



Un serveur web permet la mise à disposition de l'information
sur un réseau IP.

Apache est un serveur web

HEB-ESI · Pierre Bettens (pbt) · 2 / 16

Quel type d'informations ?

Pages HTML (CSS/JS si le navigateur le permet)

Pages PHP / Ruby on rails / ASP / ... si les
modules sont dispos.

Demande des ressources côté serveur.

Principe

Application client / serveur sur le port 80 (peut être
changé).

À priori n'a pas d'infos sur le client ... sauf si
cookies / sessions

Autres serveurs web

nginx

package / installation

Les packages concernés sont ;
apache2, libapache2-mod-php5, ...

Les packages dépendent évidemment des modules que l'on veut rendre disponibles.

configuration

Fichiers de configuration dans /etc/apache2

```
    apache2.conf  
conf.d[-available|-enabled]  
sites-[available|enabled]  
mods-[available|enabled]
```


HEB-ESI · Pierre Bettens (pbt) · 4 / 16

Commandes associées a2en

Lancer les services comme d'habitude mais :
notions d'**essaim**.

Répertoire **sites-available** → voir *virtual host* plus
loin. Au minimum *default* doit être *enabled*

It works!

 **Apache2 Debian Default Page**

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented** in [usr/share/doc/apache2/README.Debian.gz](#). Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

Gestion du contrôle d'accès

```
Order deny, allow  
Deny from all  
Allow from 127.0.0.1/8
```

Directives Auth*
Fichier de configuration du site ou .htaccess

À compléter

A woman with blue and red makeup and a red octopus tentacle around her neck.

Les hôtes virtuels permettent à un serveur web de servir plusieurs sites

hôtes virtuels

10.0.0.42:80  example.org
example.com
site1.example.org

Un fichier de configuration par site (*virtual host*)

```
ServerName    example.org
DocumentRoot  /var/www/html/org.example
```

HEB-ÉSI · Pierre Bettens (pbt) · 8 / 16

Fichier dans `/etc/apache2/sites-available`

`example.org.conf`

contient au minimum

le port : 80 ou 443

`ServerName`

`DocumentRoot`

`ServerAdmin`

l'endroit où se trouvent les logs

`a2ensite example.org` crée un lien soft dans `sites-enabled`





Quand *HyperText Transfer Protocol* devient *Secure*

chiffrer la connexion entre le client et le serveur : le contenu, la requête, *headers*, *cookies*...

HTTP encapsulé dans TLS

port 80 → port 443

Toute la communication est chiffrée. Par exemple la requête contient le nom de la page demandée.



Pour avoir confiance, il faut

confiance dans le navigateur

confiance dans l'**autorité de certification** (CA)

confiance en TLS

le site web présente un certificat valide (signé par une CA)

le certificat identifie le site

HEB-ÉSI · Pierre Bettens (pbt) · 11 / 16

Confiance dans le navigateur (firefox versus chrome)

Confiance dans le CA. Certains ont été compromis.

Confiance dans le protocole TLS : la communication sur chiffrée.

On vérifie que le certificat présenté par le site web est bien celui qui a été signé par le CA.

Le CA signe avec sa clé privée. Le site demande au CA si le serveur est bien qui il prétend être.

Le certificat certifie que le site n'est pas usurpé. Je communique bien avec « le bon site »

Autorités de certification

connues des navigateurs

permet de vérifier que le certificat présenté a été donné au bon site

« Je reçois le certificat du site example.org, est-ce bien le certificat que tu lui as donné ? »

CA vérifie via [http](#), [dns](#), [mail](#), voire plus que le détenteur du certificat est propriétaire du nom

Liste des CA accessibles dans les préférences du browser

Vérification :

- http le site a bien accès au serveur web
- dns l'auteur a bien accès à la zone dns
- mail l'auteur a accès à la gestion des mails (il peut créer une adresse spécifique)

voire plus → EV SSL (extended validation)

La vérification de l'existence légale, physique et opérationnelle de l'organisation

La vérification de l'exactitude des informations transmises sur l'organisation (adresse, n° de téléphone)

La vérification du droit exclusif d'utilisation du nom de domaine par l'organisation en question

La vérification de l'accord de l'organisation pour l'émission du certificat

Obtenir un certificat

payer une autorité de certification ou un sous-traitant

créer une CSR (PK et identité)

le CA signe le PK avec sa clé privée

utiliser [Let's Encrypt](#)

avec *Certbot* ou *dehydrated*

CSR – certificate signing request

PK – public key

création d'une csr

```
openssl req -nodes -newkey rsa:2048 -sha256 -keyout  
myserver.key -out server.csr
```

répondre aux questions : nom de domaine et localisation

certbot (voir article de blog)

dehydrated

- ajout du domaine dans `/etc/dehydrated/domains.txt`
- inclure dans le vhost le lien vers acme-challenge (pour avoir un sous-répertoire `.well-known/acme-challenges`)
- générer les fichiers avec `dehydrated -c`
- mettre à jour le vhost avec les liens vers les fichiers key et pem

Configurer Apache

rendre `mod_ssl` disponible

ajouter une section dans la configuration du *virtual host* signalant que le serveur répond sur le port 443

```
<VirtualHost *:443>
    ServerName example.org
    ServerAdmin webmaster@example.org
    DocumentRoot /var/www/html

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

    SSLEngine on
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
</VirtualHost>
```

Références

TCP / IP Network administration (Craig Hunt)

HTTP, Apache web server

... et les pages de manuel

Transparents dans le cadre de mes cours à [HEB-ESI](#).
Ces slides sont sous licence [CC-BY-NC-SA](#)



Qui suis-je ?

Pierre Bettens (pbt)
pbettens@he2b.be
<http://blog.namok.be> · <http://esi.namok.be>

Images

DeviantArt [PorcelainPoet](#)