openEuler运维变更观测工具Agith

汇报人：上官栋栋 from 华为2012服务实验室

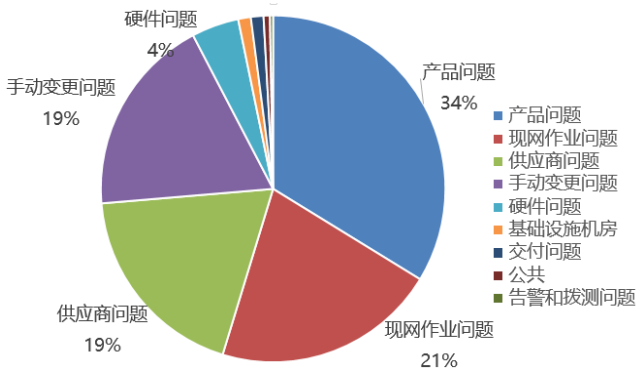
开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

目录

项目背景

变更频繁，变更故障占比大，变更监控数据分析难，风险难判断，故障难定位

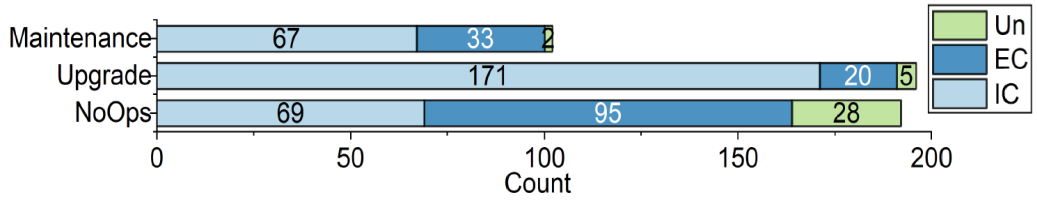
变更频繁且手动比例高:一年100万+次变更，手工变更5000+次/月（平均10.5秒一次，每天变更时间窗6-8小时），变更规模是友商的十分之一，但手工变更密度高。



