**Nginx安全配置规范**

# 概述

## 范围

本规范适用于数字广东所有服务器上部署Nginx的安全配置

## 目的

本规范旨在帮忙数字广东运维同事在安装配置Nginx时进行必要的安全限制，最大化减少安全漏洞的产生，保障公司信息资产的安全

# 下载

## 下载位置

Nginx软件的下载，应该从Nginx官方提供的下载页面下载

Nginx官网下载地址为：[http://nginx.org](http://nginx.org/en/download.html)[/](http://nginx.org/en/download.html)[en/download.html](http://nginx.org/en/download.html)

需要下载最新稳定版本(当前稳定版本是1.12.2)。注意不要下载beta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，

如果md5sum得出的hash与官网提供的不相同，则不能进行安装。

# 安装

## 安装

Nginx安装时，不引入不必要的模块

# 安全配置

## 消除目录浏览漏洞

nginx默认不允许目录浏览，请检查目录浏览的相关配置，确保没有目录浏览漏洞：

检查各个配置文件，确保autoindex的配置为off。

|  |
| --- |
| autoindex off |

## 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，nginx已开启访问日志记录，请在nginx配置文件中确认已开启访问日志

|  |
| --- |
| access\_log /backup/nginx\_logs/access.log combined; |

## 目录安全配置

nginx应该严格保证用户上传文件的目录没有执行脚本的权限，取消特定目录执行php权限可以在配置文件中设置：

|  |
| --- |
| location~\*^/data/(attachment|avatar)/.\*\.(php|php5)$  {  deny all;  } |

## 管理目录安全配置

对于管理目录，需要做到只允许合法ip可以访问，nginx限制白名单ip访问的配置日下：

|  |
| --- |
| location ~ ^/private/ {  allow 192.168.1.0/24;  deny all;  } |

管理目录建议启用密码认证，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，可启用nginx的密码认证机制，配置如下：

|  |
| --- |
| location ^~ /soft/ {  location ~ .\*\.(php|php5)?$ {  fastcgi\_pass unix:/tmp/php-cgi.sock;#这里按照你自己的设置  fastcgi\_index index.php;  include fcgi.conf;  }  auth\_basic "Authorized users only";  auth\_basic\_user\_file 这里写前面脚本返回的文件路径;  } |

## 删除默认页面

Nginx存在默认页面，



删除如下配置信息。

|  |
| --- |
| location /doc {  root /usr/share;  autoindex on;  allow 127.0.0.1;  deny all;  }  location /images {  root /usr/share;  autoindex off;  } |

# 简明checklist

|  |  |  |  |
| --- | --- | --- | --- |
| 阶段 | 检查点 | 检查方法 | 检测结果 |
| 下载 | 下载 | 是否从官方渠道下载 |  |
| 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 | 消除目录浏览漏洞 | 检查各个配置文件，确保autoindex的配置为off |  |
| 开启访问日志 | nginx配置文件中确认已开启访问日志  access\_log /backup/nginx\_logs/access.log combined; |  |
| 目录安全配置 | 严格保证用户上传文件的目录没有执行脚本的权限，检查配置文件  location~\*^/data/(attachment|avatar)/.\*\.(php|php5)$  {  deny all;  } |  |
| 管理目录安全配置 | 只允许合法ip可以访问管理页面  location ~ ^/private/ {  allow 192.168.1.0/24;  deny all;  } |  |
| 检测管理目录是否启用密码认证 |  |
| 删除默认页面 | 删除如下配置信息:  location /doc {  root /usr/share;  autoindex on;  allow 127.0.0.1;  deny all;  }  location /images {  root /usr/share;  autoindex off;  } |  |