基于eBPF的容器异常检测工具Agent进展汇报

队伍：三个臭皮匠

指导老师：任怡 赵欣

LOGO

THE MAIN CONTENTS

第 1 部分

项目进展时间线

02 主要研究内容

赛题理解与技术储备（2周）

eBPF技术学习： 完成《BPF Performance Tools》前3章实操，深入理解eBPF技术原理及应用，掌握CO-RE特性。

容器运行时监控研究： 搭建Kubernetes测试环境，使用docker stats和cadvisor分析容器资源指标，熟悉容器监控核心概念。

异常检测算法对比： 对比孤立森林、LSTM、AutoEncoder等算法，确定项目采用孤立森林算法作为异常检测核心算法。

01

数据采集框架开发（4周）

eBPF探针设计与开发： 使用libbpf开发框架，完成多个核心eBPF探针的编写，捕获系统调用、容器指标等关键数据。

数据管道构建:设计环形缓冲区存储事件数据，实现用户态数据处理程序，构建高效的数据采集管道。

性能优化： 添加过滤机制减少无效事件，测试不同map类型性能，优化数据采集框架性能。

02

异常检测算法开发（4周）

基线算法实现： 实现基于统计的阈值检测算法，开发规则引擎，完成异常进程检测、端口扫描检测等基础功能。

机器学习模块开发： 完成特征工程，从原始事件提取时序特征；使用sklearn实现孤立森林模型训练，初步完成模型部署。

03

可视化系统集成（2周）

Prometheus 监控链路搭建： 配置 Prometheus 定时拉取与存储策略，实现数据抓取的实时监控，并基于阈值规则配置告警

Grafana 多维可视化看板开发： 让集群状态、异常轨迹直观呈现，支撑从全局到细节的分层诊断。

04

容器异常注入（3周）

通过配置化场景在受控容器内产生多类型异常流量，具备强度与时长控制及结构化元数据输出，支撑检测评估与阈值调优；其以配置驱动和线程化并发发起多容器注入，有安全上限与自动清理策略，输出带标签数据便于与 AI 检测结果对齐评估，促进模型优化。

05

文档与交付（2周）

代码规范化： 打包完整环境，确保代码规范性与可移植性。

文档编写： 编写详细的API文档，生成技术白皮书，涵盖系统架构图、核心算法说明及性能对比测试报告等内容。

06

第 2 部分

项目分工

02 项目分工

01

刘周康

负责安全规则设计与实现，构建基于规则的异常检测引擎，协助 AI 检测模块集成与优化。

02

毕喜舒

负责 eBPF 探针开发与优化，包括进程、系统调用、文件、TCP 等探针的编写与调试。

03

马永媛

主导容器元信息管理模块设计与实现，构建容器与进程的映射关系，负责将Prometheus收集到的数据集成到Grafana进行可视化。

第 3 部分

项目完成情况

03 项目完成情况

核心技术框架实现

- eBPF数据采集框架：已完成process、syscall、file、tcp等eBPF 探针开发，通过 tracepoint、kprobe等挂载点，实现对容器行为的内核级实时捕获，数据采集延迟控制在毫秒级，满足动态容器监控需求。
- 容器元信息关联机制：基于 cgroup、namespace 特征与 docker API交互，通过父进程 namespace 继承关系推导新容器进程，映射更新延迟≤10ms，解决短生命周期容器追踪难题。
- 多维度异常检测引擎：已实现容器异常注入和三层检测逻辑：基于规则的安全告警、基于统计的指标异常识别、基于 Isolation Forest 的机器学习模型，告警响应延迟≤1 秒。

功能指标达成

- 安全监控功能：覆盖多种常见容器安全场景，告警记录完整包含进程 PID、容器 ID、操作路径等上下文信息。
- 容器异常注入功能：通过“容器异常注入器”构建验证采集-检测-告警闭环，确保对宿主机影响可控；同时输出标签数据，便于与 AI 检测结果对齐评估，促进模型参数与阈值的持续优化。
- 性能分析功能：通过 Prometheus+Grafana 集成，实现 指标的可视化展示，支持历史数据回溯，辅助定位性能瓶颈。
- 部署与扩展能力：核心 Agent 实现轻量化部署，支持一键启动，可动态加载/卸载eBPF探针，避免持续占用资源。

性能与兼容性验证

- 轻量化指标：核心二进制文件体积 3.8MB（≤4MB 目标），运行时 CPU 占用率稳定在 3%-4%，对容器应用吞吐量影响≤2%，满足高密度容器部署需求。
- 兼容性适配：已在 Linux 内核 5.10、5.15 版本验证通过，支持 Docker（20.10+）、Kubernetes（v1.24+）环境，可正常监控容器集群跨节点实例，实现统一视图管理。

ADD YOUR SUBTITLE HERE

谢谢您的观看

队伍：三个臭皮匠

指导老师：任怡 赵欣

LOGO