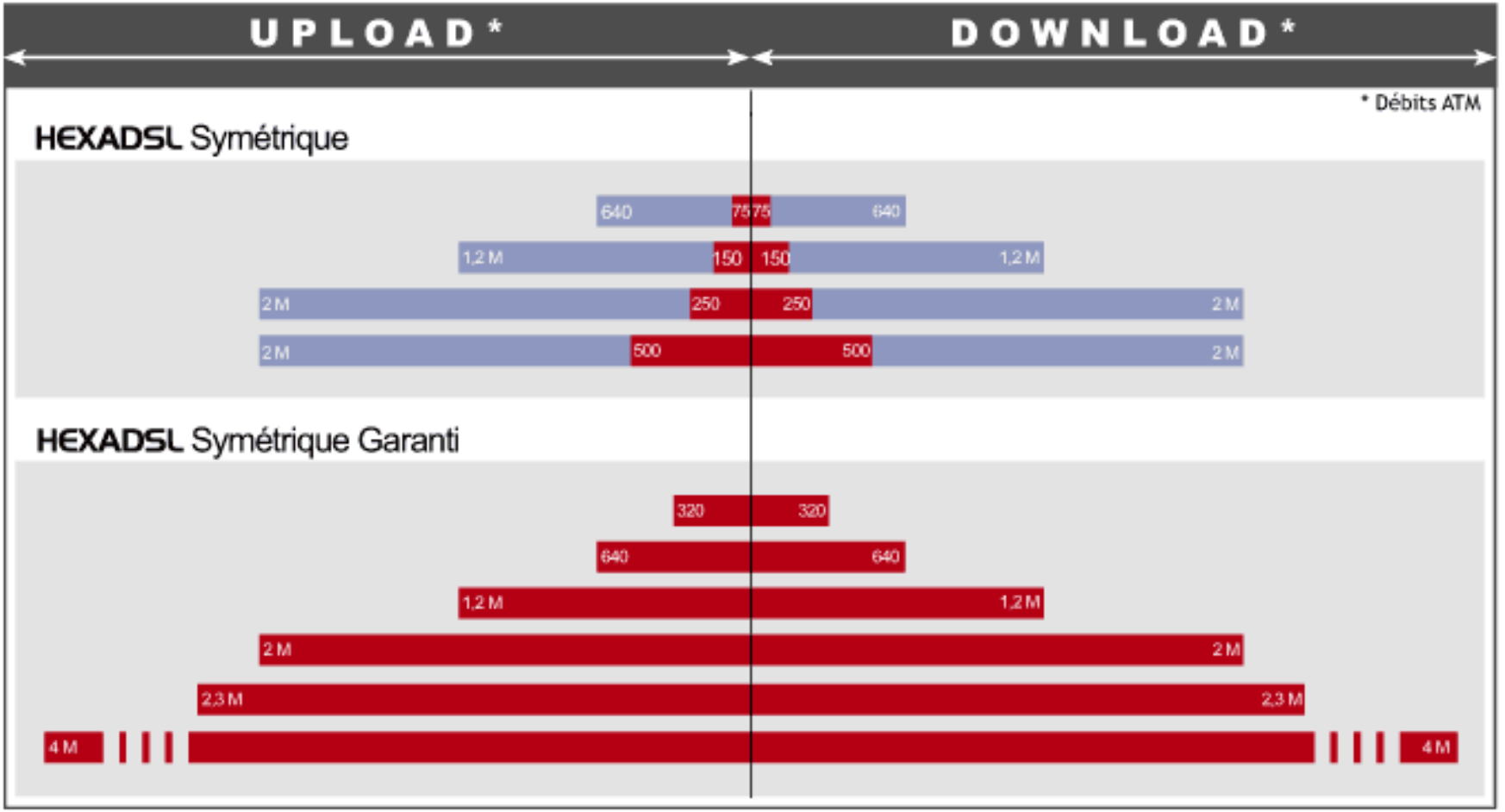
Quels réseaux ?

Sur l'Internet

- Sur site : connexion xDSL
  - débit garanti (tout ou partie)
  - GTR (H+4, 24h/24, 7j/7)
  - débit symétrique (SDSL, upload 1024, 2048)
  - opérateurs Nerim, Easynet, Completel, ...

