安全狗

服务器安全狗 Linux 版 V2.8Beta
用户手册

2016 年 7 月

厦门服云信息科技有限公司

leading provider of cloud security services and solutions.

目录

1. 软件说明

服务器安全狗 Linux 版（SafeDog for Linux Server）是为 Linux 服务器开发的一款服务器管理软件，它集成了服务器防护模块、Apache 防护模块和 Nginx 防护模块。其中服务器防护模块提供了 DDOS 攻击检测和防御系统、远程登录监控、ssh 防暴力破解、流量统计、帐户监控和设置、系统参数快速设置、系统运行状态展示、系统状态实时监控等功能。其 DDOS 攻击检测和防御系统能够有效防御 CC 攻击，并极大地减少误判。

Apache 防护模块（SafeDog for Linux Apache）是一款集网站内容安全防护、网站资源保护及网站流量保护功能为一体的服务器工具，为用户网络服务提供完善的保护，避免 Apache 服务器出现故障以及受到黑客攻击。教程下载

Nginx 防护模块（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。教程下载

本软件支持两种方式进行操作：云端（www.safedog.cn）设置（详见第 5 章节）、命令行操作（详见第 6 章节），为管理员提供多种选择，管理和配置服务器也更加简单。

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:Ubuntu 、Centos 、Fedora 和 RHEL 等发行版的较新版本,如果安装过程中提示无法安装表示系统版本太老等原因安全狗目前不支持。请根据您的系统选择 32 位安装包或 64 位安装包。

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://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://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 *.py
./install.py
```

4. 软件运行

步骤 1：打开安全狗官网 http://www.safedog.cn，进行服云账号注册登录。

步骤 2：在客户端进行命令行方式：输入命令 sdcloud –u 用户名；

