

ZABBIX 2020  
Conference  
CHINA

演讲主题

# 苏宁智能监控报警中心

演讲嘉宾

苏宁科技集团苏宁云BU平台云研发中心 智能监控与  
运维产研中心 尚海

# 目录

- 苏宁立体化监控体系
- Zabbix大规模监控实践
- 监控告警自动化
- 智能报警中心建设

# 01

## 苏宁立体化监控体系

立体化监控构建的背景介绍，立体化监控体系概览

# 苏宁立体化监控体系-背景介绍

## 业务广泛性

- 易购、置业、金融、家乐福、视频、直播、物流

## 监控范围复杂性

- 多机房部署，多云部署，多活架构
- 全面监控

## 系统和服务复杂性

- 系统多，调用关系复杂
- 端到端的监控

## 监控告警诉求

- 告警全、快、精准
- 智能化+可视化

# 苏宁立体化监控体系-背景介绍

## 监控范围

- 越来越广
- 越来越复杂

## 监控能力

- 越来越高
- 越来越智能

## 使用体验

- 越来越好



## 立体监控

- 立体化监控体系
- 点、线、面的监控
- 交叉监控

## 智能报警

- 可视化
- 智能化
- 管理+治理

# 苏宁立体化监控体系-关键点

## 容量和性能

1

- 容量够大，能支撑百万级别服务器的监控规模
- 监控全面性和完整性
- 高可用、可扩展

## 告警

2

- 告警实时
- 秒级告警
- 精准告警
- 关联分析

## 数据

3

- 监控数据可视化
- 监控数据分析
- 异常检测
- 数据价值挖掘与输出

# 苏宁立体化监控体系-建设路径



采集



