



CLOUD NATIVE + OPEN SOURCE

*Virtual Summit China 2020*

# Kubernetes 异常配置检测框架

顾静, 阿里云  
邓隽, 阿里云



## 我们来自阿里云容器服务

- 顾静，研发工程师
- 邓隽，技术专家

## 我们参与打造

- 容器服务 (ACK/ASK)
- 容器镜像服务 (ACR)
- 服务网格 (ASM)
- ...



- 1 Kubernetes 典型异常
- 2 检测框架演进
- 3 生产实践
- 4 总结



# Kubernetes 使用日常

- 应用部署
- 集群扩容
- 组件升级
- ...
- 找出集群不正常工作的原因 : (



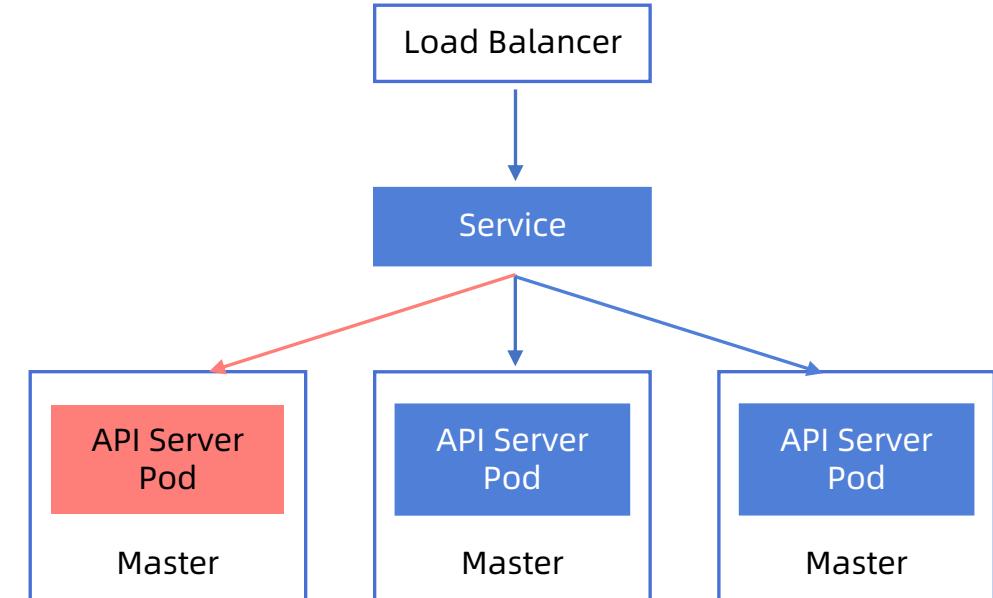
# Kubernetes 典型异常

## 组件异常

- API Server Load Balancer 异常
- API Server Pod 异常

## 影响

- 通过 API Server 访问集群概率失败
- 升级集群失败





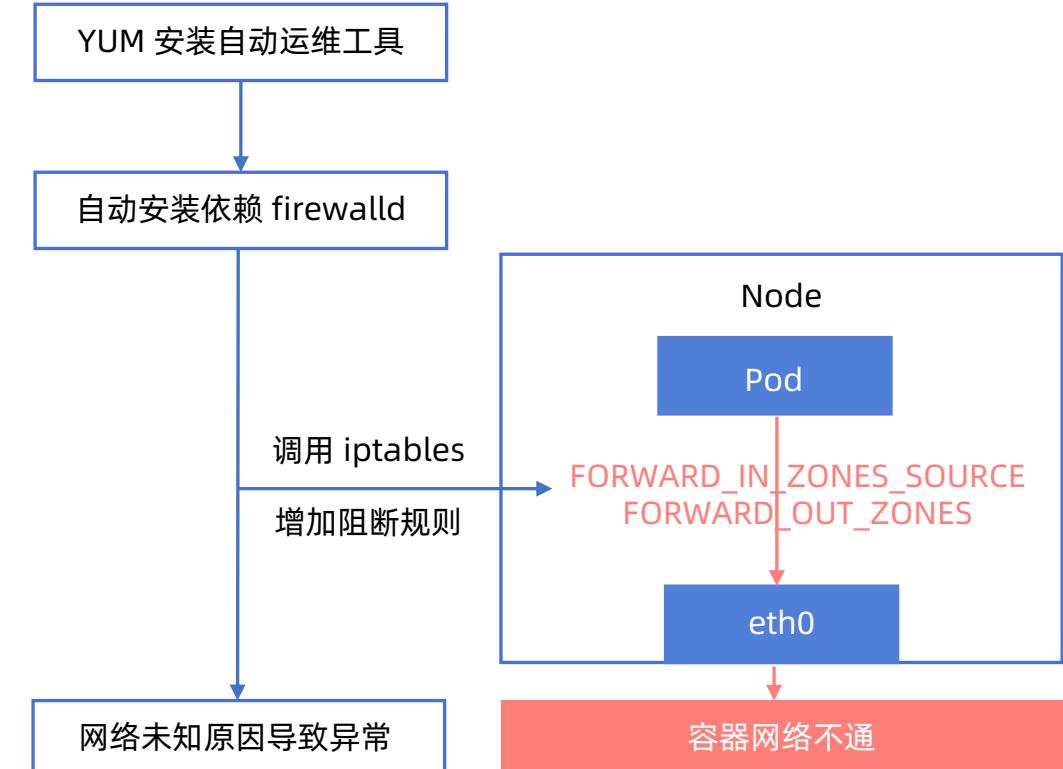
# Kubernetes 典型异常

## 网络异常

- 安全组、路由表配置错误
- 节点防火墙软件等修改 iptables、内核参数
- 网络链路长，手动排查成本高

## 异常影响

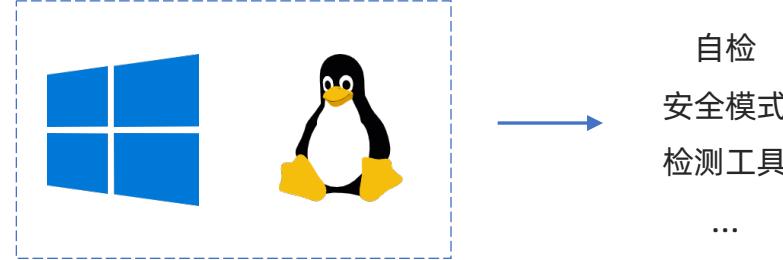
- 应用间无法正常通信
- 集群内 Controller 无法正常工作



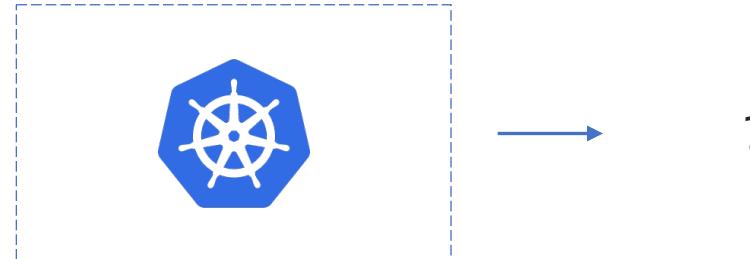


# 异常 VS 异常检测

操作系统



云原生操作系统





## 运行模式

- 集群节点 (DaemonSet /Standalone)