```
[root@centos68 safedog_linux64]# sdcloud -u safedog
Enter password:
```

步骤 3：客户端加入服云后，可进行命令行功能操作（详细见第 6 章节）；

使用：

`service safedog status` 查看安全狗服务；

`service safedog start` 启动安全狗服务；

`service safedog stop` 停止安全狗服务；

`sdstart` 重启安全狗服务。

重要提醒：

✧ 软件的防火墙等功能依赖于 iptables，在使用软件时，请勿随意修改 iptables，否则可能造成软件功能异常。建议修改 iptables 之后，执行 sdstart 重启安全软件服务。

5. 云端功能说明

服务器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 如何进入服务器安全防护

步骤 1：打开安全狗官网 http://www.safedog.cn ，登录服云账号，进入“我的服云”，

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 5.1.1 服云

图 5.1.2 服云-登录

❖ 如果没有服云账号，需要先注册，才能加入服云。

图 5.1.3 服云-注册

步骤 2：成功登录服云后，显示此账号下所有服务器的整体情况。

图 5.1.4 服云-登录首页

步骤 3：打开安全管理，展示此账号下所有服务器的风险情况。

图 5.1.5 服云-风险管理

步骤 4：点击服务器管理，展示此账号下所有服务器列表。

图 5.1.6 服云-服务器管理

步骤 5：在搜索框输入服务器 IP 后，查找到指定服务器。

步骤 6：点击服务器图标，或者服务器 IP，即可显示主机面板。

图 5.1.7 服云-主机面板

步骤 7：打开服务器安全防护，显示所有快捷防护设置。

图 5.1.8 服云-服务器安全防护

5.2 网络防火墙

5.2.1 DDOS 防火墙

图 5.2.1 网络防火墙-DDOS 防火墙

（1）已开启/已关闭：显示当前 DDOS 防火墙功能的开关状态，支持开启/关闭。

（2）规则设置：

- IP 冻结时间：设置冻结攻击 IP 访问的时间（1~1000 的整数）；
- TCP 流量防护：设置一定响应时间（1~1000 的整数）内的 TCP 连接请求数（1~0x0fffffff 的整数）；
- 扫描防护：设置一定响应时间（1~1000 的整数）内的端口连接最高请求数（1~0x0fffffff 的整数）；
- ICMP 流量攻击：设置一定响应时间（1~1000 的整数）内的服务器最多接受的 ICMP 包的次数（1~0x0fffffff 的整数）；
- UDP 流量攻击：设置一定响应时间（1~1000 的整数）内的服务器最多接受的 UDP 包的次数（1~0x0fffffff 的整数）。

5.2.2 Web 防火墙

图 5.2.2 网络防火墙-Web 防火墙

（1）已开启/已关闭：显示当前 Web 防火墙功能的开关状态，支持开启/关闭。

（2） 规则设置：

❖ 访问规则：

1） 设置某段时间(1~1000 秒)内，允许单 IP 请求同一 URL 的次数(1~0x0fffffff)；

2）设置 URL 白名单：以名单中的项作开头的 URL 进行的访问不会被当成攻击；

图 5.2.3Web 防火墙-设置 URL 白名单

3）设置冻结时间（10~1000 分钟），冻结时间内，IP 访问会被拦截。

- 会话验证：

  1）设置会话验证模式：分为宽松模式和严格模式

  A. 宽松模式：仅对判断为 CC 攻击的 IP 进行验证；

  B. 严格模式：对所有访问 IP 都进行验证；

