**题目：使用eBPF捕获容器系统调用情况**

为了充分理解容器虚拟化技术和eBPF技术对于可观测领域的优越性，编写一个简易的eBPF程序，要求能够捕获x86\_64架构下的容器虚拟化环境中进程的系统调用事件。具体来说，使用libbpf、cilium/eBPF、BCC等开源eBPF编程框架实现在宿主机操作系统中采集容器内进程的系统调用情况并关联其所在容器的container\_id。

**操作：**

* 使用常见的Linux发行版进行实验，Linux内核版本尽可能高。
* 安装Docker、eBPF编程框架（libbpf、cilium/eBPF、BCC等任选）等实验需要的组件。
* 根据示例代码进行编程，运行并获取输出。

**负载测试：**

**使用`** **docker run -it --rm ubuntu `启动一个ubuntu容器，在容器内部尝试触发系统调用并观察eBPF程序是否采集到了正确的事件。**

**示例代码见附件**

**sample\_syscall.c**