**Apache安全配置规范**

# 概述

## 范围

本规范适用于数字广东内所有服务器上部署Apache的安全配置

## 目的

本规范旨在帮助数字广东运维同事在安装配置Apache时进行必要的安全限制，最大化减少安全漏洞的产生，保障部门信息资产安全

# Window系统Apache安全配置

## 下载

Apache软件的下载，应该从Apache官方页面下载：

<http://httpd.apache.org/download.cgi>

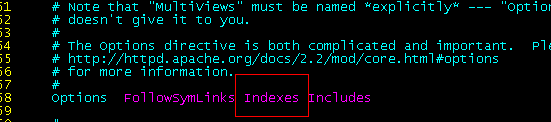
需要下载最新稳定版本，目前是2.4系列。注意不要下载beta版本和1.x版本

## 安装配置

apache主目录须删除这两个目录： icons、manual

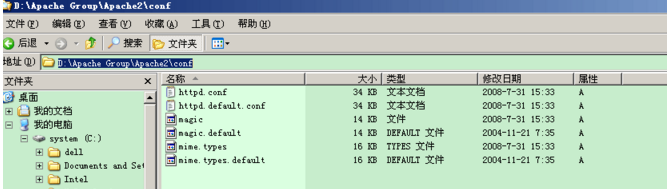
## 消除目录浏览漏洞

需要把Apache配置文件http.conf中的目录配置项的“Indexes”删除或者改为“-Indexes”



## 隐藏Apache的版本号及其敏感信息

在Apache安装目录下打开httpd.conf文件



参数设置： 在配置文件httpd.conf中加入以下语句。



## 创建Apache运行帐户及组

默认情况下，安装完后，Apache会以用户"System"(本地系统账号)运行，而SYSTEM用户的权限非常大，因此我们需要创建一个专门的用户来运行apache。