存储



计算



分析



可视化

- 支持多平台多类型数据采集 (zabbix, prometheus, flume, 探针)
- 秒级采集
- 个性化

- 时序存储
- 日志存储
- 图存储
- Metric存储

- 告警引擎计算
- 实时计算
- 离线计算
- 算法

- 告警聚合
- 告警收敛
- 根因定位

- 数据可视化
- 告警可视化
- 监控大盘

# 苏宁立体化监控体系-体系概览

配置中心

可视化平台

智能报警中心

监控开放平台

可视化

苏宁端到端立体化监控

数据可视化展示

监控大屏

链路大盘

拓扑监控

融合分析

监控视图

数据报表

监控Tree

资源视图

监控体系

苏宁智能报警中心

日志监控

日志监控

调用链监控

基础监控

Zabbix监控

动环监控

Prometheus监控

CDN监控

应用监控

拨测监控

端侧监控

组件监控

业务监控

范围

易购

置业

金融

体育

直播

家乐福

物流

门店

# 苏宁立体化监控体系-自我监控

## 数据采集监控

- 数据延时告警
- 采集失败告警

## 告警服务监控

- 告警延时告警
- 告警积压告警
- 告警服务异常

## 访问服务监控

- 用户访问异常告警
- 异常访问告警
- API服务告警

## 自动化监控

- 自动化实现过程的监控

## 集群服务监控

- 服务异常告警，高可用切换

## 交叉监控

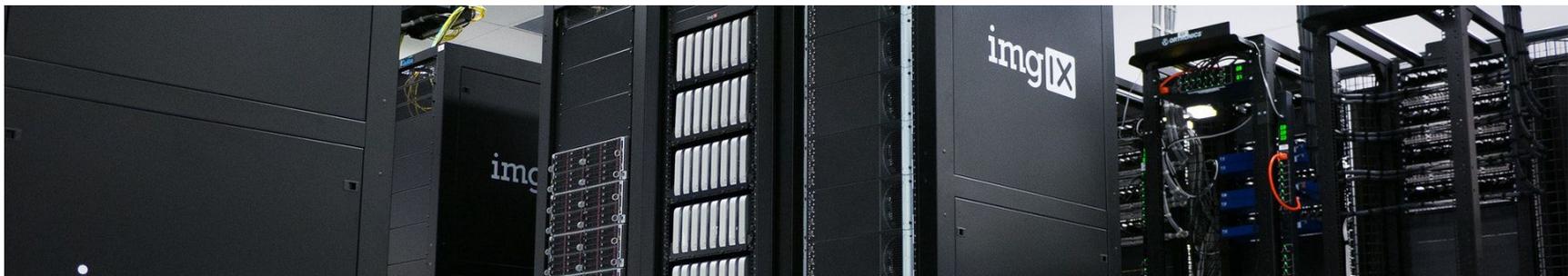
- 跨机房交叉监控