## 问题检测

- 硬件 (CPU、内存、磁盘)
- 操作系统 ( NTP、内核死锁、文件系统异常)
- Container Runtime (无响应)



node-problem-detector

## 问题上报

- API server
- Prometheus



# Sonobuoy

## 运行模式

- 集群节点 (Collector Pod + DaemonSet/One Shot)
- 需要特定版本来对接兼容的 K8s 版本

## 问题检测

- Kubernetes Conformance-testing (K8s 兼容性检查)
- 节点上自定义数据的收集(依赖于自定义插件)

## 问题上报

- 需要采集和分析结果文件





CLOUD NATIVE + OPEN SOURCE  
*Virtual Summit China 2020*

# Kube\*



kube-bench

CIS Kubernetes Benchmark



kuberhealthy

集群综合检查



kube-hunter

集群安全扫描



kubectl trace

执行 bpftrace



# 检测工具小结

工具	适用场景	局限性
kube-bench	在集群中运行 CIS Benchmark 检测项依赖于 CIS Benchmark 内容	能发现集群核心组件配置错误 无法发现如 Flannel 组件异常 增加检查项流程较复杂
kuberhealthy	在集群中运行 CronJob 实现检查 可以自定义检查项	无法检测集群核心组件配置 集群异常时无法进行检测
kube-hunter	适用于集群安全检测	仅能检测集群安全性
kubectl-trace	在集群中运行 bpftrace 检查 Kernel	仅能检测 Kernel 相关问题 要求熟悉 bpftrace 语言



