

[Logiciel](#)

Readme.debian.gz

Apache2 Configuration under Debian GNU/Linux

L'installation par défaut d'Apache2 dans Debian tente de simplifier au mieux l'ajout et la suppression de modules, d'hôtes virtuels et de directives de configuration supplémentaires, pour faciliter l'automatisation des changements et l'administration du serveur.

Du fait de l'utilisation de variables d'environnement, apache2 doit être démarré/arrêté avec **apachectl** ou **apache2ctl**. Pour appeler apache2 avec des arguments en ligne de commande, appelez apache2ctl avec les mêmes arguments.

Fichiers et répertoires dans /etc/apache2

apache2.conf	<p>Fichier de configuration principal.</p> <p>Il n'inclut aucune configuration réelle pour votre site, donc dans la mesure du possible, veuillez ne pas y toucher.</p> <p>Ce fichier est la pierre angulaire de la configuration d'Apache dans Debian et doit être à jour après les mises à niveau pour s'assurer que tous les éléments de configuration sont correctement inclus.</p> <p>Pour étendre la configuration globale, vous pouvez personnaliser le serveur web Apache en incluant des fichiers de configuration par le biais du mécanisme conf-available.</p> <p>Pour modifier les ports d'écoute et la configuration des sockets, utilisez le fichier ports.conf (voir ci-dessous).</p>
ports.conf	<p>Directives de configuration pour les ports et les adresses IP à écouter.</p>
envvars	<p>Ce fichier contient des variables d'environnement utilisables dans la configuration. Certains paramètres, comme l'utilisateur et le fichier pid, doivent figurer ici pour que d'autres scripts puissent les utiliser.</p> <p>Il peut également servir à modifier certains paramètres par défaut utilisés par apachectl, y compris la valeur ulimit pour le nombre maximum de fichiers ouverts.</p> <p>Le paramètre LANG=C par défaut se trouve également ici, et peut être changé en une autre langue.</p>
conf-available/	<p>Les fichiers de ce répertoire sont inclus dans le périmètre global du serveur par une ligne dans apache2.conf :</p> <pre>IncludeOptional conf-enabled/*.conf</pre> <p>C'est un bon endroit pour ajouter des directives de configuration.</p> <p>Tous les fragments de configuration doivent avoir un suffixe .conf pour être inclus dans la configuration réelle.</p> <p>L'administrateur local a intérêt à utiliser des noms de fichiers commençant par local- pour éviter les conflits de noms avec les fichiers installés par les paquets.</p> <p>Les fragments de configuration peuvent être activés ou désactivés en utilisant les exécutable a2enconf et a2disconf.</p> <p>Cela fonctionne comme pour les modules et les sites.</p> <p>Les fragments de configuration peuvent bien sûr aussi être inclus dans des hôtes virtuels spécifiques.</p>

conf-enabled/	Comme mods-enabled/ et sites-enabled/, un fragment de configuration est activé en créant dans ce répertoire un lien symbolique d'un fichier de conf-available/. L'assistant a2enconf est fourni pour vous aider dans cette tâche.
mods-available/	Ce répertoire contient une série de fichiers .load et .conf. Les fichiers .load contiennent les directives de configuration nécessaires au chargement du module en question. Les fichiers .conf contiennent les directives de configuration nécessaires à l'utilisation du module en question.
mods-enabled/	Pour activer un module pour Apache2, il faut créer un lien symbolique dans ce répertoire vers les fichiers .load (et .conf, s'il existe) associés au module dans mods-available/. Par exemple <code>cgi.load -> /etc/apache2/mods-available/cgi.load</code> L'assistant a2enmod peut être utilisé pour activer un module.
sites-available/	Comme mods-available/, sauf qu'il contient des directives de configuration pour des hôtes virtuels pour apache2. Notez que le nom d'hôte n'a pas besoin de correspondre exactement au nom du fichier. '000-default.conf' est l'hôte par défaut fourni par Debian.
sites-enabled/	Similaire à mods-enabled/, sites-enabled contient des liens symboliques vers des sites dans sites-available/ que l'administrateur souhaite activer. Apache utilise le premier VirtualHost qui correspond à l'IP ou au port par défaut pour les hôtes virtuels nommés. Therefore the 'default' site should be called '000-default' to make sure it sorts before other sites. Exemple : dedasys.conf → /etc/apache2/sites-available/dedasys.conf L'assistant a2ensite peut être utilisé pour activer un site.

