sudo 限制参考：http://blog.51cto.com/zxf261/748756

chattr（禁止删除文件） 限制参考：https://linux.cn/article-5590-1.html

```
#visudo Cmnd_Alias的设置

#设置 /bin/* 相应的
/bin/arch,/bin/dbus-
monitor,/bin/findmnt,/bin/ls,/bin/raw,/bin/touch,/bin/awk,/bin/db
us-run-
session,/bin/gawk,/bin/lsblk,/bin/readlink,/bin/tracepath,/bin/ba
sename,/bin/dbus-
send,/bin/grep,/bin/mkdir,/bin/rm,/bin/tracepath6,/bin/bash,/bin/
dbus-
uuidgen,/bin/gtar,/bin/mknod,/bin/rmdir,/bin/true,/bin/cat,/bin/d
d,/bin/gunzip,/bin/mktemp,/bin/rpm,/bin/umount,/bin/chgrp,/bin/df
,/bin/gzip,/bin/more,/bin/rvi,/bin/uname,/bin/chmod,/bin/dmesg,/b
in/hostname,/bin/mount,/bin/rview,/bin/unicode_start,/bin/chown,/
bin/dnsdomainname,/bin/ipcalc,/bin/mountpoint,/bin/sed,/bin/unico
de_stop,/bin/domainname,/bin/iptables-
xml,/bin/mv,/bin/setfont,/bin/unlink,/bin/vi,/bin/dumpkeys,/bin/i
ptables-xml-
1.4.7,/bin/netstat,/bin/sh,/bin/usleep,/bin/cp,/bin/echo,/bin/kbd
_mode,/bin/nice,/bin/sleep,/bin/cpio,/bin/egrep,/bin/kill,/bin/ni
sdomainname,/bin/sort,/bin/view,/bin/cut,/bin/env,/bin/link,/bin/
ping,/bin/stty,/bin/ypdomainname,/bin/dash,/bin/ex,/bin/ln,/bin/p
ing6,/bin/su,/bin/zcat,/bin/date,/bin/false,/bin/loadkeys,/bin/pl
ymouth,/bin/sync,/bin/dbus-cleanup-
sockets,/bin/fgrep,/bin/logger,/bin/ps,/bin/tar,/bin/dbus-
daemon,/bin/find,/bin/login,/bin/pwd,/bin/taskset

#设置user bin
/usr/bin/*

#设置sbin
/sbin/service

#设置过滤
!/usr/bin/chattr

```

```
15
16 #完整Cmnd_Alias
17 Cmnd_Alias OTHERUSER = /bin/arch,/bin/dbus-
   monitor,/bin/findmnt,/bin/ls,/bin/raw,/bin/touch,/bin/awk,/bin/db
   us-run-
   session,/bin/gawk,/bin/lsblk,/bin/readlink,/bin/tracepath,/bin/ba
   sename,/bin/dbus-
   send,/bin/grep,/bin/mkdir,/bin/rm,/bin/tracepath6,/bin/bash,/bin/
   dbus-
   uuidgen,/bin/gtar,/bin/mknod,/bin/rmdir,/bin/true,/bin/cat,/bin/d
   d,/bin/gunzip,/bin/mktemp,/bin/rpm,/bin/umount,/bin/chgrp,/bin/df
   ,/bin/gzip,/bin/more,/bin/rvi,/bin/uname,/bin/chmod,/bin/dmesg,/b
   in/hostname,/bin/mount,/bin/rview,/bin/unicode_start,/bin/chown,/
   bin/dnsdomainname,/bin/ipcalc,/bin/mountpoint,/bin/sed,/bin/unico
   de_stop,/bin/domainname,/bin/iptables-
   xml,/bin/mv,/bin/setfont,/bin/unlink,/bin/vi,/bin/dumpkeys,/bin/i
   ptables-xml-
   1.4.7,/bin/netstat,/bin/sh,/bin/usleep,/bin/cp,/bin/echo,/bin/kbd
   _mode,/bin/nice,/bin/sleep,/bin/cpio,/bin/egrep,/bin/kill,/bin/ni
   sdomainname,/bin/sort,/bin/view,/bin/cut,/bin/env,/bin/link,/bin/
   ping,/bin/stty,/bin/ypdomainname,/bin/dash,/bin/ex,/bin/ln,/bin/p
   ing6,/bin/su,/bin/zcat,/bin/date,/bin/false,/bin/loadkeys,/bin/pl
   ymouth,/bin/sync,/bin/dbus-cleanup-
   sockets,/bin/fgrep,/bin/logger,/bin/ps,/bin/tar,/bin/dbus-
   daemon,/bin/find,/bin/login,/bin/pwd,/bin/taskset,/usr/bin/*,/sbi
   n/service,!/usr/bin/chattr
18
19 #用户权限设置
20 zero    ALL=(ALL)    NOPASSWD:OTHERUSER
```

