Gdevops

全球敏捷运维峰会

破局:传统企业自动化运维平台建设与实践

演讲人：邹德裕

互联网时代IT支撑的挑战

运维尤其处在风口浪尖

业务部门

XX业务系统又出现问题了
维护部门赶紧处理

被动响应

IT运维

主机、数据库、中间件、应用一齐上阵
好像大家都没有问题

缺少有效的处理手段

IT运维

检查日志、检查应用、分析数据库、主机分析，一通忙乱后，最后通过重起应用解决

问题处理时间超长

运维经理

到底是什么原因引起？
下次还会不会发生？
发生了怎么快速处理？

问题定位困难

虽然大部份企业都已构建了监控运维的能力，但以点对点的状态监控为主，难以应对复杂IT环境下的运维场景，相对互联网公司，能力缺失较大。

运维尤其处在风口浪尖

业务压力

- 不断严格的KPI考核
- 不断叠加的业务需求
- 不断缩小的上线周期

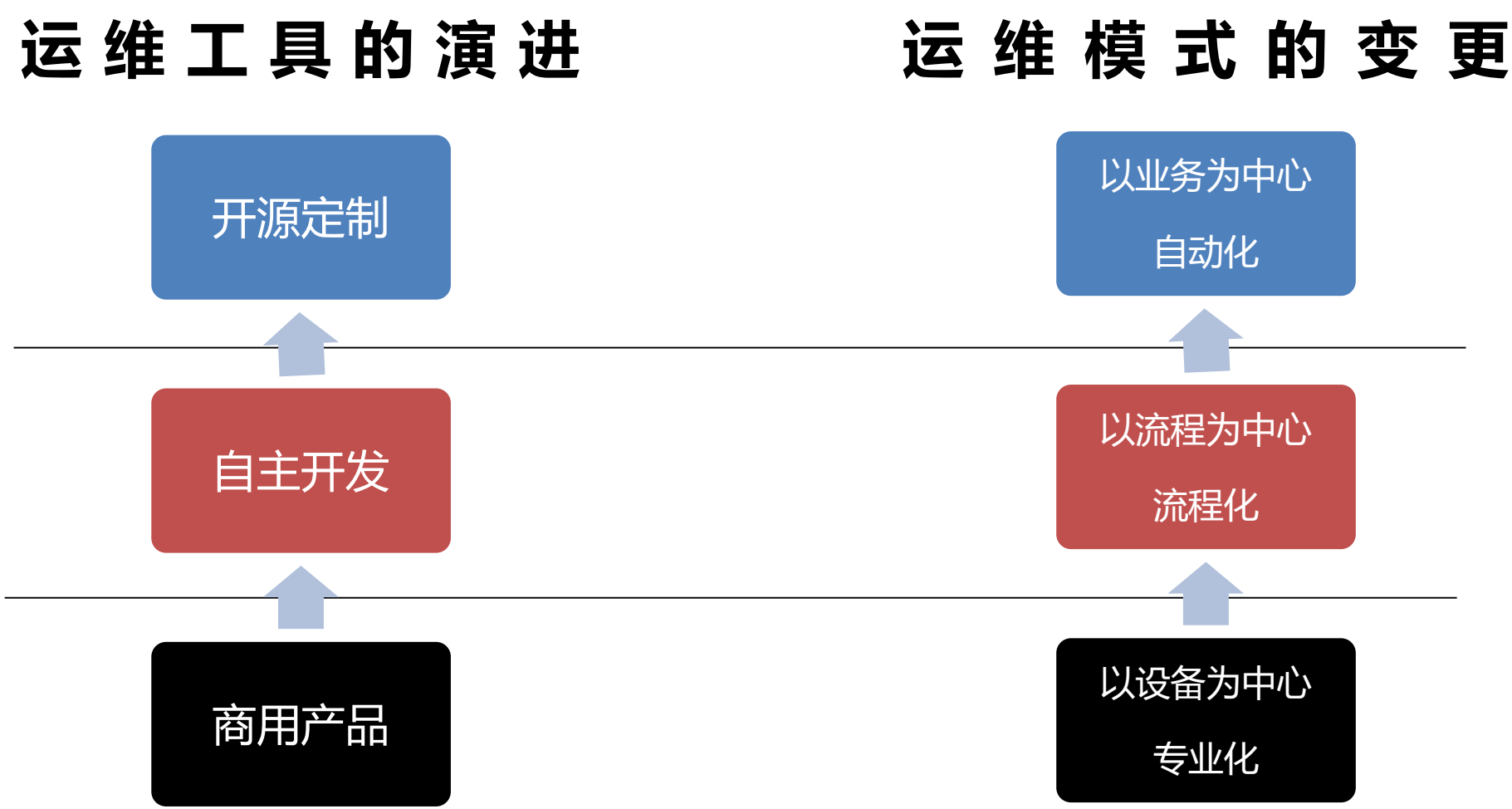
规模压力

- 数据中心规模不断增长
- 系统架构越来越复杂
- 大量分布式部署架构的引入

团队压力

- 运维支撑团队人员增长相对缓慢
- 各种新技术层出不穷
- 人员流动性大

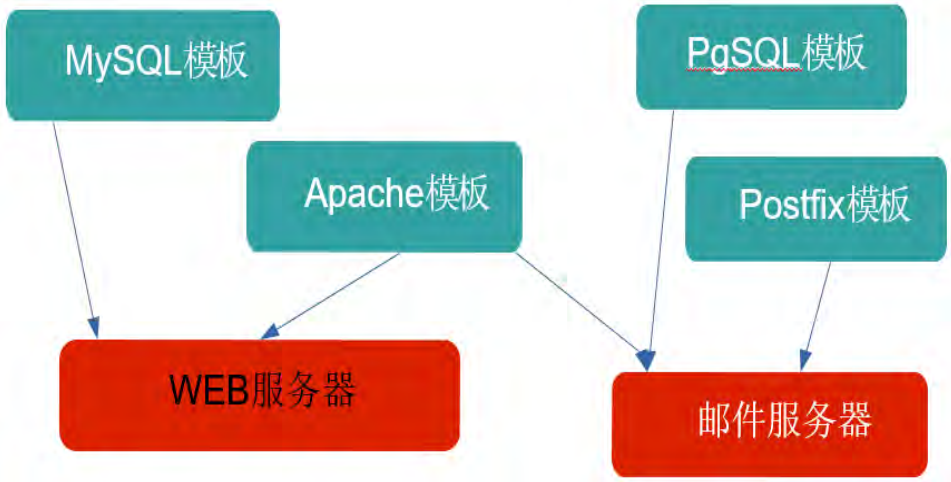
我们的运维能力需要不断的提升



ZABBIX介绍：企业级的开源解决方案

- 监控
- 告警
- 问题分析定位
- 自动处理修复

ZABBIX介绍：预置丰富的管理监控对像模板及扩展



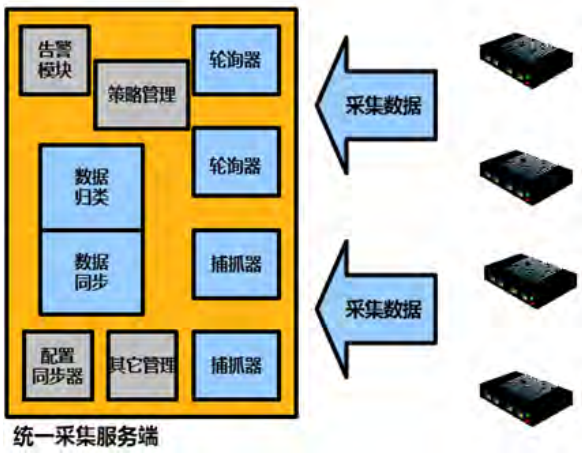
通过模板管理实现采集范围的扩展

Template-App-APC-(thecamels)	Template-App-APC-(thecamels)
Template-App-API-Gandi-(jjmartres)	Template-App-API-Gandi-(jjmartres)
Template-App-AWS-(ike-dai)	Template-App-AWS-(ike-dai)
Template-App-AWS-Cloudwatch-ELB-...	Template-App-AWS-Cloudwatch-ELB-(akomic)
Template-App-AWS-EC2-(ike-dai)	Template-App-AWS-EC2-(ike-dai)
Template-App-AWS-ELB-(bcarpio)	Template-App-AWS-ELB-(bcarpio)
Template-App-AWS-ELB-(datorama)	Template-App-AWS-ELB-(datorama)
Template-App-Amavisd-(thecamels)	Template-App-Amavisd-(thecamels)
Template-App-Apache-(marijngiesen)	Template-App-Apache-(marijngiesen)
Template-App-Apache-(red-tux)	Template-App-Apache-(red-tux)
Template-App-Apache-Stats-(gpmidi)	Template-App-Apache-Stats-(gpmidi)
Template-App-Apache-Traffic-Server---...	Template-App-Apache-Traffic-Server---ATS-(kometchtech)
Template-App-Asterisk-(alkali147)	Template-App-Asterisk-(alkali147)
Template-App-Audiocodes-(jjmartres)	Template-App-Audiocodes-(jjmartres)
Template-App-BackupPc-(szimszon)	Template-App-BackupPc-(szimszon)
Template-App-Bacula-(selivan)	Template-App-Bacula-(selivan)
Template-App-Barracuda-Spam-Firew...	Template-App-Barracuda-Spam-Firewall-(phroton)
Template-App-Bind-(m4ce)	Template-App-Bind-(m4ce)
Template-App-Bind9-(Pesticles)	Template-App-Bind9-(Pesticles)
Template-App-Bind9-(itxx00)	Template-App-Bind9-(itxx00)
Template-App-BlackBerry-Enterprise-...	Template-App-BlackBerry-Enterprise-Server-(jamie1921)
Template-App-Blacklist-RBL-(jjmartres)	Template-App-Blacklist-RBL-(jjmartres)
Template-App-Brocade-HBA-(thecam...	Template-App-Brocade-HBA-(thecamels)
Template-App-CUPS-(a-schild)	Template-App-CUPS-(a-schild)
Template-App-Ceph-(thelan)	Template-App-Ceph-(thelan)

