**文件权限修改观测功能实现**

# 目录

目录

[目录 1](#_Toc73101894)

[需求任务 1](#_Toc73101895)

[整体需求 1](#_Toc73101896)

[整体设计 1](#_Toc73101897)

[详细设计 1](#_Toc73101898)

[后续优化 1](#_Toc73101899)

# 1.需求任务

## 整体需求

1. 基于ebpf系统实现chmod系统调用的的观测，具体的，至少包括以下指标：namespace、pid、comm(进程名) 、文件名、mode(权限值)；
2. 程序具备CO-RE特性，在linux kernel > 5.4系统上可以移植，被执行节点不需要安装内核头文件；
3. 实现语言不限。

## 需求分解

1. 关于需求点2，考虑到需要支持CO-RE特性，不能使用bcc等ebpf前端开发，选择c语言开发编译为二进制可执行程序。选择ebpf CO-RE的方式：

BTF + libbpf +clang +kernel CONFIG\_DEBUG\_INFO\_BTF特性，具体可以参考<https://github.com/torvalds/linux/tree/master/tools/bpf/runqslower>

# 整体设计

略

# 详细设计

略

# 后续优化

优化点主要集中在以下两个方面：

1. 考虑实现文件名的路径补全，即当用户空间执行chmod 777 filename(相对路径) 时，ebpf程序输出结果为文件的绝对路径；
2. 如果后续有大量数据监控需求时，可以考虑通过ebpf exporter接prometheus以及grafana做可视化监控。