  2） 验证失败 N 次进行拦截：N 的区间为 2~99。

- 端口设置：设置要保护的端口，所设置端口会在规则下进行保护。
- 代理规则：设置代理访问服务器的访问规则，最大 IP 数（0~0x0fffffff）。

5.2.3 FTP 防暴力破解

图 5.2.4 网络防火墙-FTP 防暴力破解

（1）已开启/已关闭：显示当前 FTP 防暴力破解功能的开关状态，支持开启/关闭。

（2）规则设置：

- 访问规则：设置某段时间（1~1000 秒）内，允许单 IP 请求数（1~0x0fffffff）。
- 冻结时间：设置冻结时间（10~1000 分钟）。冻结时间内，IP 访问会被拦截。
- 端口设置：设置要保护的端口，所设置端口会在规则下进行保护。

5.2.4 远程桌面防暴力破解

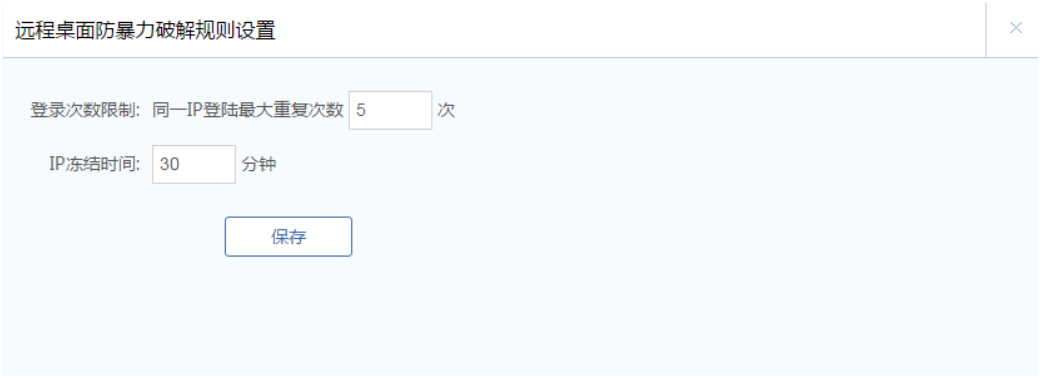

图 5.2.5 网络防火墙-远程桌面防暴力破解

（1）已开启/已关闭：显示当前远程桌面防暴力破解功能的开关状态，支持开启/关闭；

（2）规则设置：

- 访问规则：设置 600 秒内，允许单 IP 请求数（1~0x0fffffff）。
- 冻结时间：设置冻结时间（10~1000 分钟）。冻结时间内，IP 访问会被拦截。

5.2.5 安全策略

图 5.2.6 网络防火墙-安全策略

安全策略功能通过执行具体的端口保护规则，限制或者允许对端口的连接请求，从而保护服务器安全。

（1）已开启/已关闭：显示当前安全策略功能的开关状态，支持开启/关闭。

（2）规则设置：

- 增加规则：增加新的策略规则；

图 5.2.7 安全策略-增加规则

- ❖ 修改规则：修改所选策略规则；
- ❖ 删除规则：删除所选策略规则；

5.2.6 超级黑白名单

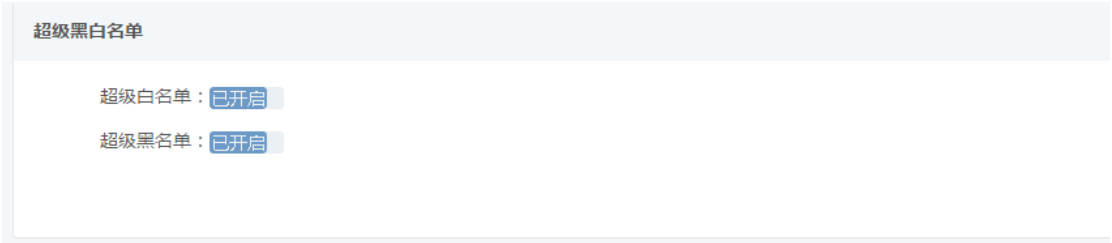

图 5.2.8 网络防火墙-超级黑白名单

超级白名单，使指定 IP 或者 IP 段不受网络防火墙策略限制。

（1）已开启/已关闭：显示当前超级黑白名单功能的开关状态，支持开启/关闭；

5.3 系统防火墙

图 5.3.1 服务器安全防护-系统防火墙

5.3.1 异地登录监控

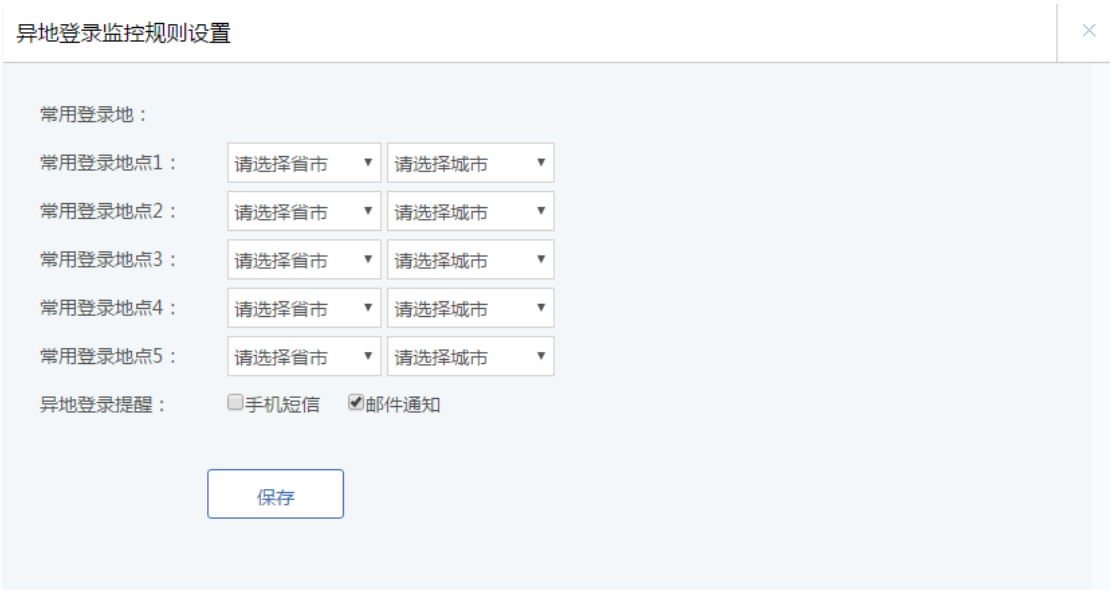

图 5.3.2 系统防火墙-异地登录提醒

设置常用登录地点后，异地登录时支持手机短信提醒和邮件通知两种提醒方式，避免服

务器异常登录的情况发生。

（1）已开启/已关闭：显示当前异地登录监控功能的开关状态，支持开启/关闭；

（2）规则设置：

- 常用登录地：支持设置五个常用登录地；
- 异地登录提醒：支持两种提醒方式，即手机短信和邮件通知；

5.3.2 远程登录保护

图 5.3.3 系统防火墙-远程登录保护

通过阻止未授权的用户远程登录，为服务器提供实时、主动的 SSH 远程桌面登录保护。在此功能中，用户可以设置允许远程登录的白名单等。

（1）已开启/已关闭：显示当前系统登录保护（SSH 远程桌面保护）功能的开关状态，支持开启/关闭。

（2）规则设置：

- 增加规则：增加新的 IP 白名单。白名单列表内的 IP 才允许 SSH 远程登录。

图 5.3.4 远程登录保护-增加 IP 白名单

- ❖ 修改规则：修改所选 IP 白名单；
- ❖ 删除规则：删除所选 IP 白名单；

5.3.3 文件实时防护

图 5.3.5 系统防火墙-文件实时防护

文件实时防护，即发现危险文件，立即处理。

注意：此功能只提供云端设置和命令行操作，不提供客户端界面。

（1）已开启/已关闭：显示当前文件实时防护的开关状态，支持开启/关闭。

（2）规则设置：

- 病毒处理方式：支持自动隔离和不处理两种方式。自动隔离，即发现危险文件立即隔离，可在隔离列表中查看隔离文件，并且在告警中心可以查看防护日志，如下图。

