ZABBIX 2020 Conference CHINA

苏宁易购 30th SUNING 苏宁科技

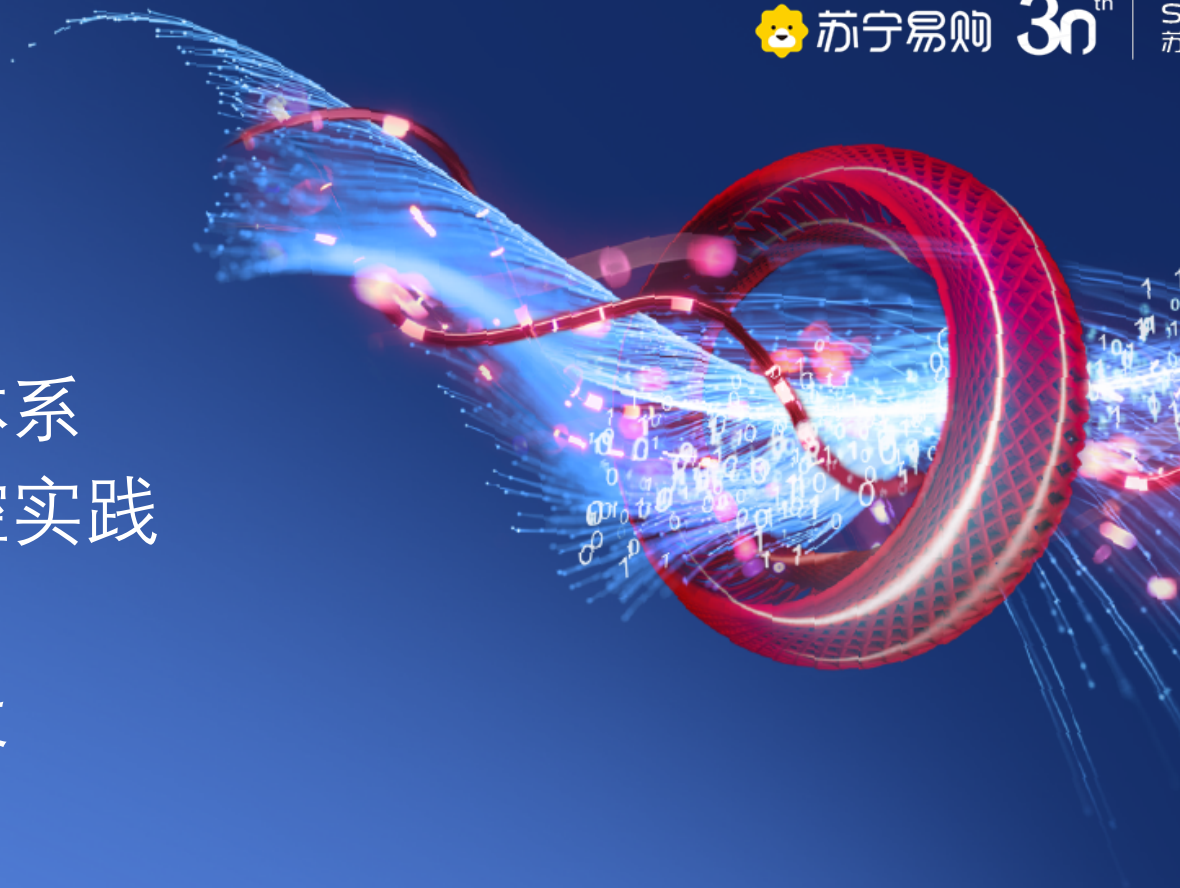
演讲主题

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

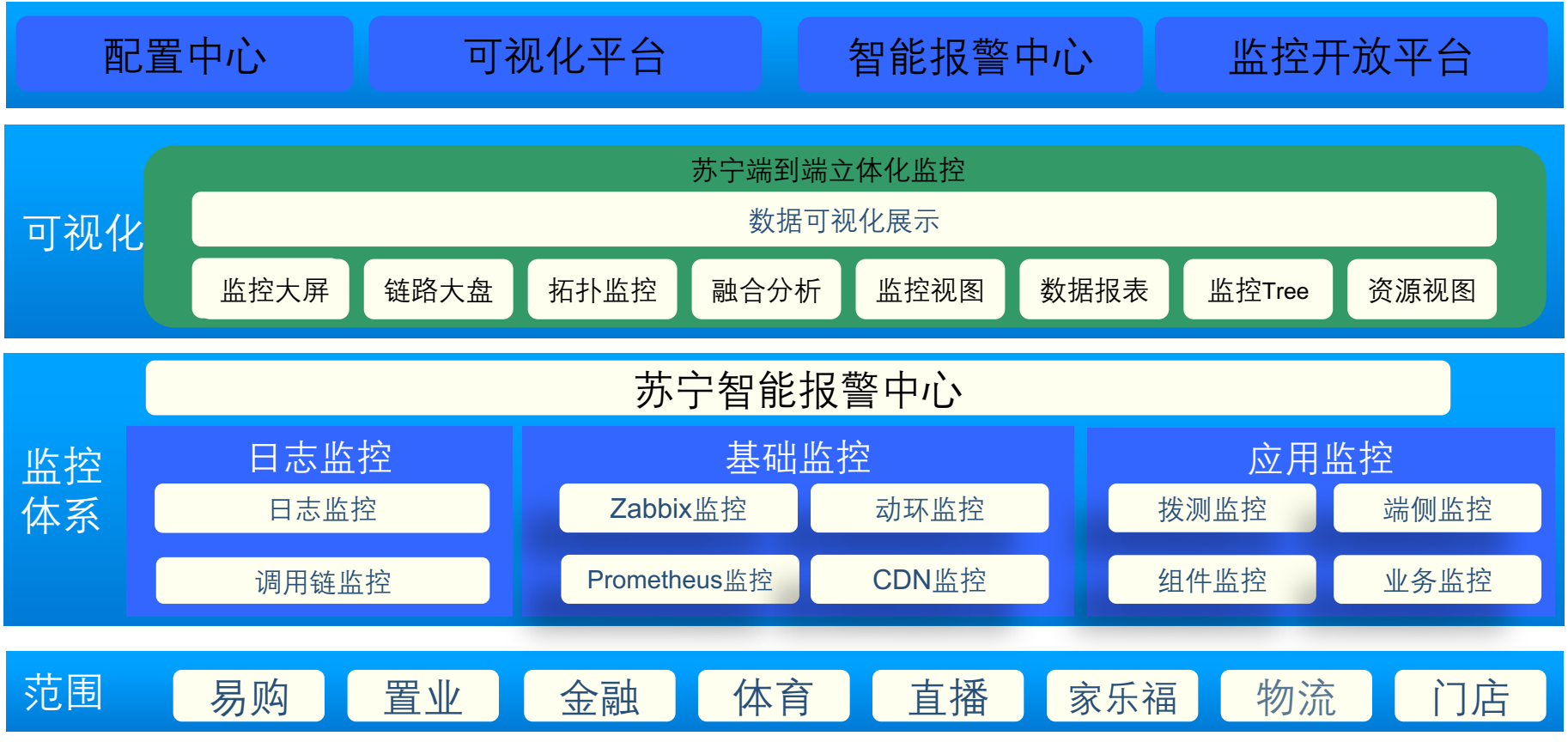
