safe_cp 用户手册

Product Name : safe_cp

Product Version : V1.0

Release Date : 2025.11.07

Contact : liyanqing1987@163.com

目录

一、简介

safe_cp 是一个安全的拷贝命令，用于取代 linux 系统上的 cp 命令，和 cp 命令相比，它主要增加了如下功能：

- **数据保护功能**

  保护指定数据不被拷贝。

- **日志功能**

  为所有的 cp 操作保留日志记录，可追溯。

- **报警功能**

  试图拷贝保护数据的行为，会直接触发安全报警。

safe_cp 底层默认仍然使用系统 cp 命令来完成拷贝操作，但是其数据保护功能可以防止重要数据被拷贝，并且日志和报警功能可以帮助 IT 管理员的事后追溯和安全管理，具有很高的安全价值。

二、环境依赖

safe_cp 基于 python3 开发，需要调用系统的“env”、“python3”和“cp”等命令，理论上 linux 发行版均可满足要求。

safe_cp 的开发和测试操作系统为 centos 和 rocky。

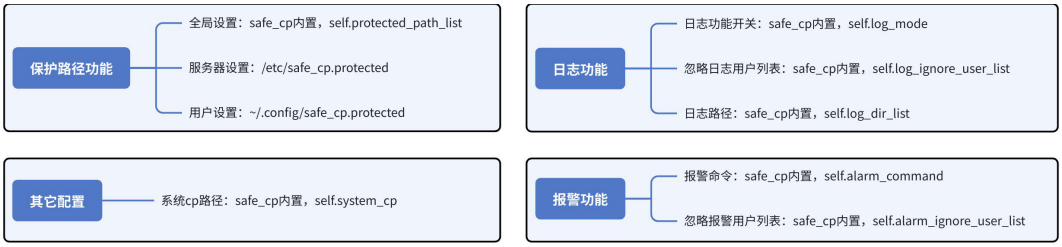
三、工具配置和引用

3.1 工具配置

safe_cp 是开箱即用型工具，**免安装，无需任何配置即可直接使用**。

如果想更好地使用路径保护功能/日志功能/报警功能，根据业务需求增加一些个性化的设置，则需要修改 safe_cp 的一些内置配置，或者增加一些配置文件。

下面用一张图来说明一下可配置项有哪些。



大多数配置项都在 safe_cp 脚本的 SafeCp 类的“__init__()”函数中配置，也有部分保护路径和回收站功能配置是在系统/用户下的配置文件中实现的。

3.1.1 保护路径配置

保护路径的配置分为 3 部分。

- **全局设置**：safe_cp 内置，self.protected_path_list，默认设置如下。

```
        # [Editable] self.protected_path_list : specify protected
paths (absolute path), globally effective.
        self.protected_path_list = []
```

- **共享设置**：通过 extend_list_with_config 添加，一般为<共享目录>/safe_cp.protected

依赖共享目录生效，效果同“全局设置”，但具备更高的可配置性，下面是一个例子。

```
/ic/tech/lib
```

- **服务器设置**：通过 extend_list_with_config 添加，一般为/etc/safe_cp.protected

建议指定服务器相关的受保护路径，下面是一个例子。（支持“*”符号，会做路径展开）

```
/etc/passwd
/etc/ssh/*
```

- **用户设置**：extend_list_with_config，一般为~/.config/safe_cp.protected

建议指定用户用户相关的受保护路径，下面是一个例子。

```
~/.config
```

请务必注意，被保护路径、其上层路径和下层路径均无法被拷贝！

3.1.2 日志功能配置

safe_cp 中的日志功能用于记录所有的数据 cp 信息，其相关的设置如下。

```
        # [Editable] self.log_mode : enable the behavior of saving
logs.
        # [Editable] self.log_ignore_user_list : specify a user
list, will not save logs fro copy operations of users in the list.
        # [Editable] self.log_dir_list : Specify log dir(s) to
save log file, make sure permission is "1777".
        self.log_mode = True
        self.log_ignore_user_list = []
        self.log_dir_list = ['/tmp/safe_cp/log']
```

self.log_mode：指定是否打开日志功能，默认打开，可以通过置为“False”关闭。

self.log_ignore_user_list：指定忽略日志功能的用户，只有在 self.log_mode 为“True”的情况下生效。特殊系统用户可能有非常频繁的拷贝操作，记录日志的行为是没有意义的。

self.log_dir_list：指定日志保存路径（可以配置多个），只有在 self.log_mode 为“True”的情况下生效。如未指定则默认为“/tmp/safe_cp/log”。**log_dir 最好设置为 1777 权限，否则会出现用户执行 safe_cp 无法保存日志的问题。**

