Apache2 Configuration under Debian GNU/Linux

Contents

Apache2 Configuration under Debian GNU/Linux

Debian's default Apache2 installation attempts to make adding and removing modules, virtual hosts, and extra configuration directives as flexible as possible, in order to make automating the changes and administering the server as easy as possible.

Please be aware that this layout is quite different from the standard Apache configuration. Due to the use of environment variables, apache2 needs to be started/stopped with /etc/init.d/apache2 or apache2ctl. Calling /usr/bin/apache2 directly will not work with the default configuration. To call apache2 with specific command line arguments, just call apache2ctl with the same arguments.

Files and Directories in /etc/apache2:

apache2.conf

```
This is the main configuration file.
```

envvars

```
This contains environment variables that may be used in the
configuration. Some settings, like user and pid file, need to
go in here so that other scripts can use them. It can also
be used to change some default settings used by apache2ctl,
including the ulimit value for the max number of open files.
Here is also the default LANG=C setting that can be changed
to a different language.
```

conf.d/

```
Files in this directory are included by this line in
apache2.conf:

# Include generic snippets of statements
Include /etc/apache2/conf.d

This is a good place to add additional configuration
directives. Packages should not use configuration
files that start with 'local-' or end with '.local'.
The local administrator can use these filenames to make
sure that there are no conflicts with files provided by
packages.

If the local administrator is not comfortable with packages
activating their config files by default, it is possible
to change the 'Include /etc/apache2/conf.d/' in apache2.conf
into 'Include /etc/apache2/conf.d.enabled/' and create that
directory. He can then put symlinks to the files in conf.d
which he wants to enable into conf.d.enabled.
```

httpd.conf

```
Empty file.
```

magic

```
Patterns for mod_mime_magic. This is not compatible with the format
used by current versions of the file/libmagic packages.
```

mods-available/

```
This directory contains a series of .load and .conf files.
The .load files contain the Apache configuration directive
necessary to load the module in question.  The respective
.conf files contain configuration directives necessary to
utilize the module in question.
```

mods-enabled/

```
To actually enable a module for Apache2, it is necessary to
create a symlink in this directory to the .load (and .conf, if
it exists) files associated with the module in
mods-available/.  For example:

cgi.load -> /etc/apache2/mods-available/cgi.load
```

ports.conf

```
Configuration directives for which ports and IP addresses to
listen to.
```

sites-available/

```
Like mods-available/, except it contains configuration
directives for different virtual hosts that might be used with
apache2.  Note that the hostname doesn't have to correspond
exactly with the filename.  'default' is the default host.
```

sites-enabled/

```
Similar in functionality to mods-enabled/, sites-enabled
contains symlinks to sites in sites-available/ that the
admnistrator wishes to enable.

Apache uses the first VirtualHost that matches the IP/Port
as default for named virtual hosts. Therefore the 'default'
site is linked to '000-default' so that it will be read first.

Example:
dedasys -> /etc/apache2/sites-available/dedasys
```

The Include directive ignores files with names that

- do not begin with a letter or number
- contain a character that is neither letter nor number nor _-.
- contain .dpkg

Other files

For historical reasons, the pid file is in /var/run/apache2.pid and not in /var/run/apache2/apache2.pid.

Tools

a2enmod and a2dismod are available for enabling and disabling modules utilizing the above configuration system.

a2ensite and a2dissite do essentially the same thing as the above tools, but for sites rather than modules.

apxs2 -a/-A is modified to use a2enmod to activate newly installed modules.

Using mod*disk*cache

To ensure that the disk cache does not grow indefinitely, htcacheclean is started when mod*disk*cache is enabled. Both daemon and cron (daily) mode are supported. The configuration (run mode, cache size, …) is in /etc/default/apache2 .

Normally, htcacheclean is automatically started and stopped by /etc/init.d/apache2. However, if you change the state of mod*disk*cache or the configuration of htcacheclean while apache2 is running, you may need to manually start/stop htcacheclean with “/etc/init.d/apache2 start-htcacheclean” or “/etc/init.d/apache2 stop-htcacheclean”.

SSL

Enabling SSL

To enable SSL, type (as user root):

```
a2ensite default-ssl
a2enmod ssl
```

If you want to use self-signed certificates, you should install the ssl-cert package (see below). Otherwise, just adjust the SSLCertificateFile and SSLCertificateKeyFile directives in /etc/apache2/sites-available/default-ssl to point to your SSL certificate. Then restart apache:

```
/etc/init.d/apache2 restart
```

The SSL key file should only be readable by root, the certificate file may be globally readable. These files are read by the Apache parent process which runs as root. Therefore it is not necessary to make the files readable by the www-data user.

Creating self-signed certificates

If you install the ssl-cert package, a self-signed certificate will be automatically created using the hostname currently configured on your computer. You can recreate that certificate (e.g. after you have changed /etc/hosts or DNS to give the correct hostname) as user root with:

```
make-ssl-cert generate-default-snakeoil --force-overwrite
```

To create more certificates with different host names, you can use

```
make-ssl-cert /usr/share/ssl-cert/ssleay.cnf /path/to/cert-file.crt
```

This will ask you for the hostname and place both SSL key and certificate in the file /path/to/cert-file.crt . Use this file with the SSLCertificateFile directive in the Apache config (you don't need the SSLCertificateKeyFile in this case as it also contains the key). The file /path/to/cert-file.crt should only be readable by root. A good directory to use for the additional certificates/keys is /etc/ssl/private .