数据

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

苏宁立体化监控体系-体系概览



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

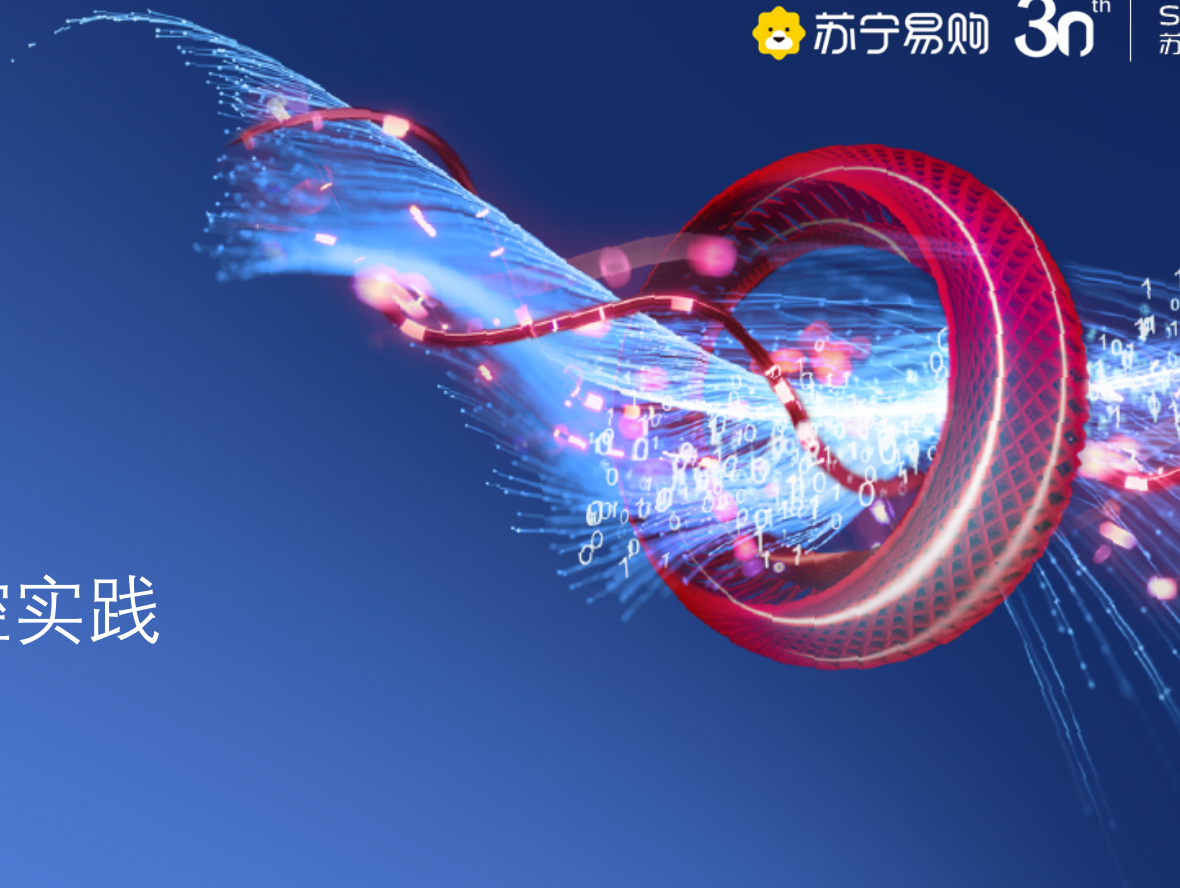
