Apache 2.4

Security

Modules

Install the following modules and configure settings in /etc/apache2/mods-available/*.conf:

- mod-evasive
- mod-qos
- mod-reqtimeout
- modsecurity

Links

- Defending Against Apache Web Server DDoS Attacks
- mod_evasive on Apache
- How To Mitigate Slow HTTP DoS Attacks in Apache HTTP Server
- How To Set Up mod_security with Apache on Debian/Ubuntu
- Stop Traffic From China IP Addresses
- IP Location Finder
- DoS
- Using Multiple SSL Certificates in Apache with One IP Address

Upgrade Apache 2.2 to 2.4

Config files

1. All config files in /etc/apache2/sites-available, sites-enabled, conf-available, and conf-enabled need to have extension ".conf"
2. Folder "conf.d" is deprecated, use conf-enabled instead
3. Place a config file in conf-available with the directory path to your document root where you keep your own sites, if you do not keep them in the standard path /var/www. Replace "order allow,deny" statements with "Require" statements in all your VirtualHost definitions:

```
<Directory /path/to/www/>
  Options Indexes FollowSymLinks
  AllowOverride None
  Require all granted
</Directory>
```

4. Don't forget to modify phpmyadmin.conf in conf-available

Links

- Upgrading to 2.4 from 2.2