- 1 Kubernetes 典型异常
- 2 检测框架演进
- 3 生产实践
- 4 总结



# 我们的目标

实现 Kubernetes 集群异常检测框架

支持集群多维度异常检测能力

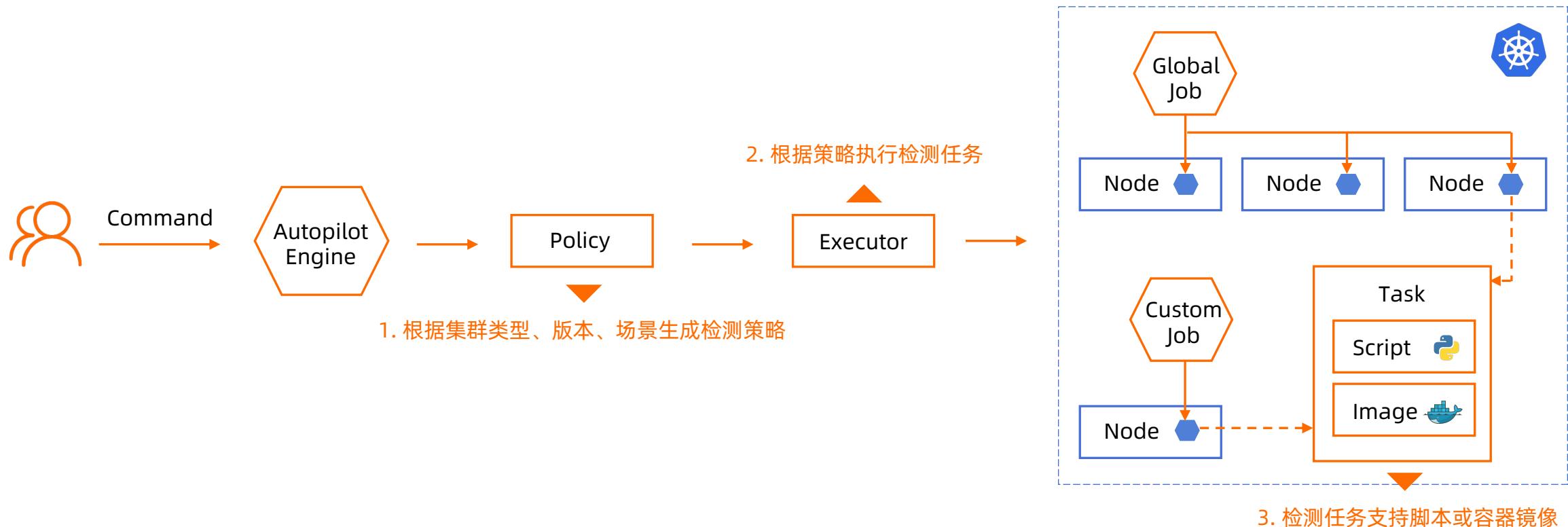
支持集成开源检测组件



# 检测框架 Ver.1 { 自动化



# Ver.1 自动化





# Ver.1 优化点

## 快速迭代的 Kubernetes 版本

- 月度发版
- 版本间的配置、参数、API 差异

## 多样集群类型（阿里云容器服务）

- 托管版集群、Serverless 集群