下面是一个实例配置。(浅蓝色背景为修改部分)

```
        self.log_mode = True
        self.log_ignore_user_list = []
        self.log_dir_list = ['/tmp/safe_cp/log',
'/ic/data/CAD/it/safe_cp/log']
```

3.1.5 报警功能配置

safe_cp 中的报警功能用于为拷贝保护文件的行为发送报警，是一个安全功能（防止攻击行为），不配置则报警功能不生效。其相关的设置如下。

```
        # [Editable] self.alarm_command : specify alarm command.
("<TITAL>", "<MESSAGE>" and "<USER>" are replaceable string.")
        # [Editable] self.alarm_ignore_user_list : specify a user
list, no alarms will be sent fro copy operations of users in the
list.
        self.alarm_command = ''
        self.alarm_ignore_user_list = []
```

self.alarm_command：指定报警命令，如未指定，或者指定命令无法执行，则报警功能自动失效。self.alarm_command 中支持变量字符串“<MESSAGE>”，它会在执行报警命令时自动替换为对应的报警信息。

self.alarm_ignore_user_list：指定忽略报警功能的用户，只有在 self.alarm_mode 为“True”的情况下生效。特殊系统用户可能有拷贝保护路径（包含系统和用户保护路径）的操作，这种行为有可能在特殊情况下是允许的。

下面是一个实例配置。(浅蓝色背景为修改部分)

```
        self.alarm_command =
'/ic/software/cad_tools/bin/send_lark2 -T "Security Alarm: high
risk copy" -c "<MESSAGE>" -r liyanqing.1987'
        self.alarm_ignore_user_list = []
```

说明：示例中的 send_lark2 是内部工具，用于在研发环境中向指定用户的飞书发送消息。

3.1.6 其它配置

还可以通过如下命令配置系统“rm”命令的路径，也可以不配置，不配置的情况下，safe_cp 会默认从'/usr/bin/system_cp'、'/usr/bin/cp'、'/bin/system_cp'、'/bin/cp'中选择一个二进制文件来当做系统“cp”命令。

```
        # [Editable] self.system_cp : specify system cp.
        self.system_cp = ''
```

3.2 工具引用

为了使 safe_cp 对当前服务器上的全体用户生效，需要用 safe_cp 取代系统默认的“cp”命令，同时确保它保持 755 的权限。

注意，这个操作只有通过 root 账号来执行。

```
[root@ic-monitor01 ~]# which cp
/usr/bin/cp
[root@ic-monitor01 ~]# mv /usr/bin/cp /usr/bin/system_cp
[root@ic-monitor01 ~]# cp -f
/ic/software/cad_tools/it/tools/safe_cp /usr/bin/cp
[root@ic-monitor01 ~]# chmod 755 /usr/bin/cp
```

同时将 safe_cp 中的 self.system_cp 指向真正的系统“cp”。

```
        self.system_cp = '/usr/bin/system_cp'
```

当然，如果真正的 cp 命令“/usr/bin/cp”被迁移到“/usr/bin/**sytem_cp**”，那么此处无需指定它也可以自己找到的。

3.3 工具打包

safe_cp 本身是一个 python 脚本，明文存放，配置可读可篡改，在安全场景下使用存在一定的安全漏洞，因此建议在实际使用的时候，将 safe_cp 使用 pyinstaller 打包为不可读的独立可执行文件使用。

```
[root@ic-monitor01 install]# pyinstaller --onefile safe_cp
5 DEPRECATION: Running PyInstaller as root is not necessary nor
sensible. Do not use PyInstaller with sudo. PyInstaller 7.0 will
block this.
871 INFO: PyInstaller: 6.11.1, contrib hooks: 2025.1
...
11708 INFO: Copying bootloader EXE to /root/install/dist/safe_cp
11710 INFO: Appending PKG archive to custom ELF section in EXE
11752 INFO: Building EXE from EXE-00.toc completed successfully.
```

生成的目录结构如下。

```
[root@ic-monitor01 install]# ls
build  dist  safe_cp  safe_cp.spec
```

其中关键打包文件位于 dist 目录下，尺寸约为 17M，使用此文件更安全。

```
[root@ic-monitor01 install]# du -hs dist/safe_cp
17M     dist/safe_cp
```

四、工具使用示例

用户 cp 确认：

实际使用的确实是/usr/bin/cp，也就是 safe_cp。

```
[liyanqing.1987@ic-monitor01 ~]$ which cp
/usr/bin/cp
```