- 健康管理

# 02

## Zabbix大规模监控实践

监控范围，困难与挑战，部署架构

# Zabbix大规模监控实践-监控范围



## 网络

- 交换机
- 负载均衡
- 防火墙
- 路由器
- 虚拟网络

## 服务器

- 物理服务器
- 虚拟机
- 硬件指标
- openstack

## 操作系统

- Windows
- RHEL
- SUSE
- IBM AIX
- CentOs

## 中间件

- WildFly
- Nginx
- Suengine
- Redis
- Apache

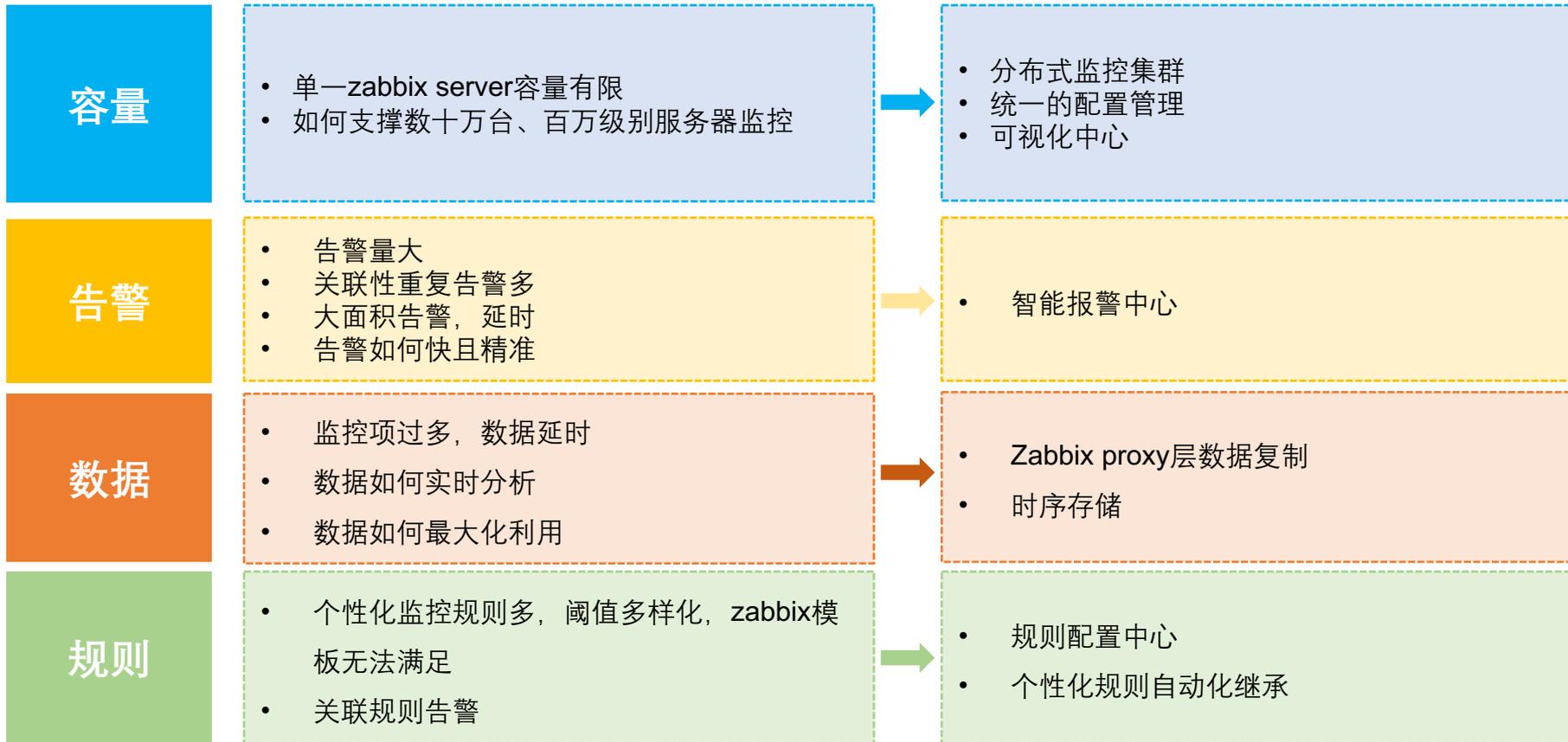
## 数据库

- Mysql
- DB2
- Oracle
- Sybase
- Mycat
- PG
- SQL Server

## 应用系统

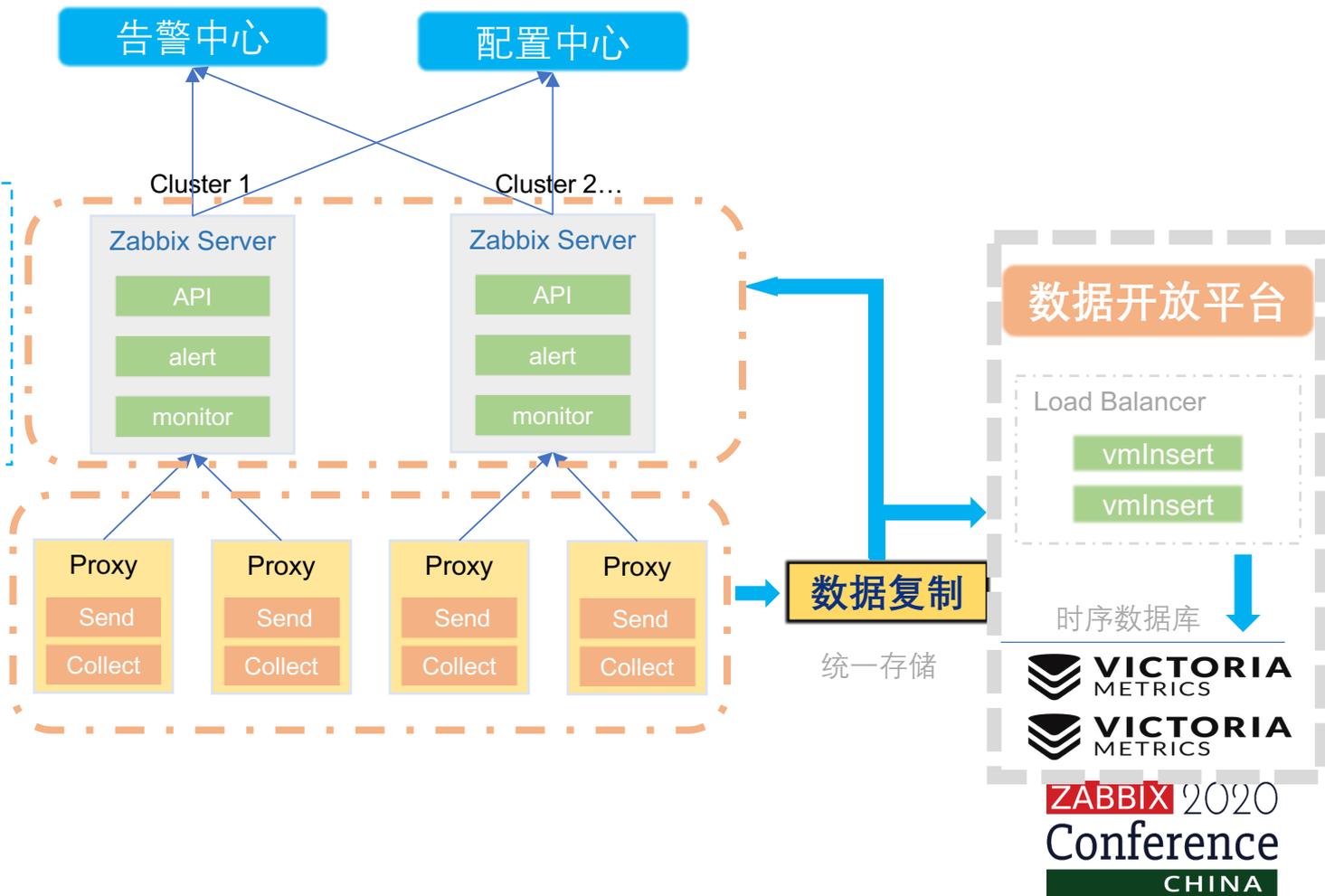
- URL检活
- 状态
- 接口
- 健康指标

# Zabbix大规模监控实践-挑战



# Zabbix大规模监控实践-部署架构

- 多机房部署
- 分布式监控集群
- 统一配置管理
- Proxy层数据复制



# 03

## 监控告警自动化

监控前、中、后的全生命周期自动化，无人值守的监控

# 监控告警自动化



## 背景

- 数十万服务器规模下，每天有大量的服务器上线、下线、变更操作，监控变化频繁
- 业务系统多，监控告警规则多样化，个性化，传统的监控模板难以满足监控需要
- 监控对象存在常态化的扩缩容，个性化监控规则需要自动化