图 5.3.6 告警中心

不处理，即发现危险文件后，写日志文件，不进行隔离或其他操作。可在客户端指定路径查看日志，即 etc/safedog/monitor/rtdfend.txt。

- 引擎设置：目前只支持安全狗云查杀引起，此引擎为云查杀引擎，具有丰富的特征库，通过云端智能识别病毒。

（3）信任查看：

图 5.3.7 文件实时防护-信任查看

显示已信任的文件或文件夹，此列表中的文件或文件夹不参与文件实时防护，支持增加文件夹或文件进行信任，同时支持取消信任。

❖ 添加信任：

图 5.3.8 信任查看-添加信任

（4）隔离查看

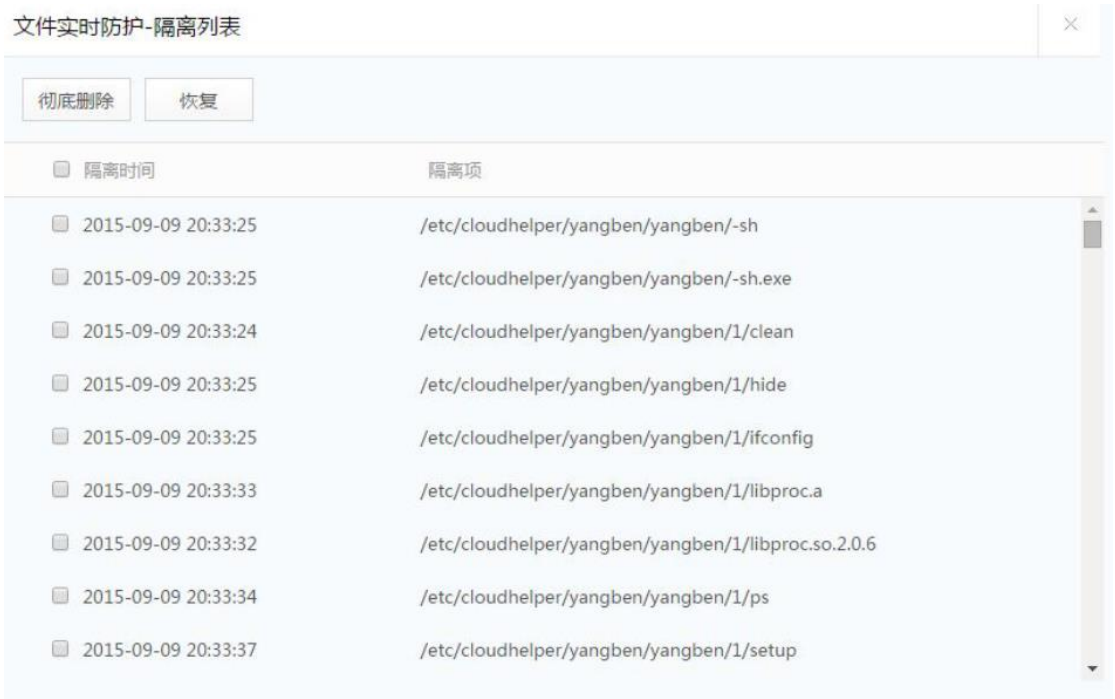

图 5.3.9 文件实时防护-隔离查看

显示已隔离的文件或文件夹，支持客户端彻底删除和恢复操作，特别注意，删除后无法恢复，请谨慎操作。

删除命令：`sdcmd rtddel 隔离项`

恢复命令：`sdcmd rtdrestore 隔离项`

5.4 安全体检

图 5.4.1 安全体检

云端和 Linux 客户端进行联动：

- 支持云端向客户端发送命令进行扫描，修复；
- 客户端向云端上传扫描和修复结果。

6.命令行功能说明

6.1 首页

6.1.1 加入服云

1. 加入服云

命令：sdcloud -u 用户名

参数：服云帐号用户名

2. 查看加入服云命令

命令：sdcloud -h
参数：

6.1.2 系统体检

1. 自动体检开关
命令：sdcmd autoexam
参数：0/1

6.2 网络防火墙

6.2.1 DDOS 攻击防护

1. DDOS 开关
命令：sdcmd ddosflag
参数：0/1

2. 冻结攻击 IP 时长
命令：sdcmd ddosdenytimelen
参数：时间长度（10-1000），单位分钟

3. TCP 端口数
命令：sdcmd portmax
参数：tcp 端口个数（2-1000）

4. TCP 请求数
命令：sdcmd syncountmax
参数：tcp 请求次数（1~268435455）

5. UDP 包个数
命令：sdcmd udpmax
参数：UDP 包最大个数（1~268435455）

6. ICMP 包个数
命令：sdcmd icmpmax
参数：icmp 包最大个数（1~268435455）

6.2.2 CC 攻击防护

1. CC 开关

命令：sdcmd webflag

参数：0/1

2. web 端口号

命令：sdcmd webport

参数：端口号，多个端口号之间用英文逗号隔开

例子：[sdcmd webport 80,8080]

3. URL 白名单

命令：sdcmd ddosurlwhite

参数：白名单的 URL 列表

例子：[sdcmd ddosurlwhite /discus/index.php/date/image]

4. 同一 URL 请求次数

命令：sdcmd urlsameuri

参数：最大请求次数（2-268435455）

5. 代理个数

命令：sdcmd proxyipmax

参数：最大代理个数（0-268435455）

6. 会话验证开关

命令：sdcmd verifyflag

参数：0/1

7.会话验证模式

命令：sdcmd verifyfirstflag

参数：0/1

（1 表示对所有访问 IP 都进行验证，0 表示仅对判定为 CC 攻击的 IP 进行验证）

8.验证失败次数

命令：sdcmd verifymax

参数：次数（2-99）

9.IP 冻结时间

命令：sdcmd ccdentyime
参数：时间长度（10-1000），单位分钟

6.2.3 安全策略

1. 安全策略开关

命令：sdcmd ssflag
参数：0/1

2. 添加安全策略