Points faibles : prix, ligne, salle

Quels réseaux ?



Quels réseaux ?

- Chez un hébergeur technique
  - hébergement mutualisé
  - serveur dédié (loué)
  - baies ou demi-baies (traffic en sus)
  - opérateurs : OVH, Sivit, Amen, Ikoula, ...

Points faibles : accès physique, compétences nécessaires

Service Web

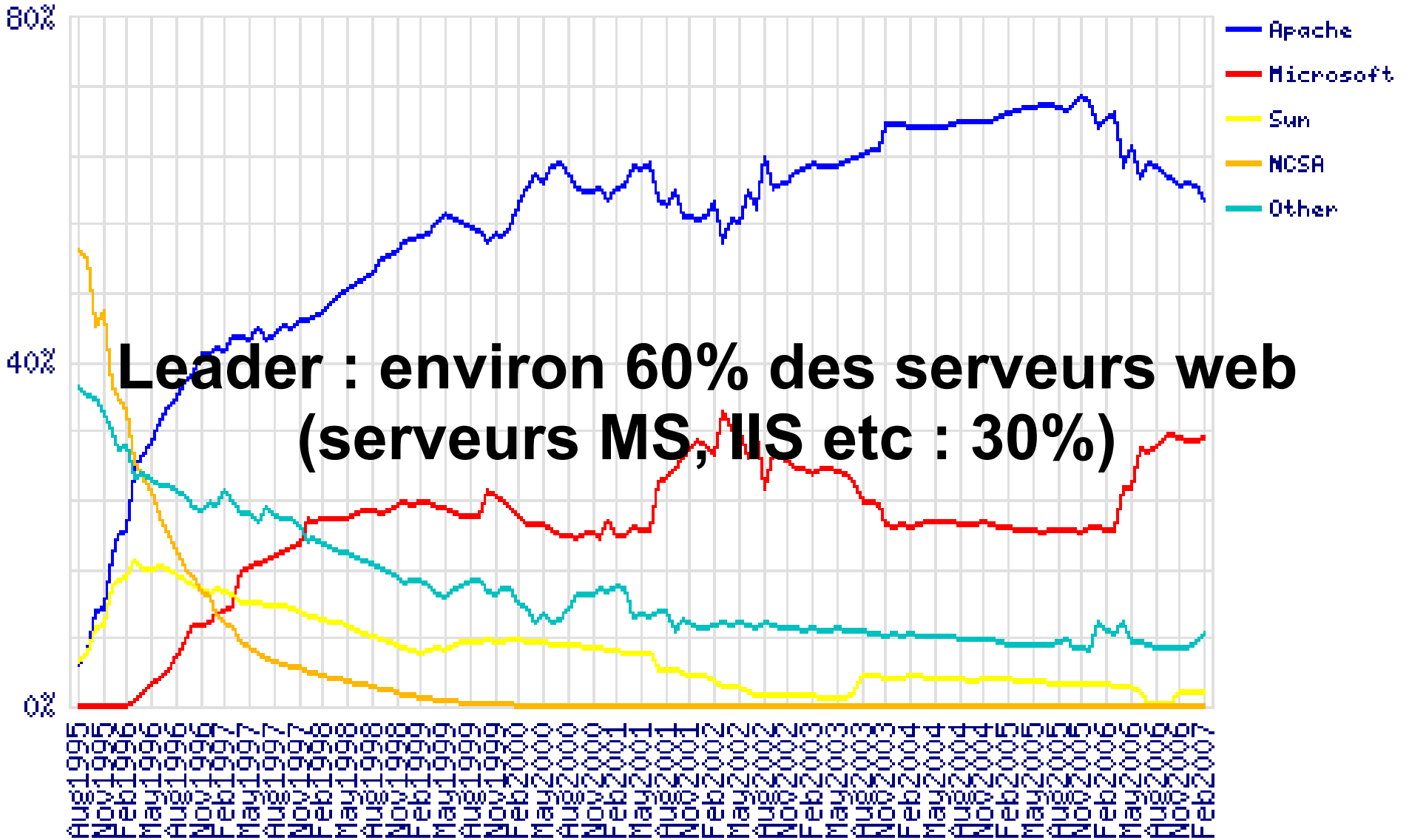
Apache, serveur HTTP

Présentation d'Apache

Rappel chronologique

1989, Tim Berners-Lee propose les premières bases d'HTTP (*Hypertext Transfer Protocol*) au CERN
1991, il publie le premier navigateur, *"WorldWideWeb"*, avec le serveur correspondant
1993, *NCSA Mosaic 1.0*, 1er navigateur populaire (icônes, signets, etc), co-écrit par Marc Andreessen,
1994, Marc Andreessen fonde Netscape, avec Jim Clark, ex de Silicon Graphics
1994, RFC 1738 (URL)
1995, Apache Group
1996, RFC 1945 (HTTP/1.0)
1998, Netscape, définitivement battu par Microsoft dans sa guerre des navigateurs web, délivre les sources de Netscape Navigator et fonde le groupe de développement *Mozilla*
1999, Apache Software Foundation
1999, RFC 2616 (HTTP/1.1)

Présentation d'Apache



Leader : environ 60% des serveurs web (serveurs MS, IIS etc : 30%)

Présentation d'Apache

Apache vs Microsoft IIS

- gros effort depuis 1 an de MS afin de remonter la pente
- passé de 20 à 30% en 1 an, pris sur Apache
- prix sacrifiés des licenses Windows 2003 Serveur Web Edition chez les hébergeurs

Présentation d'Apache

Apache Software Foundation

Organisation à but non lucratif US, créée en 1999

Fondateurs : Apache Group, depuis 1995
développeurs du serveur Apache sur la base du **serveur HTTPD** de NCSA

Comité de direction ASF :
chercheurs, développeurs influents, venant de l'université ou de grands noms de l'industrie (IBM, Google, Covalent, etc)

Présentation d'Apache

Apache Software Foundation

Ken Coar

Greg Stein

Présentation d'Apache

Apache Software Foundation

Donations : matériels et autres par Apple, HP, IBM, Sun

Autres projets :

- Tomcat (serveur Java),
- SpamAssassin (anti-spam),
- mod_perl (module perl pour Apache),
- etc

Configuration d'Apache

Open-source = diversité

Versions : Apache 1.3 ou 2.0 (2.2)