Depuis la version 2.4, les directives Include ignorent les fichiers dont les noms ne se terminent pas par un suffixe .conf.

Vous pouvez vouloir activer un élément de configuration spécifique pour un hôte virtuel particulier uniquement et non globalement comme par défaut.

Dans de tels cas, vous pouvez désactiver la configuration de portée globale par exemple en faisant

```
...@...:~ $ a2disconf some-configuration
```

Ensuite, il peut être inclus dans un hôte virtuel particulier dans un fichier dans sites-enabled/.

vous pouvez ajouter

```
Include conf-available/some-configuration.conf
```

dans la configuration de ce site.

Mais soyez prudent, car cela peut ne pas fonctionner pour certaines configurations, selon le contexte et les implications de certaines directives.

Outils

a2enmod et **a2dismod** permettent d'activer et de désactiver les modules.

a2ensite et **a2dissite** font la même chose, mais pour les sites plutôt que les modules.

Enfin, **a2enconf** et **a2disconf** sont les outils correspondants pour les fragments de configuration.

a2query est un script d'assistance fournissant des informations d'exécution sur l'instance de serveur en cours d'exécution.

Par exemple, il peut être utilisé pour interroger les modules activés, le MPM sélectionné et d'autres informations.

Cet outil est principalement destiné aux mainteneurs de packages qui ont besoin d'interagir avec les packages Apache pour activer leurs configurations lors de l'installation des packages, mais il peut également être utilisé par les utilisateurs.

Utilisation de mod_cache_disk

Pour s'assurer que le cache disque n'augmente pas indéfiniment, htcacheclean est démarré lorsque mod_cache_disk est activé.

Les modes démon et cron (quotidien) sont pris en charge.

La configuration (mode d'exécution, taille du cache, etc.) est dans **/etc/default/apache2**.

Normalement, htcacheclean est automatiquement démarré et arrêté par **/etc/init.d/apache2**.

Cependant, si vous modifiez l'état de mod_cache_disk ou la configuration de htcacheclean pendant l'exécution d'Apache2, vous devrez peut-être démarrer/arrêter manuellement htcacheclean avec `"/etc/init.d/apache2 start-htcacheclean"` ou `"/etc/init.d /apache2 stop-htcacheclean"`.

Notez que mod_cache_disk s'appelait mod_disk_cache dans les versions 2.2 et antérieures.

SSL

Activer SSL

Pour activer SSL :

```
...@...:~ $ sudo a2ensite default-ssl
...@...:~ $ sudo a2enmod ssl
```

Pour utiliser des certificats auto-signés, vous devez installer le package **ssl-cert**

Sinon, ajustez simplement les directives SSLCertificateKeyFile et SSLCertificateFile dans

/etc/apache2/sites-available/default-ssl.conf pour pointer vers votre certificat SSL.

Then restart apache:

```
...@...:~ $ sudo apachectl restart
```

Le fichier de clé SSL ne doit être lisible que par root ; le fichier de certificat peut être globalement lisible.

Ces fichiers sont lus par le processus parent Apache qui s'exécute en tant que root, et il n'est donc pas nécessaire de rendre les fichiers lisibles par l'utilisateur www-data.

Création de certificats auto-signés

Si vous installez le package ssl-cert, un certificat auto-signé sera automatiquement créé en utilisant le nom d'hôte actuellement configuré sur votre ordinateur.