命令：sdcmd addss
参数：共有 4 个参数，依次为“协议”，“端口”，“策略”，“例外 IP”
协议：1 表示 tcp；2 表示 udp；3 表示 icmp；4 表示 igmp
端口：tcp 或 udp 端口号，若“协议”不是 tcp 或 udp，则设为 0
策略：1 表示 Accpet；2 表示 Drop
例外 IP：多个 ip 地址之间用英文逗号隔开
例子：
除了 110.123.1.2 和 182.12.14.46 外，所以 IP 都禁止访问 tcp 端口 3453【sdcmd addss 1 3453 2 110.123.1.2,182.12.14.46】
除了 110.123.1.2 外，所有 IP 都禁止 ping 本服务器【sdcmd addss 3 0 2 110.123.1.2】

3. 删除某条安全策略规则

命令：sdcmd rmss
参数：安全策略规则的 ID 号（ID 号从 0 开始计数，即最小的 ID 应该是 0，而不是 1）
注意：安全策略规则列表中，每天规则前有个“序号”，该序号是从 1 开始计数的。所有，ID 号和序号的关系是：ID=序号-1。

4. 清空安全策略规则

命令：sdcmd clrss
参数：无

5. 修改某条安全策略规则

命令：sdcmd modss
参数：共有 5 个参数：依次为“要修改的策略规则序号”，“协议”，“端口”，“策略”，“例外 IP”
要修改的策略规则序号：从 0 开始
其他四个参数的说明见“2. 添加安全策略”

6.2.4 暴力破解防御

1. FTP 防暴力破解

（1）开关

命令：sdcmd ftpflag

参数：0/1

（2）FTP 端口

命令：sdcmd ftpport

参数：端口号，多个端口号之间用英文逗号隔开

例子：[sdcmd ftpport 21]

（3）登录次数

命令：sdcmd ftppwdmax

参数：最大错误次数（3-100）

（4）IP 冻结时间

命令：sdcmd ftpdenytime

参数：时间长度（10-1000），单位分钟

2. SSH 防暴力破解

（1）开关

命令：sdcmd sshddenyflag

参数：0/1

（2）登录次数

命令：sdcmd sshdallowerrormax

参数：最大次数（1-99）

（3）IP 冻结时间

命令：sdcmd sshddenytimelen

参数：时间长度（10-1000），单位分钟

（4）SSH 立即解除拦截

命令：sdcmd sshdcanceldenyip

参数：IP 地址

例子：[sdcmd sshdcanceldenyip 110.10.23.2]

6.2.5 IP 黑名单

1. 开关

命令：sdcmd superblackflag

参数：0/1

2. IP 黑名单列表

命令：sdcmd superblack

参数：IP（段）列表，以空格分隔多个

例子：[sdcmd superblack 1.2.3.4 111.111.0.0-111.111.256.256]

6.2.6 IP 白名单

1. 开关

命令：sdcmd superwhiteflag

参数：0/1

2. IP 白名单列表

命令：sdcmd superwhite

参数：IP（段）列表，以空格分隔多个

例子：[sdcmd superwhite 1.2.3.4 111.111.0.0-111.111.256.256]

6.2.7 邮件告警

1. 开关

命令：sdcmd ddosmail

参数：0/1

6.3 主动防御

6.3.1 系统帐号保护

1. 系统帐号变动邮件报警开关

命令：sdcmd accountmail
参数：0/1

6.3.2 SSH 远程异地登录保护

1. SSH 端口号
命令：sdcmd sshport
