网站安全狗 Linux-Nginx 版

用户手册

厦门服云信息科技有限公司

www.safedog.cn

2015 年 10 月

目录

1. 软件说明

网站安全狗 Linux-Nginx 版（SafeDog For Linux-Nginx）是一款集网站漏洞防护、网站防盗链、网站特定资源保护、IP 黑白名单功能为一体的服务器安全防护软件，为用户在 Internet 的网络服务提供完善的保护，避免 Nginx 服务器出现故障以及受到黑客攻击。

2. 软件运行环境

❖ 软件当前版本支持的 Linux 服务器的操作系统包括：centos 5.3、RHEL 5.0、Ubuntu 11.04，其它版本号的支持，未经过完整测试。

❖ 安装前请确保安装有 Nginx 1.0/1.2/1.4/1.6/1.7/1.8/1.9 版本，否则软件中的功能无效。

3. 软件安装

以 32 位安装包为例，64 位安装包把对应的 32 改成 64 即可。

步骤 1 ：到 http://www.safedog.cn 下载软件发布包（.tar.gz 格式）：

safedog_linux32.tar.gz

也可以采取 wget 的方式下载发布包：

```
wget http://down.safedog.cn/safedog_linux32.tar.gz
```

步骤 2：在 root 帐户下执行以下命令：

```
tar xzvf safedog_linux32.tar.gz
cd safedog_linux32
chmod +x install.py
./install.py
```

运行时，安装脚本将自动获取 Nginx 服务器的安装路径，若自动获取失败则将提示输入 Nginx 服务器的安装路径（绝对路径），请根据您所安装的 Nginx 的目录，填写真实的安装路径。

举例：/usr/local/nginx

注意：

1） 提示：若您在输入时，不慎输入错误，请按组合键 CTRL+Backspace 删除。

2） 网站狗的安装目录为/etc/NginxSafedog，请不要删除此目录及目录下的任何内容。

3） 若安装脚本自动重启 Nginx 服务器失败，请手动重启 Nginx，以使网站安全狗软件生效。

4） 如果重启 Nginx 服务器时失败，并提示 Permission denied 错误，请参考 5.7 章节。

4. 软件卸载

步骤 1：以 root 身份进入网站安全狗的安装目录。

步骤 2：运行如下命令进行卸载：

进入安装包目录：cd safedog_linux32

增加执行权限：chmod +x uninstall.py

执行卸载脚本：./uninstall.py

注意：

（1）当出现提示：Would you like to backup the files of isolation?[Y/n]::时，根据是否备份隔离文件输入 Y 或 n。

（2）卸载完成后，若自动启动 Nginx 服务器失败，请手动启动 Nginx 服务器。

5. 云端功能说明

网站安全狗云端设置功能，必须基于已成功将服务器加入服云。

5.1 如何加入服云

步骤 1 ：安装服务器安全狗；

步骤 2 ：通过输入服云帐号的用户名和密码，自动下载证书，将服务器加入服云。

备注：如何安装服务器安全狗详见：服务器安全狗安装教程

5.2 如何进入网站安全防护

步骤1 ：打开服云官网http://fuyun.safedog.cn ，使用加入服云的同一个帐号登

录，即可方便设置相应的服务器防护功能，告别必须登录服务器才能操作的传统方式。

图 5.2.1 服云

图 5.2.2 服云-登录

❖ 如果没有服云帐号，需要先注册，才能加入服云。

图 5.2.3 服云-注册

步骤 2 ：成功登录服云后，显示此帐号下所有服务器的整体情况。

图5.2.4 服云-登录首页

步骤 3 ： 打开服务器管理，展示此帐号下所有服务器列表。

图5.2.5 服云-服务器管理

步骤4 ： 在搜索框输入服务器IP后，查找到指定服务器。

步骤 5 ： 点击服务器图标，或者服务器 IP，即可显示主机面板。

图5.2.6 服云-主机面板

步骤 6 ： 打开网站安全防护，显示所有快捷防护设置。

图 5.2.7 服云-网站安全防护

5.3 主动防御

图 5.3.1 服云-网站安全防护

主动防御模块包含网站漏洞防护、URL 长度上限值、URL 地址全检测、检测 Get、Post 之外的请求等功能，用户可以通过各个功能对应的开关进行开启/关闭操作。完成操作后点击“确定”按钮，保存配置，等待 1 分钟后即可生效。

