ebpf学习资料总结

Repo：

GitHub - libbpf/libbpf-bootstrap: Scaffolding for BPF application development with libbpf and BPF CO-RE

> 基于C和libbpf的稍微高层次抽象的ebpf repo

> **Note**
>
> 这个repo的example/c下面有众多简单ebpf程序示例，可以多去看看怎么写的，熟悉流程

GitHub - iovisor/bcc: BCC - Tools for BPF-based Linux IO analysis, networking, monitoring, and more

> 更高抽象层的一个快速上手repo

GitHub - cilium/cilium: eBPF-based Networking, Security, and Observability

> 基于Go生态和云原生的ebpfrepo

书籍/原理

- 《Linux Observability with BPF》，作者David Calavera和Lorenzo Fontana, 这本书篇幅不长，是来自sysdig的两位大佬写的BPF手册书，推荐入门阅读
- 《Linux内核观测技术BPF》，是最近刚出版的第一本BPF中文书籍，为上面英文书的翻译版本，由范彬和狄卫华两位翻译

> **Note**
>
> 这本比较薄，可以先看这个

- 《BPF Performance Tools》，这是Brendan Gregg大神对于BPF技术如何做系统性能优化的一本集大成者的秘籍，BPF学习者必备。
- 《Systems Performance: Enterprise and the Cloud, 2nd Edition》，这是Brendan Gregg大神系统优化书籍的第二版，篇幅较长，但是值得一啃。

Blog

Building BPF applications with libbpf-bootstrap

> **Hint**
>
> nakryiko是libbpf-bootstrap的核心贡献者，我们基于这个框架去写ebpf程序可以多看他的博客

[译]用libbpf-bootstrap 构建 BPF 应用程序 - 知乎

【BPF入门系列-2】BPF 学习路径总结 | 深入浅出 eBPF

ebpf - 搜索结果 - 知乎

Linux 内核学习笔记

颠覆传统、应用大爆发，eBPF何以改变Linux?

eBPF 入门开发实践教程：使用 libbpf 开发程序—bootstrap

深入浅出运维可观测工具（一）：聊聊eBPF的前世今生

高效入门eBPF

> **Important**
>
> 这篇文章特别特别特别好！！值得反复去看去实践的在源码中进行跟踪理解。下面那个我的博客的文章也是对这个的理解和总结。

BPF(ebpf)核心原理(Part.1) - JiaHuann's Blog.

公众号/社区

- 我们学校陈老师的ebpf社区：Linux内核之旅 影响力很大，文章很多。
- 【BPF入门系列-2】BPF 学习路径总结 | 深入浅出 eBPF（www.bpf.top）
- eBPF - Introduction, Tutorials & Community Resources ebpf.io

会议录制的视频

- libbpf-bootstrap for android流程详解
- 还有kprobe编写的视频 具体可以问梁老师要
  可以去网上搜索编写kprobe程序/uprobe程序等视频

总结

需要学的核心几大件：

- 理解观测点类型：tracepoint，kprobe，uprobe...etc
- 内核态ebpf程序
- 用户态ebpf程序
- ebpf-Map内核态用户态的沟通机制
- ebpf程序加载器（libbpf-bootstrap框架下编译出来的程序本身集成了内核态程序，用户态程序，以及加载器）
- kernel给内核态程序提供的helper函数

> **Success**
>
> 祝你快速进入内核和ebpf观测运维可编程内核的海洋~