

Présentation

Apache HTTP Server, ou simplement **Apache**, est l'un des serveurs web les plus utilisés au monde. Il est modulaire, robuste, extensible et compatible avec la majorité des systèmes Unix/Linux.

- **Type** : Serveur HTTP open-source
 - **Port par défaut** : 80 (HTTP), 443 (HTTPS)
 - **Modules supportés** : PHP, SSL, Rewrite, Proxy, etc.
 - **Utilisation typique** : Hébergement de sites web, reverse proxy, serveur d'applications
-

Prérequis système

- **OS** : Debian, Ubuntu, Arch, CentOS, etc.
 - **Paquets requis** : apache2 , libapache2-mod-*
 - **Droits** : root ou utilisateur avec sudo
-

Installation d'Apache

Ubuntu / Debian

```
sudo apt update  
sudo apt install apache2 -y
```

CentOS / RHEL

```
sudo dnf install httpd -y
```

Arch Linux

```
sudo pacman -S apache
```

Gestion du service

```
sudo systemctl start apache2
sudo systemctl enable apache2
sudo systemctl status apache2
```

Sur CentOS : `httpd` remplace `apache2`

Accès au serveur

- Depuis un navigateur :
`http://<IP_SERVEUR>`
- Page par défaut :
`/var/www/html/index.html`

☐ Modules essentiels à activer

☐ PHP (Apache avec `mod_php`)

```
sudo apt install php libapache2-mod-php -y
sudo systemctl restart apache2
```

Fichiers `.php` dans `/var/www/html` sont désormais interprétés.

☐ `mod_rewrite` (réécriture d'URL)

```
sudo a2enmod rewrite
sudo systemctl restart apache2
```

↻ Modifier `/etc/apache2/apache2.conf` pour autoriser `.htaccess` :

```
<Directory /var/www/html>
    AllowOverride All
</Directory>
```

☐ HTTPS avec SSL/TLS (`mod_ssl`)

```
sudo apt install openssl
sudo a2enmod ssl
sudo systemctl restart apache2
```

Création de certificat auto-signé

```
sudo mkdir /etc/apache2/ssl
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/apache2/ssl/apache.key \
-out /etc/apache2/ssl/apache.crt
```

Activer le VirtualHost SSL :

```
sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-
available/monssl.conf
sudo nano /etc/apache2/sites-available/monssl.conf
```

Exemple de bloc VirtualHost :

```
<VirtualHost *:443>
    ServerAdmin admin@example.com
    DocumentRoot /var/www/html
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/apache.crt
    SSLCertificateKeyFile /etc/apache2/ssl/apache.key
</VirtualHost>
```

Activer :

```
sudo a2ensite monssl.conf
sudo systemctl reload apache2
```

mod_proxy (reverse proxy)

```
sudo a2enmod proxy
sudo a2enmod proxy_http
sudo systemctl restart apache2
```

Exemple de configuration (reverse proxy vers un backend local)

```
<VirtualHost *:80>
    ProxyPreserveHost On
    ProxyPass / http://127.0.0.1:8080/
    ProxyPassReverse / http://127.0.0.1:8080/
</VirtualHost>
```

❑ Autres modules utiles

Module	Commande d'activation	Utilité
headers	<code>sudo a2enmod headers</code>	Gérer les en-têtes HTTP
deflate	<code>sudo a2enmod deflate</code>	Compression GZIP
http2	<code>sudo a2enmod http2</code>	HTTP/2 support
cache	<code>sudo a2enmod cache</code>	Mise en cache
status	<code>sudo a2enmod status</code>	Monitoring via <code>/server-status</code>

❑ Gestion des VirtualHosts

Création d'un nouveau site :

```
sudo mkdir /var/www/mon_site
sudo nano /etc/apache2/sites-available/mon_site.conf
```

Contenu :

```
<VirtualHost *:80>
    ServerAdmin admin@monsite.fr
    DocumentRoot /var/www/mon_site
    ServerName monsite.fr
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Activation :

```
sudo a2ensite mon_site.conf
sudo systemctl reload apache2
```

Vérifications

```
apache2ctl -t          # Vérifie la syntaxe de la conf
apache2ctl configtest
sudo systemctl status apache2
```

Sécurité

- Activer un pare-feu :

```
sudo ufw allow 'Apache Full'
```

- Utiliser Let's Encrypt :

```
sudo apt install certbot python3-certbot-apache -y
sudo certbot --apache
```

- Désactiver les modules inutiles :

```
sudo a2dismod autoindex status
```