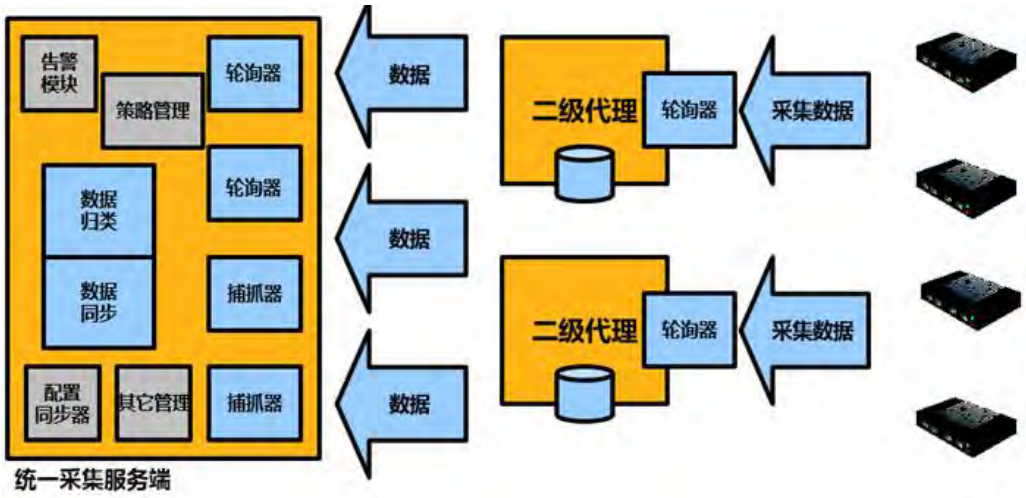
ZABBIX介绍：支持大规模IT系统的管理能力

- 可通过灵活配置方式，添加采集机，避免手工静态部署，实现采集处理能力的平滑扩展；
- 可通过采集源、适配器的灵活配置，实现采集范围的灵活扩展；
- 通过集中方式管理采集源和任务策略；
- 扩展后的采集机具有对等性和可互换能力。