操作步骤：

1）打开和编辑httpd.conf文档，增加

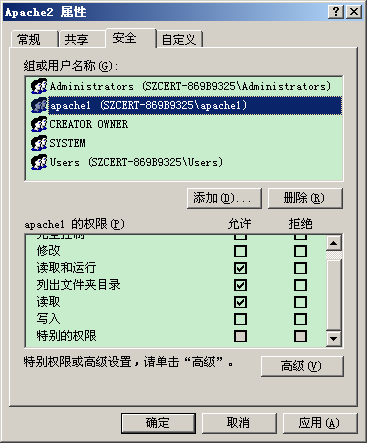
User Apache

Group Apache

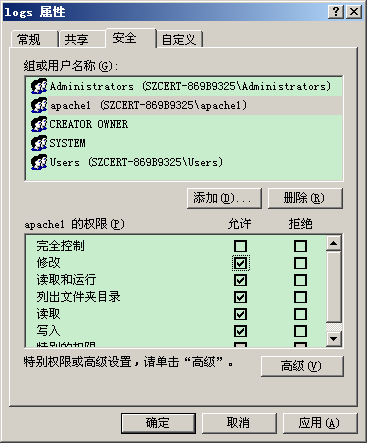
2）创建一个用户叫Apache，组名叫Apache

并且将该apache用户加入Apache组

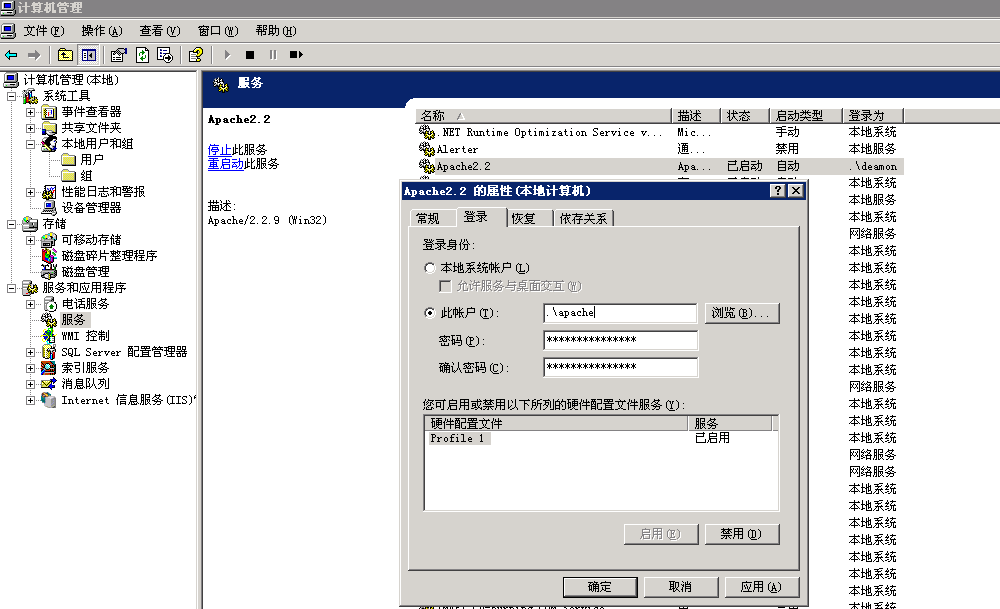
1. 将apache的安装目录赋予apache组有读、运行、浏览目录的权限：



4）将apache的日志记录文件logs赋予apache组有读、写、运行、浏览目录、修改的权限：



5)以apache用户来启用apache服务：



## 开启访问日志

默认情况下，Apache已开启访问日志记录，请在Apache配置文件中确认已开启访问日志, OA正式环境Apache日志须至少保存一年。

|  |
| --- |
| CustomLog /www/logs/access\_log common |

## 管理目录安全配置

对于管理目录，需要做到两重限制：访问IP白名单限制和密码认证

Apache配置文件中配置某IP可访问：

|  |
| --- |
| <Directory "D:/apache2/htdocs/ForCgiTest/uploadfiles">  order deny,allow  deny from all  allow from pair 10.2.122.112  </Directory> |

密码认证依靠Web应用自身的认证机制。如果Web应用无认证机制，请启用Apache的密码认证机制

## 去掉UserDir功能

早期版本的Apache默认会开启UserDir，这个无关功能会泄漏主机的账户名，也可能由于配置不当导致敏感文件被下载

新版apache默认不开启UserDir；对于旧版本，确保apache配置文件中注释掉以下UserDir相关项

|  |
| --- |
| #<IfModule mod\_userdir.c>  #UserDir public\_html  #</IfModule> |

如果配置文件中没有上述三行，则需要添加或者修改以下项目

|  |
| --- |
| UserDir disable |

## 简明Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 阶段 | 检查点 | 检查方法 | 检查结果 |
| 下载 | 下载 | 是否从官方或安全平台部提供的下载渠道下载 |  |
| 安装配置 | 编译和安装 | 删除/icons、/manual等默认目录 |  |
|  | 消除目录浏览漏洞 | 是否删除Indexes功能 |  |
| 隐藏banner | 是否隐藏版本信息 |  |
| 访问日志 | 是否开启访问日志 |  |
| 创建apache运行账号和组 | 创建Apache用户和组 |  |
| apache的安装目录赋予apache组有读、运行、浏览目录的权限 |  |
| apache的日志记录文件logs赋予apache组有读、写、运行、浏览目录、修改的权限 |  |
| 管理目录安全 | 是否管理目录启用了IP认证和口令认证 |  |
| 启动权限 | Apache普通用户(非system、adminstrator)权限启动 |  |
| 管理目录安全 | 是否管理目录启用了IP认证和口令认证 |  |
| 消除UserDir | 是否禁用UserDir功能 |  |