操作:

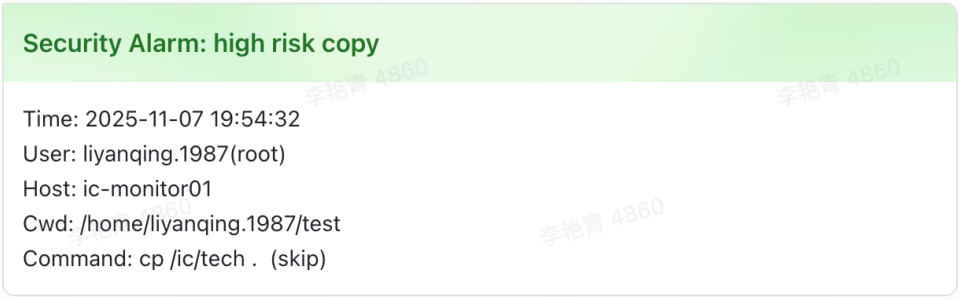
- 拷贝普通数据（行为如常）

```
[liyanqing.1987@ic-monitor01 test]$ touch a_file
[liyanqing.1987@ic-monitor01 test]$ cp a_file b_file
[liyanqing.1987@ic-monitor01 test]$ ls
a_file  b_file
```

- 拷贝保护数据

```
[liyanqing.1987@ic-monitor01 test]$ cp /ic/tech .
*Warning*: Cannot copy protected path "/ic/tech", skip!
```

我们看到拷贝保护路径“project_data”的行为则被直接拒绝，同时由于设置了报警功能，还会收到如下飞书报警信息。



五、高级功能

5.1 日志检索

比如执行如下 cp 操作，有正常拷贝，也有保护数据的违规拷贝。

```
[liyanqing.1987@ic-monitor01 test]$ cp /ic/tech .
*Warning*: Cannot copy protected path "/ic/tech", skip!
```

那么在 safe_cp 的用户日志中，关键词“*Warning*”和“skip”是需要特殊关注的。

```
{"time": "2025-11-07 19:54:32", "message_level": "Warning",
"user": "liyanqing.1987", "login_user": "root", "host": "ic-
monitor01", "cwd": "/home/liyanqing.1987/test", "message":
"*Warning*: Cannot copy protected path \"/ic/tech\", skip!"}
```

5.2 debug 功能

设置环境变量“**SAFE_CP_DEBUG**”可以开启 safe_cp 的 debug 模式，主要是打印更多的信息。

值	行为
1	打印 safe_cp 本身的 warning，主要是一些行为故障，比如无法保存 log 等。
2	输出内部执行的实际命令。
3	打印出各种配置信息。

示例，SAFE_CP_DEBUG=1

```
[liyanqing.1987@ic-monitor01 ~]$ export SAFE_CP_DEBUG=1
[liyanqing.1987@ic-monitor01 ~]$ cp a b
[WARNING] Specified system cp "/usr/bin/system_cp" is missing.
```

示例，SAFE_CP_DEBUG=2

```
[liyanqing.1987@ic-monitor01 ~]$ export SAFE_CP_DEBUG=2
[liyanqing.1987@ic-monitor01 ~]$ cp a b
[COMMAND] cp -rf a b
```

示例，SAFE_CP_DEBUG=3

```
[liyanqing.1987@ic-monitor01 test]$ cp a b
[CONFIG] protected_path_list : ['/ic/tech']
[CONFIG] log_dir(s) : ['/tmp/safe_cp/log']
[CONFIG] alarm_command : /ic/software/cad_tools/bin/send_lark2 -T
"Security Alarm: high risk copy" -c "<MESSAGE>" -r
liyanqing.1987 >& /dev/null
[CONFIG] system_cp : /usr/bin/system_cp
[COMMAND] /usr/bin/system_cp a b
```

5.3 登陆用户识别

如果 root 用户切换为其它用户，并尝试危险拷贝动作，这个时候可以识别出 login user 和 current user，并加以标注。

下面的实例中，root 用户切换成 liyanqing.1987，并尝试拷贝受保护数据。

```
[root@ic-monitor01 ~]# su - liyanqing.1987
Last login: Fri Nov  7 17:45:31 CST 2025 on pts/1
Welcome root ~
[liyanqing.1987@ic-monitor01 ~]$ cp /ic/tech .
*Warning*: Cannot copy protected path "/ic/tech", skip!
```