基本采集模式



分布式采集模式



ZABBIX介绍：丰富的告警策略配置及规则

系统支持近100种监控策略配置，可以灵活设置告警规则。包括以下三大类的告警规则，每一大类又能分为多种小类：

例如：

CPU使用率大于、小余或等于某个阈值

例如：

连续N个周期内性能最大值大于X

N个周期内，最大值和最小值之间的差值大于X

在连续N个周期内，没有接收到数据

例如：

根据自定义、自编辑的正则表达式自行制定告警规则。

告警方式支持前台展示、手机网管、短信、邮件等；

支持多种级别的告警，包括：信息、警告、一般、严重、灾难等；

ZABBIX介绍：开源版本更适合互联网架构

开源版本ZABBIX的缺陷

监控告警

- 商用产品支持能力较弱
- 支持指标较单一
- 缺少设备关联分析能力
- **告警聚合能力较弱**

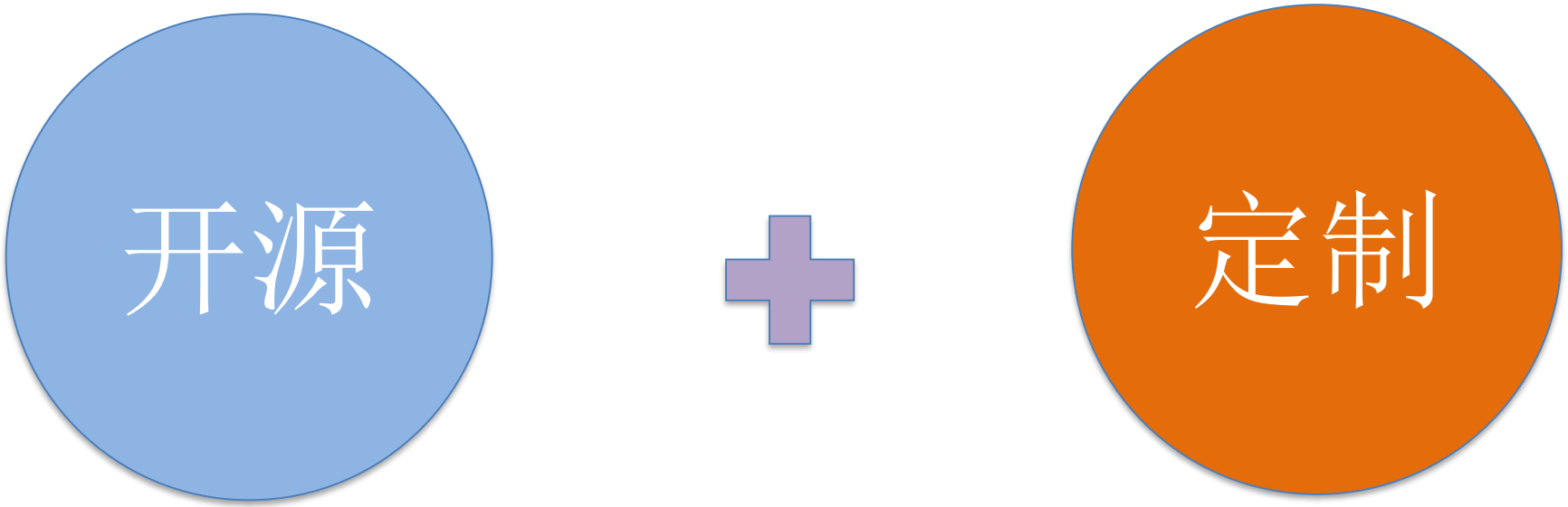
分析定位

- 只能针对单个设备的告警
- 不具备关联分析能力
- 不具备告警根源分析能力

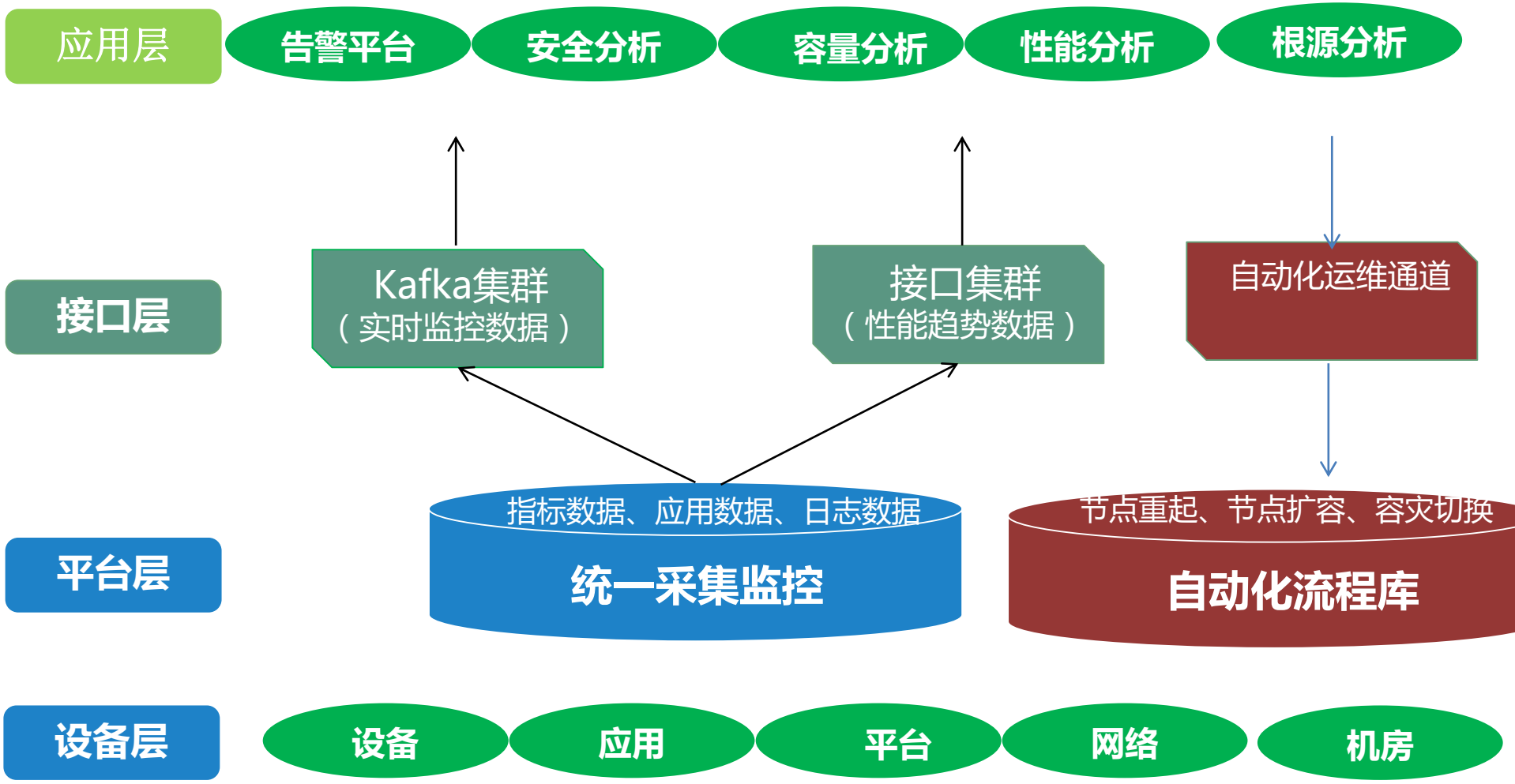
自动化运维

- 不支持复杂场景的分析处理
- 不具备自动化运维能力
- 不具备代理端的批量配置管理能力

构建适合于传统企业的自动化运维平台

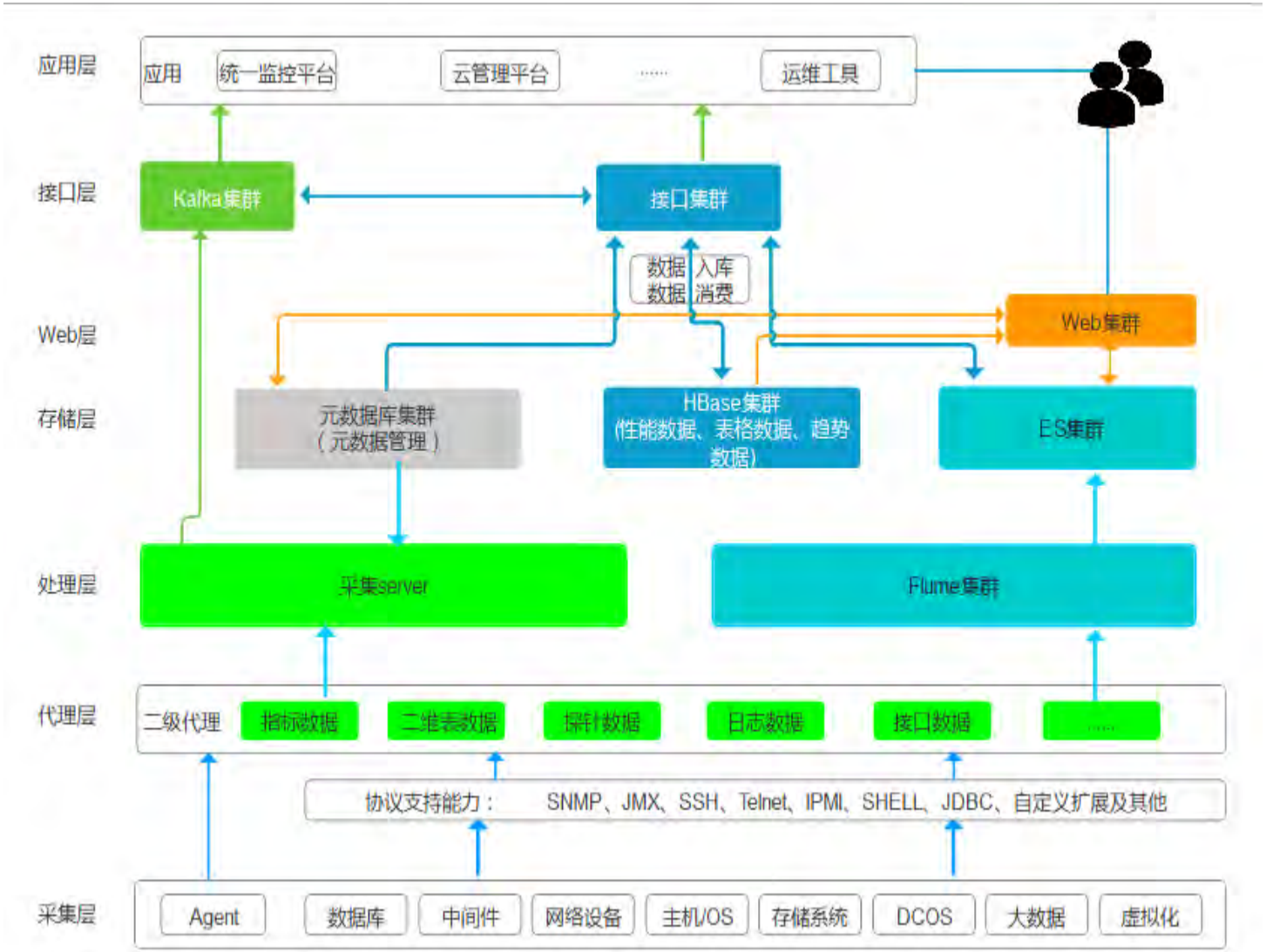


架构设计：整体功能架构设计



架构设计：技术架构

- 用户
- 业务
- 应用
- 中间件
- 数据库
- 主机
- 存储/网络



架构设计：各层架构说明

- 数据采集
- 执行命令

- 统一分发采集的数据
- 提供WebService、RESTful、MQ等接口
- 清洗数据入库HBase

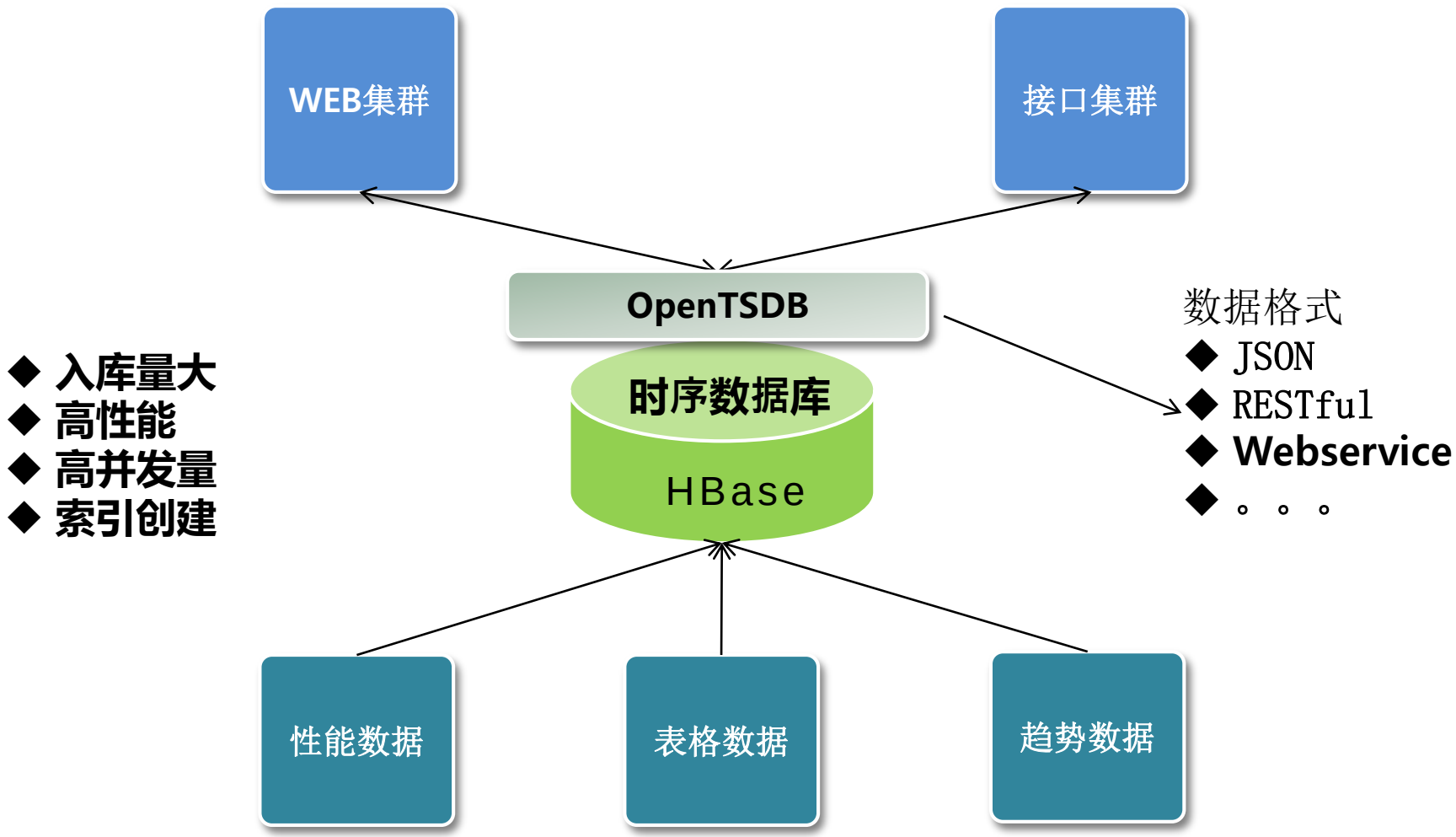
- Zabbix Proxy
  KEY-VALUE数据
  趋势数据
- AMP Proxy
  表格数据的采集
  操作通道的提供
- 现有Kafka
  非结构化数据