(version 2.0 disponible depuis 2000 !)

Emplacements :

- installation par défaut depuis les sources : `/usr/local/apache/conf`
- Debian stable : `/etc/apache2`
- RedHat, Fedora et Mandriva : `/etc/httpd/conf` et `/etc/httpd/conf.d`

Idem noms des fichiers, emplacement des sites.

Configuration d'Apache

Configuration d'Apache = directives

Fichier principal : httpd.conf, apache2.conf, etc

Directive Include : diviser en plusieurs fichiers

```
Include /etc/apache2/ports.conf
Include /etc/apache2/conf.d/[^.#]*
```

Une directive par ligne.
Caractère « \ » en fin : poursuite sur la ligne suivante.
Caractère « # » en début : commentaire.

Configuration d'Apache

Portée des directives

Certaines directives définissent une portée :

```
<Directory> ... </Directory>
<Files> ... </Files>
<Location> ... </Location>
<VirtualHost>... </VirtualHost>
```

Directive hors de toute portée : tout le serveur.
Pour chaque directive : contexte d'emploi

Configuration d'Apache

Lecture de la configuration

Au lancement du serveur.

Relecture :

```
/etc/init.d/httpd restart
/etc/init.d/httpd reload
killall -HUP httpd
```

Mais : privilèges nécéssaires, affecte tout le serveur

Configuration d'Apache

Configuration à la volée

Fichiers `.htaccess`

Pas de signal à envoyer au serveur.
Nouvelle portée : répertoire contenant .htaccess
Nouveau contexte d'emploi : quelques directives
Faculté limitée par une directive :

`AllowOverride`

Exemple : `None AuthConfig Indexes`

Configuration d'Apache

Principales directives

Répertoire de base pour la configuration :

`ServerRoot`

Mention de l'administrateur (messages d'erreur) :

`ServerAdmin`

Adresses et ports écoutés :

`Listen` (`adresse:port`, `*:port` possible)

Configuration d'Apache

Principales directives

Fichiers admissibles pour l'index d'un répertoire :

`DirectoryIndex`

Exemple classique :

```
DirectoryIndex index.html index.htm index.php
```

Gestionnaires pour les fichiers qui ne sont pas à renvoyer tels quels :

`AddHandler`

Exemple pour les CGI :

```
AddHandler cgi-script .cgi
```

Configuration d'Apache

« Scripts » CGI

Common Gateway Interface : interface permettant de passer le contrôle à un programme tiers.