Vous pouvez recréer ce certificat (par exemple après avoir modifié '/etc/hosts' ou DNS pour donner le nom d'hôte correct) :

```
...@...:~ $ sudo make-ssl-cert generate-default-snakeoil --force-overwrite
```

Pour créer plus de certificats avec des noms d'hôtes différents :

```
...@...:~ $ sudo make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /path/to/cert-file.crt
```

Cela vous demandera le nom d'hôte et placera à la fois la clé SSL et le certificat dans le fichier **/path/to/cert-file.crt**.

Utilisez ce fichier avec la directive SSLCertificateFile dans la configuration Apache (vous n'avez pas besoin du SSLCertificateKeyFile dans ce cas car il contient également la clé).

Le fichier **/path/to/cert-file.crt** ne doit être lisible que par root.

Un bon répertoire à utiliser pour les certificats/clés supplémentaires est **/etc/ssl/private**.

Contournement SSL pour MSIE

La solution de contournement SSL pour MS Internet Explorer doit être ajoutée à votre section SSL VirtualHost :

```
BrowserMatch "MSIE [2-6]" \  
    nokeepalive ssl-unclean-shutdown \  
    downgrade-1.0 force-response-1.0  
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
```

L'hôte virtuel SSL par défaut dans **/etc/apache2/sites-available/default-ssl.conf** contient déjà cette solution de contournement.

Suexec

Debian fournit deux versions du programme d'assistance suexec requis par mod_suexec.

Il n'est pas installé par défaut, pour éviter d'éventuels problèmes de sécurité.

Le package apache2-suexec-pristine contient la version standard qui fonctionne uniquement avec la racine du document /var/www, le suffixe userdir public_html et l'utilisateur d'exécution Apache www-data.

Le package apache2-suexec-custom contient une version personnalisable qui peut être configurée avec un fichier de configuration pour utiliser différents paramètres (comme /srv/www comme racine du document).

Étant donné qu'apache2-suexec-custom a reçu moins de tests et peut être légèrement plus lent, apache2-suexec est la version recommandée, sauf si vous avez besoin des fonctionnalités d'apache2-suexec-custom.

À partir d'Apache 2.4, les deux alternatives peuvent être installées en même temps et le mécanisme suexec par défaut peut être sélectionné en utilisant le système update-alternatives(8).

Normalisation des noms de fichiers Unicode

L'utilisation d'Apache avec la racine du document sur un système de fichiers qui effectue une normalisation unicode sur les noms de fichiers peut entraîner des problèmes de sécurité.

Dans Debian, cela affecte ZFS avec l'option non définie par défaut pour activer la normalisation des noms de fichiers et HFS+.

Il est fortement déconseillé d'utiliser Apache avec de tels systèmes de fichiers.

Documentation

La documentation complète d'Apache 2 est disponible sur le Web à l'adresse <http://httpd.apache.org/docs/2.4/> ou, si vous avez installé le package apache2-doc, dans **/usr/share/doc/apache2-doc/manual/** ou sur <http://localhost/manual/>

Un wiki contient des informations utiles : <http://wiki.apache.org/httpd/>

Quelques conseils sur la sécurisation d'Apache 2 sur Debian sont disponibles sur <http://wiki.debian.org/Apache/Hardening>

Problèmes courants

? Message d'erreur <> lors du démarrage

Il peut généralement être ignoré, mais cela signifie qu'Apache httpd n'a pas pu obtenir un nom d'hôte complet en effectuant une recherche inversée sur l'adresse IP de votre serveur.

✓ Vous pouvez ajouter le nom d'hôte complet à **/etc/hosts**.

Une alternative consiste à spécifier **ServerName 127.0.0.1** dans le contexte de serveur global de la configuration, par ex. dans **/etc/apache2/conf-enabled/local-servername.conf**.

? Message d'erreur "mod_rewrite: could not create rewrite_log_lock"

Cela signifie probablement qu'il existe des sémaphores SYSV périmés.

Cela se produit généralement après qu'apache2 a été tué avec kill -9 (SIGKILL).