- 边缘集群、GPU 集群

## 各类检测场景

- 节点、组件、配置等
- 集群升级、集群巡检

版本差异 \* 类型差异 \* 场景差异

检测项



# Ver.1 优化点

检测代码在膨胀

检测能力迭代需要加速



# 检测框架 Ver.2

{  
    动态定制  
    动态扩展



# Ver.2 DSL

## DSL (Domain-Specific Language)

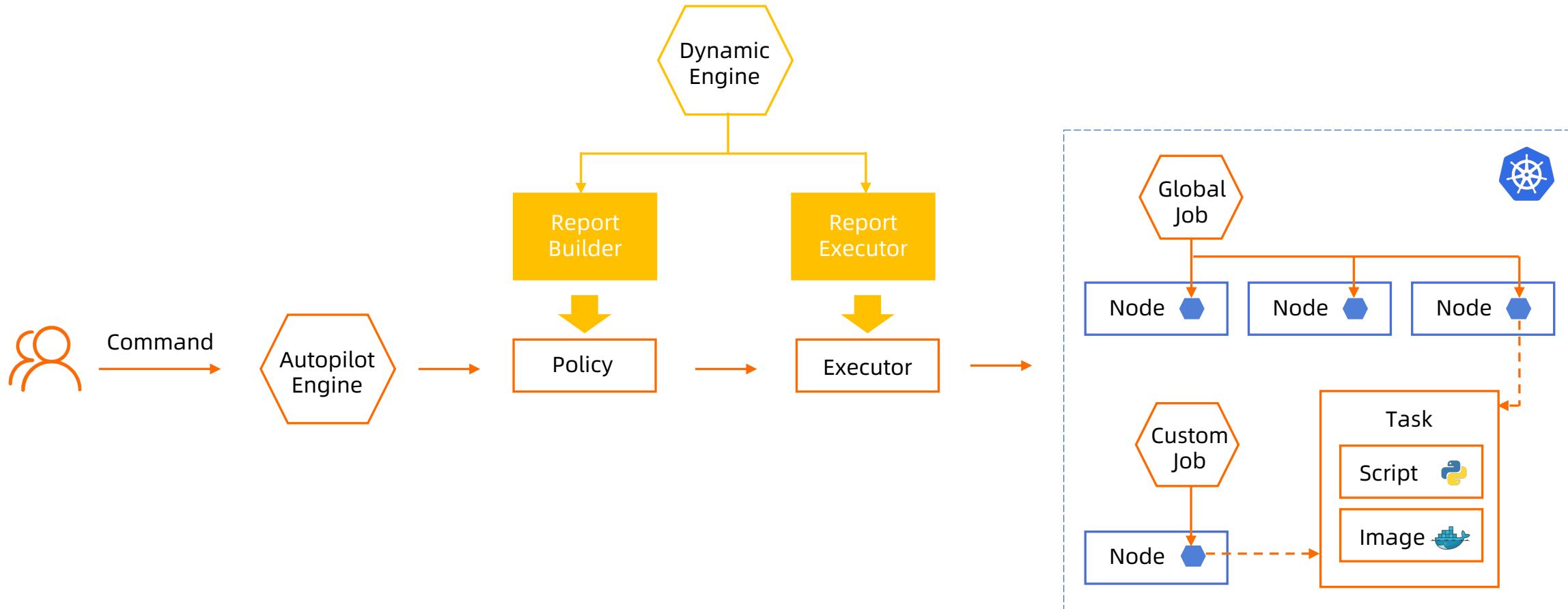
- 领域特定语言指专注于某个应用程序领域的计算机语言
- 目标受众为非程序员、业务员或最终客户