- Web页面展现
- 统一采集页面
- Zabbix管理界面

- 采集任务调度
- 采集数据推送Kafka
- 自动化运维通道

- 元数据库集群：配置数据、汇总的配置信息等
- HBase集群：性能数据、表格数据、趋势数据等
- ES集群：非结构化数据

架构设计：10000+级主机及200W/分钟+指标支撑



监控能力：监控采集能力扩展

监控能力：监控采集能力扩展

采集范围覆盖硬件、OS、数据库、中间件、网络、备份、大数据、DCOS以及虚拟化

设备类型	二级类型	细分类型
数据库	Oracle	Oracle10/11/12
		Oracle12
	开源数据库	MySQL
		mongodb
		rdb(PG-XC postgresql)
大数据	开源大数据	NameNode
		DataNode
		ResourceManager
		NodeManger
		RegionServer
		Kafka
		Flume
		Spark
		华为管理平台-数据库
		Zookeeper
		Hive
		Hmaster
	非开源大数据	MPP(aster)
		dispserver
		IBM Streams
		Zookeeper
		Redis
		SQLFire
		Docker Container
		HDFS
		YARN
中间件	中间件	Weblogic
		Tomcat
		Websphere
		active MQ
		Redis
		memcache
		nginx
		Haproxy

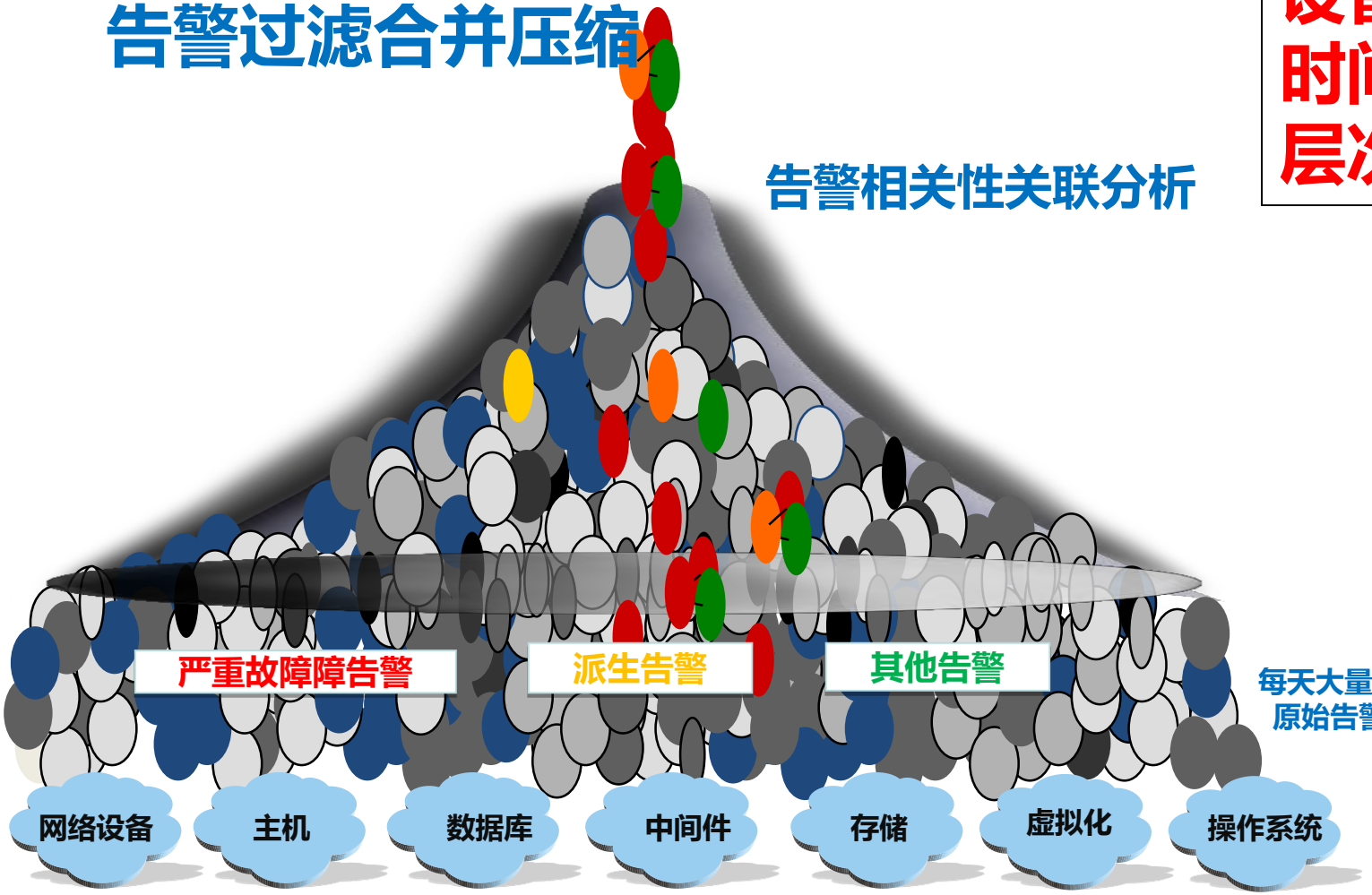
设备类型	二级类型	细分类型
硬件	服务器	X86服务器
		小机
	存储	HP存储（10000/9500/12000/24000）
		IBM（DS8000系列、DS5000系列）
		EMC存储（DMAX）
		HDS存储（VSP）
		富士通存储
		华为NAS存储（N8000系列）
		华为SDS
		光纤交换机（博科）
网络设备	华为系列	S9300
		NE20E
		NE40E
		NE80E
		S3352
		S9303
		S9306
		S9312
		交换机路由器
		防火墙（E1000E/E8000E）
	JUNIPER	JUNOS
		SCREENOS
		ISG2000
		NS5000
	H3C系列	交换机（H3C S76/S125系列）
		防火墙（H3C 9000系列）
	Array系列	Array负载均衡
操作系统	操作系统	Linux（suse 9、10、11 SP1-SP4）
		Linux（centos 7、redhat 6.5）
		Linux（redhat 7.0、7.1）
		AIX(5.3、6.1)
		AIX 7.1
		HP-UX(11.11、11.23、11.31)
		windows(03、08)、备份
		vmware
DCOS	DCOS	mesos-master
		mesos-slave
		业务容器
		marathon
		Zookeeper
		Haproxy