5.4 网站防护

图 5.4.1 服云-网站安全防护

网站防护模块包含网站资源防盗链、网站特定资源防下载、IP 黑白名单等功能，用户可以通过各个功能对应的开关进行开启/关闭操作。完成操作后点击“确定”按钮，保存配置，等待 1 分钟后即可生效。

6. 软件功能说明

修改网站安全狗的配置文件所在目录/etc/NginxSafedog/conf 下的配置文件来启用网站安全狗的相应功能。

注意：

（1）以下配置文件各字段的值只是举例，请根据您的实际需要自行设定。设定前请参考每个字段前的注释信息；

（2）修改完的配置后，将会自动生效。如果未立即生效，请重启 Nginx 服务器；

（3）白名单和黑名单的优先级高于其他防护，其中白名单又高于黑名单。如果您在设置了某个防护后，发现其未起效等异常，请检查是否是设置了白名单和黑名单导致的；

（4）修改配置中的字段时，请在英文状态下输入，正则表达式规则说明字段 Description 除外；

6.1 主动防御

6.1.1 网站漏洞防护（WPCDefSql.conf）

网站安全狗的设计是根据攻击特征库，对用户输入进行过滤，从而达到防护 SQL 注入的目的。此功能中用户可以根据实际需要对过滤规则进行新增、修改、删除。

SQL 注入英文名叫 SQL Injection，是存在于应用程序数据库层的安全漏洞。攻击者利用这个漏洞在输入的资料字串中夹带 SQL 指令。一旦应用程序忽略了检查，这些夹带进去的指令就会被数据库服务器误认为正常的 SQL 指令而执行，从而导致数据库结构以及系统资料外泄，最终使系统遭到破坏。