集群服务监控

- 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

苏宁易购 30th



02

Zabbix大规模监控实践

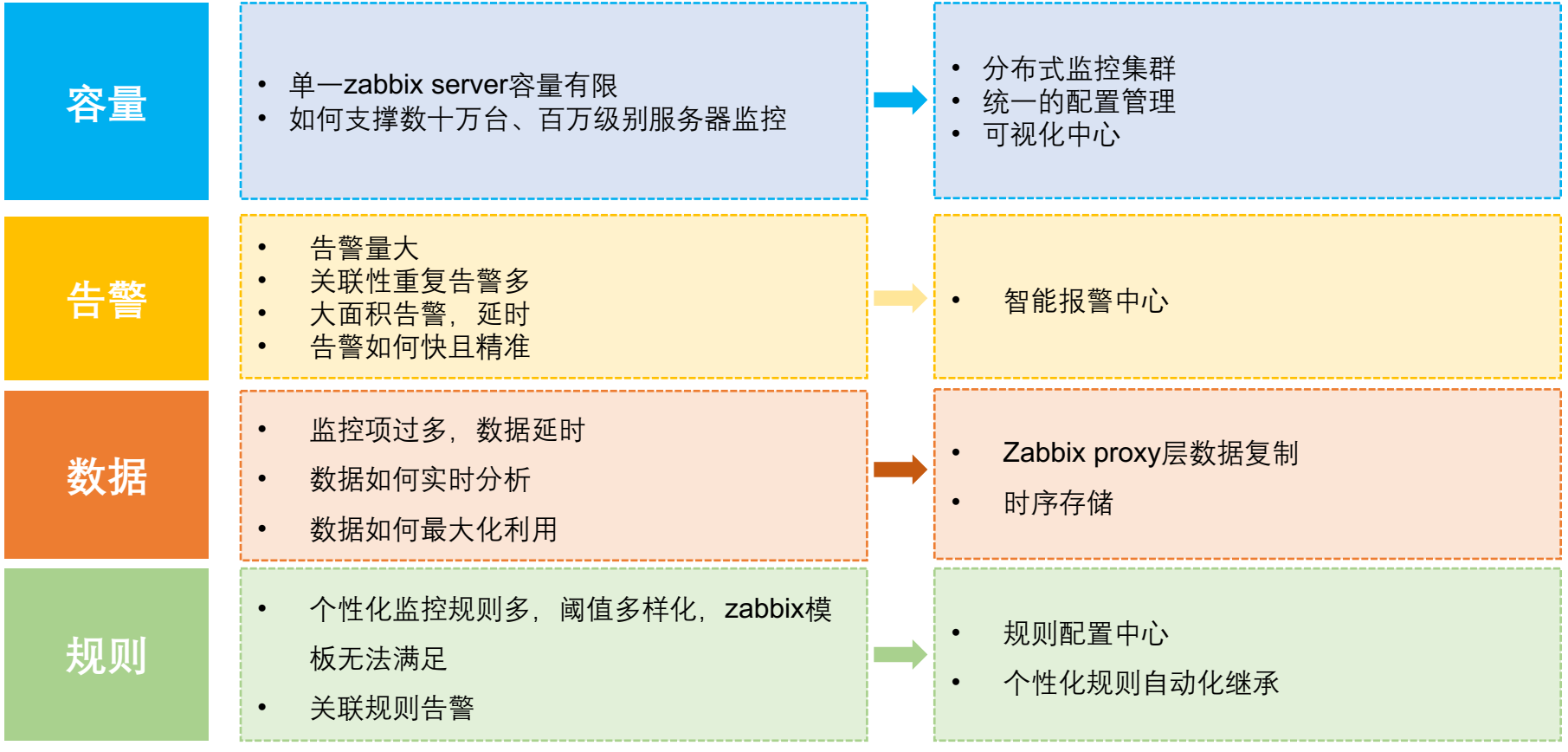
监控范围，困难与挑战，部署架构