# Linux系统Apache安全配置

## 下载

Apache软件的下载，应该从Apache官方页面下载：

<http://httpd.apache.org/download.cgi>

需要下载最新稳定版本，目前是2.4系列。注意不要下载beta版本和1.x版本

## 下载后的校验

下载的同时，需记录下官方提供的文件hash（推荐MD5）

下载完毕后立即判断下载的文件hash是否与官网提供一致，Linux下可以使用以下命令来判断：

|  |
| --- |
| md5sum filepath.tar.gz |

如果md5sum得出的hash与官网提供的不相同，则不能进行安装

## 编译和安装

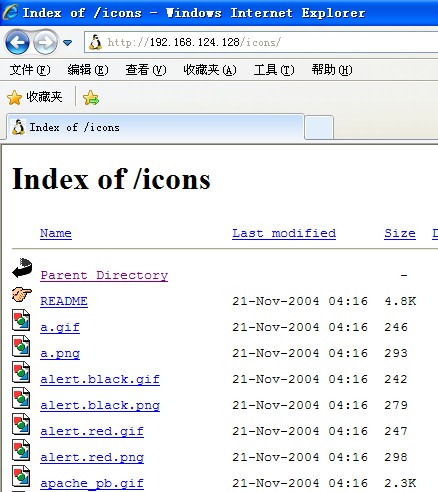
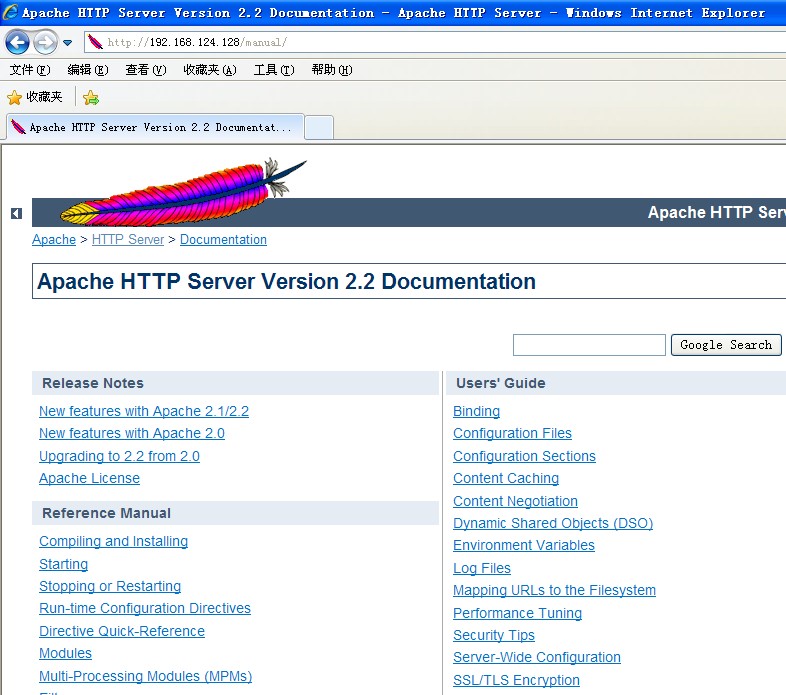
### 编译和安装

Apache编译安装时，不引入不必要的模块

## 安全配置

### 删除默认页面

Apache安装好后，存在默认的示例页面：

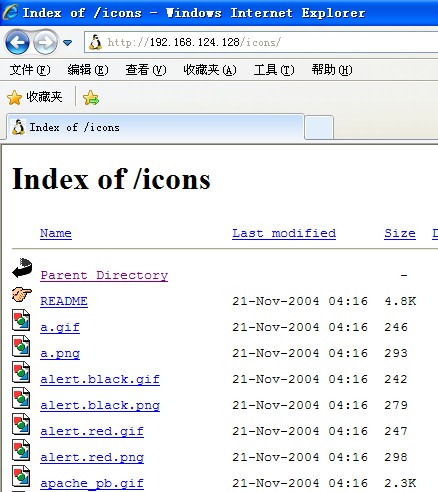


需要删除这两个目录： icons、manual ；也可以通过注释Apache配置文件中的以下两行内容实现同样的效果：

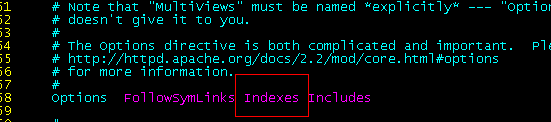
|  |
| --- |
| Alias /icons/ "/usr/share/apache2/icons/"  AliasMatch ^/manual(?:/(?:de|en|es|fr|ja|ko|ru))?(/.\*)?$ "/usr/share/apache2/manual$1" |

