等级:F

服务器安全狗Linux版 V2.1.10001

使用手册

安全狗互联网安全实验室

www.safedog.cn

2012年12月

目录

1. 软件说明

服务器安全狗 Linux 版 V2.1.10001(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 DDOS 攻击检测和防御系统、流量统计、帐户监控和设置、登录监控、系统参数快速设置、系统运行状态直观展示、系统状态实时监控、常用服务或设备的快速安装和配置等功能，帮助管理员快速直观地管理服务器。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。本软件提供纯字符界面下的界面交互接口和详细的操作指引，使得管理员对服务器的状态更加了解，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。
- 确保 linux 服务器能够连接互联网并且设置有效的 dns。
- 请确保 selinux（若有安装）有打开相关权限或者禁用 selinux，否则无法访问服务，具体请参考文档后面的 FAQ。

3. 软件安装

到 http://safedog.cn 下载软件发布包（zip 压缩包），解压得到其中的.tar.gz 格式的安装包：`safedog_linux_32.tar.gz` 或 `safedog_linux_64.tar.gz`

执行以下命令（以 32 位安装包为例，64 位安装包把命令中的 32 改成 64 即可）：

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

完成安装后可运行命令 sdui 进入操作界面。

4. 软件运行

直接运行命令：

```
sdui
```

即可进入软件操作界面。具体每一步的操作方法在软件界面的底部都有提示。

使用：

```
service safedog status
service safedog start
service safedog stop
```

查看、启动或停止服务。

在 sdui 界面的首页，连续按 F5 或 CTRL+L 组合键，切换到合适的显示文字

在软件的大部分页面直接按 F12，可以显示详细的帮助信息。

5. 软件功能说明

重要提醒：

- ✧ 服务器重启或者安全狗服务重启后，**所有监控功能都会关闭**，如有需要，须重新打开。
- ✧ DDOS 防火墙和 SSH 白名单限制通过操作 iptables 规则实现，当开启这些功能的时候，在您不

清楚 iptables 规则的情况下，请**不要操作 iptables 规则**，否则可能导致网络异常。如果开启这些功能的状态下重启安全狗服务，需要进入 DDOS 设置页面，**重新打开或者关闭开关**，否则网络状态可能会不一致。

5.1. 系统安全防护

5.1.1. Ddos 攻击防护

修改拦截参数后，需要等到下一次 DDOS 防护开启后才会效，如果需要立即生效，要先关闭防护开关，再重新打开。参数参考值：

拦截攻击 IP 的时长： 服务器正常运行期间设置为 900 秒即可，如果发现有遭受 CC 攻击时，建议设置为 9000，该值表示某个 IP 被拦截这么长时间后，会被放行，如果仍然在攻击，可能会再重新拦截。

- TCP 访问限制规则
  - 每 10 秒内最大请求次数： 300
  - 规则状态： 针对 CC 攻击时可以关闭，不需要该规则。
- HTTP 访问限制规则
  - 每 300 秒内最多连续相同 url 请求次数： 5
  - 每 300 秒内最多连续非资源请求次数： 10
  - 规则状态： 建议一直打开，防 CC 攻击的主要规则。
- HTTP 代理访问限制规则
  - 每 60 秒内最大 IP 数(0 表示禁止代理访问)： 5
  - 规则状态： 一般建议打开 ，某些特殊站点除外，防 CC 攻击的主要规则。
- 搜索引擎爬虫规则
  - 是否拦截伪造的爬虫 IP： 是
  - 规则状态： 建议一直打开，否则可能导致搜索引擎的爬虫被误拦截。