Suivant la méthode de l'appel (`get` ou `post`) les éventuels paramètres sont fournis via la variable d'environnement `QUERY_STRING` ou via l'entrée standard.

Le serveur HTTP reçoit le résultat sur la sortie standard et l'envoie au navigateur.

Configuration d'Apache

« Scripts » CGI

Le serveur appelle le programme **dans les conditions de l'OS**.

Sous UNIX (Linux en particulier) :

- fichier exécutable binaire : exécuté tel quel
- fichier texte : on cherche un interpréteur en première ligne, s'il existe il est exécuté sur le fichier

Configuration d'Apache

« Scripts » CGI

Exemples :

- scripts bash (shell) :
  `#!/bin/bash`
- scripts perl :
  `#!/usr/bin/perl`
- scripts php :
  `#!/usr/local/bin/php`

Un exécutable binaire peut avoir été programmé en C, C++, etc : « script CGI » est un abus de langage !

Configuration d'Apache

Principales directives

Fonctionnalités particulières :

```
Options
   [+]|[-]Indexes
   [+]|[-]FollowSymLinks
   [+]|[-]ExecCGI
   [+]|[-]Includes
   ...
```

Il n'est pas toujours souhaitable d'autoriser le listage d'un répertoire, le suivi des liens symboliques, l'exécution des CGI ou les macros SSI (Server Side Includes).

Configuration d'Apache

Principales directives

Journal global des erreurs :

`ErrorLog`

Journal des accès :

`CustomLog` (+ format)

Format = « `combined` » (standard) ou détaillé

Configuration d'Apache

Journal des accès

```
"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\""

74.6.73.52 - - [20/Feb/2007:14:04:42 +0100] "GET
/quartz_info/n02/quartzinfo2.pdf HTTP/1.0" 200 3069953 "-"
"Mozilla/5.0 (compatible; Yahoo! Slurp;
http://help.yahoo.com/help/us/ysearch/slurp)"

80.11.66.3 - - [20/Feb/2007:14:08:25 +0100] "GET /
HTTP/1.1" 304 - "-" "Mozilla/4.0 (compatible; MSIE 6.0;
Windows NT 5.1; SV1; .NET CLR 1.1.4322; .NET CLR
2.0.50727)"

80.11.66.3 - - [20/Feb/2007:14:08:25 +0100] "GET
/styles.css HTTP/1.1" 304 - "http://www.quartz.fr/"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1;
.NET CLR 1.1.4322; .NET CLR 2.0.50727)"
```

Configuration d'Apache

Serveur virtuels

Un serveur = un site : gaspillage des ressources

Hébergement : plusieurs sites sur le même serveur

Problème : connexion TCP/IP sur l'IP, pas le nom

Solution : un serveur, plusieurs IP
pas plusieurs interfaces réseau : ip alias
(eth0:0, eth0:1, ...)

Configuration d'Apache

Serveurs virtuels

Directive VirtualHost :

```
 <VirtualHost 1.2.3.4>
ServerAdmin webmaster@mail.exemple.com
DocumentRoot /home/exemple/www
ServerName www.exemple.com
ErrorLog /var/log/exemple-error_log
TransferLog /var/log/exemple-access_log
</VirtualHost>
```

Ici, `ServerName` est presque inutile.

(En cas de reverse DNS impossible sur son IP, Apache peut l'utiliser pour certaines pages qu'il génère)

Configuration d'Apache

Serveur virtuels

Problème : les IP sont rares

Solution : plusieurs sites sur la même IP

Contrepartie : modification importante du protocole

> Il faut pouvoir indiquer le nom du serveur dans l'en-tête de la requête HTTP
> d'où HTTP/1.1 : `Host`

Configuration d'Apache

Serveurs virtuels

Directive VirtualHost :

```
NameVirtualHost 1.2.3.4

<VirtualHost 1.2.3.4>
ServerAdmin webmaster@mail.exemple.com
DocumentRoot /home/exemple/www
ServerName www.exemple.com
ErrorLog /var/log/exemple-error_log
TransferLog /var/log/exemple-access_log
</VirtualHost>
```

Ne pas oublier Listen...