华为云故障根因分析

现网作业+手动变更占：40%

产品问题+供应商问题：53%



公开云故障数据根因分析【1】

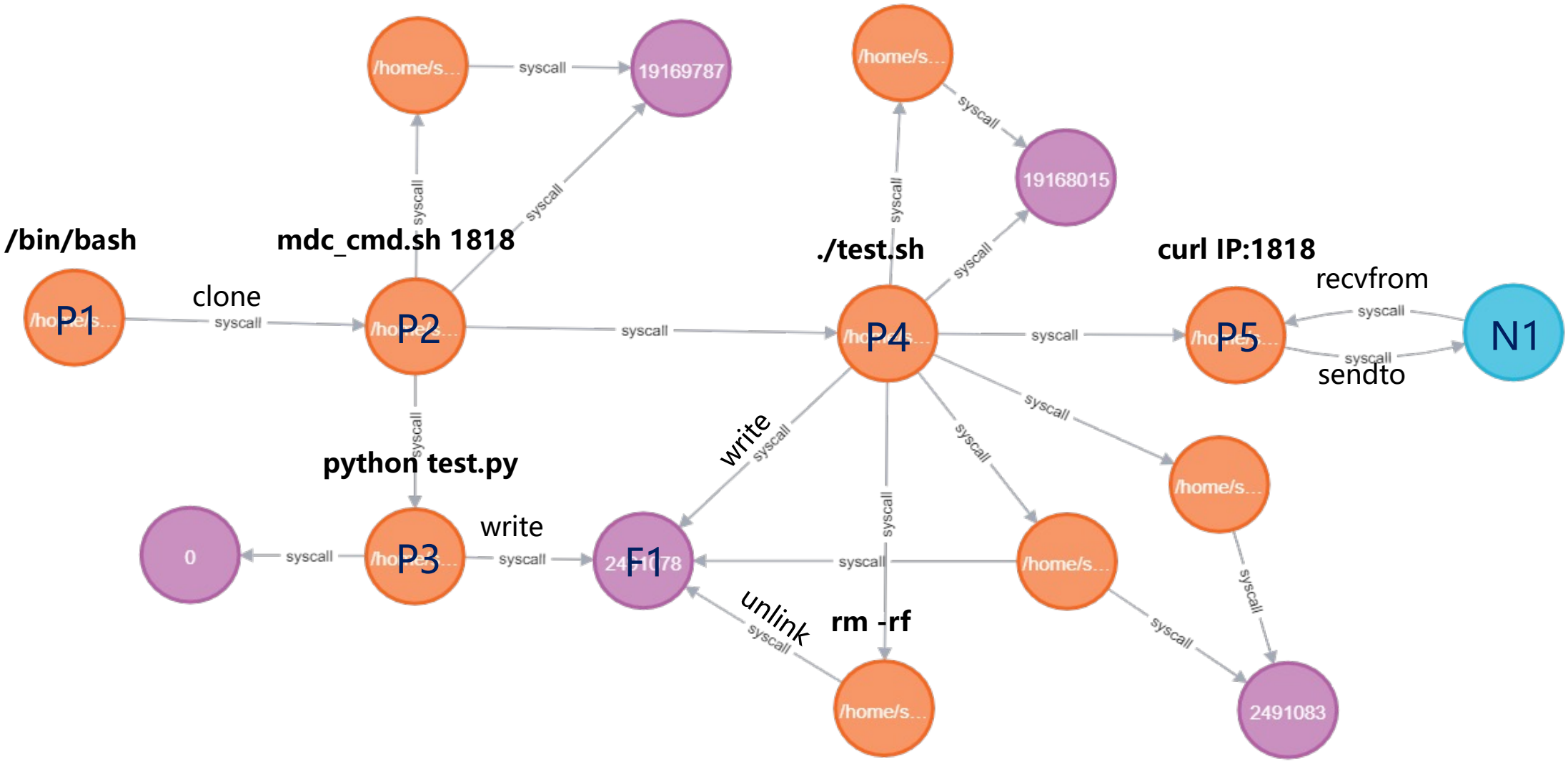
84.7%的故障发生在系统升级与维护过程中

2022-09-12 00:00:00.0 张三(z00123456) mdc_cmd.sh 1818 例行运维 cn-east-201 10.10.0.11 非ip白名单（常规） 存储服务产品部 对象存储服务域项目群 OBS OBS dryrun01,sysconfig,plogserver,plogmanager,fma,oam-ftds-agent,plogagent,dryrun02 OBS-DFV-persistence,OBS-DFV-ftds,OBS-DFV-oam white

- **命令语义模糊**：变更规章制度完善，时间、节点、人员、行为要素齐全。但是变更命令“mdc_cmd.sh 1818”不能表示实际操作。
- **依赖专家经验**：通过NLP方法的准确率与召回率依赖专家经验。例如将“rm”判定为风险。但是部分命令名与操作并不对应。
- **非常规的命令模式处理困难**：
  1. ssh `hostname –i` “kill -9 31881”
  2. ls & mv *
  3. time rm –f a.sh
- **故障定位困难**：缺乏命令含义（执行过程）导致故障与变更命令难匹配