拦截的报告文件为
/etc/safedog/monitor/antiddos.txt
sdui 界面上仅显示最近的拦截信息，并且在关闭拦截后清空。

- DDOS 防护功能通过 iptables 拦截攻击 IP，开启 DDOS 防护功能时，请不要随意修改 iptables，否则防护功能可能不能正常工作。
- 如果有误判发生，可以将需要的 IP 加入白名单。如果已知经常访问服务器的爬虫 IP 的名单，可以先将爬虫 IP 加入白名单。
- 拦截过程中，可以通过下面的命令查看当前已拦截的 IP 数
  ```
  iptables -nL ANTI_DDOS | wc -L
  ```
  可以通过下面的命令查看拦截 IP 的过程
  ```
  tail -f /etc/safedog/monitor/antiddos.txt
  ```
- 如果因为服务器被攻击导致负载过高，从而进入 sdui 界面操作较为困难，可以通过下面的命令启动拦截
  ```
  sdcmd ddosflag 1
  ```
  如果仍然无法生效，建议先重启服务器，重启后马上打开 DDOS 防护开关。或者进行下面的操作：
  先屏蔽 web 端口，比如 80 端口，使用下面的命令
  ```
  iptables -I INPUT --destination-port 80 -j DROP
  ```
  然后执行下面的命令开启 DDOS 防护
  ```
  sdstart ; sdcmd ddosflag 1
  ```

5.1.2. 系统帐户保护

显示当前系统中所有帐户的详细信息。对系统帐户的任何改变都会被安全狗记录到日志文件"/etc/safedog/monit/accountmonit.txt"中，如果在该菜单下开启邮件报告，相关变化还会发送到接收报告的邮箱中。

注意事项：

- ✧ 如果您不是十分清楚自己在做什么，请不要对 root 用户和 root 组做任何相关操作。

5.1.3. 远程登陆保护

显示系统最近的 100 条历史登录记录。服务启动后，任何帐户的登录和登出动作均会被记录到日志文件"/etc/safedog/monit/loginmonit.txt"中，如果在该菜单下开启邮件报告，相关变化还会发送到接收报告的邮箱中。

注意事项：

- ✧ 开启登录白名单时，确保服务器的 ssh 端口为默认的 22，否则该功能暂时不可用。
- ✧ 同时，确保已经将本地机器的外部 IP 添加到白名单列表中，否则设置过后就把自己关在服务器门外，连不上服务器，只能通过以下办法重新恢复连接：
  - ■ 要求机房管理员重启电脑，重启后白名单会禁用，同时安全的所有监控都会关闭，需要重新打开
  - ■ 要求机房管理员在机器上以 root 身体执行如下命令(注意大小写)：

```
iptables  -D INPUT -p tcp --destination-port 22 -j SSHWHITE
iptables  -F SSHWHITE
iptables  -X SSHWHITE
```

重新连上机器后要马上手动进入安全狗手动关闭白名单限制

5.2. 系统快速配置

5.2.1. 网络接口配置

手动设置 IP 时需要填写 IP 和掩码信息，网关和 DNS 信息可选填写，。

如果显示值为"??"，表示软件无法探测到该项参数或者该项参数不存在。

[注意]

软件显示的 dynamic 或 static 为当前 IP 的获取方式，仅仅作为参考，可能并不一定是正确的。

5.2.2. 系统状态配置

本菜单下每隔二到三秒会自动刷新状态。

5.2.3. 网络优化

忽略所有 ping 请求包	开启时不响应 ping 请求。
启用 SynCookies	开启后对防范 syn flood 攻击有一定效果
Tcp TIME_WAIT 端口重用	建议开启

5.2.4. 资源优化

如果您不清楚本页面各个参数的功能，请不要进行修改。

5.2.5. 邮件参数

设置用于发送和接收邮件报告邮箱的参数，包括接收报告的邮箱帐号，发送报告的邮箱帐号和密码以及服务器参数，设置完以后可以在该界面尝试发送测试邮件，如果能够在接收邮箱里面收到测试邮件表明设置正确且工作正常，否则可能是设置有错或者是网络工作不正常。目前可以支持 smtp 的邮件发送协议，建议使用 qq,163 等免费邮箱，其它邮箱未经过测试验证。。