告警能力：告警能力扩展

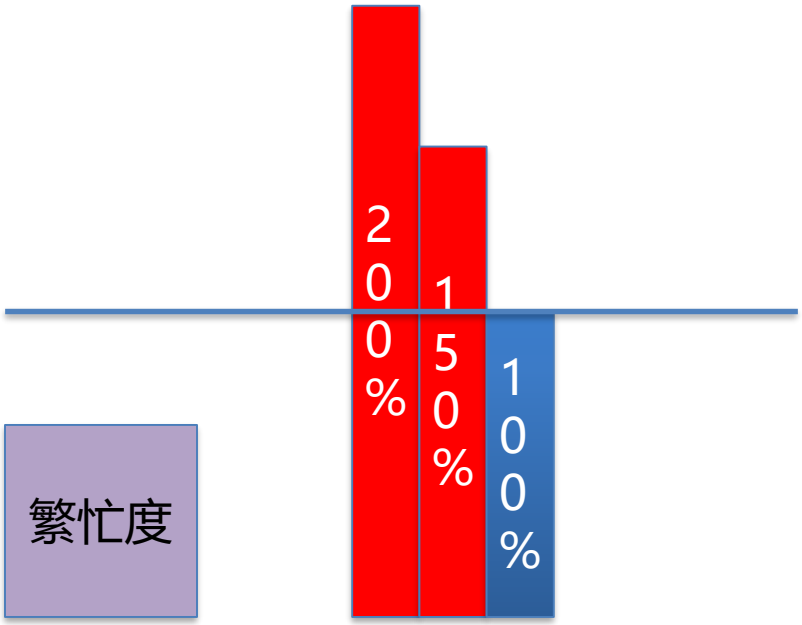
业务
系统
设备
时间
层次

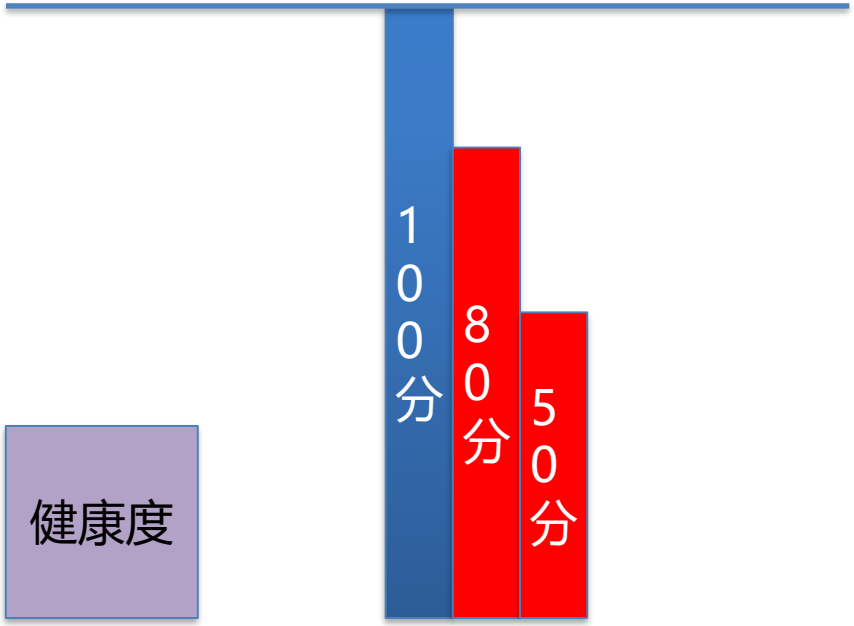
告警过滤合并压缩

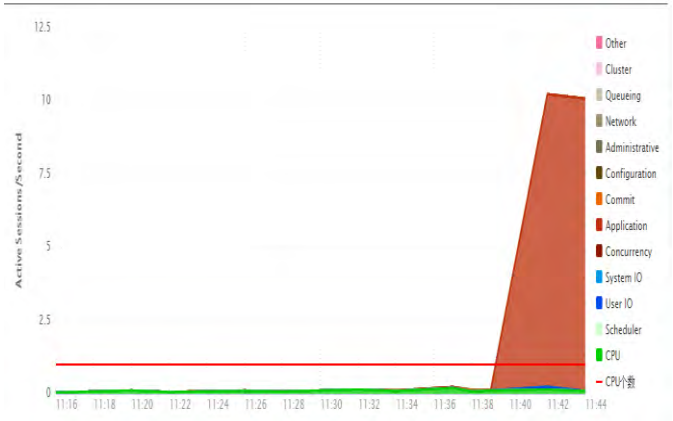
告警相关性关联分析



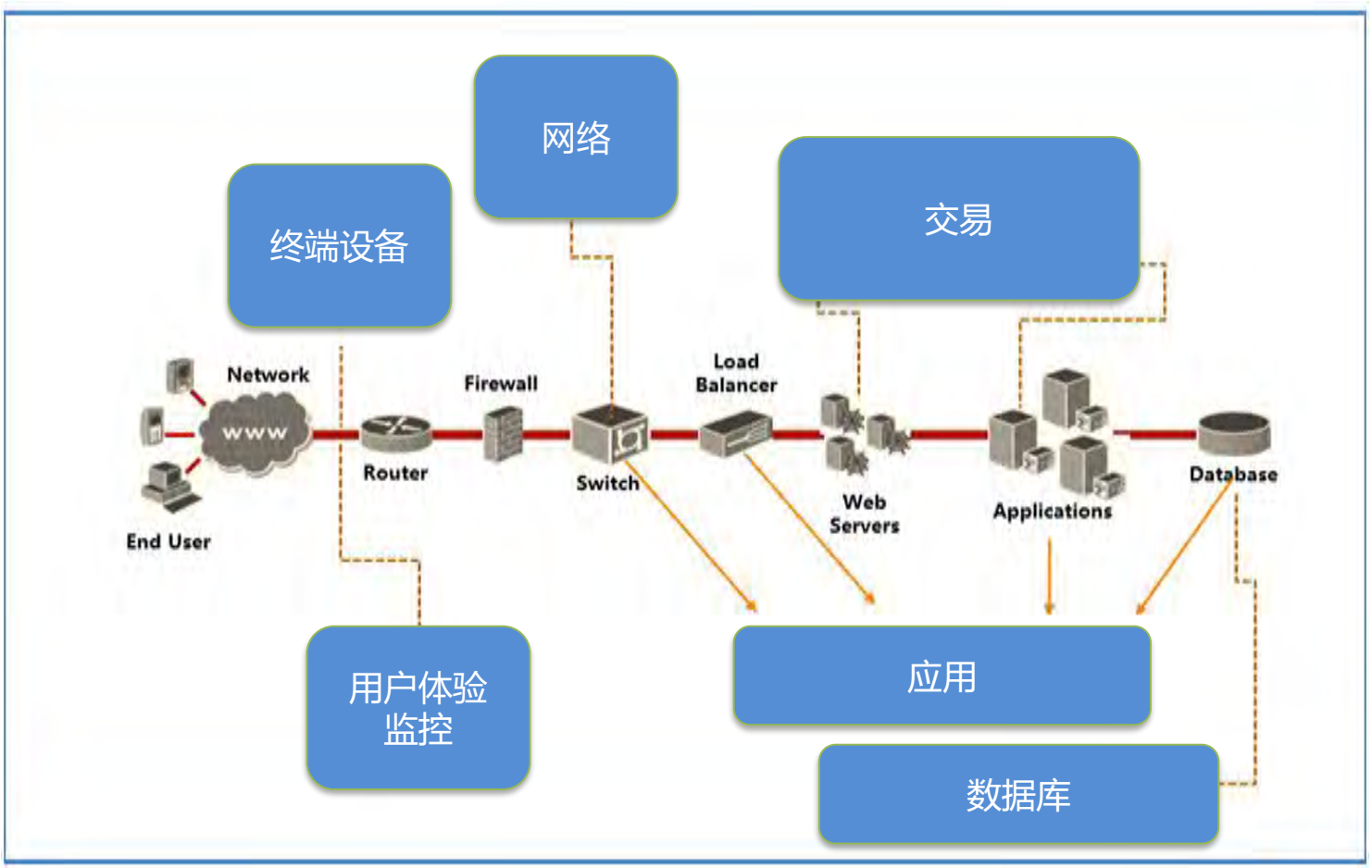
告警能力：聚合单一告警指标，直观展示设备状态







采集能力：实现业务交易端到端的监控与分析

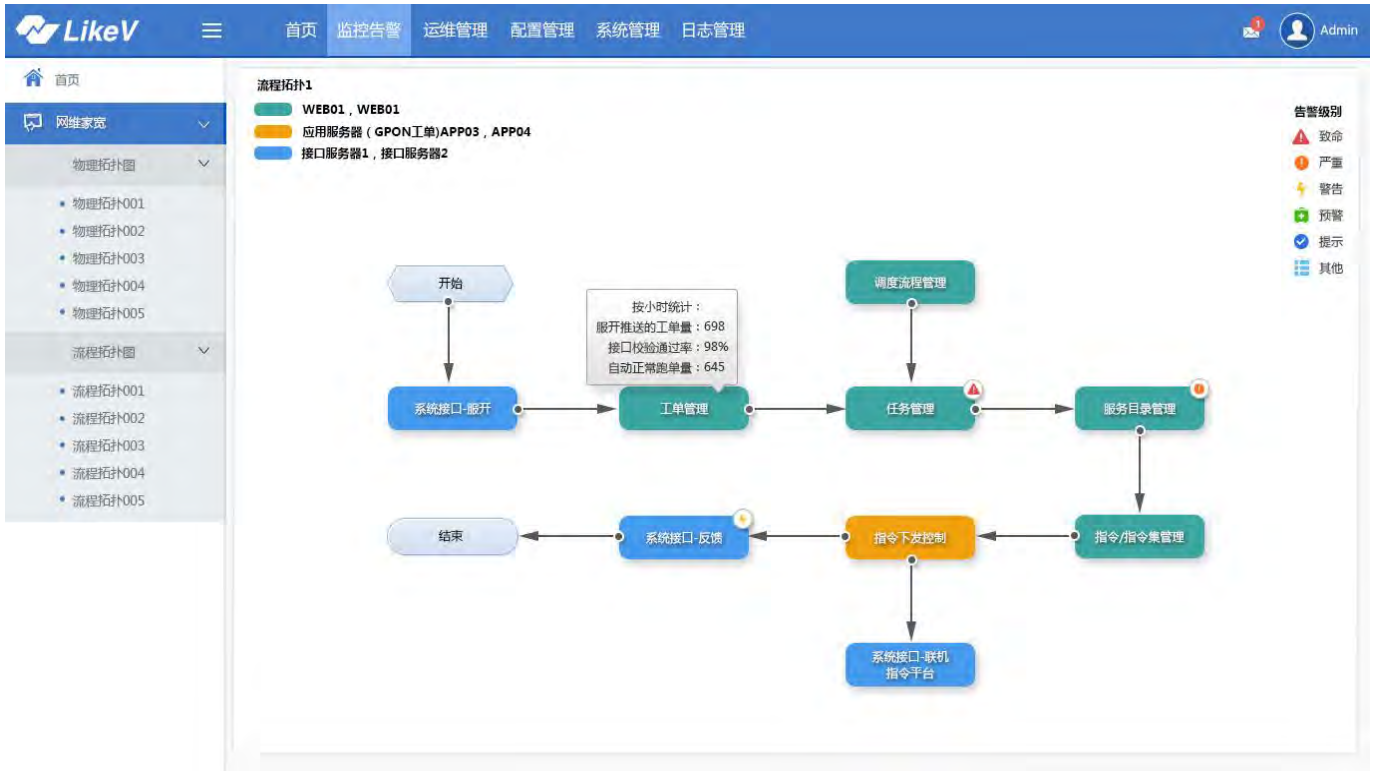


日志数据采集

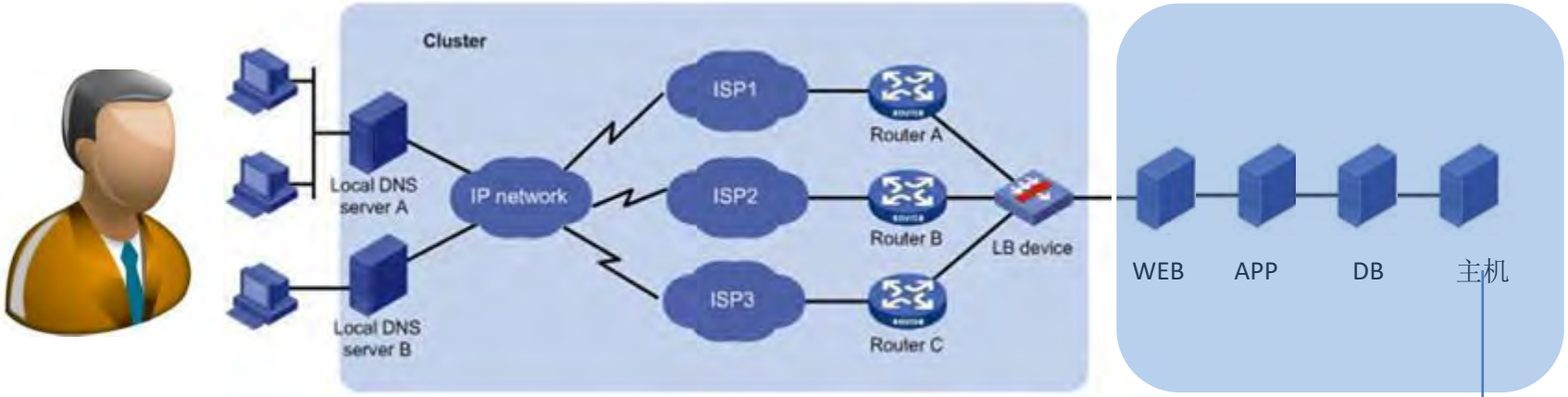
代理数据采集

分析能力：业务流程及节点关联展示分析

通过关键业务流程梳理，实现业务全流程的监控



分析能力：告警根源分析能力是自动化处理的关键



故障 → 业务、应用、中间件、数据库、主机一连串告警 → 自动化处理，无从下手

