**一.账号设置**

以专门的用户帐号和组运行 Apache。

1. 根据需要为 Apache 创建用户、组
2. 参考配置操作 如果没有设置用户和组，则新建用户，并在 Apache 配置文件中指定 (1) 创建 apache 组：groupadd apache

(2) 创建 apache 用户并加入 apache 组：useradd apache –g apache

(3) 将下面两行加入 Apache 配置文件 httpd.conf 中

1. User apache
2. Group apache
3. 检查 httpd.conf 配置文件。 检查是否使用非专用账户(如 root)运行 apache
4. 默认一般符合要求，Linux下默认apache或者nobody用户，Unix默认为daemon用户

**二.授权设置**

严格控制Apache主目录的访问权限，非超级用户不能修改该目录中的内容

1. Apache 的 主目录对应于 Apache Server配置文件 httpd.conf 的Server Root控制项中应为：
2. “Server Root /usr/local/apache”
3. 判定条件

非超级用户不能修改该目录中的内容

1. 检测操作

尝试修改，看是否能修改

一般为/etc/httpd目录，默认情况下属主为root:root，其它用户不能修改文件，默认一般符合要求

严格设置配置文件和日志文件的权限，防止未授权访问。

* chmod 600 /etc/httpd/conf/httpd.conf”设置配置文件为属主可读写，其他用户无权限。
* 使用命令”chmod 644 /var/log/httpd/\*.log”设置日志文件为属主可读写，其他用户只读权限。
* /etc/httpd/conf/httpd.conf默认权限是644，可根据需要修改权限为600。
* /var/log/httpd/\*.log默认权限为644，默认一般符合要求。

**三.日志设置**

设备应配置日志功能，对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的 IP 地址等内容。

1. 编辑 httpd.conf 配置文件，设置日志记录文件、记录内容、记录 格式。　　其中，错误日志：
2. LogLevel notice #日志的级别
3. ErrorLog /…/logs/error\_log #日志的保存位置(错误日志)
4. 访问日志：
5. LogFormat %h %l %u %t \”%r\” %>s %b “%{Accept}i\”%{Referer}i\” \”%{User-Agent}i\””
6. combined
7. CustomLog /…/logs/access\_log combined (访问日志)

* ErrorLog 指令设置错误日志文件名和位置。错误日志是最重要的 日志文件，
* Apache httpd 将在这个文件中存放诊断信息和处理请 求中出现的错误。
* 若要将错误日志送到 Syslog，则设置： ErrorLog syslog。
* CustomLog 指令指定了保存日志文件的具体位置以及日志的格式。访问日志中会记录服务器所处理的所有请求。
* LogFormat 设置日志格式，建议设置为 combined 格式。
* LogLevel 用于调整记录在错误日志中的信息的详细程度，建议设置为notice。
* 日志的级别，默认是warn，notice级别比较详细，在实际中由于日志会占用大量硬盘空间，一般没有设置

**四.禁止访问外部文件**

禁止 Apache 访问 Web 目录之外的任何文件。

1. 参考配置操作

　　编辑 httpd.conf 配置文件：

1. Order Deny,Allow
2. Deny from all
3. 设置可访问目录
4. Order Allow,Deny
5. Allow from all

　　其中/web 为网站根目录

1. 默认配置如下:
2. Options FollowSymLinks
3. AllowOverride None

一般可根据业务需要设置

**五.禁止目录列出**

1. 目录列出会导致明显信息泄露或下载，禁止 Apache 列表显示文件,编辑 httpd.conf 配置文件：
2. #Options Indexes FollowSymLinks #删掉Indexes
3. Options FollowSymLinks
4. AllowOverride None
5. Order allow,deny
6. Allow from all

　　将Options Indexes FollowSymLinks 中的 Indexes 去掉，就可以禁 止 Apache 显示该目录结构。 Indexes 的作用就是当该目录下没 有 index.html 文件时，就显示目录结构。