24 小时最大邮件发送数从设置时刻开始算起，每次重新设置该值都会重置起始时刻和邮件计数。

[举例]

qq 邮箱的 smtp 服务器为：smtp.qq.com ，端口号为 465

5.3. 系统实时监控

5.3.1. 文件监控

设置完文件列表后，再开启监视器开关，报告文件为

/etc/safedog/monitor/filemonit.txt

[注意]

不会递归监控到子目录里面,并且当文件名列表为空时无法启动监视器。

不允许监控"/etc/safedog/monitor"这个目录及目录下的文件，否则可能导致异常。

5.3.2. 进程监控

设置完进程名（必须包括运行参数）列表后，再开启监视器开关，报告文件为

/etc/safedog/monitor/processmonit.txt

使用命令

top 或 ps aux

能够看到进程是否正在运行，一旦进程结束或被 kill，监视器会马上重启进程。

比如设置进程名列表为

/bin/sleep 5

/bin/sleep 15

可以看到，进程中将一直有这两个进程在运行，只要一结束，马上就会被重启。

注意当进程名列表为空时，无法启动监视器。

[注意]

本功能只适用于监控可以通过一条命令启动的守护进程，本功能正确的使用方法是，初始时不要启动要监控的服务，通过添加要监控的进程启动命令，让安全狗自动启动被监控的进程，否则可能因为启动过程不同导致安全狗无法匹配出进程列表中的进程名。(比如要监控 vsftpd 进程，如果用户添加的监控内容为"vsftpd &"，但是用户在此之前通过命令 service vsftpd start 启动了 vsftpd 的命令就会出错。)

请对所设置的规则进行测试之后再启用，某些命令不适合该功能，比如 apachectl 脚本命令，实际启动的进程名字为 apache，这种情况下不适用本功能。

5.3.3. CPU 监控

设置完监视范围后，再开启监视器开关，报告文件为

/etc/safedog/monitor/cpumonit.txt

计算 CPU 使用率的时长般设置为 2~5 秒，太短则可能经常告警，太长则可能会告警不明显。

5.3.4. 内存监控

设置完监视范围后，再开启监视器开关，报告文件为

/etc/safedog/monitor/memorymonit.txt

5.3.5. 磁盘容量监控

设置完监视范围后，再开启监视器开关，报告文件为

/etc/safedog/monitor/ diskvolumemonit.txt

5.3.6. 文件备份

本功能适用于监控日志类的文件，该类文件会随着时间不停地增大。使用本功能可以在指定文件在增加多少体积时进行压缩备份，可以在备份的同时清空原文件，以避免原文件体积过大影响性能。

报告文件为

/etc/safedog/monitor/bakforsizemonit.txt

5.3.7. TCP 连接状态

显示当前系统中 TCP 连接的状态及相应的地址、进程 ID 和进程名字。

[注意]

在受到攻击时尽量不要进入该菜单，因为被攻击时，系统中的连接数非常多，进入该菜单查看连接状态可能导致系统负载过高或响应时间很长。

5.3.8. TCP 监听端口

显示当前系统中正在监听的 tcp 端口及相应的地址、进程 ID 和进程名字。

5.4. 应用程序设置

5.4.1. iptables

可以对 iptables 的 filter 表添加一些简单的规则，包括协议类型（TCP/UDP），源地址，源端口，目的地址，目的端口，行为等。

iptables 在系统重启后需要重新配置，除非启用了自动载入功能，并且手动保存过 iptables 表。

5.4.2. vsftpd

对系统中已安装未配置过的 vsftpd 进行一些简单的配置。

配置完成后启动 vsftpd，然后通过网络访问本机的 ftpd 服务器测试配置项是否生效。

在浏览器上输入

ftp://服务器 ip/

访问 ftp 服务器

[注意]

本软件只能对 vsftpd 进行简单的配置，如果需要更加复杂的设置，请直接参考 vsftpd 手册编辑配置文件。使用本功能时，必须先对配置进行初始化，初始化以后，vsftpd 之前的配置信息会丢失，同时，匿名用户的根目录设置到了/srv/ftp，同时/srv/ftp/upload 目录是匿名用户的上传目录。通过软件也可以重新修改相关设置。通过软件配置完毕后，要使用配置生效，需要重启 ftp 服务。