参数：ssh 端口号

2. SSH 远程异地登陆提醒
命令：sdcmd sshdloginalarmflag
参数：0/1

3. 白名单访问控制开关
命令：sdcmd sshwhiteflag
参数：0/1

4. 登录日志邮件告警开关
命令：sdcmd loginmail
参数：0/1

5. SSH 远程登录白名单列表
命令：sdcmd sshwhite
参数：IP（段）列表，以空格分隔多个
例子：[sdcmd sshwhite 1.2.3.4 111.1111.0.0-111..111.256.255]

6.3.3 文件实时防护

1. 文件实时防护开关
命令：sdcmd rtdflag
参数：0/1

2. 设置处理方式
命令：sdcmd rtdprocess
参数：0/1
例子：[只记录日志：sdcmd rtdprocess 0]
[隔离并记录日志：sdcmd rtdprocess 1]

3. 恢复隔离

命令：sdcmd rtdrestore

参数：被隔离的文件路径

例子：[sdcmd rtdrestore /path/tp/file]

4. 删除隔离

命令：sdcmd rtddel

参数：被隔离的文件路径

例子：[sdcmd rtddel /path/to/file]

6.4. 系统监控

6.4.1 文件监控

1. 文件监控开关

命令：sdcmd fmonitflag

参数：0/1

例子：设置为“是”【sdcmd fmonitflag 1】；设置为“否”【sdcmd fmonitflag 0】

2. 邮件告警开关

命令：sdcmd fmail

参数：0/1

例子：设置为“是”【sdcmd fmail 1】；设置为“否”【sdcmd fmail 0】

3. 监控列表

命令：sdcmd fmonitlist

参数：文件或目录的路径列表，以空格分隔

例子：【sdcmd fmonitlist /home/a.txt /homt/dirnew /var/log/mylog.log】

6.4.2 进程监控

1. 开关

命令：sdcmd pmonitflag

参数：0/1

2. 邮件告警开关

命令：sdcmd pmail

参数：0/1

6.4.3 CPU 监控

1. 开关
   命令：sdcmd cmonitflag
   参数：0/1

2. 邮件告警开关
   命令：sdcmd cmail
   参数：0/1

3. 最大使用率
   命令：sdcmd cceil
   参数：使用率（1-99）
   例子：设置最大使用率为 90%【sdcmd cceil 90】

4. 计算 CPU 使用率的时长
   命令：sdcmd ccalctime
   参数：时间长度（1-999），单位秒

6.4.4 内存监控

1. 开关
   命令：sdcmd mmonitflag
   参数：0/1

2. 邮件开关
   命令：sdcmd mmail
   参数：0/1

3. 最大内存使用百分比
   命令：sdcmd mceil
   参数：内存最大使用百分比（%），取值范围：10-99

6.4.5 磁盘容量监控

1. 开关

命令：sdcmd dmonitflag

参数：0/1

2. 邮件告警开关

命令：sdcmd dmail

参数：0/1

3. 磁盘使用率安全边界值

命令：sdcmd diskpercent

参数：磁盘使用率（6-99），单位%

6.4.6 文件备份监控

1. 开关

命令：sdcmd bakforsizeflag

参数：0/1

2. 邮件告警开关

命令：sdcmd bfmail

参数：0/1

3. 添加规则

命令：sdcmd bakforsizeadd