1. 重新启动 Apache 服务
2. 可以设置 /etc/httpd/httpd.conf 段中删除Options的Indexes设置

一般可根据业务需要设置

**六.错误页面重定向**

Apache 错误页面重定向功能防止敏感信息泄露。

1. 修改 httpd.conf 配置文件：
2. ErrorDocument 400 /custom400.html
3. ErrorDocument 401 /custom401.html
4. ErrorDocument 403 /custom403.html
5. ErrorDocument 404 /custom404.html
6. ErrorDocument 405 /custom405.html
7. http://www.013188.com
8. ErrorDocument 500 /custom500.html
9. 注：Customxxx.html 为要设置的错误页面。
10. 重新启动 Apache 服务
11. 此项需要应用系统设有错误页面，或者不在httpd中设置完全由业务逻辑实现，可根据业务需求加固。

**七.拒绝服务防范**

根据业务需要，合理设置 session 时间，防止拒绝服务攻击

1. 编辑 httpd.conf 配置文件:
2. Timeout 10 #客户端与服务器端建立连接前的时间间隔
3. KeepAlive On
4. KeepAliveTimeout 15 #限制每个 session 的保持时间是 15 秒 注：此处为一建议值，具体的设定需要根据现实情况。
5. 重新启动 Apache 服务
6. 默认Timeout 120 KeepAlive Off，KeepAliveTimeout 15，该项设置涉及性能调整，一般不做。

**八.隐藏 Apache 的版本号**

隐藏 Apache 的版本号及其它敏感信息。

1.配置操作

修改 httpd.conf 配置文件：

1. ServerSignature Off ServerTokens Prod

**九.关闭 TRACE功能**

关闭 TRACE，防止 TRACE 方法被访问者恶意利用。

配置修改vim /etc/httpd/conf/httpd.conf

1. 添加 “TraceEnable Off”
2. 注：适用于 Apache 2.0 以上版本

**十.禁用 CGI**

如果服务器上不需要运行 CGI 程序，建议禁用 CGI

1.修改配置vim /etc/httpd/conf/httpd.conf，把 cgi-bin 目录的配置和模块都注释掉

1. #LoadModule cgi\_module modules/mod\_cgi.so
2. #ScriptAlias /cgi-bin/ “/var/www/cgi-bin/”
3. #
4. #AllowOverride None
5. # Options None
6. #Order allow,deny
7. #Allow from all
8. #

2.根据需要设置，如果没有CGI程序，可以关闭

**十一.监听地址绑定**

服务器有多个 IP 地址时，只监听提供服务的 IP 地址

1.使用命令查看是否绑定IP地址

1. cat /etc/httpd/conf/httpd.conf|grep Listen

2.修改配置vim /etc/httpd/conf/httpd.conf 修改

1. Listen x.x.x.x:80

默认设置是Listen 80监听所有地址，如果服务器只有一个IP地址可不做该项设置，如果有多个IP可以按照需要设。

**十二.删除缺省安装的无用文件**

删除缺省安装的无用文件.

* 参考配置操作删除缺省 HTML 文件

1. # rm -rf /usr/local/apache2/htdocs/\*

* 删除缺省的CGI脚本

1. # rm –rf /usr/local/apache2/cgi-bin/\*

* 删除 Apache 说明文件

1. # rm –rf /usr/local/apache2/manual

* 删除源代码文件

1. # rm -rf /path/to/httpd-2.2.4\*
2. 根据安装步骤不同和版本不同，某些目录或文件可能不存在或位置不同。

* 删除CGI

可根据实际情况删除，一般是 /var/www/html /var/www/cgi-bin 默认就是空的

**十三.禁用非法 HTTP 方法**

禁用PUT、DELETE等危险的HTTP 方法.

编辑 httpd.conf 文件,只允许 get、post 方法

1. <Location />
2. <LimitExcept GET POST CONNECT OPTIONS>
3. Order Allow,Deny
4. Deny from all
5. </LimitExcept>
6. </Location>

根据需要可设置，如果没有不需要用到put delete HTTP 方法的话，加在/etc/httpd/conf/httpd.conf的段中。