## 目标

- 监控实时
- 无人值守

自动化

# 监控告警自动化-上下线

1

## 自动注册

监控对象按策略向指定监控集群自动注册，进入监控系统纳管体系

2

## 自动发现

基于CMDB自动发现监控对象，利用zabbix自动发现功能

3

## 监控模板

根据监控对象属性，自动匹配其对应的监控模板

4

## 自动化配置

基于状态，类型，完整的自动化配置体系,包括监控配置，告警配置

5

## 个性化继承

监控对象权限继承  
个性化配置继承

# 监控告警自动化-总结

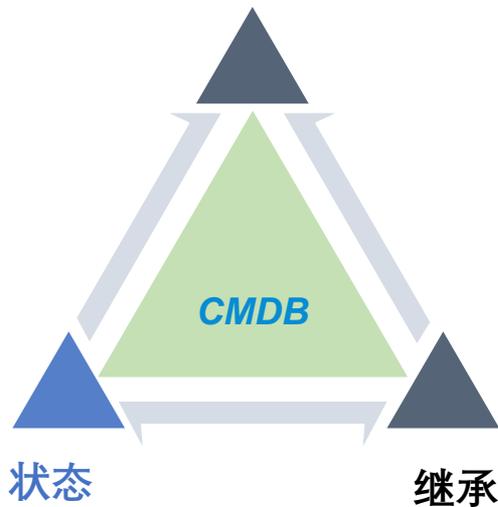


## 监控流程自动化

监控系统配置中心基于CMDB数据，围绕状态，类型，继承实现监控对象生命周期的自动化管控；无人值守同时，确保监控全面性、完整性、及时性。

### 软件类型

- 监控模板个性化应用
- 对象配置个性化匹配



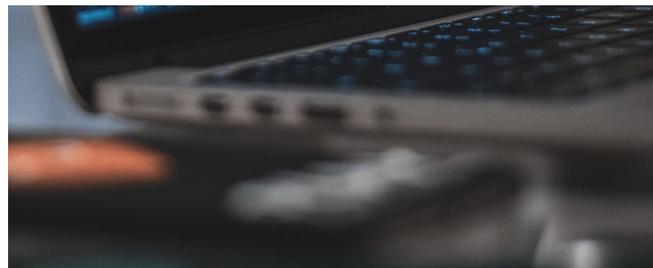
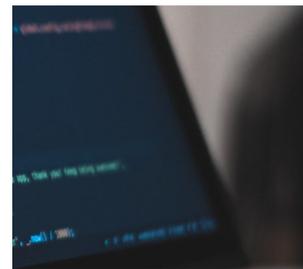
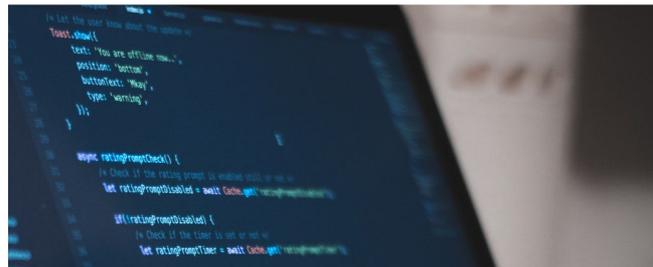
- 监控生命周期管控
- 对象创建&销毁自动化
- 告警规则继承
- 个性化监控项继承
- 权限继承

# 04

## 智能报警中心建设

智能化管理，告警收敛

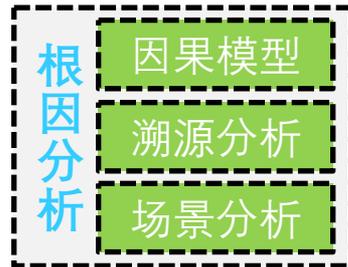
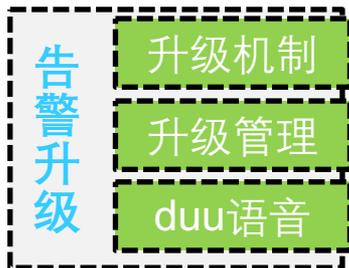
告警，不唯是告警  
告警，不止于送达  
告警，仅仅是开始