分析能力：智能告警分析方法

故障ROOT分析

告警短信：XX缓存硬件故障，影响XX、XX业务，可能原因为磁盘故障

架构分层原则：越底层的设备可能性越大

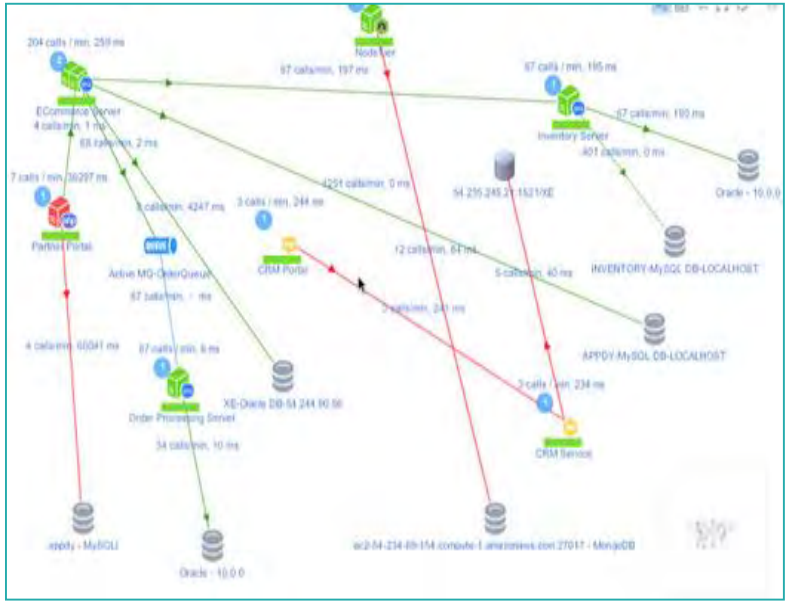
用户层

接入层

逻辑层

数据层

路径分析原则：当某个设备出现问题，属于这个调用链上的节点都可能出现告警，按访问顺序，最末端的可能性越大



时间面积原则：结合告警时间先后顺序，告警影响面积等权重分析

时间相关性

面积权重

分析能力：告警根源分析示例

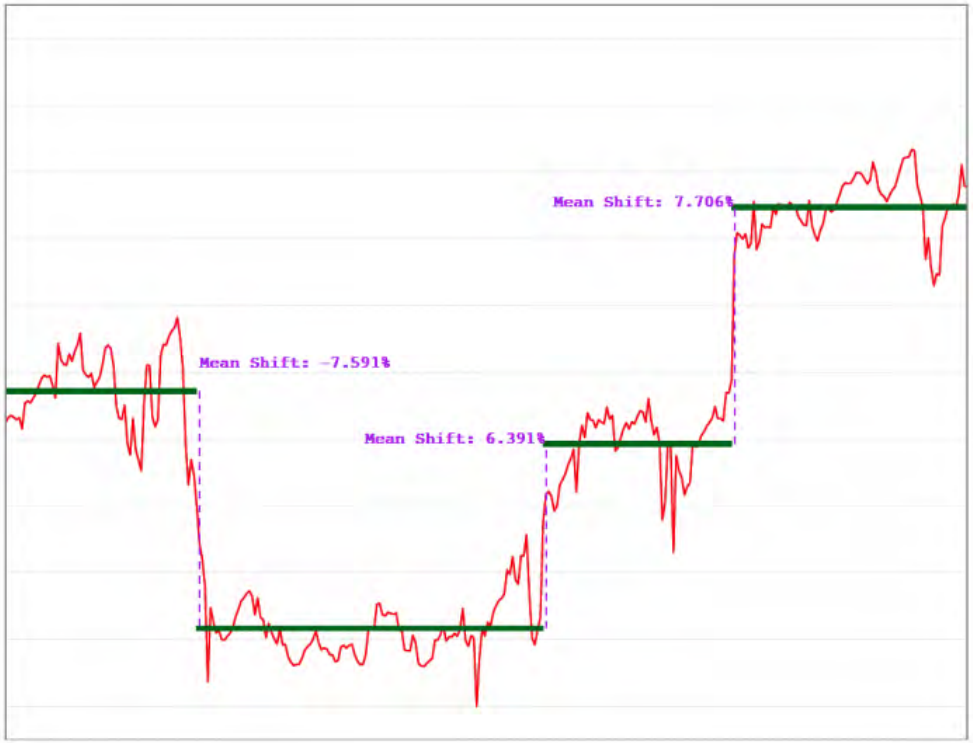
大数据结合：引入大数据技术，进行运维大数据分析

ROOT分析 | 性能基线分析 | 容量分析 | 告警阀值优化 | 基线偏离告警

安全事件分析 | 故障预测 | 容量预测 | 关联告警 | 事件关联分析

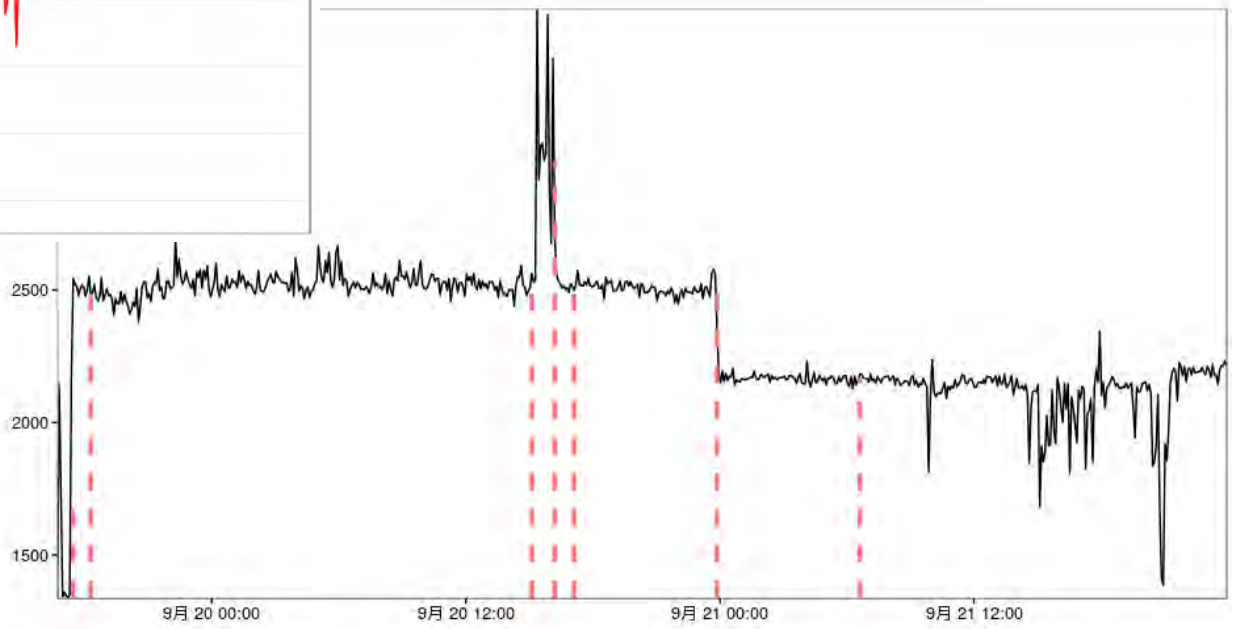