Sécurisation d'Apache

Retarder l'identification du serveur

Telnet sur port 80 :

```
get / HTTP/1.1

HTTP/1.1 400 Bad Request
Date: Mon, 19 Feb 2007 19:19:05 GMT
Server: Apache-AdvancedExtranetServer/1.3.22 (Mandrake
  Linux/10.1mdk)
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=iso-8859-1
Directive VirtualHost :
```

Informations importantes facilement gagnées !

Sécurisation d'Apache

Retarder l'identification du serveur

Directive `ServerTokens` :

```
ServerTokens Prod[uctOnly]
    Server: Apache
ServerTokens Major
    Server: Apache/2
ServerTokens Minor
    Server: Apache/2.0
ServerTokens Min[imal]
    Server: Apache/2.0.41
ServerTokens OS
    Server: Apache/2.0.41 (Unix)
ServerTokens Full (or not specified)
    Server: Apache/2.0.41 (Unix) PHP/4.2.2 MyMod/1.2
```

Sécurisation d'Apache

Retarder l'identification du serveur

Directive `ServerSignature` :

```
ServerTokens On|Off|Email
```

Avec On :

```
Not Found
The requested URL /absent.html was not found on this
server.

---

Apache/1.3.33 Server at www.example.com Port 80
```

Sécurisation d'Apache

Verrouiller l'accès aux répertoires

Directives `<Directory>`

```
<Directory />
  Options -Indexes -FollowSymLinks -ExecCGI
  AllowOverride None
  Order deny,allow
  Deny from all
</Directory>
```

Cas particulier de la racine du système de fichiers : ce qui n'est pas autorisé est interdit !

Sécurisation d'Apache

Verrouiller l'accès aux répertoires

Directives `<Directory>`

```
<Directory /home/exemple/cgi-bin>
    AllowOverride None
    Options ExecCGI
    Order allow,deny
    Allow from all
</Directory>
```

Accès à tous, possibilité d'exécution CGI limitée (on l'a interdit ailleurs).
Gestion des droits draconienne sur ce répertoire !

Sécurisation d'Apache

Verrouiller l'accès aux URL

Directives `<Location>`

```
<Location /admin>
    Order deny,allow
    Deny from all
    Allow from 1.2.3.4
    AuthName "Accès protégé"
    AuthType Basic
    AuthUserFile /home/exemple/admin_passwd
    Require user Admin1 Admin2
</Location>
```

Accès limité à une IP et deux utilisateurs (login et mot de passe requis).

Sécurisation d'Apache

Verrouiller l'accès aux URL

Directives `<Location>`

```
<Location /server-status>
    SetHandler server-status
    Order deny,allow
    Deny from all
    Allow from 127.0.0.1
    Allow from 192.168.0.
</Location>
```

Accès réservé à l'hôte et au réseau local.
(URL spécifique, nécessitant un module)

Sécurisation d'Apache

Verrouiller l'accès aux URL

```
Server Version: Apache-AdvancedExtranetServer
   Server Built: Mar 30 2005 12:41:28

   Current Time: Monday, 19-Feb-2007 20:27:11 CET
   Restart Time: Thursday, 01-Feb-2007 04:02:03 CET
   Parent Server Generation: 1
   Server uptime: 19 days 16 hours 25 minutes 7 seconds
   Total accesses: 712555 - Total Traffic: 402.4 MB
   CPU Usage: u187.36 s20.06 cu.19 cs0 - .00951% CPU load
   .326 requests/sec - 193 B/second - 592 B/request
   7 requests currently being processed, 10 idle workers

KW____KK_K__K__K_.....................................
........................................................
........................................................
........................................................
........................................................
```

Sécurisation d'Apache

Verrouiller l'accès aux fichiers

Directive <Files>

```
<Files ~ "^\.ht">
    Order allow,deny
    Deny from all
</Files>
```

Expression régulière : faire précéder de `~`
Tout fichier commençant par « .ht » est interdit.
Protège les fichiers `.htaccess`.