用chattr 限制文件修改

```
1 #a：让文件或目录仅供附加用途；
2 #b：不更新文件或目录的最后存取时间；
3 #c：将文件或目录压缩后存放；
4 #d：将文件或目录排除在倾倒操作之外；
5 #i：不得任意更动文件或目录；
6 #s：保密性删除文件或目录；
7 #S：即时更新文件或目录；
```

```
#u：预防意外删除。
#-R：递归处理，将指令目录下的所有文件及子目录一并处理；
#-v<版本编号>：设置文件或目录版本；
#-V：显示指令执行过程；
#+<属性>：开启文件或目录的该项属性；
#-<属性>：关闭文件或目录的该项属性；
#=<属性>：指定文件或目录的该项属性。
sudo chattr -R +i XXX
sudo chattr -R -i XXX
```

chown 修改禁止

参考safe-rm的方式改写

```
#!/usr/bin/perl -t
use warnings;
use strict;
use Cwd 'realpath';
our $VERSION = '0.12';
my $homedir = $ENV{HOME} || q{};
my $LEGACY_CONFIG_FILE = "$homedir/.safe-rm";
my $USER_CONFIG_FILE = ($ENV{XDG_CONFIG_HOME} ||
"$homedir/.config") . "/safe-rm";
my $GLOBAL_CONFIG_FILE = '/etc/safe-chown.conf';
my %default_protected_dirs = (
    '/bin' => 1,
    '/boot' => 1,
    '/dev' => 1,
    '/etc' => 1,
    '/home' => 1,
    '/initrd' => 1,
    '/lib' => 1,
    '/lib32' => 1,
    '/lib64' => 1,
    '/proc' => 1,
    '/root' => 1,
    '/sbin' => 1,
    '/sys' => 1,
    '/usr' => 1,
```

```
    '/usr/bin' => 1,
    '/usr/include' => 1,
    '/usr/lib' => 1,
    '/usr/local' => 1,
    '/usr/local/bin' => 1,
    '/usr/local/include' => 1,
    '/usr/local/sbin' => 1,
    '/usr/local/share' => 1,
    '/usr/sbin' => 1,
    '/usr/share' => 1,
    '/usr/src' => 1,
    '/var' => 1,
);
my %protected_dirs = ();
sub read_config_file {
    my $filename = shift;
    if ( -e $filename ) {
        if ( open my $fh, '<', $filename ) {
            while (<$fh>) {
                chomp;
                foreach my $file (glob) {
                    $protected_dirs{$file} = 1;
                }
            }
            close $fh; # deliberatly ignore errors
        }
        else {
            print {*STDERR} "Could not open configuration file:
$filename\n";
        }
    }
    return;
}
read_config_file($GLOBAL_CONFIG_FILE);
read_config_file($LEGACY_CONFIG_FILE);
read_config_file($USER_CONFIG_FILE);
if ( 0 == scalar keys %protected_dirs ) {
    %protected_dirs = %default_protected_dirs;
}
my @allowed_args = ();
foreach (@ARGV) {
    my $pathname = $_;
```

```
    # Normalize the pathname
    my $normalized_pathname = $pathname;
    if ( $normalized_pathname =~ m{/}xms or -e
"$normalized_pathname" ) {
        # Convert to an absolute path (e.g. remove "..")
        $normalized_pathname = realpath($normalized_pathname);
        if ( !$normalized_pathname ) {
            $normalized_pathname = $pathname;
        }
    }
    if ( $normalized_pathname =~ m{^(.+?)/+$}xms ) {
        # Trim trailing slashes
        $normalized_pathname = $1;
    }
    # Check against the blacklist
    if ( exists $protected_dirs{$normalized_pathname} and not -l
$pathname ) {
        print {*STDERR} "safe-chown: skipping $pathname\n" || 0;
    }
    elsif ( $pathname =~ /(.*)/xms ) { # pointless untainting
        push @allowed_args, $1;
    }
}
# Prepare for actually deleting the file
local $ENV{PATH} = q{}; # pointless untainting
local $ENV{CDPATH} = q{}; # pointless untainting
local $ENV{IFS} = " \t\n"; # pointless untainting
my $real_chown = '/bin/chownreal';
# Make sure we're not calling ourselves recursively
if ( realpath($real_chown) eq realpath($0) ) {
    die 'safe-chown cannot find the real "chown" binary' . "\n";
}
# Run the real rm command, returning with the same error code
my $status = system $real_chown, @allowed_args;
my $errcode = $status >> 8;
exit $errcode;
```