参数：共有 4 个参数，参数间用空格隔开，依次为“监控文件的路径” “备份文件存放的目录” “文件增大多少 KB 进行备份” “备份时是否清空原文件，用 0/1 表示”

例子：

/var/test.log 增大 1024kB 时，将其备份到/home/backup 目录，并清空/var/test.log 文件：【sdcmd bakforsizeadd /var/test.log /home/backup 1024 1】

4. 删除规则

命令：sdcmd bakforsizedel

参数：文件备份规则的序号

例子：删除第 3 条文件备份规则 【sdcmd bakforsizedel 3】

5. 清空规则

命令：sdcmd bakforsizeclr
参数：无

6.4.7 网络流量监控

1. 重置网络流量统计
命令：sdcmd resetflow
参数：无

6.5 系统配置

6.5.1 网络优化

1. 忽略所有 ping 请求包
命令：sdcmd ping
参数：0/1
例子：设置为“是”【sdcmd ping 1】；设置为“否”【sdcmd ping 0】

2. 启用 SynCookies
命令：sdcmd tcpsyn
参数：0/1
例子：设置为“是”【sdcmd tcpsyn 1】；设置为“否”【sdcmd tcpsyn 0】

3. Tcp TIME_WAIT 端口重用
命令：sdcmd twreuse
参数：0/1

6.5.2 资源优化

1. 最大共享内存
命令：sdcmd shmmax
参数：字节数

2. 共享内存总大小限制
命令：sdcmd shmall

参数：字节数

3. 共享内存段最大个数
   命令：sdcmd shmmni
   参数：字节数

4. 最大线程个数
   命令：sdcmd threadmax
   参数：线程个数（512-99999）

5. 可分配的文件句柄最大个数
   命令：sdcmd filemax
   参数：文件句柄个数（4096-1000000）

6.5.3 邮件告警

1. 接收告警的邮箱设置
   命令：sdcmd mailrecvacc
   参数：邮箱账号
   例子：【sdcmd mailrecvacc abctest@xxx.xxx】

2. 发送告警的邮箱设置
   命令：sdcmd mailsendacc
   参数：邮箱账号
   例子：【sdcmd mailrecvacc testsendacc@yyy.yyy】

3. 发送告警的邮箱的服务器
   命令：sdcmd mailsmtpserver
   参数：服务器 IP 地址
   例子：【sdcmd mailsmtpserver 123.123.123.123】

4. 发送告警的邮箱的服务器的端口号
   命令：sdcmd mailsmtpport
   参数：端口号
   例子：【sdcmd mailsmtpport 465】

5. 发送告警的邮箱的密码
   命令：sdcmd mailsendpwd

参数：邮箱账号的正确密码
例子：【sdcmd mailsendpwd mypasswd】

6. 告警邮件的最小间隔时间
命令：sdcmd mailintv
参数：分钟数
例子：【sdcmd mailintv 30】

7. 告警邮件中显示的机器名
命令：sdcmd mailmachinename
参数：机器名字符串
例子：【sdcmd mailmachinename host001】

8. 每日告警邮件最大数量
命令：sdcmd mailmaxperday
参数：邮件数
例子：【sdcmd mailmaxperday 20】

9. 发送测试邮件
命令：sdcmd mailtest
参数：无

6.6 其他

6.6.1 获取服务器安全狗的所有设置

命令：sdcmd check
参数：无

7. 软件卸载

在由安装包解压出来的目录下执行命令：