Sécurisation d'Apache

Verrouiller l'accès aux fichiers

Problème : .htaccess peut être une cible privilégiée.

Exemples :

- détourner un script (par injection) pour lui faire dévoiler le contenu de `.htaccess`.
- détourner un script (par injection) pour lui faire écrire dans `.htaccess`, en ayant supprimé l'authentification, et/ou l'interdiction de lister le répertoire (`-Indexes`).

Solution : renommer les fichiers `.htaccess`

```
AccessFileName .myhtaccess
```

Sécurisation d'Apache

Verrouiller l'accès aux fichiers

Problème : les fichiers CGI des sites hébergés sur le même serveur sont exécutés par le même utilisateur : celui exécutant Apache.

Exemple :

- un script d'un site voisin peut consulter ou écraser des fichiers d'un autre.

Solution : faire exécuter les CGI par un utilisateur différent par serveur virtuel.

Mécanisme optionnel « suexec » (voir dans /usr/sbin, actif si bit SUID : chmod u+s)

Sécurisation d'Apache

Verrouiller l'accès aux fichiers

```
<Directory /home/exemple/www/>
    AllowOverride All
    Options -ExecCGI
</Directory>
<Directory /home/exemple/cgi-bin>
    AllowOverride None
    Options ExecCGI
</Directory>
<VirtualHost 1.2.3.4>
DocumentRoot /home/exemple/www
ServerName www.exemple.com
ScriptAlias /cgi-bin/ /home/exemple/cgi-bin
User exemple
Group exemple
</VirtualHost>
```

L'utilisateur `exemple` seul peut écrire dans ses répertoires (avec `chmod` adéquat).

Sécurisation d'Apache

Verrouiller l'accès aux fichiers

Problème : les liens symboliques peuvent permettre d'accéder à des fichiers sensibles.

Exemple :

- un utilisateur ayant un compte FTP pour déposer les fichiers de son site peut créer un lien symbolique vers /etc/passwd et récupérer la liste des comptes dans son navigateur.
- idem pour une attaque par injection.

Solution : interdire à Apache de suivre les liens (`-FollowSymLinks`) ou ne l'autoriser que sur un même propriétaire `SymLinksIfOwnerMatch`).

Extension d'Apache

Conception modulaire

API publiques et documentées

Compilation statique ou dynamique (DSO, Dynamic Shared Object)

Compilation des modules : simultanée à celle d'Apache ou différée (apxs, Apache Extension Tool)

Extension d'Apache

Appels des modules dans le fichier de configuration

```
LoadModule access_module       modules/mod_access.so
LoadModule auth_module         modules/mod_auth.so
LoadModule auth_digest_module modules/mod_auth_digest.so
LoadModule include_module      modules/mod_include.so
LoadModule log_config_module   modules/mod_log_config.so
LoadModule env_module          modules/mod_env.so
LoadModule expires_module      modules/mod_expires.so
LoadModule headers_module      modules/mod_headers.so
LoadModule usertrack_module    modules/mod_usertrack.so
##LoadModule unique_id_module modules/mod_unique_id.so
LoadModule setenvif_module     modules/mod_setenvif.so
LoadModule proxy_module        modules/mod_proxy.so
LoadModule mime_module         modules/mod_mime.so
LoadModule status_module       modules/mod_status.so
LoadModule info_module         modules/mod_info.so
LoadModule cgi_module          modules/mod_cgi.so
...
```

Extension d'Apache

Appels des modules dans le fichier de configuration

```
LoadModule access_module      modules/mod_access.so
LoadModule status_module      modules/mod_status.so
<IfModule mod_status.c>
    <Location /server-status>
        SetHandler server-status
        <IfModule mod_access.c>
          Order deny,allow
          Deny from all
          allow from 127.0.0.1
          Allow from 192.168.5.
        </IfModule>
    </Location>
    ExtendedStatus On
</IfModule>
```

Extension d'Apache

Exemples de modules

Interpréteurs de langages :
- mod_php, mod_perl

Authentification :
- mod_auth_basic, mod_auth_digest (MD5)

Réécriture d'URL :
- mod_rewrite

Gestion de la charge :
- mod_bandwidth, mod_throttle

Proxy HTTP :
- mod_proxy