SSL workaround for MSIE

The SSL workaround for MS Internet Explorer needs to be added to your SSL VirtualHost section (it was previously in ssl.conf but caused keepalive to be disabled even for non-SSL connections):

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

The default SSL virtual host in /etc/apache2/sites-available/default-ssl already contains this workaround.

Suexec

Debian ships two version of the suexec helper program required by mod*suexec. It is not installed by default, to avoid possible security issues. The package apache2-suexec contains the standard version that works only with document root /var/www, userdir suffix public*html, and Apache run user www-data. The package apache2-suexec-custom contains a customizable version, that can be configured with a config file to use different settings (like /srv/www as document root). For more information see the suexec(8) man page in the apache2-suexec-custom package.

Since apache2-suexec-custom has received less testing and might be slightly slower, apache2-suexec is the recommended version unless you need the features from apache2-suexec-custom.

Documentation

The full Apache 2 documentation can be found on the web at

http://httpd.apache.org/docs/2.2/

or, if you have installed the apache2-doc package, in

/usr/share/doc/apache2-doc/manual/

or at

http://localhost/manual/

There is also a wiki that contains useful information:

http://wiki.apache.org/httpd/

Some hints about securing Apache 2 on Debian are available at

http://wiki.debian.org/Apache/Hardening

Upgrades

Changes in the Apache packages that require manual configuration adjustments are announced in NEWS.Debian. Installing the apt-listchanges package is recommended. It will display the relevant NEWS.Debian sections before upgrades.

Multiple instances

There is some support for running multiple instances of Apache2 on the same machine. See /usr/share/doc/apache2.2-common/README.multiple-instances for more information.

Common Problems

1) Error message "Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName" during start

This can usually be ignored but it means that Apache httpd was unable to obtain a fully-qualified hostname by doing a reverse lookup on your server's IP address. You may want to add the fully-qualified hostname to /etc/hosts . An alternative is to specify "ServerName 127.0.0.1" in the global server context of the configuration, e.g. in /etc/apache2/conf.d/servername.local .

2) Error message "mod*rewrite: could not create rewrite*log_lock"

This probably means that there are some stale SYSV semaphores around. This usually happens after apache2 has been killed with kill -9 (SIGKILL). You can clean up the semaphores with:

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

3) Message "NameVirtualHost *:80 has no VirtualHosts" in error log

Probably the VirtualHost definitions have not been adjusted after the NameVirtualHost directive was changed in ports.conf. See /usr/share/doc/apache2.2-common/NEWS.Debian.gz

4) Message "File does not exist: /etc/apache2/htdocs" in error log

In most cases this means that no matching VirtualHost definition could be found for an incoming request. Check that the target IP address/port and the name in the Host: header of the request actually match one of the virtual hosts.

5) Message "Couldn't create pollset in child; check user or system limits" in error log

On Linux kernels since 2.6.27.8, the value in

```
/proc/sys/fs/epoll/max_user_instances
```

needs to be larger than

```
for prefork/itk  MPM: 2 * MaxClients
for worker/event MPM: MaxClients + MaxClients/ThreadsPerChild
```

It can be set on boot by adding a line like

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

to /etc/sysctl.conf.

There are several other error messages related to creating a pollset that can appear for the same reason.

On the other hand, errors about to adding to a pollset are related to the setting fs.epoll.max*user*watches. On most systems, max*user*watches should be high enough by default.

6) Message “Server should be SSL-aware but has no certificate configured” in error log

Since 2.2.12, Apache is stricter about certain misconfigurations concerning name based SSL virtual hosts. See NEWS.Debian.gz for more details.

7) Apache does not pass Authorization header to CGI scripts

This is intentional to avoid security holes. If you really want to change it, you can use mod_rewrite:

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

8) mod_dav is behaving strangely

In general, if you use mod*dav*fs, you need to disable multiviews and script execution for that directory. For example:

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

9) Message “apache2: bad user name ${APACHE*RUN*USER}” when starting apache2 directly

Use apache2ctl (it accepts all options of apache2).

10) Apache is using a lot of memory and is not freeing it even when idle

By default, Apache will not give back unused memory but keep it around for later use.

- Tune StartServers, MaxRequestsPerChild, MinSpareThreads/MinSpareServers, MaxSpareThreads/MaxSpareServers in /etc/apache2/apache2.conf

- If you are really starved for memory, try adding ‘MaxMemFree 4’ to your Apache configuration. This will reduce Apache’s performance. Because of the way Apache’s memory allocator interacts with glibc’s malloc, higher values of MaxMemFree don’t have much effect.

11) A PUT with mod*dav*fs fails with “Unable to PUT new contents for /… [403, #0]” even if Apache has permission to write the file.

Apache also needs write permission to the directory containing the file, in order to replace it atomically.