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

变更影响面



“mdc_cmd.sh 1818”变更影响面

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

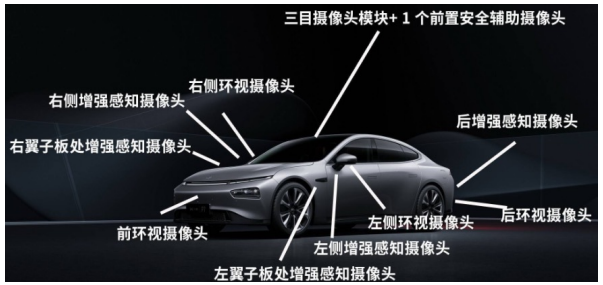
变更数据分析

根据驾驶场景布置摄像头：

前进：激光雷达，三目摄像头

倒车：后侧深度感知摄像头

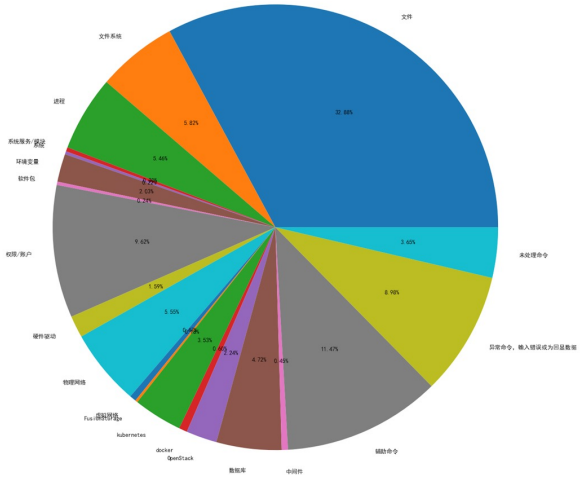
侧方停车：两侧环视摄像头



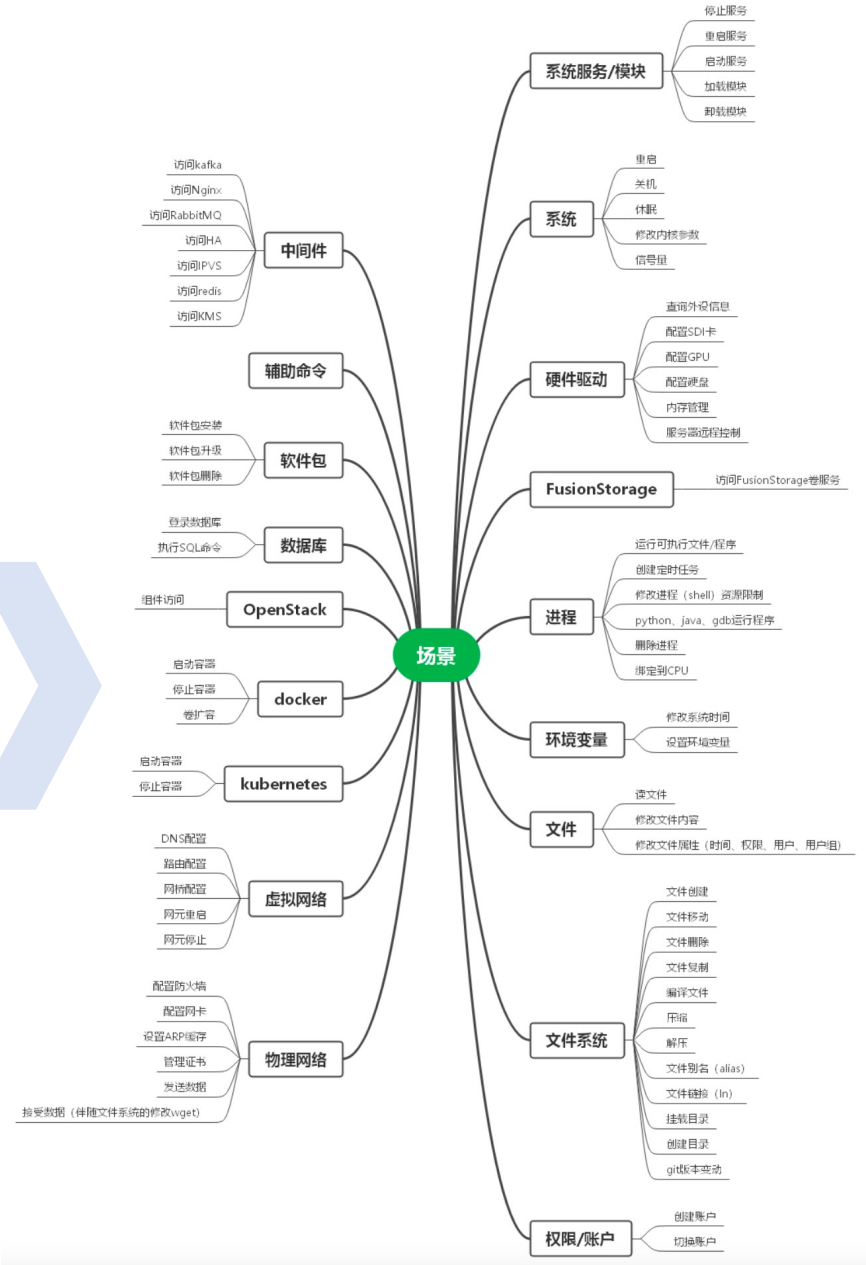
车辆摄像头布置

根据变更场景建立影响面定义方法，构建<object, action>知识库。

1. 从240万条运维命令种梳理出运维操作的对象（object）类型。
2. 针对每种object，继续划分具体的action。
3. 将<object, action>作为一种场景。在每种场景下确定需要监控的具体变量。