## 典型的 DSL

- 正则表达式



# Ver.2 动态化

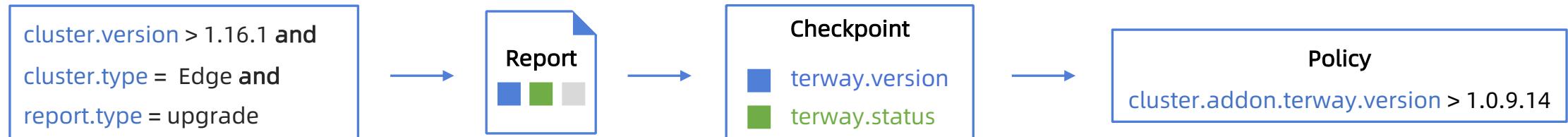




# Ver.2 动态定制

## Report Builder

- 不同集群版本、类型、场景动态定制检测报告
- 不同检测点动态定制检测策略

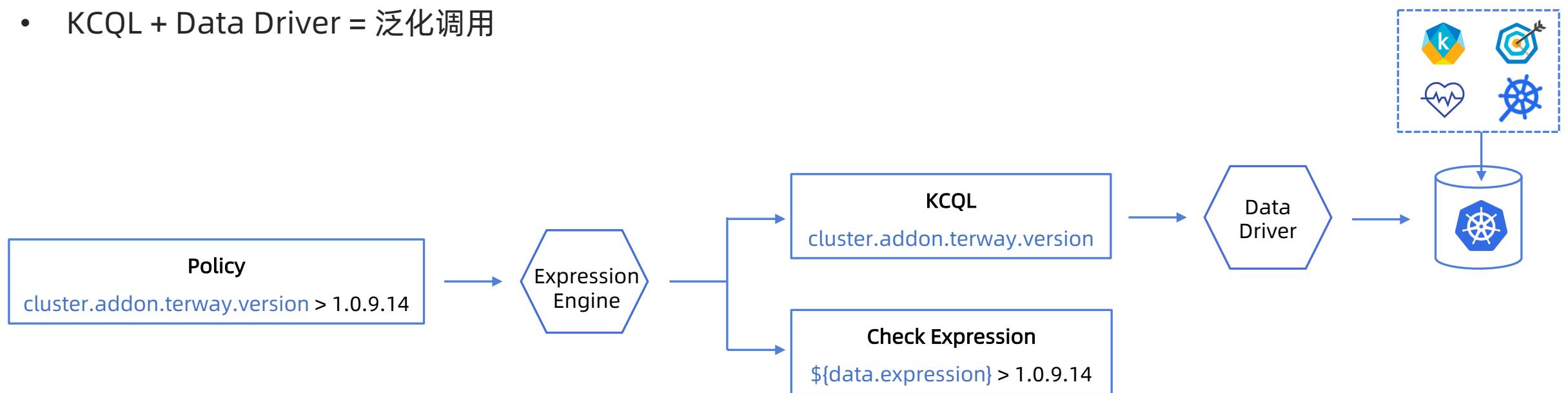




# Ver.2 动态扩展

## Report Executor

- 不同检测策略动态扩展检测任务
- KCQL + Data Driver = 泛化调用





- 1 Kubernetes 典型异常
- 2 检测框架演进
- 3 生产实践
- 4 总结

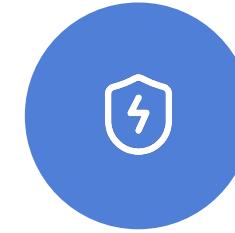


# 生产实践



望闻问切

识别集群常态或运维操作后可能存在的问题



防患于未然

在集群运维操作前识别导致操作异常的问题



# 集群巡检

## 现象

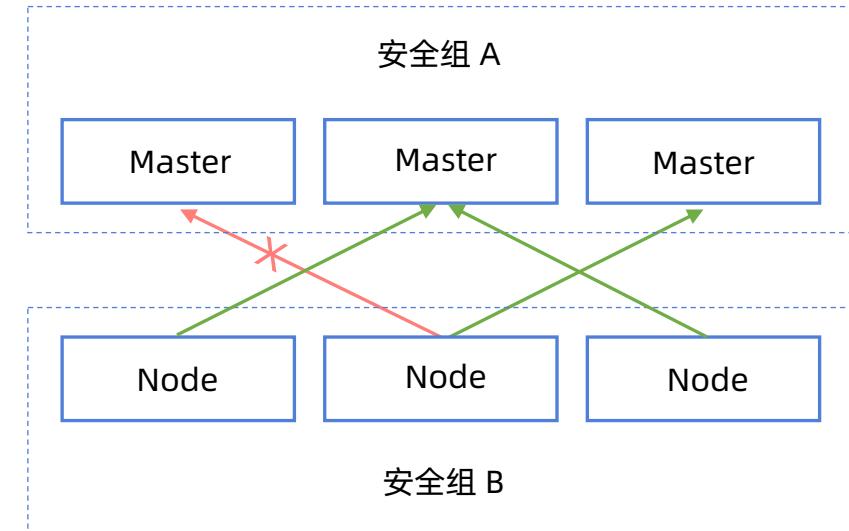
- Node 节点新增安全组，一段时间后发现 Node 节点状态异常

## 原因

- 集群 Master 节点和 Node 节点处在不同的安全组中且安全组并未相互放开。新建安全组仅对新建连接生效，不会拦截已有连接，因此一段时间后问题才会浮现

## 预防

- 配置安全组后可通过集群巡检功能检测集群安全组配置是否符合预期





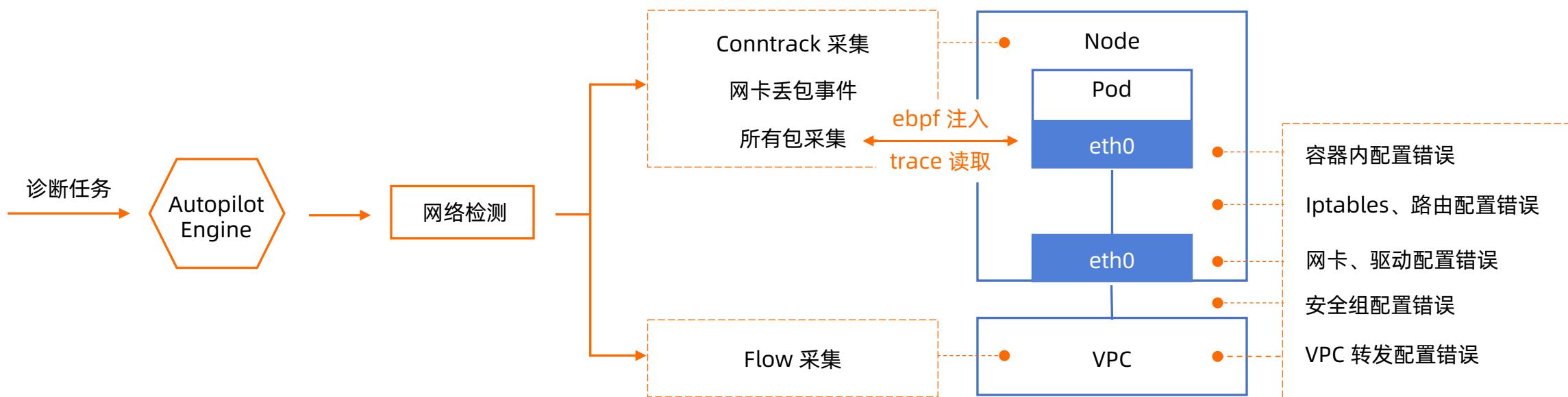
# 集群网络

## 网络配置静态检测

- 集群外部网络安全组、路由表
- 节点 iptables、路由、网卡配置

## 网络动态异常巡检

- 全链路网络异常收集