配置说明：

1. 是否开启防注入功能：1 开启，0 关闭

   ChkSqlAttackStatus=1

2. 发现被注入时，是否将该攻击写入日志：1 发送，0 不发送

   SendAlert=1

3. 手动在线更新 SQL 规则地址：

   UpdateUrl=http://www.safedog.cn/upload/configFile/sqlRule.dat

4. 白名单路径个数：白名单中的路径不受防注入功能的保护。

   WhitePathCount=3

5. SQL 防注入白名单：

路径的格式有两种，分别为：

（1）域名/目录路径名称;6

（2）域名/文件路径名称;5

举例：

WhitePath0=www.test.com/;6

WhitePath1=www.test.com/hello/;6

WhitePath2=www.test.com/world/index.html;5

6. 防 sql 注入正则表达式规则数：Count=5

7. 正则表达式规则：

（1）第 0 条正则表达式：

- 检测 Cookie 内容是否用第 0 条正则表达式：

  CheckCookie0=1

- 检测 Post 内容是否用第 0 条正则表达式：

  CheckPost0=1

- 检测 URL 内容否用第 0 条正则表达式：

  CheckUrl0=1

- 第 0 条正则表达式规则

  Sql0=;{0,1}'{0,1}\){0,1}(\+|)*\b(and|or)\b(\+|)+.*(=|<|>).*

- 对第 0 条正则表达式规则的说明：

  Description0=防止 and or 方式注入

这个字段是为了向用户说明该正则表达式的用途，安全狗程序不会使用该字段，故该字段可有可无，但建议用户在新建一个正则表达式时都添加该字段，方便理解和记忆。

（2）第 1 条正则表达式：

- 检测 Cookie 内容是否用第 1 条正则表达式：

  CheckCookie1=1

- 检测 Post 内容是否用第 1 条正则表达式 ：

  CheckPost1=1

- 检测 URL 内容否用第 1 条正则表达式：

  CheckUrl1=1

- 第 1 条正则表达式规则

  Sql1=\b(create|drop|backup)\b(\+|)+\bdatabase\b(\+|)+\w*

- 第 1 条正则表达式的说明

  Description1=防止对数据库进行创建、删除、备份操作

（3）第 2 条正则表达式：

CheckCookie2=1

CheckPost2=1

CheckUrl2=1

Sql2=\b(drop|truncate|create)\b(\+|)+\btable\b(\+|)+\w*

Description2=防止对数据库进行删除、创建表操作

（4）第 3 条正则表达式：

CheckCookie3=1

CheckPost3=1

CheckUrl3=1

Sql3=\bdbo\.\w+

Description3=防止数据库系统的存储过程被执行

（5）第 4 条正则表达式：

CheckCookie4=1

CheckPost4=1

CheckUrl4=1

Sql4=\bdeclare\b(\+|)+.+

Description4=防止注入存储过程

8. 是否检测 URL 路径长度（1 是，0 否）

ChkUrlLenStatus=1

9. URL 路径最长的长度

MaxUrlLen=16385

验证生效方法：

如果你开启了 SQL 防注入功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服务器会阻止访问并会返回您所设定的提示信息。

6.1.2 网马防护（WPCDefTrojan.conf）

主动拦截上传或浏览的网页木马，保护网站安全。

配置说明：

1. 是否开启网马防护功能：

ChkTrojan=1 其中 1 表示开启，0 表示关闭。

- ❖ 该字段是防护总开关，若该字段被设置为关闭，那所有子功能都不会起作用。

2. 网站白名单配置

（1）不受此功能保护的网站白名单总数,0 表示无网站白名单

SpeSiteCount=0

（2）网站白名单列表 无白名单时此项省略

Site0=www.test.com:80

例子：

SpeSiteCount=2

Site0=www.test0.com:80

Site1=www.test1.com:81

3. 网站路径白名单配置

（1）不受此功能保护的网站路径白名单总数,0 表示无网站路径白名单

```
WhitePathCount=0
```

（2）路径白名单后的参数说明：3 表示物理文件路径；4 表示物理目录路径；5 表示网络文件路径；6 表示网络目录路径

```
WhitePath1=/var/www/htdocs/mine.db;3
WhitePath0=/var/www/htdocs/hello/;4
WhitePath2=www.test.com:80/me.gif;5
WhitePath3=www.test.com:80/world/;6
```

4. 网站后台扫描（浏览防御）功能配置

（1）是否开启。1 表示开启浏览防御，0 表示关闭浏览防御

```
ChkWTBrowsyFile=1
```

（2）受浏览防御保护的文件类型

```
Resource=asa|asax|ascx|ashx|asmx|asp|aspx|cdx|cer|cgi|jsp|php
```

5. 文件上传防护功能配置

（1）是否开启。1 表示开启文件上传防御，0 表示关闭文件上传防御

```
ChkForbidPostExt=1
```

（2）受文件上传保护的文件类型

```
ForbidPostExt=asa|asax|ascx|ashx|asmx|asp|aspx|cdx|cer|cgi|dll|exe|jsp
|php
```

6. 发现被攻击时，是否将该攻击写入日志：1 发送，0 不发送

```
SendAlert=1
```

7. 是否禁止 GET、POST 之外的请求类型：1 禁止，0 不禁止

```
ForbidOtherRequests=1
```

6.1.3 网站后台防护（WPCBackGroundProtect.conf）

该功能对指定网站后台管理页面访问控制。

配置说明：

1. 后台防护开关。其中 1 表示开启，0 表示关闭。

```
UsedBackGroundProtect=0
```

该字段是防护总开关，若该字段被设置为关闭，那所有网站后台防护子功能都不会起作用

2、是否开启临时 ip 黑名单开关。其中 1 表示开启，0 表示关闭。

```
bUsedBlackTempIPControl=1
```

3、临时 ip 黑名单的生效时间，单位分钟

```
nFreeTempBlackIPTime=1
```

4、密码防护模式下，密码错误重试间隔时间，单位：秒

```
nAllowedPWDCheckErrNumsInterval=60
```

5、密码防护模式下，密码错误重试次数

```
nPWDCheckErrNums=3
```

6、防护的后台 url 数目

```
Count=1
```

7、防护 url 设置

```
[SiteSec0]
```

（1）防护模式。1 为 IP 防护模式，2 为密码防护模式，4 为 session 防护模式

```
ProtectMode=2
```

（2）防护的域名或 IP

```
Domain=www.test.com
```

（3）session 防护模式时配置，用户名

```
UserName=test
```

（4）防护模式 2 或 4 时，需要配置密码

```
Password=test
```

（5）防护的 url 路径数目

```
ProtectPathCount=1
```

（6）防护的 url 路径数目

```
ProtectPathCount=1
```

- 以下根据需要配置的路径数目，添加如下配置

#注释

```
Comments0=test
```

#防护的 url 相对路径

```
ProtectPath0=/test.php
```
(防护路径数为 0 时，此项为空)

