Run all commands as root (#)

Install `fapolicyd`

Debian based distributions:

```
# apt install fapolicyd
```

RHEL based distributions:

```
# yum install fapolicyd
```

Create rules directory:

```
# mkdir -p /etc/fapolicyd/rules.d
```

Create this rule in `/etc/fapolicyd/rules.d/50-custom.rules`

```
## Custom fapolicyd rules for Ubuntu
%languages=application/x-bytecode.ocaml,application/x-
bytecode.python,application/java-archive,text/x-
java,application/x-java-
applet,application/javascript,text/javascript,text/x-awk,text/x-
gawk,text/x-lisp,application/x-elc,text/x-lua,text/x-m4,text/x-
nftables,text/x-perl,text/x-php,text/x-python,text/x-R,text/x-
ruby,text/x-script.guile,text/x-tcl,text/x-luatex,text/x-
systemtap
allow perm=any uid=0 : dir=/var/tmp/
allow perm=any uid=0 trust=1 : all
deny_audit perm=any pattern=ld_so : all
deny_audit perm=any all : ftype=application/x-bad-elf
allow perm=open all : ftype=application/x-sharedlib trust=1
deny_audit perm=open all : ftype=application/x-sharedlib
allow perm=execute all : trust=1
allow perm=execute all : ftype=application/x-executable trust=1
deny_audit perm=execute all : ftype=application/x-executable
allow perm=execute all : path=%ld_so_path% trust=1
allow perm=open all : ftype=%languages trust=1
deny_audit perm=any all : ftype=%languages
allow perm=any all : ftype=text/x-python trust=1
allow perm=open all : ftype=application/x-bytecode.python
trust=1
deny_audit perm=any all : ftype=text/x-python
deny_audit perm=any all : ftype=application/x-bytecode.python
allow perm=any all : ftype=text/x-shellscript
```

```
allow perm=any all : ftype=text/x-perl trust=1
deny_audit perm=any all : ftype=text/x-perl
allow perm=any all : ftype=application/x-bytecode.ocaml trust=1
deny_audit perm=any all : ftype=application/x-bytecode.ocaml
allow perm=any all : ftype=text/x-php trust=1
deny_audit perm=any all : ftype=text/x-php
allow perm=any all : ftype=text/x-ruby trust=1
deny_audit perm=any all : ftype=text/x-ruby
allow perm=any all : ftype=text/x-lua trust=1
deny_audit perm=any all : ftype=text/x-lua
allow perm=any all : ftype=application/vnd.microsoft.portable-
executable trust=1
deny_audit perm=any all :
ftype=application/vnd.microsoft.portable-executable
deny_audit perm=execute all : all
deny_audit perm=execute all : all
deny_audit perm=open all : ftype=%languages
allow perm=open all : all
```

Run these commands to reload `fapolicyd` rules and restart the `fapolicyd` daemon:

```
# fagenrules --load
# systemctl enable fapolicyd
# systemctl restart fapolicyd
```