ZABBIX 2020 Conference CHINA

Zabbix大规模监控实践-监控范围

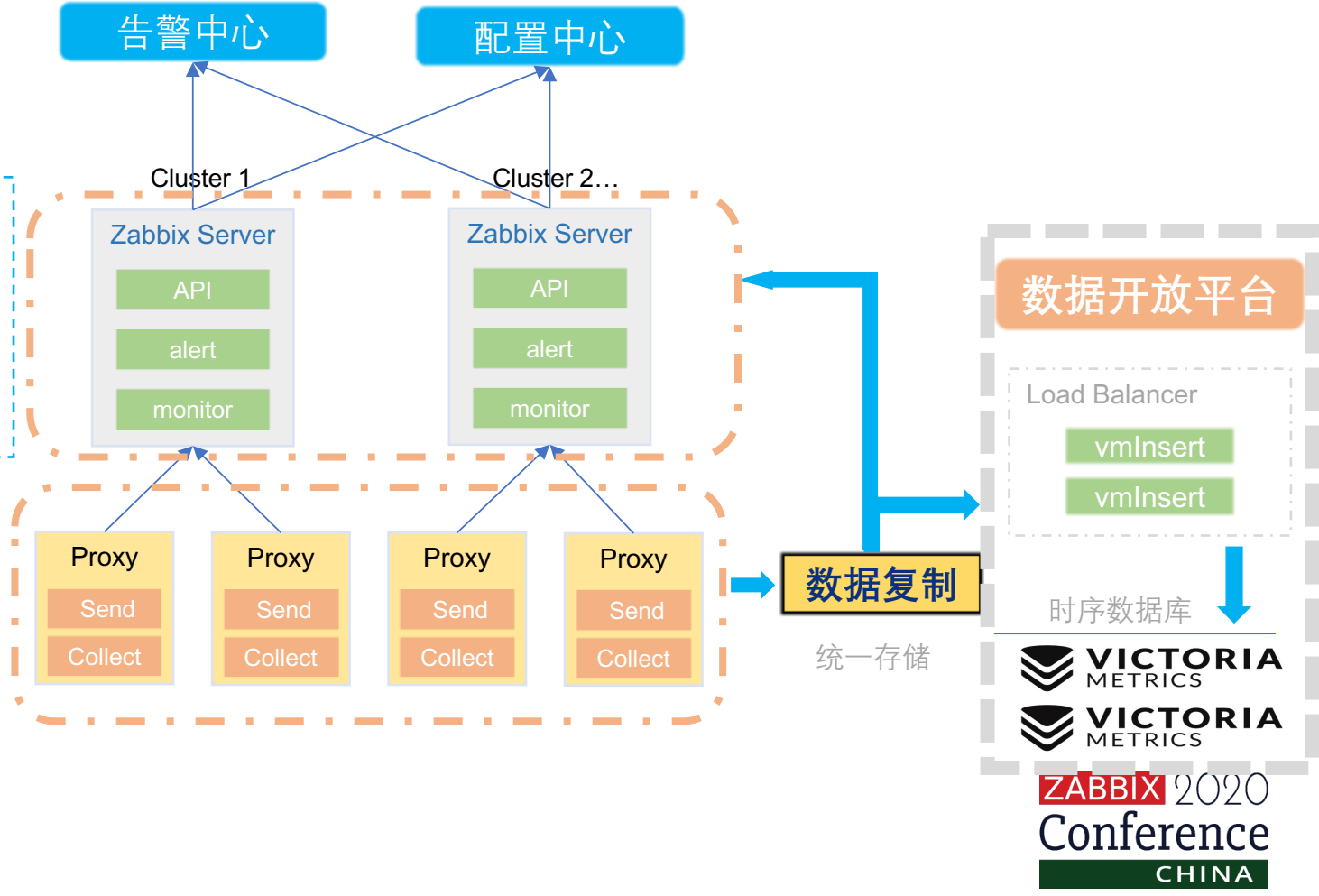
网络	服务器	操作系统	中间件	数据库	应用系统
• 交换机	• 物理服务器	• Windows	• WildFly	• Mysql	• URL检活
• 负载均衡	• 虚拟机	• RHEL	• Nginx	• DB2	• 状态
• 防火墙	• 硬件指标	• SUSE	• Suengine	• Oracle	• 接口
• 路由器	• openstack	• IBM AIX	• Redis	• Sybase	• 健康指标
• 虚拟网络		• CentOs	• Apache	• Mycat	
				• PG	
				• SQL Server	

