

服务器安全狗Linux版 V1.0.0

使用手册



安全狗工作室

www.safedog.cn

版权所有 侵权必究

2011年10月

目录

1. 软件说明	3
2. 软件运行环境	3
3. 软件安装	3
4. 软件运行	3
5. 软件功能说明	3
5.1. 系统快速配置	4
5.1.1. 网络接口配置	4
5.1.2. 系统状态配置	4
5.2. 系统快速优化	4
5.2.1. 网络优化	4
5.2.2. 进程资源优化	4
5.3. 系统实时监控	5
5.3.1. 文件监控	5
5.3.2. 进程监控	6
5.3.3. CPU 监控	6
5.3.4. 内存监控	6
5.3.5. 磁盘容量监控	7
5.3.6. 文件备份	7
5.3.7. TCP 监听端口	7
5.4. 应用程序设置	7
5.4.1. iptables	7
5.4.2. vsftpd	7
5.4.3. samba	8
6. 软件卸载	8
7. FAQ	9

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、设备或软件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。本软件还提供了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 11.04、Centos 6 、Fedora 15 和 RHEL 6, 对于 Ubuntu 、Centos、Fedora 和 RHEL 的其它版本号的支持, 未经过完整测试。当前发布包仅支持 32 位的操作系统。
- 确保 linux 服务器能够连接互联网。
- 系统中按默认选项安装有 vsftpd 2.3.2 或更新版本的 vsftpd, 否则软件中的 vsftpd 配置功能无效。
- 系统中按默认选项安装有 samba3.5 或更新版本的 samba, 否则软件中的 samba 配置功能无效。
- 使用 vsftpd 和 samba 之前请确保 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。

3. 软件安装

下载软件的安装包, safedog_1.0.0.tar.gz 到 linux 服务器上, 以 root 身份进入安装包所在的目录, 运行如下命令进行安装:

```
tar xzvf safedog_1.0.0.tar.gz
cd safedog_1.0.0
chmod +x install.sh
./install.sh
```

根据提示输入相应的发行版序号, 完成安装。

4. 软件运行

直接运行命令:

```
sdui
```

即可进入软件界面。具体每一步的操作方法在软件界面中有提示。

使用:

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

查看、启动或停止服务。

使用以下命令

```
sdcmd lang en
sdcmd lang chutf8
sdcmd lang chgb2312
```

改变 sdui 的显示界面语言, 支持英文, 中文 utf8 编码, 中文 gb2312 编码。

运行 sdui -h 或 sdui -help 打印部分提示信息。

5. 软件功能说明

5.1. 系统快速配置

5.1.1. 网络接口配置

界面显示系统各个网卡的 IP，子网掩码，MAC 地址，IP 设置方式，网卡激活状态等信息，还显示系统的 DNS 服务器 (nameserver) 设置。

快捷键支持修改网卡的 IP 获取方式，如果设置手动需要填写 IP 和掩码信息，网关和 DNS 信息可选填写，同时提供停用网卡，启动网卡等功能。

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，仅仅作作为参考，可能并不一定是正确的。

5.1.2. 系统状态配置

界面显示系统的机器名，系统日期和时间，快捷键支持修改系统的机器名，系统中的账号和密码，系统日期和时间。本菜单下每隔二到三秒会自动刷新状态。

5.2. 系统快速优化

5.2.1. 网络优化

Icmp Echo Ignore All 开启或关闭“禁止响应 ping 包策略”

[验证生效方法]

```
cat /proc/sys/net/ipv4/icmp_echo_ignore_all
```

结果为 1 表示生效，为 0 表示不生效

[测试方法]

可通过在本机执行命令

```
ping 127.0.0.1
```

查看配置前后效果

Tcp SynCookies 开启或关闭“防范 syn flood 攻击策略”

[验证生效方法]

执行命令

```
cat /proc/sys/net/ipv4/tcp_syncookies
```

结果为 1 表示生效，为 0 表示不生效

[测试方法]

暂无

TcpTimeWaitReuse 开启或关闭“TIME-WAIT 状态的端口重用”

[验证生效方法]

执行命令

```
cat /proc/sys/net/ipv4/tcp_tw_reuse
```

结果为 1 表示生效，为 0 表示不生效

[测试方法]