#防护 url 相对路径开关 1：开启 0：关闭

```
ProtectPathState0=1
```

（7）IP 防护模式配置：IP 白名单

```
WhiteIP=10.10.10.11
```

（8）IP 防护模式：IP 白名单生效时间，单位分钟

WhiteIPTempValidTime=10

6.2 流量保护

6.2.1 网站资源防盗链（WPCLinkGate.conf）

盗链是指服务提供商自己不提供服务的内容，通过技术手段绕过其它有利益的最终用户界面(如广告)，直接在自己的网站上向最终用户提供其它服务提供商的服务内容，骗取最终用户的浏览和点击率。受益者不提供资源或提供很少的资源，而真正的服务提供商却得不到任何的收益。

本程序通过 Reference 技术解决防盗链问题。Reference 技术通常用于图片、mp3 等资源这种容易被人用 html 嵌入到其他网站资源的资源。

两种防护方式：

（1）引用（Reference）方式：是通过判断 referer 变量的值来判断图片或资源的引用是否合法，只有在设定范围内的 referer，才能访问指定的资源，从而实现了防盗链的目的。Reference 方式能够让本域名和其他指定信任域名正常链接被保护资源。该技术主要用来保护下载类资源，如 rar，jpg 等

配置说明：

1. 是否开启防盗链功能：

ChkLinkGate=1 1 开启，0 关闭

2. 引用方式：

（1）reference 校验设置：状态（0 不启用 1 启用）

Reference=1

（2）reference 校验：本域名信任（0 关闭 1 开启）

RLocalSite=1

（3）reference 校验：其他域名信任（0 关闭 1 开启）

ROtherSite=1

（4）其他信任域名列表个数：若为 0，则 TSite0 等字段不存在

TrustCount=2

（5）其他信任域名列表：

本机网站域名,本机网站域名,本机网站域名…;信任域名,信任域名…

- 这里的本机网站域名必须与 nginx 配置的 server_name 字段所设的字段匹配。
- 多个本机网站域名之间用英文逗号隔开（这些本机网站域名指的是同一个网站的多个域名），多个信任域名之间也用英文逗号隔开。
- “本机网站域名”和“信任域名”之间用英文分号隔开。最后一个本机网站域名和最后一个信任域名之后不包括逗号（,）。
- 填写以下字段时请注意字段名末尾的数字：TSite0，TSite1，TSite2。请严格按照此规则定义字段名字。

举例：

如果你只有一个 site 需要定义，则字段名应为：TSite0；如果你有四个 site 需要定义，则字段名应为：TSite0，TSite1，TSite2，TSite3.

```
TSite0=www.test.com,www.test1.com;www.google.com.hk,www.baidu.com
TSite1=www.test2.com;www.sina.com,www.sohu.com
```

（6）引用方式保护的资源类型：

```
后缀名|后缀名|后缀名
```

- 各字符间不要有空格或制表符。最后一个后缀名之后不要包含竖线（|）

举例：`Resource=rar|jpg`

（7）不受引用方式防盗链规则保护的本服务器上的域名数目：

```
SpeSiteCount=1
```

- 若为 0，则 Site0 等字段不存在。

（8）不受引用方式防盗链规则保护的域名：

```
Site0= www.test3.com
```

- 这里的站点必须是本服务器上的站点。
- 域名必须与 nginx 配置的 server_name 字段所设的字段匹配

验证生效方法：

如果你开启了网站资源防盗链功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服务器会阻止访问并返回您所设定的提示信息。

6.2.2 网站特定资源保护（WPCRejectDown.conf）

网站特定资源保护通过对某些特定资源的设置来确保它们不被下载或盗用。

注意：

填写的路径（Path）和保护资源类型（Resource）中只要客户端的访问条件满足其中一种都会被拦截。

配置说明：

1. 是否开启防下载功能：1 表示是，0 表是否

   ChkRejectDown=1

2. 禁止下载的路径规则数，

   PathCount=3

3. 禁止下载的路径：

   本机网站域名/目录名称或文件名称;类型值

   其中类型值表示分号前面的路径的类型，其定义如下：

   - 5　表示域名+文件名称；
   - 6　表示域名+目录名称。

注意：

- 本机网站域名必须与 nginx 配置的 server_name 字段所设的字段匹配。
- 填写以下字段时请注意字段名末尾的数字：Path0，Path1，Path2。请严格按照此规则定义字段名字。