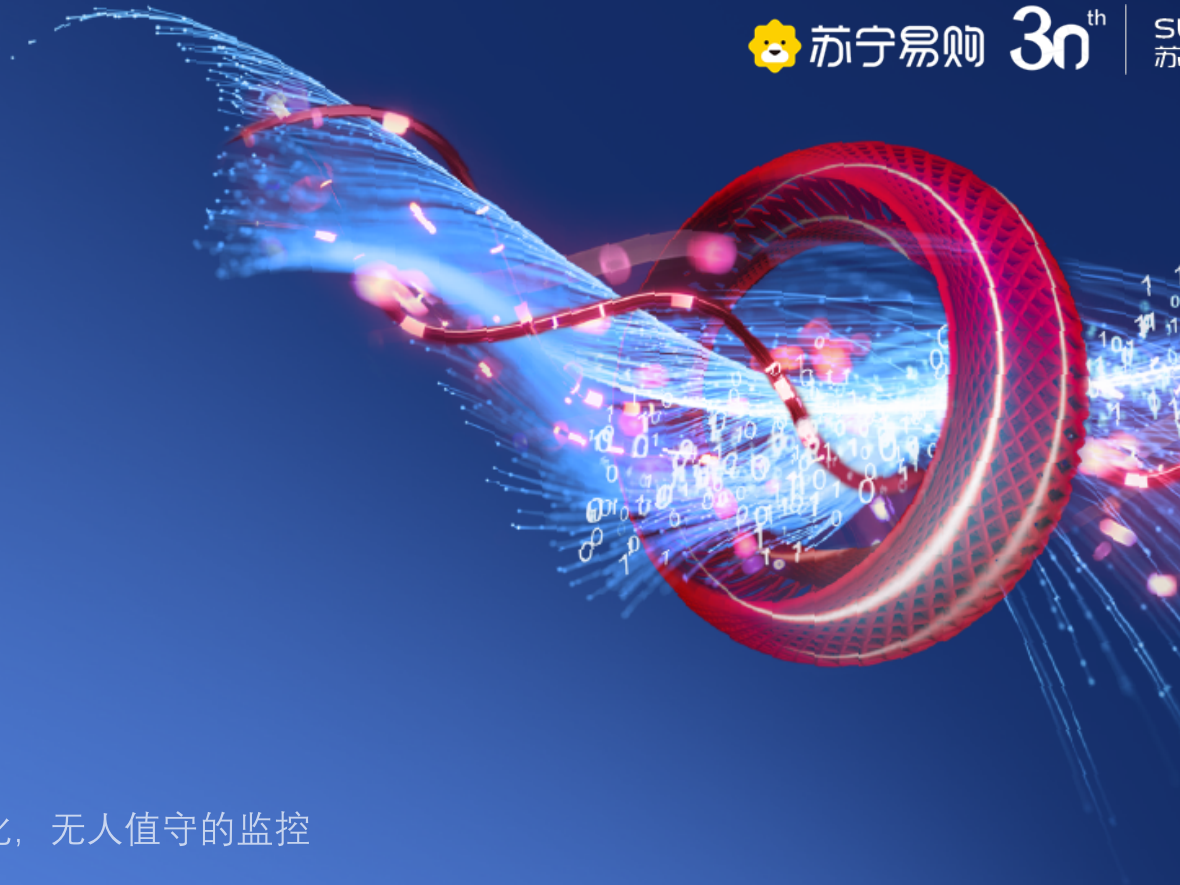
Zabbix大规模监控实践-挑战



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

ZABBIX 2020 Conference CHINA

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