# 智能报警中心建设-总览



## 全生命周期智能化管理



# 智能报警中心建设-智能收敛

## 提升告警精准性，预减少告警量

80%的告警会引发其依赖节点的衍生告警，如何发现告警传播链，聚焦根源告警，抑制关联性告警，至关重要。



### 时间相关性

以时间为锚点，聚合窗口内告警信息



### 链路相关性

追溯告警节点上下游，根据公约节点权比系数，进行根因收敛，聚合次生告警



### 收敛规则

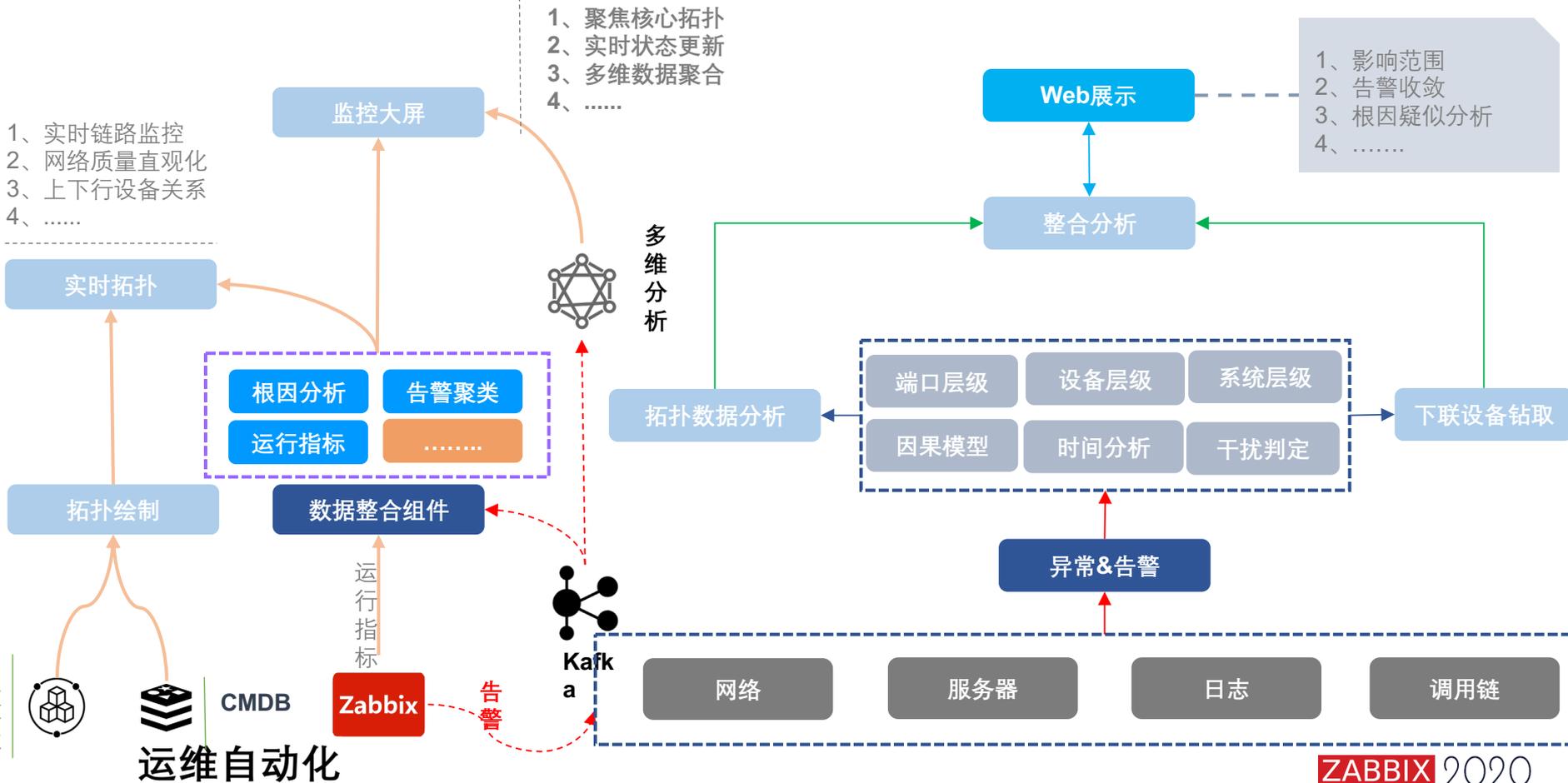
用户可订阅告警规则，根据系统、宿主机、机房等维度，自定义告警聚合规则



### 静默告警

根据用户的告警静默配置，自动屏蔽静默区间内告警

# 智能报警中心建设-智能收敛分析



# 智能报警中心建设-收敛分析架构

UI

概览

事件数量

告警数量

Situation数量

Situation

根因展示

告警展示

事件时间线展示

拓扑展示

局部DU拓扑

局部IP逻辑拓扑

局部垂直拓扑

Pipeline

Cookbook配置

时间关联规则配置

事件过滤规则配置

拓扑关联规则配置

Situation构建及管理

事件预处理

Situation构建

Situation管理

根因分析

因果推理

告警收敛

数据源

事件

ZABBIX

ARES

拓扑

DU 拓扑

IP 拓扑

物理机&虚拟机映射

共物理机虚拟机映射

因果模型

水平因果模型

垂直因果模型

事件辅助信息

事件词库

事件类型库

# 智能报警中心建设-收敛分析过程

Situation展示

局部拓扑展示

告警分析

事件预处理

原始事件过滤

信息提取

原始事件分词

事件属性构建