举例：

如果你只有一个 site 需要定义，则字段名应为：Path0 ，如果你有两个 site 需要定义，则字段名应为：Path0，Path1.

```
Path0=www.test.com/me.gif;5
Path1=www.test.com/world/;6
```

4. 保护的资源类型：

   后缀名丨后缀名丨后缀名

   - 各字符间不要有空格或制表符，最后一个后缀名之后不要包含|号。

举例：Resource=mdb|dll

5. 发现文件被非法下载时，是否将该攻击写入日志：1 表示是，0 表是否

   SendAlert=1

验证生效方法：

如果你开启了特定资源防下载功能，并且有客户端（浏览器）在访问您的网站时，违反了您所设定的规则，服务器会阻止访问并返回您所设定的提示信息。

6.2.3 多线程下载保护（WPCThreadControl.conf）

开启该功能后，nginx 服务的配置文件 nginx.conf 中会自动生成网狗相关配置信息；关闭该功能后，配置文件中的相关信息自动删除。

配置说明：

1. 是否开启多线程下载包含功能：1 开启，0 关闭

```
ChkThreadCtrl=0
```

2. 下载速度限制　50k 表示最大访问下载速度 50kb 每秒

```
LimitRate=50k
```

3. 下载并发数 10 表示单 ip 只能同时 10 个并发访问 nginx

```
LimitConn=10
```

6.3 IP 黑白名单

6.3.1 IP 白名单（WPCWhiteIP.conf）

IP 白名单设置可以通过设置一些值得信赖 IP 地址为白名单地址，从而使它们能够顺利的访问网站。

注意：

IP 白名单的优先级比 IP 黑名单的高。

配置说明：

1. 是否开启允许白名单 IP 功能，1 表示开启，0 表示关闭

```
ChkWhiteIP=1
```

2. 是否允许爬虫网站功能，1 表示允许，0 表示不允许

```
AllowSpider=1
```

3. 搜索引擎爬虫的关键字数量，若个数为 0，则 SpiderKey0 等字段不存在

```
SpiderCount=8
```

4. 搜索引擎爬虫的关键字

```
SpiderKey0=baiduspider+
SpiderKey1=googlebot/
SpiderKey2=iaskspider/
SpiderKey3=msnbot/
```

```
SpiderKey4=sogou push spider/
SpiderKey5=sogou web spider/
SpiderKey6=yahoo! slurp
SpiderKey7=yodaobot/
```