运维object占比扇形图



影响面知识库

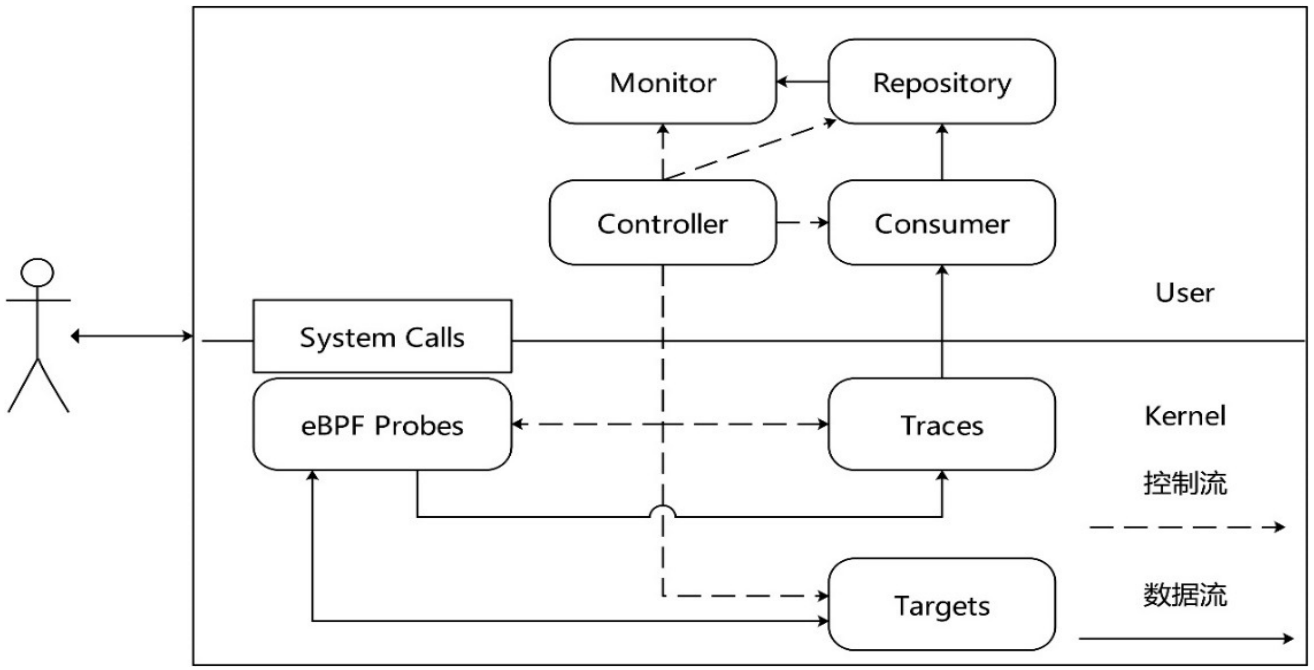
开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

系统架构

Agith 在设计中采用**数据流与控制流分离**的策略。

数据流：由eBPF模块、Consumer、Repository 和 Monitor 组成，分为筛选-采集-整理-输出。

控制流：以 Controller 模块为核心，其他模块受 Controller 模块的统一管理。



eBPF模块：包含eBPF Probes、Traces、Targets，采用基于动态目标的监控技术，采集与变更相关的Trace数据。

Consumer：读取并缓存Trace数据，涉及读写速率控制，数据异常处理，数据融合。

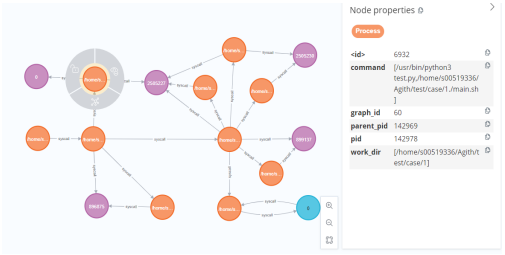
Repository：存储Trace数据，绘制变更影响面拓扑数据。

Monitor：告警模块，根据变更影响面拓扑数据与配置规则，判断是否需要发送告警信息。

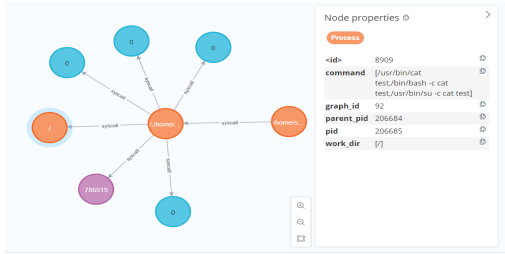
开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