业务 | 应用 | 中间件 | 数据库 | 主机 | 存储/网络

异常时段识别：借助开源模型与算法

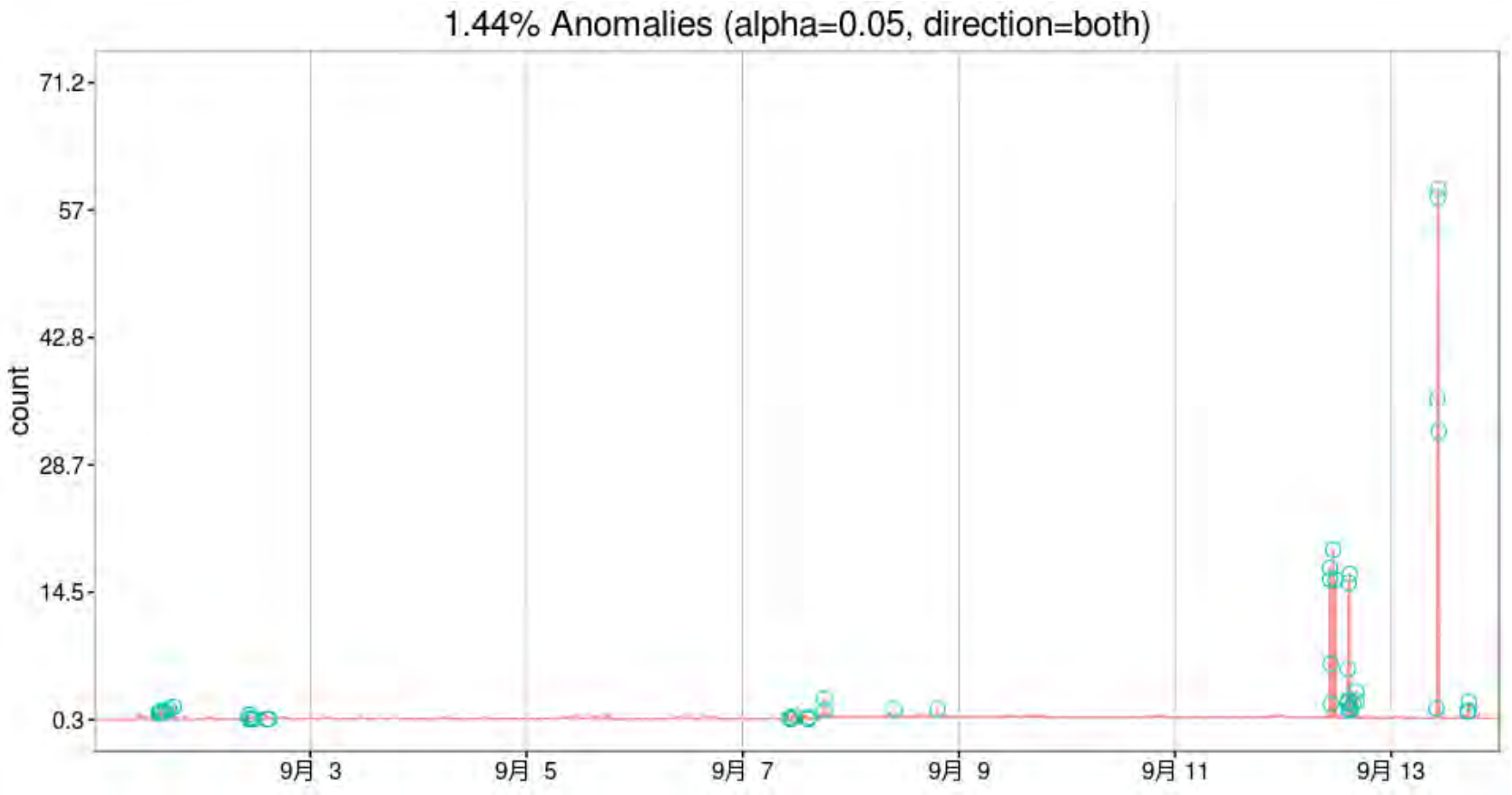


均值漂移：时间序列的突发性变化

平滑改变：一个渐变的过程，两个平稳状态之间平滑的转变



异常时段识别：借助开源模型与算法



分析能力扩展：运维大数据分析示例

指标数据采集

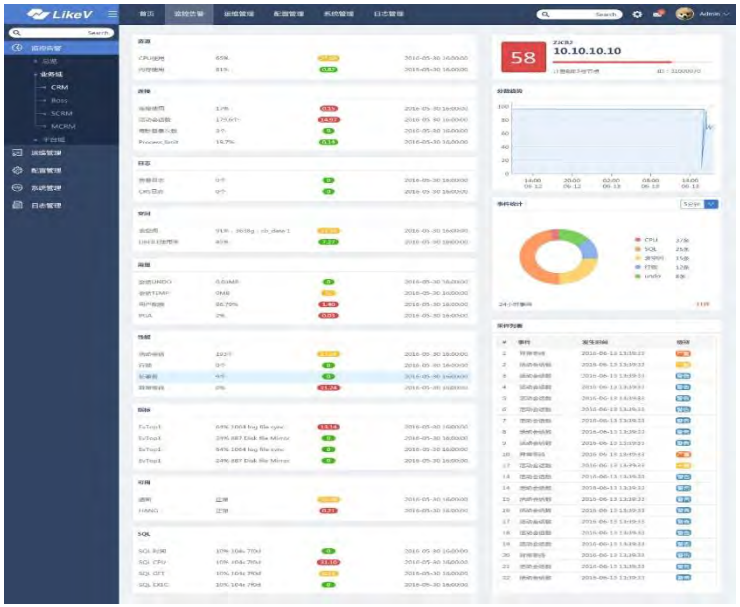
影响权重计算

综合分数计算

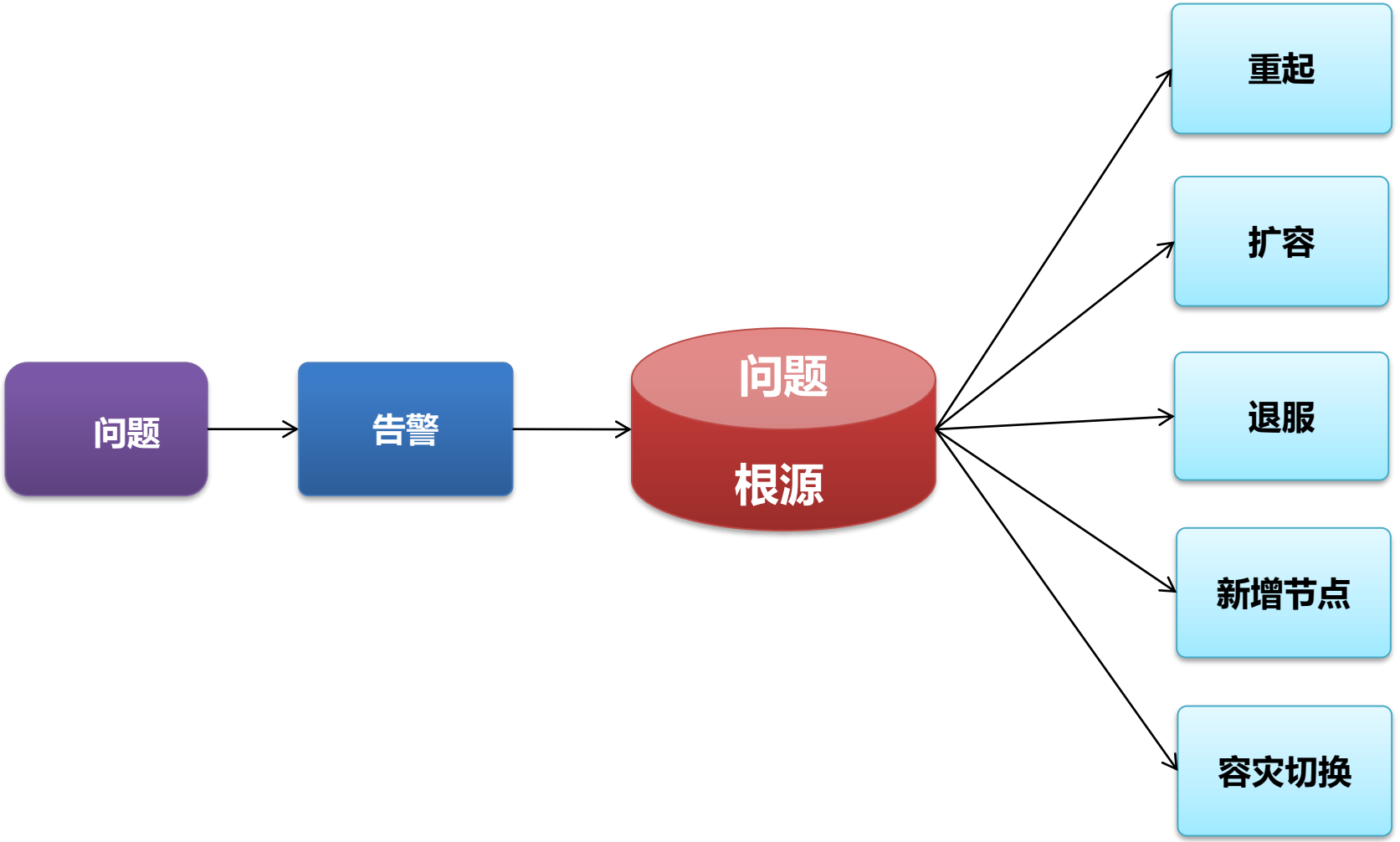
综合指标告警

影响权重回朔

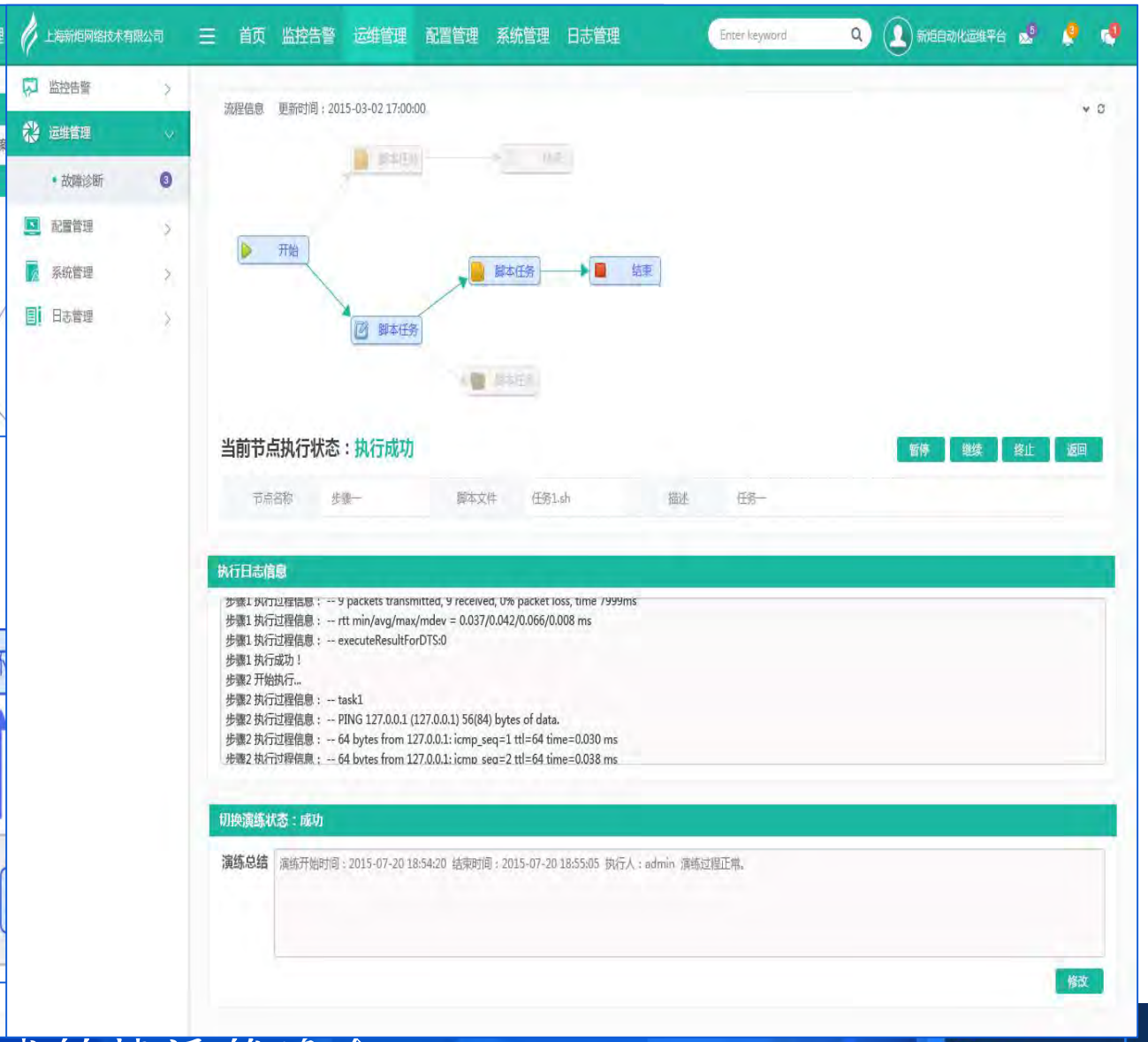
问题定位处理



自动化处理：根据问题根源进行自动化处理

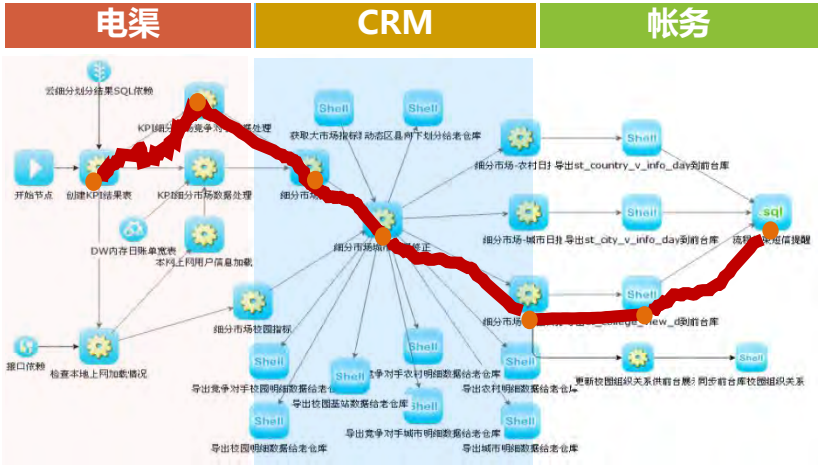


自动化处理：脚本编排，支持复杂场景的自动化处理



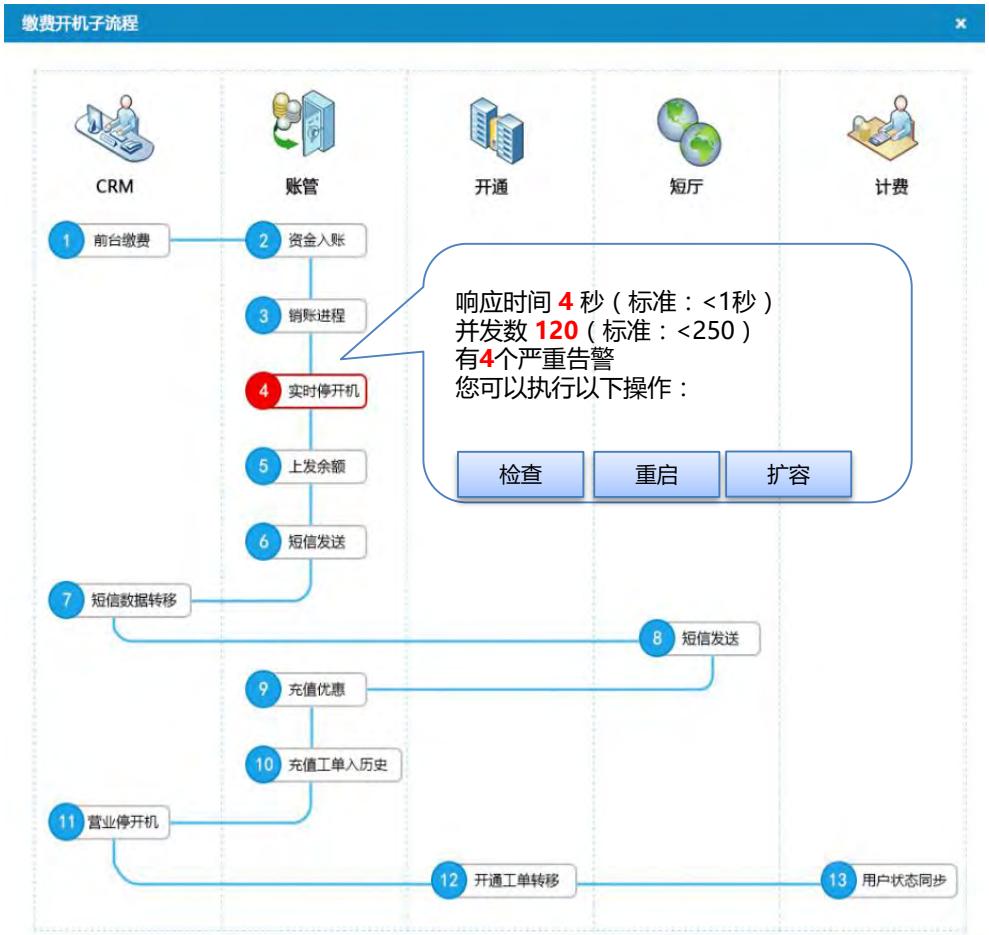