Situation构建

Situation属性构建/更新

Situation事件映射

Situation管理

Situation active

Situation存储

Situation inactive

根因分析

因果变量构建

告警收敛

因果推理

Kafka

事件源

ZABBIX

ARES

告警事件数据

Situation中告警事件

ES

Cookbook数据

时间/拓扑关联规则

Mysql

拓扑数据/因果模型

DU调用拓扑  
IP 逻辑拓扑  
因果图

Neo4j

Situation数据

Situation/事件属性

词库 告警类型库

因果变量 垂直映射

Red Conference

CHINA

ZABBIX 2020

# 智能报警中心建设-收敛分析过程

## 1、构建图

图中的节点为系统组件和告警，边为组件和组件间，组件和告警间的依存关系

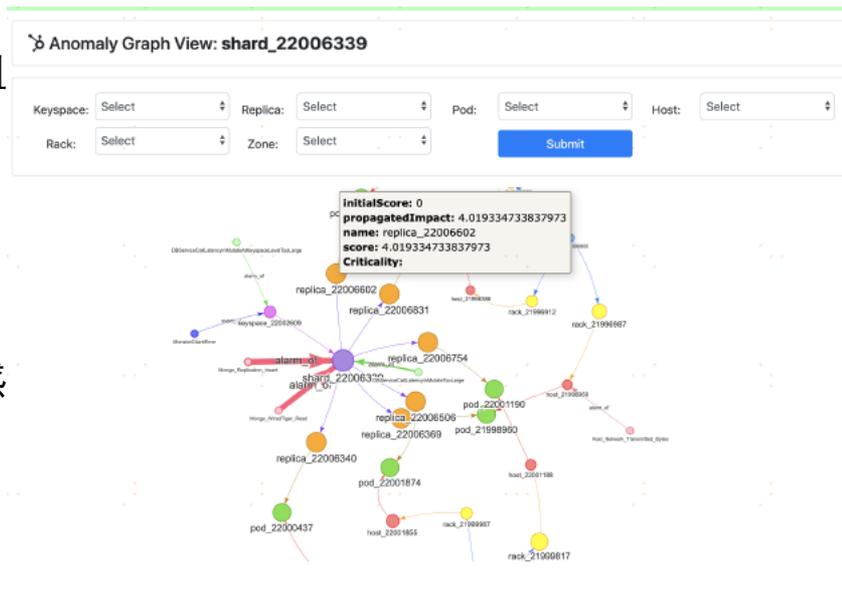
## 2、告警边得分计算

根据告警级别及时间通过指数平滑计算每个告警的敏感度

$$\sigma_{e(a,c)}^0 = x_0$$
$$\sigma_{e(a,c)}^t = \alpha x_t + (1 - \alpha)\sigma_{e(a,c)}^{t-1} (t > 0)$$

根据告警在所有组件及关联组件的频次计算边的最终得分

$$s_{e(a,c)} = \sigma_{e(a,c)} \log\left(\frac{|C|}{|C_a|}\right)$$



# 智能报警中心建设-收敛分析过程

## 3、组件节点得分计算

计算该组件关联的所有告警边加权得分