```
chmod +x uninstall.py
./uninstall.py
```

即可。

8. FAQ

8.1 Q:软件无法安装，提示如下:

```
sdsvrd: error while loading shared libraries:
/usr/lib/safedog/libcmdprosvr.so: cannot restore segment prot after reloc:
Permission denied
```

A：配置 selinux 权限允许软件安装和运行，或者关闭 selinux 服务。

8.2 Q:软件无法安装，提示：

```
need … to install safedog for linux.
```

A：系统版本过老或者系统某些文件丢失，无法安装服务器安全狗。如果提示的文件确认已经存在，比如 iptables 程序在/sbin/目录下，但是仍然提示找不到。需要将该目录加入到 PATH 环境变量下。具体做法是修改/etc/profile，在文件的最后面加上一行

PATH=$PATH:/sbin

然后重启系统后，再重新安装即可。

8.3 Q:系统重启后功能失效

A：软件所有监控会在安全狗服务被关闭或重启后停止，请在重启服务或系统后重新打开相关监控和功能。

8.4 Q：配置 vsftpd 后，匿名用户登录后无法创建文件夹和上传文件

A：首先，确认配置的时候开启了相关的权限；然后，匿名用户登录后的根目录是只读的，只能下载不能修改和删除。在根目录下的 upload 目录是里面可以实现创建文件夹和上传文件，但是不能修改和删除。

8.5 Q：service safedog start 出现提示 unrecognized service

A：请使用命令 sdstart 重启 safedog 服务。

8.6 Q：软件功能部分失效

A：检查 selinux 是否开启。需要关闭 selinux 才能正常运行本软件，如果您的 selinux 正在运行，则运行安全狗的时候可能会因为诸多权限被限制而出错，这时选可以选择

设置 selinux 开放相关权限，或者关闭 selinux，要检查 selinux 状态可以使用"getenforce"命令查看，要关闭 selinux 可以使用命令"setenforce 0"。如果不是 selinux 的问题，请提交 bug 详情给我们，并提交相关日志信息，谢谢！

8.7 Q：软件安装过程中在打印出" start initializing configuration, please wait seconds ..." 之后或卸载过程中卡住

A：服务器由于网络原因连接不上升级中心，耐心等待 3~5 分钟，会跳过此步骤，继续完成后面的安装或卸载。如果已经手动中断了，要重新运行安装或卸载脚本。

9.关于我们

9.1 关于我们

安全狗，国内领先的云安全服务与解决方案提供商，依托云端技术和大数据安全分析能力，基于“云+端+服务”一体化 SaaS 服务模式为用户提供专业的安全产品、服务及解决方案。在云化 IT 基础架构下，安全狗提出了全新的理念“软件定义防御 数据驱动安全”，即以可视化方式快速搭建多层次联动纵深防御体系，并通过基于持续监控和分析的大数据安全分析平台加强安全防御能力，实时展示威胁风险。

安全狗自创立以来，始终坚持信息安全技术的自主创新，并专注于云安全相关技术和产品的研发，拥有多项安全技术发明专利，产品先后通过公安三所、西海岸实验室“东方之星”、可信云等权威机构认证。

同时，安全狗还积极参与到国内云计算生态的建设中，目前已经和亚马逊 AWS、阿里云、腾讯云、UCloud、华为企业云、金山云等主流云平台建立了合作伙伴关系，联合打造云端安全生态。安全狗希望聚合产业势能，提升网络安全产品和服务水平，与合作伙伴共同营造良好的互联网安全环境，维护网络信息安全。

截至 2016 年 3 月，安全狗云安全服务平台目前已经为客户保护超过 200 万台（云）服务器及 100 万个网站，日均拦截超过近亿次的攻击，已成为国内该领域用户量最大的云安全服务平台。

9.2 联系我们

9.2.1 官方网站

http://www.safedog.cn

9.2.2 官方论坛

http://bbs.safedog.cn

9.2.3 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

9.2.4 市场与合作

（1）在线支持：工作日 8:40-18:00

（2）电话号码：0592-3775556

（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 7 楼

10.Apache/Nginx 防护模块教程下载

1.Apache 防护模块教程
http://www.safedog.cn/download/software/safedogwz_linux_Apache_Help.pdf

2.Nginx 防护模块教程
http://www.safedog.cn/download/software/safedogwz_linux_Nginx_Help.pdf

服云信息科技有限公司

地址：中国福建省厦门市软件园二期观日路58号7楼
电话：400-1000-221　　邮箱：web@safedog.cn
企业QQ：800000174　　网址：www.safedog.cn