功能示例

Agith目前完成内核探针 27 个，覆盖文件、进程、网络的常规行为，可以监控变更过程中脚本嵌套、匿名命令、python 脚本等监控难点，输出变更影响面拓扑数据。

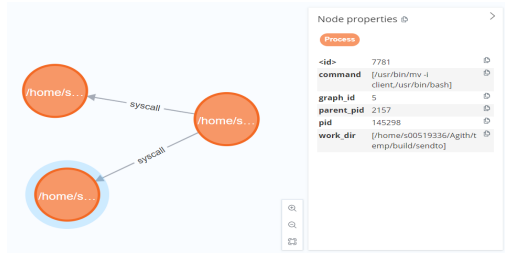


main.sh (含python命令)
可执行文件15例

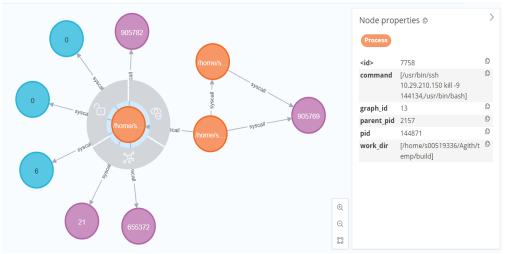


su –c “cat test”
通过su违规执行命令15例

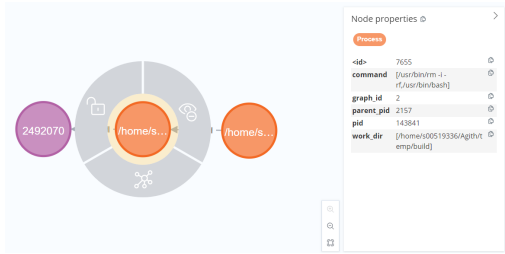
echo “hello” > test.txt
通过重定向符号写入文件35例



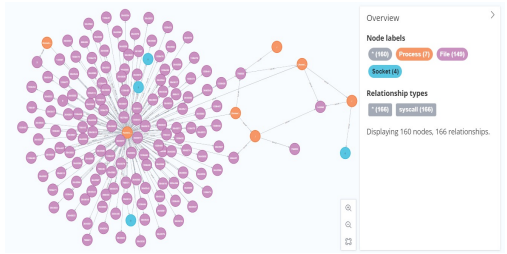
ls & mv * testdir
使用&执行多条命令4例



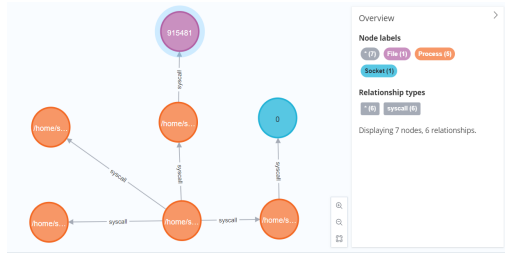
ssh `hostname –i` "kill -9 144134 “
远程执行文本