$$cs_c = \sum_{a \in A_c} \rho_a s_{e(a,c)}$$

## 4、得分传播

根据组件节点及其周边有告警关联的组件计算组件的传播得分

$$p_c = \begin{cases} \beta cs_c & \text{if } |V_c| = 1 \\ \gamma \frac{\sum_{\hat{c} \in V_c} cs_{\hat{c}}}{|V_c|} & \text{if } |V_c| > 1 \end{cases}$$

# 智能报警中心建设-总结

## 智能报警中心

智能报警中心：实现告警的全生命周期闭环管理，确保告警及时响应，及时处理，及时关闭，告警全、快、精准的基础上，通过智能化的分析，提升告警处理效率，快速定位问题。



### 全自动

- 监控&告警流程自动化
- 无人值守

### 精准快

- 告警链路优化，提升告警触达时效
- 核心指标快速触达

### 闭环

- 告警全周期管控
- 提供普适化的告警管理机制.

### 智能

- 告警聚合收敛
- 根因分析

# 联系我们

Contact us

Zabbix 中国致力于为国内用户提供培训、咨询、以及其他的专业技术支持。也为国内的用户搭建交流学习的平台。



138-1772-0274



china@zabbix.com



www.grandage.cn  
www.zabbix.com/cn



上海市徐汇区虹梅路1905号



Zabbix开源社区



Zabbix中国



Zabbix\_China



Zabbix\_team



Zabbix 开源社区



加入技术交流群

ZABBIX 2020  
Conference  
CHINA

THANK 😊  
YOU