5.4.3. samba

对系统中已安装未配置过的 samba 进行一些简单的配置。

配置完成后启动 samba，然后通过网络访问本机的 samba 共享文件夹测试配置项是否生效。

在浏览器上输入

\\服务器 ip\

访问 samba 共享服务器

[注意]

参考 vsftpd 的注意事项。

6. 软件卸载

在由安装包解压出来的目录下执行命令：

```
chmod +x uninstall.sh
./uninstall.sh
```

即可。

7. FAQ

7.1. 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。

7.2. 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。

7.3. 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进入 sdui 打开相关监控和功能。

7.4. Q:执行 sdui 时一直卡住，无法弹出界面，只能 ctrl+c 结束掉。

A：请等待一段时间，可能在执行任务过程中。如果几分钟后仍然没反应，执行 sdstart 重启安全狗服务，同时向我们报告 bug 现象。

7.5. 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。下个版本可能会增加允许匿名用户删除和修改的配置项。

7.6. Q: ftp 或者 samba 连接不上。

A：首先检查服务是否开启，可以在 sdui 的系统实时监控->TCP 监听端口菜单下查看，然后检查防火墙端口是否开放，可以在 sdui 的应用程序配置->iptables 子菜单下查看。

7.7. Q: service safedog start 出现提示 unrecognized service

A：请使用命令 sdstart 重启 safedog 服务。

7.8. 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！

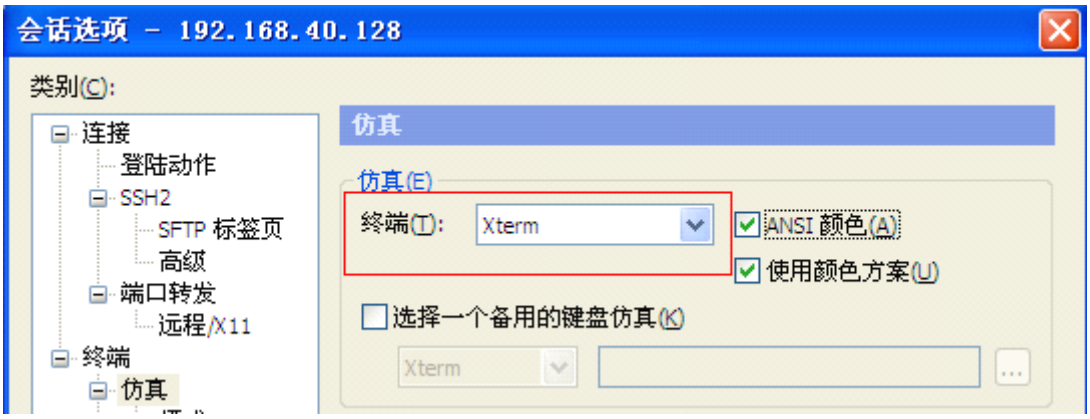
7.9. Q: 软件安装过程中在打印出" start initializing configuration, please wait seconds ..."之后或卸载过程中卡住。

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。

7.10. Q: 使用 SecureCRT 运行 sdui 时报错：Error! Ncurses's initializition was failed!Please replace the ssh terminal with xshell,putty or SecureCRT.

A：这个是由于终端类型不匹配引起的，请按照以下步骤操作：

Step 1：依次选择“选项”->“会话选项”->“终端”->“仿真”：



将终端类型修改为 Xterm。

Step2：将当前连接断开，再重新连接。

7.11. Q: 运行 sdui 时，画面没有颜色，首页如下图：

A：Step 1：依次选择“选项”->“会话选项”->“终端”->“仿真”：

把“ANSI 颜色”和“使用颜色方案”两 个打勾

Step2：重启 SecureCRT。

7.12. **Q: 如何联系开发者。**

A： website: http://www.safedog.cn

bbs: http://bbs.safedog.cn

mail: web@safedog.cn

欢迎参与安全狗软件的讨论