time rm –rf testfile.txt
命令含有前缀



yum install perf
安装程序

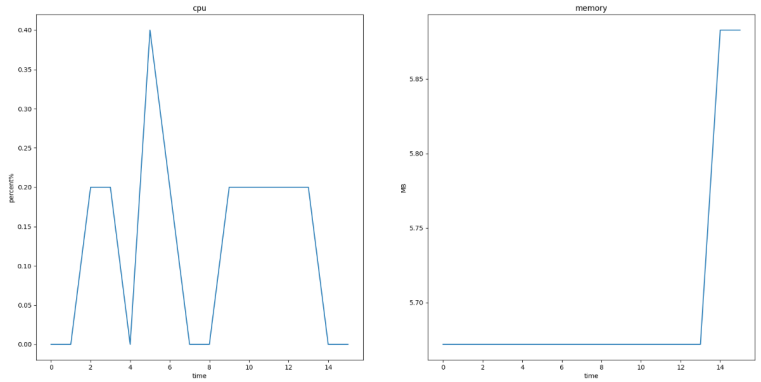


ps -ef | grep sendto/server |
awk '{print 'kill -9 ' $2}' | sh
使用|执行多条命令7例

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

性能分析

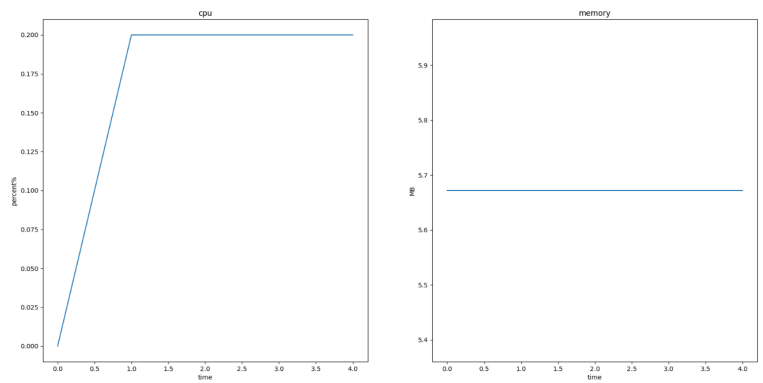
Agith监控工具对于一般的手动或自动变更场景，CPU利用率单核0.4%。极限场景中达到3.8%，内存用量在10M以内。对于一些异常状况，CPU利用率也可以快速降低到标准限制（5%）以下。



手动变更：

执行文件的增删改查以及网络访问等操作。

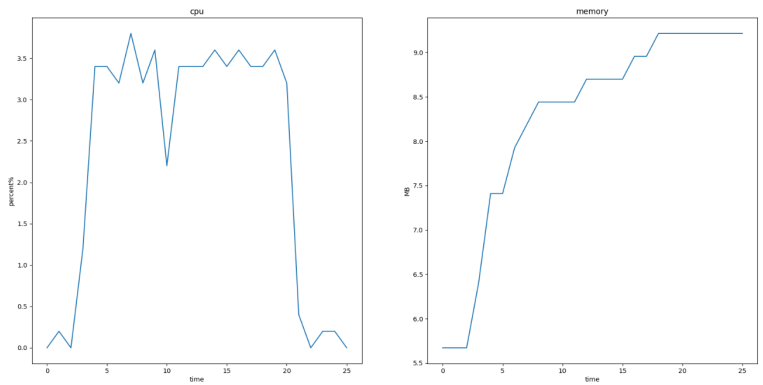
Trace	CPU	MEM	File
747	0.4%	5.8M	95kb



自动变更：

通过shell脚本或python脚本执行手动变更的操作

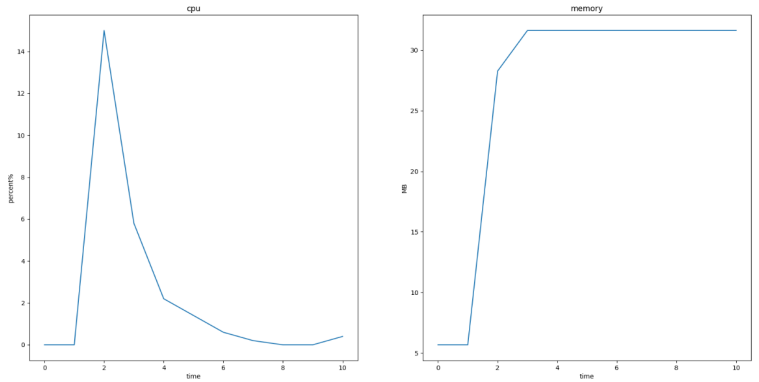
Trace	CPU	MEM	File
306	0.2%	5.6M	50kb



极限场景：

执行命令5000条，执行速率58条/秒

Trace	CPU	MEM	File
126544	3.8%	9.2M	21.2M



异常场景：

剔除网络访问与文件IO，只查询内存。执行速率1667条/秒)

Trace	CPU	MEM	File
46906	15%	31M	7.6M

开放原子开源基金会 OPENATOM FOUNDATION | OpenEuler

开发计划

功能模块		24.03	24.09	已实现	规划中
基础观测	进程 文件 网络链接 辅助命令				
OS系统观测	OS模块管理 服务控制 账户权限 修改网络配置 外设管理 环境变量				
业务观测	kubernetes 容器 OpenStack 数据库 软件包 中间件				
风险告警	自定义告警规则 告警信息发送				
控制模块	观测账户 自定义数据存储				

THANKS

Cooperator：王龙、刘畅、李浩哲、高宇睿

THANKS

Cooperator：王龙、刘畅、李浩哲、高宇睿

THANKS

Cooperator：王龙、刘畅、李浩哲、高宇睿

THANKS

Cooperator：王龙、刘畅、李浩哲、高宇睿