

云原生网络全域监控

概念设计

概要

全域流量监控是在用户无感的情况下监控全域流量，构建更加全面的网络拓扑结构，可以更加全面实时的了解公司内基础架构的网络流量情况。全域监控可以捕获网络拓扑、接口、命名空间属性等。捕获分类 L2-L7 层流量，提供动态预测、报警设置、流事件跟踪。提高系统可靠性、稳定性。对故障定位故障排除更加实时。

系统实现

全域监控，是一款无侵入、实时、超低损耗的流量监控平台并且与平台无关，无侵入针对上层开发用户不需要改动任何代码既可以使用接入全域监控。实时监控：全域监控平台在实时的捕获东西流量，将捕获流量传送至远程流分析平台实时分析、检测和趋势分析。超低损耗：尽管实时捕获流量在任意大量的报文前不会超过单核 CPU 5% 的损耗，在高性能全域流量系统下更是低于 1% 几乎不会对应用和系统产生任何影响。

全域监控分为：mix、sidecar-agent、analysis 三大模块

mix 数据平面

主要负责统一管理命令，并且将全域监控命令下发至 sidecar-agent。并提供动态预测、报警等相关设置。mix 与 sidecar-agent 通信采用 grpc 通信模式，配置更新可以实时的反推至 sidecar-agent。反推订阅协议如下：

```
{
  "NIC": ["ens33", "eth0"],
  "L3": ["172.101.2.33", "19.66.44.8"],
  "L3Match": ["172.10.2.33/24"],
  "L3Miss": ["10.10.0.4"],
  "L3MissRange": ["10.10.2.33/24"],
  "L4CLASS": ["TCP", "UDP"],
  "L4": ["8080", "9090"],
  "L4Range": "5000-6000",
  "L4Miss": ["6666", "7777"],
  "L4MissRange": "6666-7777",
  "L7": ["HTTP", "GET", "POST"],
  "L7Miss": ["PUT", "DELETE"]
}
```

sidecar-agent

全域监控 agent，该模块负责执行 mix 下发命令，按照命令格式执行监控，对报文进行分类。可以作用于裸机、虚拟机、容器。可在裸机 NIC 实现全局流量监控和管控。通过 agent 收集全域流量无需担心性能损耗问题，agent 可以在极低的性能损耗下完成报文的收集任务。

sidecar 存在的必要性：

1. 全域流量监控不全，对于大量分布式流量的无法全面的监控到所有流量。
2. 目前对系统流量的监控多在于日志、L7 记录，对于 L7 和漏加日志的流量无法监控，遇到问题不好复现增加了故障排查的难度。
3. 对应用系统的拓扑结构了解不全，应用的流量来源与依赖的无法通过日志展现，对运维人员不友好，遇到问题无法及时联系上下游链路负责人
4. 系统报警缺失，在部分接口没有加入监控的情况，出现异常流量无法立即发起报警引起应用负责人的关注

sidecar-agent 可以通过全域的流量收集解决上述等问题。

具体实现

sidecar-agent 分为高性能版本与普通版本，区别在与采用的技术栈不通，对系统的影响和损耗不同。

高性能版本

高性能版本在较新 BPF 技术编写实现，可以实时的、透明的、几乎无损耗的情况下进行全域流量监控。BPF 程序运行开发这动态的将编写的代码加载到内核中运行。在强大的加载器面前可以将编写的数据包监控程序加载到内核中，只在内核态运行减少数据报文的拷贝，以极低的代价处理报文的出入口的监控和拦截技术。

普通版本

普通版本采用较为稳定的 libbpf_mmap 技术。可以实时的、透明的、低损耗的情况下进行全域流量监控。Libbpf_mmap 是在稳定版本 libbpf 上的改进，减少了一次从内核空间到用户的

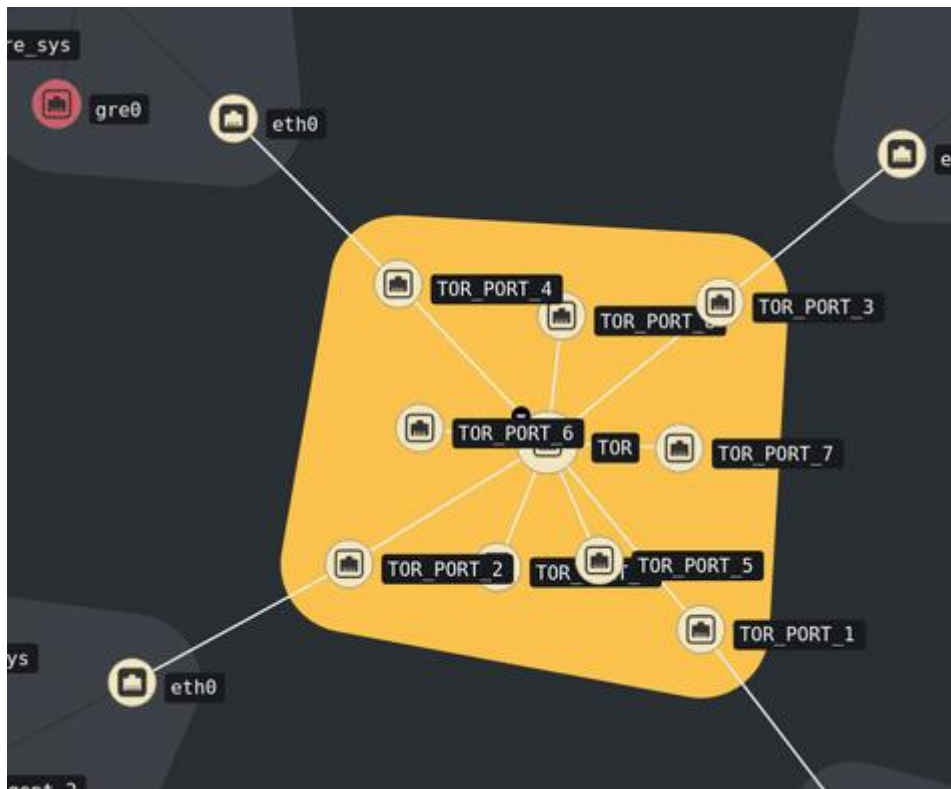
空间的 copy 。减少了多次系统调用提高了 libbpf 的性能，很大程度上的降低了性能损耗

agent 收集到的报文不会在本地磁盘写入任何内容也就是说 agent 如果在宿主机宕机的情况下就会发生数据的丢失。agent 会将数据报文实时的发送 analysis 由 analysis 对实时流具体的分析。发送报文如下：

```
{  
  "NIC": "eth0",  
  "L3": "110.10.2.33",  
  "L3Frame": "....",  
  "L4Class": "TCP",  
  "L4": "5666",  
  "L4Frame": "....",  
  "L7": "GET",  
  "L7Frame": "...."  
}
```

analysis

主要负责将 sidecar-agent 监控到的流量进行实时分析，加入管控和趋势分析和报警流程，并通过图形的形式将实时分析和监控的信息展示出来。展示其上下文拓扑关系、应用及其运维负责人。最终的展示效果如下：



仅供参考

analysis 负责将设备信息与应用信息关联，从多层次分析信息：应用级、L3 级、L4 级、L7 级根据用户设

置的规则进行流量分析和动态预测报警。尽量更大程度的多维度的分析报文信息挖掘更大的价值。