构建以业务为中心的自动化监控运维能力

业务状态可视化



问题定位可视化

问题处理自动化



不只是监控

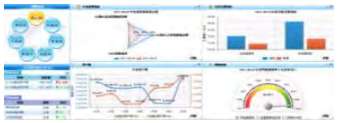
以ZABBIX为基础的整体运维解决方案

移动运维

大屏视图

个人门户

专业报表

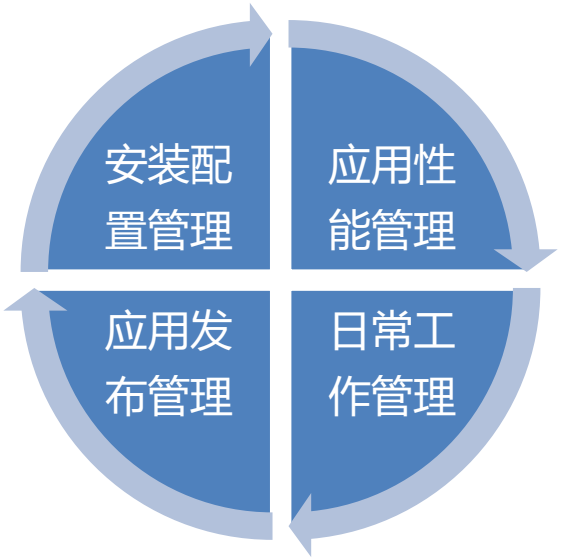


资产管理

配置管理 | 变更管理 | 事件管理 | 问题管理 | 服务管理 | 容量管理 | 知识管理

系统安装、软件安装、网络开通、IP地址、防火墙配置、补丁安装...

应用发布、应用配置、批量部署、应用回退



端到端性能分析、应用拓扑分析、接口调用分析、关键事务分析、数据库性能分析....

设备管理、云平台管理、日常巡检、深度巡检、脚本管理、批量执行、安全审计.....

智能告警

业务监控 | 应用监控 | 平台监控 | 设备监控 | 机房监控

Gdevops

全球敏捷运维峰会

THANK YOU！