- 通过 ebpf 追踪丢包调用栈

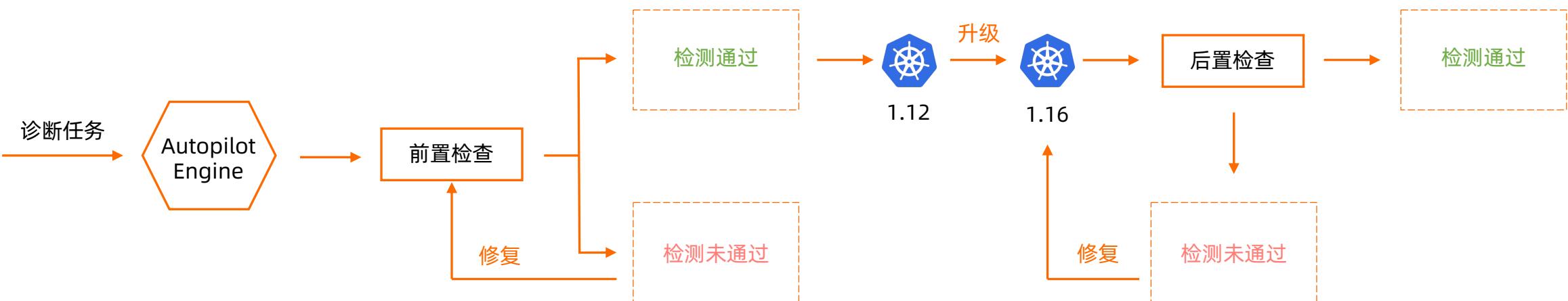




# 集群升级

## 集群异常检测闭环

- 集群升级前置检查
- 集群升级
- 集群升级后置检查





# Demo

集群资源 集群组件

集群资源检查结果 全部 待处理 3

负载均衡

节点	状态
apiserver (内网)	正常 (1)

网络

节点	状态
专有网络	正常 (1)
交换机	正常 (1)

服务器 (3个异常或警告) 目前检查前50个节点

节点	状态
云服务器 (Node)	异常 (3)

集群组件检查结果 全部 待处理 3

集群组件 (3个异常或警告) 全量检查, 目前展示前20项检查结果 (异常或警告结果优先)

组件	状态
Kube Proxy Master	异常 (1)
Kube Proxy Worker	异常 (1)
Flannel	正常 (1)

检查结果 实例信息

- ✓ 云服务器实例存在
- ❗ 云服务器实例状态正常
- ✓ 云服务器实例服务期正常
- ✓ 云服务器实例类型正常



- 1 Kubernetes 典型异常
- 2 检测框架演进
- 3 生产实践
- 4 总结



## Summary

- 基于 DSL 的 Kubernetes 集群异常检测框架支撑了阿里云上万集群常态运行和关键运维动作执行
- 框架具有强通用性和扩展性，适用于多种集群版本、类型、场景
- 框架可实现零代码定制集群检查报告
- 框架可实现低代码扩展、集成多种异常检测能力

## Next

- 更多异常检测数据源
- 集群配置推荐
- 自动修复



CLOUD NATIVE + OPEN SOURCE

*Virtual Summit China 2020*