收到的报警信息如下，User 为“liyanqing.1987(root)”，即 liyanqing.1987 是由 root 用户切换而来。

同时在 log 中也会明确标识出 user 和 login_user。


```
{"time": "2025-11-07 20:20:51", "message_level": "Warning",
"user": "liyanqing.1987", "login_user": "root", "host": "ic-
monitor01", "cwd": "/home/liyanqing.1987", "message": "*Warning*:
Cannot copy protected path \"/ic/tech\", skip!"}
```

六、行为测试

safe_cp 在 Linux 系统中正式部署前，需要测试如下设置是否符合预期。

测试项	设置	期望结果
debug 设置 SAFE_CP_DEBUG	export SAFE_CP_DEBUG=1	输出如下**[WARNING]**信息： [WARNING] Specified system cp "xxx" is missing.
	export SAFE_CP_DEBUG=2	输出**[WARNING]**和**[COMMAND]**信息，**[COMMAND]**信息如下： [COMMAND] /usr/bin/system_cp a b
	export SAFE_CP_DEBUG=3	输出**[WARNING]**、**[COMMAND]**和**[CONFIG]**信息，**[CONFIG]**信息如下： [CONFIG] protected_path_list : []
参数测试	执行 cp	输出如下信息： cp: missing file operand Try 'cp --help' for more information.
	执行 cp --version	输出为空如下信息： cp (GNU coreutils) xxx Copyright (C) 2018 Free Software Foundation, Inc. ...
参数测试 (系统 cp 丢失)	执行 cp	输出如下信息： cp: missing file operand Try 'cp --help' for more information.
	执行 cp --version	无任何信息输出
拷贝测试	cp file_a file_b 拷贝单文件到文件	文件被拷贝

	cp file_a file_b dir_c 拷贝多文件到目录（目录存在）	文件被拷贝
	cp -r dir_a dir_b 拷贝目录到目录（目录存在）	目录被拷贝到目录内
	cp -r dir_a dir_b 拷贝目录到目录（目录不存在）	目录被拷贝成新目录
	cp "a b" ab 拷贝带空格的文件	文件被拷贝
	cp 'a"c' ac 拷贝带引号的文件	文件被拷贝
	cp file_a file_b 拷贝不存在的文件或目录	输出如下信息： cp: cannot stat ‘xxx’: No such file or directory
	拷贝保护数据	数据未被拷贝，输出如下信息： *Warning*: Cannot copy protected path "xxx", skip! 同时会收到报警（如配置）
	拷贝保护数据的上层路径	数据未被拷贝，输出如下信息： *Warning*: Cannot copy path "xxx", there is protected date under it, skip! 同时会收到报警（如配置）
	拷贝保护数据的下层路径	数据未被拷贝，输出如下信息： *Warning*: Cannot copy path "xxx", it is located under a protected path, skip! 同时会收到报警（如配置）

拷贝测试 (系统 cp 丢失)	cp file_a file_b 拷贝单文件到文件	文件被拷贝
	cp file_a file_b dir_c 拷贝多文件到目录（目录存在）	文件被拷贝
	cp -r dir_a dir_b 拷贝目录到目录（目录存在）	目录被拷贝到目录内
	cp -r dir_a dir_b 拷贝目录到目录（目录不存在）	目录被拷贝成新目录
	cp "a b" ab 拷贝带空格的文件	文件被拷贝
	cp 'a"c' ac 拷贝带引号的文件	文件被拷贝
	cp file_a file_b 拷贝不存在的文件或目录	输出如下信息： cp: cannot stat ‘xxx’: No such file or directory
	拷贝保护数据	数据未被拷贝，输出如下信息： *Warning*: Cannot copy protected path "xxx", skip! 同时会收到报警（如配置）
	拷贝保护数据的上层路径	数据未被拷贝，输出如下信息： *Warning*: Cannot copy path "xxx", there is protected date under it, skip! 同时会收到报警（如配置）
	拷贝保护数据的下层路径	数据未被拷贝，输出如下信息： *Warning*: Cannot copy path "xxx", it is located under a protected path, skip!

		同时会收到报警（如配置）

七、技术支持

本工具为开源工具，由开源社区维护，可以提供如下类型的技术支持:

- 部署和使用技术指导。
- 接收 bug 反馈并修复。
- 接收功能修改建议。(需审核和排期)

获取技术支持的方式包括:

- 通过 Contact 邮箱联系开发者。
- 添加作者微信 “liyanqing_1987”，注明“真实姓名/公司/safe_cp”，由作者拉入技术支持群。

附录

附 1. 变更历史

日期	版本	变更描述	备注
2025.11	1.0	发布第一个版本 safe_cp。	