5. 白名单 IP 段的个数，若个数为 0，则 WhiteIP0 等字段不存在

```
WhiteIPCount=3
```

6. 针对保护模块的 IP 白名单：

开始 IP-结束 IP,规则名称#保护模块编号$

其中，功能模块编号标志 IP 白名单适用的保护模块，其定义如下：

- 1 网站漏洞防护；
- 5 网站资源防盗链；
- 6 网站特定资源保护。

注意：

- 支持同一个 IP 白名单适用多个保护模块，每个模块以$分隔，并且以$结尾。

举例：

```
WhiteIP0=192.168.1.1-192.168.1.255,规则1#1$2$5$
```

以上IP白名单只针对网站漏洞防护、网马防护、网站资源防盗链三个保护模块生效。

- 若未写保护模块，则 IP 白名单全局生效。

举例：

```
WhiteIP1=192.168.2.1-192.168.2.255,规则 2
```

以上 IP 白名单全局生效。

验证生效方法：

如果你将某个 IP 添加进了白名单，即使客户端（浏览器）在访问您的网站时，违反了您所设定的防护规则，服务器也会允许此行为。

6.3.2 IP 黑名单（WPCBlackIP.conf）

IP 黑名单设置可以通过设置一些不良 IP 地址为黑名单地址，从而限制它们访问网站。

配置说明：

1. 是否开启拦截黑名单 IP 功能（1 开启，0 关闭）

ChkBlackIP=0

2. 发现黑名单访问时，是否将该攻击写入日志（1 开启，0 关闭）

SendAlert=1

3. 黑名单 IP 段的个数，若个数为 0，则 BlackIP0 等字段就不存在

Count=3

4. 黑名单 IP 段：

IP,子网掩码:IP 段开始-IP 段结束

举例：

BlackIP0=192.16.3.23,255.255.255.255:192.16.3.23-192.16.3.23

BlackIP1=10.23.45.44,255.255.255.224:10.23.45.33-10.23.45.62

BlackIP2=175.62.6.32,255.255.255.248:175.62.6.33-175.62.6.38

验证生效方法：

如果你将某个 IP 添加进了黑名单，该 IP 在访问您的网站时，服务器会阻止访问并返回您所设定的提示信息。

6.4 防护日志（WPCLog.conf）

网站安全狗会将其防护攻击的日志写入其安装目录下的 Analysis/SynSvr.dat 数据库。

配置说明：

1. 日志保存天数：SaveDays=30

6.5 防护总开关（WPCGeneralDefInfo.conf）

该文件是网站安全狗防护功能的总开关。

注意：

如果关闭总开关，网站安全狗所有防护功能均失效。

配置说明：

1. [GeneralInfo]：

Switch=1

SynServerStatus=1

这里必须要保持两个字段都为 1，总开关才能开启，若其中一个为 0，或两个都为 0 时，总开关都会关闭。

6.6 日志查看工具——sdalog

sdalog 工具可以从安装目录下的 Analysis/SynSvr.dat 数据库中读取日志并展示给用户。

支持分时间段查询，分类型查询，将查询结果输出到文件。

使用说明:

1. 在 linux 的 shell 终端中运行 sdalog 命令，并带上相应参数。

参数说明如下：

（1）`sdalog --help` 或 `sdalog -h`

该命令可以在线查看 sdalog 的帮助信息

（2）`sdalog --file -n` 或 `sdalog -n -f`

该命令将在网站安全狗的安装目录下新建一个.log 文件，文件的名称是当前时间。并将查询到的防护记录存放到该文件中。

（3） `sdalog -n --time=2011-10-12-07:45:42/2011-12-30-22:32:10`

该命令将会查询并显示2011-10-12-07:45:42到2011-12-30-22:32:10之间的防护记录。

该参数的格式为：

- 查询“起始时间”到“结束时间”之间的记录：

  `sdalog -n --time=起始时间/结束时间`

- 查询“起始时间”之后的所有记录：

  `sdalog -n --time=起始时间/`

- 查询“结束之间”之前的所有记录

  `sdalog -n --time=/结束时间`

- 时间格式：`YYYY-MM-DD-HH:MM:SS` （如：2011-06-20-15:22:59）

也可以省略掉后面的时间，但至少保留年份。这个格式会将后面省略掉的时间默认为最小。如：

`YYYY-MM` （如：2011-07，等同于：2011-07-01-00:00：00）

`YYYY` （如：2011，等同于：2011-01-01-00:00:00）

YYYY-MM-DD-HH （如：2010-08-12-18，等同于：2010-08-12-18:00:00）

（4）sdalog -n --type=all

该命令将查询所有类型的防护记录，格式为：

sdalog -n --type=类型

其中，“类型”为下面其中一项：

- all （所有类型）
- inject （SQL 防注入防护记录）
- link （防盗链防护记录）
- dl （防下载防护记录，dl 即 download）
- blackip （IP 黑名单防护记录）

2. 参数--time、--type 和-f 可以组合使用，都必须带参数 -n。

如果参数中不带--time 参数，则默认为查询所有时间的记录。

如果参数中不带--type 参数，则默认为查询所有类型的记录。

如果参数中不带-f 或-file 参数，则默认将查询结果输出到终端。

举例：

直接运行命令 sdalog -n，不带任何参数，表示查询所有时间所有类型的防护记录，并向结果输出到终端。

3. 输出到终端时，每一栏都有固定的宽度，如果结果很乱，请将终端设置为全屏。如果某一栏的记录超过固定宽度，则会被截断，剩余的部分用省略号代替。输出到文件时，每一栏会保留完整结果。