暂无

5.2.2. 进程资源优化

shmmax 设置单个共享内存段的最大值，单位为 Byte

[验证生效方法]

执行命令

```
cat /proc/sys/kernel/shmmax
```

[测试方法]

使用以下命令

```
ipcmk
```

shmall 全部允许使用的共享内存大小，单位为页面

[验证生效方法]

执行命令

```
cat /proc/sys/kernel/shmall
```

[测试方法]

使用以下命令

```
ipcmk
```

shmmni 系统范围内共享内存段的最大数量

[验证生效方法]

执行命令

```
cat /proc/sys/kernel/shmmni
```

[测试方法]

使用以下命令

```
ipcmk
```

threadsmx 系统最大线程数

[验证生效方法]

执行命令

```
cat /proc/sys/kernel/threads-max
```

[测试方法]

暂无

filemax 分配给进程的最大文件描述符数目

[验证生效方法]

执行命令

```
cat /proc/sys/kernel/file-max
```

[测试方法]

暂无

5.3. 系统实时监控

5.3.1. 文件监控

Monit Toggle 文件监视器开关

File List 监视的文件列表

[测试方法]

设置完文件列表后，再开启监视器开关，可以使用如下命令查看报告文件

```
tail -f /etc/safedog/monitor/filemonit.txt
```

对文件列表中的文件或文件夹进行的生成、修改、删除会马上反应到报告文件中，
对文件列表中的文件夹内的文件或一级文件夹进行的生成、修改、删除也会马上反应到报告文件中。

[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。

5.3.2. 进程监控

Monit Toggle

进程监视器开关

Process List

监视的进程名（必须包括运行参数）列表

[测试方法]

设置完进程名列表后，再开启监视器开关，可以使用如下命令查看报告文件

```
tail -f /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。）

5.3.3. CPU 监控

Monit Toggle

CPU 使用率监视器开关

CPU Ceil

CPU 使用率监视上限（高于该值写入报告）

CPU Floor

CPU 使用率监视下限（低于该值写入报告）

[测试方法]

设置完监视范围后，再开启监视器开关，可以使用如下命令查看报告文件

```
tail -f /etc/safedog/monitor/cpumonit.txt
```

5.3.4. 内存监控

Monit Toggle

内存使用率监视器开关

Memory Use Ceil

内存使用率监视上限（高于该值写入报告）

同时显示系统当前内存使用量和空闲量

[测试方法]

设置完监视范围后，再开启监视器开关，可以使用如下命令查看报告文件

```
tail -f /etc/safedog/monitor/memorymonit.txt
```

5.3.5. 磁盘容量监控

Partition	监视的磁盘分区，比如/dev/sda1
Ceil	监视的磁盘容量的上限（高于该值写入报告）
Floor	监视的磁盘容量的下限（低于该值写入报告）
Interval	监视的磁盘容量的报告间隔值（增减量大于该值时写入报告）

[测试方法]

设置完监视范围后，再开启监视器开关，可以使用如下命令查看报告文件