✓ Vous pouvez nettoyer les sémaphores avec :

```
...@...:~ $ ipcs -s | grep www-data | awk ' { print $2 } ' | xargs  
ipcrm sem
```

? Message "File does not exist: /etc/apache2/htdocs" dans le journal des erreurs

Dans la plupart des cas, cela signifie qu'aucune définition VirtualHost correspondante n'a pu être trouvée pour une demande entrante.

✓ Vérifiez que l'adresse IP/le port cible et le nom dans l'en-tête Host: de la requête correspondent bien à l'un des hôtes virtuels.

? Message "Couldn't create pollset in child; check user or system limits" dans le journal des erreurs

✓ Sur les noyaux Linux depuis 2.6.27.8, la valeur dans **/proc/sys/fs/epoll/max_user_instances** doit être supérieure à

- pour prefork/itk MPM: $2 * \text{MaxClients}$
- pour worker/event MPM: $\text{MaxClients} + \text{MaxClients}/\text{ThreadsPerChild}$

Il peut être défini au démarrage en ajoutant une ligne comme

```
fs.epoll.max_user_instances=1024
```



à '/etc/sysctl.conf'.

Il existe plusieurs autres messages d'erreur liés à la création d'un pollset qui peuvent apparaître pour la même raison.

D'un autre côté, les erreurs d'ajout à un pollset sont liées au paramètre `fs.epoll.max_user_watches`. Sur la plupart des systèmes, `max_user_watches` doit être suffisamment élevé par défaut.



Message "Server should be SSL-aware but has no certificate configured" dans error log



Depuis le 2.2.12, Apache est plus strict sur certaines erreurs de configuration concernant les hôtes virtuels SSL basés sur les noms.



Apache ne transmet pas l'en-tête d'autorisation aux scripts CGI

Ceci est intentionnel pour éviter les failles de sécurité. Si vous voulez vraiment le changer, vous pouvez utiliser `mod_rewrite` :



```
RewriteCond %{HTTP:Authorization} (.*)  
RewriteRule . - [env=HTTP_AUTHORIZATION:%1]
```



mod_dav se comporte étrangement

En général, si vous utilisez `mod_dav_fs`, vous devez désactiver les vues multiples et l'exécution de scripts pour ce répertoire. Par exemple:



```
<Directory /var/www/dav>  
    Dav on  
    Options -MultiViews -ExecCGI  
    SetHandler none  
<IfModule mod_php5.c>
```



```
php_admin_value engine Off
</IfModule>
</Directory>
```



Message "apache2: bad user name \${APACHE_RUN_USER}" lors du démarrage direct d'apache2



Utilisez apache2ctl (il accepte toutes les mêmes options qu'apache2).



Un PUT avec mod_dav_fs échoue avec "Unable to PUT new contents for /...

[403, #0]" même si Apache a la permission d'écrire le fichier.



Apache a également besoin d'une autorisation d'écriture sur le répertoire contenant le fichier, afin de le remplacer de manière atomique.



Au démarrage/rechargement d'Apache, il y a le message d'erreur "ulimit: open files: cannot modify limit: Operation not permitted"

Si vous exécutez Apache dans un environnement vserver, le script de démarrage peut ne pas être autorisé à définir le nombre maximal de fichiers ouverts.



Vous devez ajuster APACHE_ULIMIT_MAX_FILES dans /etc/apache2/envvars

Vous pouvez désactiver la modification des limites en définissant
APACHE_ULIMIT_MAX_FILES=true .

For Developers

The Apache 2 web server package provides several helpers to assist packagers to interact with the web server for both, build and installation time. Please refer to the PACKAGING file in the apache2 package for detailed information.

Voir aussi

- `/usr/share/doc/apache2/README.Debian.gz`

Basé sur « `/usr/share/doc/apache2/README.Debian.gz` »

From:

<http://doc.nfrappe.fr/> - **Documentation du Dr Nicolas Frappé**

Permanent link:

<http://doc.nfrappe.fr/doku.php?id=logiciel:internet:apache:apachectl:readme.debian.gz> 

Last update: **2022/08/13 22:14**