Apache Web Server Cheatsheet

A quick reference guide covering essential Apache HTTP Server configuration, commands, and modules for effective web server management.

Basic Commands & Configuration

Core Commands

`apachectl start`	Starts the Apache web server.
`apachectl stop`	Stops the Apache web server.
`apachectl restart`	Restarts the Apache web server. Graceful restart.
`apachectl graceful`	Gracefully restarts the server. Finishes current requests before restarting.
`apachectl status`	Shows the server status page (requires `mod_status`).
`apachectl configtest`	Tests the configuration file syntax.

Configuration Files

`httpd.conf` (or `apache2.conf`) - Main configuration file. Location varies by OS (e.g., `/etc/httpd/conf/httpd.conf` or `/etc/apache2/apache2.conf`).

`ports.conf` - Configures ports Apache listens on (usually located in `/etc/apache2/ports.conf`).

`conf.d/` (or `sites-available/`) - Directory for additional configuration files (often used for virtual hosts).

Important Directives

`Listen`	Specifies the port(s) Apache listens on. Example: `Listen 80`
`DocumentRoot`	Defines the root directory for web files. Example: `DocumentRoot /var/www/html`
`ServerName`	Sets the server's hostname. Example: `ServerName example.com`
`<Directory>`	Configures access control and features for specific directories. Example: `<Directory /var/www/html> ... </Directory>`
`ErrorLog`	Specifies the path to the error log file. Example: `ErrorLog /var/log/apache2/error.log`
`CustomLog`	Specifies the path to the access log file. Example: `CustomLog /var/log/apache2/access.log combined`

Virtual Hosts

Virtual Host Configuration

Virtual hosts allow you to run multiple websites on a single server.

Create a virtual host configuration file (e.g., `/etc/apache2/sites-available/example.com.conf`).

Virtual Host Directives

`<VirtualHost *:80>`	Defines a virtual host listening on port 80 (HTTP). Use `*:443` for HTTPS.
`ServerAdmin`	Specifies the administrator's email address. Example: `ServerAdmin webmaster@example.com`
`ServerName`	The primary domain name for the virtual host. Example: `ServerName example.com`
`ServerAlias`	Alternative domain names for the virtual host. Example: `ServerAlias www.example.com`
`DocumentRoot`	The directory containing the website's files. Example: `DocumentRoot /var/www/example.com/public_html`
`ErrorLog`	Log file for errors specific to this virtual host. Example: `ErrorLog /var/log/apache2/example.com_error.log`
`CustomLog`	Log file for access logs specific to this virtual host. Example: `CustomLog /var/log/apache2/example.com_access.log combined`

Enabling/Disabling Virtual Hosts

`a2ensite example.com.conf`	Enables the virtual host (creates a symbolic link in `sites-enabled/`).
`a2dissite example.com.conf`	Disables the virtual host (removes the symbolic link from `sites-enabled/`).
`systemctl reload apache2`	Reload Apache to apply the changes.

Common Modules

Essential Modules

`mod_rewrite` - Provides URL manipulation capabilities.

`mod_ssl` - Enables HTTPS support.

`mod_deflate` - Compresses output for faster loading.

`mod_expires` - Controls browser caching.

`mod_headers` - Modifies HTTP request and response headers.

`mod_status` - Provides server status information.

`mod_authnz_file` - Provides file-based authentication.

Module Commands

`a2enmod module_name`	Enables the specified module.
`a2dismod module_name`	Disables the specified module.
`systemctl reload apache2`	Reload Apache to apply the changes after enabling/disabling modules.

Example: mod_rewrite

To enable URL rewriting, ensure `mod_rewrite` is enabled (`a2enmod rewrite`). Then, use `.htaccess` files or `<Directory>` sections to define rewrite rules.

Example `.htaccess`:

```
RewriteEngine On
RewriteRule ^old-page.html$ new-page.html [R=301,L]
```

Security Tips

General Security

Keep Apache up to date with the latest security patches.
Disable unnecessary modules to reduce the attack surface.
Use a firewall to restrict access to the server.
Regularly review and update your configuration files.

Access Control

`<Directory>`	Use `<Directory>` blocks to control access to specific directories. Example:
	`<Directory /var/www/example.com/private>`
	`Require all denied`
	`</Directory>`

`Options`	Control directory features. Avoid `Options +Indexes` to prevent directory listing. Example: `Options -Indexes`
`Require`	Specify access restrictions. Examples: `Require all granted`, `Require ip 192.168.1.0/24`

HTTPS Configuration

Enable `mod_ssl` and configure virtual hosts to listen on port 443. Obtain and install an SSL/TLS certificate.

Example VirtualHost configuration:

```
<VirtualHost *:443>
  ServerName example.com
  DocumentRoot /var/www/example.com/public_html
  SSLEngine On
  SSLCertificateFile /etc/ssl/certs/example.com.crt
  SSLCertificateKeyFile /etc/ssl/private/example.com.key
</VirtualHost>
```