```
tail -f /etc/safedog/monitor/diskvolumemonit.txt
```

5.3.6. 文件备份

File	需要备份的文件绝对路径
Backup Directory	存方向备份文件的目标目录
Backup Size	监视的文件大小超过此值时，文件将被压缩备份到备份目录，同时清空原文件

[测试方法]

设置完监视路径和备份后，再开启监视器开关，当文件大小超过设定值时，可以检查备份的目标目录和所监视的文件内容。

5.3.7. 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

显示 iptables 的当前规则集列表以及规则链的默认策略(policy)。

可以对 iptables 中的 input 链或 output 链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。

[测试方法]

通过软件添加相应规则后测试通过网络测试相应规则是否生效。

[注意]

通过本软件对 iptables 的设置重启后丢失。

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。

Anonym Enable	是否允许匿名用户登录
Anonym Upload	是否允许匿名用户上传权限
Anonym Make Directory	是否允许匿名用户建立文件夹权限
Anonym Root Path	匿名用户的根目录路径
Local User Enable	是否允许本地用户登录
Write Enable	是否允许写权限，些开关影响所有需要用到写权限的操作
Ftp Start	启动停止 ftp 服务
Ftp Restore Default	初化或恢复用的默认配置，第一次进入时必须先进行初始化

[测试方法]

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，必须先启动一次“`Ftp Restore Default`”功能，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，需要在软件界面上的“`Ftp Start`”中先关闭服务再重新打开服务（即重启服务）。

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。

Share Directory Path 共享文件夹的路径

Share Write Enable 共享文件夹的匿名写权限

Samba Start 启动停止共享

Samba Restore Default 初始化配置文件，第一次进入时必须先进行初始化

[测试方法]

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

在之前的解压出来的 `safedog_1.0.0` 目录下执行命令：

`./uninstall.sh`

即可。

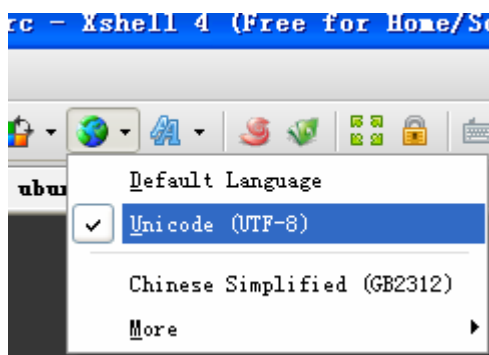
7. FAQ

7.1. Q:中文界面显示为乱码怎么办？

A:首先，linux 纯字符界面下无法直接显示中文，如果要显示中文，可以通过安装 zhcon 等软件支持。如果在远程终端或图形桌面上的终端运行软件的中文界面显示为乱码，首先在当前终端工具的菜单栏查看当前终端的字符编码，一般可以设置为 utf-8 或 gb，然后执行相应的命令，`export LANG=zh_CN.UTF-8` 或 `export LANG=zh_CN.gb2312`，再设置软件的显示编码 `sdcmd lang chutf8` 或 `sdcmd lang chgb2312`，即可。注意只有当环境变量值，终端编码和软件显示编码三者都一致时才能够正常显示中文。

示例 1，xshell 环境下设置显示 UTF-8 编码的中文过程：

首先，设置 xshell 的编码为 utf8



然后，设置环境变量值，先查看一下当前值，执行命令 `locale` 看到当前值为