### 消除目录浏览漏洞

Apache默认允许目录浏览，如果目录下没有索引文件则会出现目录浏览漏洞：



需要把Apache配置文件中的目录配置项的“Indexes”删除或者改为“-Indexes”



### 隐藏版本信息

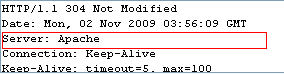
Apache默认输出的banner会泄漏关键信息，如服务器OS类型、Apache版本、安装的应用程序类型及版本。暴露过多的信息只会给黑客带来便利，但是隐藏了版本信息可能导致安全平台部Web漏洞扫描器不能获取服务器相关信息

是否隐藏版本信息，视业务重要程度而定，这里不做硬性要求

在Apache配置文件中，修改ServerToken、ServerSignatre设置：

|  |
| --- |
| ServerTokens ProductOnly  ServerSignatre Off |

（修改前）

（修改后）

### 开启访问日志

开启日志有助于发生安全事件后回溯分析整个事件的原因及定位攻击者

默认情况下，Apache已开启访问日志记录，请在Apache配置文件中确认已开启访问日志

|  |
| --- |
| CustomLog /www/logs/access\_log common |

### 目录安全配置

Apache启动时权限是nobody（或者其他非root账户，参考4.7“不以root启动”），如果黑客通过Web应用漏洞获取到权限也是nobody，故应当保证目录的安全配置。确保“**解析CGI的目录Apache不可写，Apache可写的目录不解析PHP”**：

1、apache的文件和目录，属主需要是root（或者其他非apache启动用户），普通文件和目录权限需要是755。特殊的目录，如允许上传文件的目录，可以为777

2、对于不需要执行PHP脚本的目录（如允许上传文件的目录），建议设置为不可执行PHP（这里的执行是指Apache不解析目录下的CGI，而不是指Linux文件系统的x权限）

需要Apache配置文件中对目录权限做修改：

|  |
| --- |
| <Directory "/usr/local/apache2/yourpath">  php\_flag engine off  </Directory> |

### 管理目录安全配置

对于管理目录，需要做到两重限制：访问IP白名单限制和密码认证

Apache配置文件中配置某IP可访问：

|  |
| --- |
| <Directory "/usr/local/apache2/htdocs/ForCgiTest/uploadfiles">  order deny,allow  deny from all  allow from pair 10.2.122.112  </Directory> |

密码认证依靠Web应用自身的认证机制。如果Web应用无认证机制，请启用Apache的密码认证机制

### 不以root用户启动

不能以root权限启动Apache

新版apache已经禁止以root启动的行为；对于旧版本，确保apache配置文件中的配置项，User和Group的值不能为root

|  |
| --- |
| User daemon  Group daemon |

### 去掉UserDir功能

早期版本的Apache默认会开启UserDir，这个无关功能会泄漏主机的账户名，也可能由于配置不当导致敏感文件被下载

新版apache默认不开启UserDir；对于旧版本，确保apache配置文件中注释掉以下UserDir相关项

|  |
| --- |
| #<IfModule mod\_userdir.c>  #UserDir public\_html  #</IfModule> |

如果配置文件中没有上述三行，则需要添加或者修改以下项目

|  |
| --- |
| UserDir disable |

## 简明Checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 阶段 | 检查点 | 检查方法 | 检查结果 |
| 下载 | 下载 | 是否从apahce官方渠道下载 |  |
| 校验 | 是否在下载完成后校验文件hash |  |
| 编译和安装 | 编译和安装 | 是否安装时引入不必要的组件 |  |
| 配置 | 删除默认页面 | 是否删除/icons等默认页面 |  |
| 消除目录浏览漏洞 | 是否删除Indexes功能 |  |
| 隐藏banner | 是否隐藏版本信息 |  |
| 访问日志 | 是否开启访问日志 |  |
| 目录安全配置 | 是否web目录文件属主为非Apache用户 |  |
| 是否web目录Apache用户不可写 |  |
| 是否为不需要解析CGI的目录配置不解析 |  |
| 管理目录安全 | 是否管理目录启用了IP认证和口令认证 |  |
| 启动权限 | 是否以非root用户启动 |  |
| 消除UserDir | 是否禁用UserDir功能 |  |