6.7 SElinux 的相关设置

1. 如果您的系统中开启了 SElinux，网站安全狗安装后，重启 nginx 时可能会失败，并给出 Permission denied 错误。

如下内容是解决此问题的方案，并不是网站安全狗的功能。若您的系统中并没有开启 SElinux，或重启 nginx 并没有失败，请略过以下内容。

2. 查看是否开启 SElinux 的命令：getenforce

运行结果为以下三种情况时：

- Enforcing：表示 SElinux 正在运行，并会限制相关程序的资源访问权限。

- Permissive：表示 SElinux 正在运行，但不会限制程序的资源访问权限。
- Disabled：表示 SElinux 被关闭。

只有在 Enforcing 状态下，重启 nginx 时才会报 Permission denied 的错误。请参考如下解决方案。

三种解决方案：

方案 1. 关闭 SElinux（推荐）。

1. 打开文件/etc/selinux/config；
2. 将 SELINUX=enforcing 改为 SELINUX=disabled；
3. 重新启动系统。

方案 2. 设置 nginx 对网站安全狗文件的 SElinux 相关访问权限。

- 在开始之前请确保您已安装 setroubleshoot 服务，并已经启动这项服务。

1. 当重启 nginx 失败并提示 Permission denied 的错误时，运行命令：

```
cat /var/log/messages|grep setroubleshoot
```

运行结果类似于下边这样：

```
Jan 10 15:09:46 localhost setroubleshoot:SELinux is preventing httpd from loading /usr/lib/libSPModule.so.0.0.0 which requires text relocationl.For complete SELinux messages. run sealert -l d4365f9-7a80-4928-9dd0-6447aebb0b2b
```

2.根据上面的输出提示中的

```
run sealert -l d4365f9-7a80-4928-9dd0-6447aebb0b2b
```

运行命令：

```
sealert -l d4365f9-7a80-4928-9dd0-6447aebb0b2b
```

3. 上面这条命令的输出结果中会详细描述该错误产生的原因,解决方法及相应的附加信息等内容。您只需按照解决方法中的指示操作即可解决问题。例如：上面的输出结果中会有如下两栏：

```
以下命令将允许这个权限：
chcon  -t textrel_shlib_t  '/usr/lib/libSPModule.so.0.0.0'
```

你只需运行以下命令即可：

```
chcon  -t textrel_shlib_t  '/usr/lib/libSPModule.so.0.0.0'
```

注意：

如果有多个错误，您需要重复步骤(2)和(3)多次。

方案 3. 用命令重新启动 nginx。

注意：

此方案不一定在所有机器上都适用。

7. 关于我们

7.1 关于我们

安全狗是国内知名的互联网安全品牌，专注于（云）服务器安全。首创的云+端云安全管理平台（SAAS 模式）为用户解决公有云、私有云和混合云环境中可能遇到的安全及管理问题，提供包含自动化系统风险识别和加固、系统级安全防护（防黑/防入侵/抗攻击）、云监控（安全监控/性能监控/日志监控）、云管理（多公有云管理/混合云管理)以及基于大数据架构的安全事件分析等功能。

安全狗云安全服务平台目前已经保护超过百万台的（云）服务器，日均为用户拦截超过千万次的攻击，是国内该领域用户量最大的云安全服务平台。

同时安全狗也积极参与到国内云计算安全生态的建设，目前已经跟国内主流大型云计算平台建立合作伙伴关系；安全狗云安全服务平台已经成功对接各大云计算平台。

安全狗归属的厦门服云信息科技有限公司在成立不到两年时间内，获得了 IDG 等国内一线投资机构的 A、B 轮投资。作为一家年轻的云安全领域创业公司，我们致力于通过领先的安全技术、大数据处理平台为用户提供创新性的安全服务。

7.2 联系我们

7.2.1 官方网站

http://www.safedog.cn

7.2.2 官方论坛

http://bbs.safedog.cn

7.2.3 服务与支持

1）在线支持：（工作日 8:40-22:00 非工作日：8:40-18:00 ）

2）电话号码：400-1000-221

3）邮箱地址：tech@safedog.cn

7.2.4 市场与合作

1）在线支持：（工作日 8:40-18:00 ）

2）电话号码：0592-3833142 0592-3775556

3）邮箱地址：kangjian@safedog.cn

4）联系地址：福建省厦门市软件园二期观日路 58 号