```
LANG=en_US.UTF-8
```

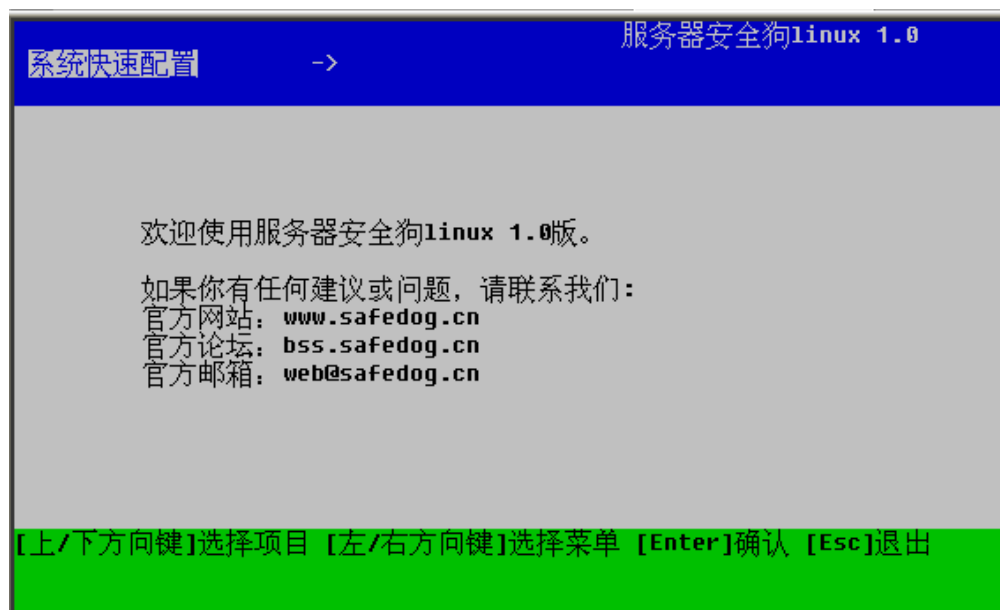
执行命令

```
LANG=zh_CN.UTF-8
```

最后，设置软件的显示语言为 utf8 编码，执行命令

```
sdcmd lang chutf8
```

再执行 `sdui` 即可正常显示中文界面如下：

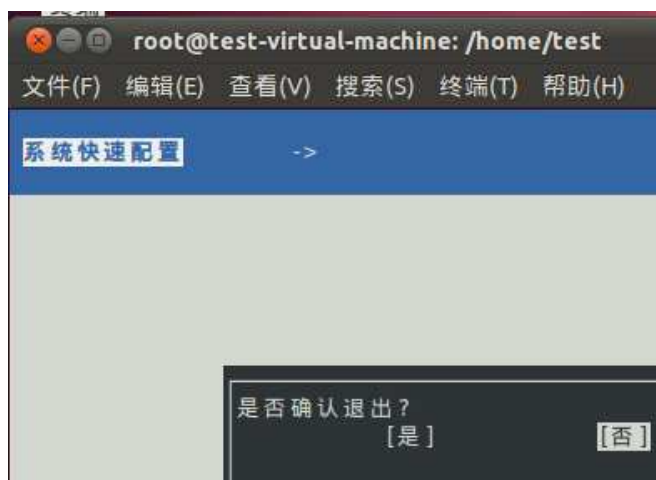


示例 2，在图形桌面终端下显示 gb2312 编码的软件界面



```
root@test-virtual-machine: /home/test
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@test-virtual-machine:/home/test# locale
LANG=en_US.UTF-8
LANGUAGE=en_US:en
LC_CTYPE="en_US.UTF-8"
LC_NUMERIC="en_US.UTF-8"
LC_TIME="en_US.UTF-8"
LC_COLLATE="en_US.UTF-8"
LC_MONETARY="en_US.UTF-8"
LC_MESSAGES=zh_CN.UTF-8
LC_PAPER="en_US.UTF-8"
LC_NAME="en_US.UTF-8"
LC_ADDRESS="en_US.UTF-8"
LC_TELEPHONE="en_US.UTF-8"
LC_MEASUREMENT="en_US.UTF-8"
LC_IDENTIFICATION="en_US.UTF-8"
LC_ALL=
root@test-virtual-machine:/home/test# export LANG=zh_CN.gb2312
root@test-virtual-machine:/home/test#
```

```
root@test-virtual-machine: /home/test
文件(F) 编辑(E) 查看(V) 搜索(S) 终端(T) 帮助(H)
root@test-virtual-machine:/home/test# locale
LANG=en_US.UTF-8
LANGUAGE=en_US:en
LC_CTYPE="en_US.UTF-8"
LC_NUMERIC="en_US.UTF-8"
LC_TIME="en_US.UTF-8"
LC_COLLATE="en_US.UTF-8"
LC_MONETARY="en_US.UTF-8"
LC_MESSAGES=zh_CN.UTF-8
LC_PAPER="en_US.UTF-8"
LC_NAME="en_US.UTF-8"
LC_ADDRESS="en_US.UTF-8"
LC_TELEPHONE="en_US.UTF-8"
LC_MEASUREMENT="en_US.UTF-8"
LC_IDENTIFICATION="en_US.UTF-8"
LC_ALL=
root@test-virtual-machine:/home/test# export LANG=zh_CN.gb2312
root@test-virtual-machine:/home/test# sdcmd lang chgb2312
set up ok!
changed language of sdui to chinese(GB2312).
root@test-virtual-machine:/home/test#
```



7.2. **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。

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

A:执行 sdstart 重启安全狗服务，同时向我们报告 bug 现象或提交日志(/var/log/sd*.log)

7.4. **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。下个版本可能会增加允许匿名用户删除和修改的配置项。

7.5. **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。

7.6. **Q: service safedog start 出现提示 unrecognized service**

A:可能是系统的服务管理器出现异常，可以使用命令 sdstart 重启 safedog 服务。

7.7. **Q: 软件功能大部分失效。**

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！

7.8. **Q: 软件安装过程中在打印出”step 003 done.”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 1~2 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。

7.9. **Q: 如何联系开发者。**

A: website: <http://www.safedog.cn>
bbs: <http://bbs.safedog.cn>
mail: web@safedog.cn