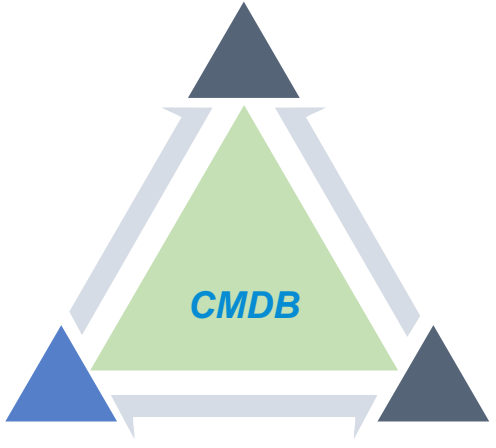
监控告警自动化-总结

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

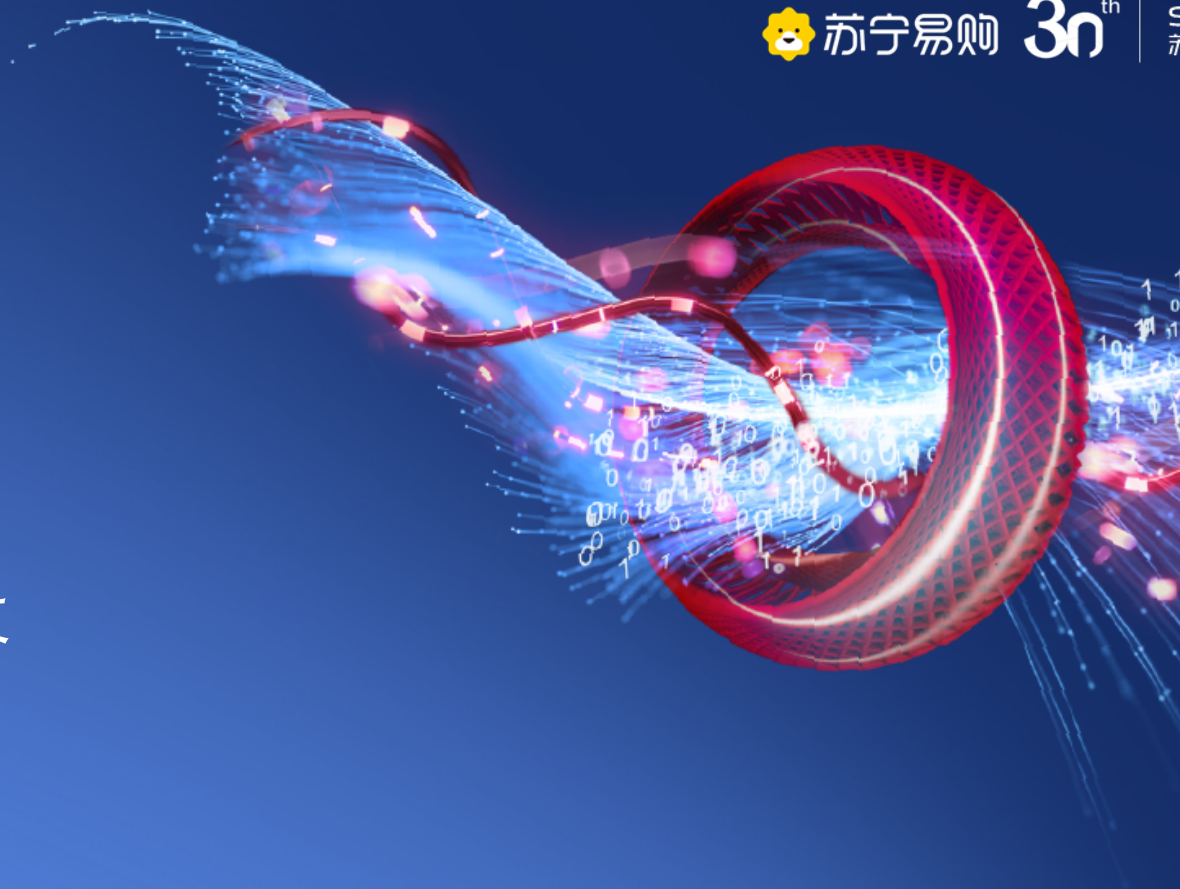
- 告警规则继承
- 个性化监控项继承
- 权限继承

苏宁易购 30th

04

智能报警中心建设

智能化管理，告警收敛

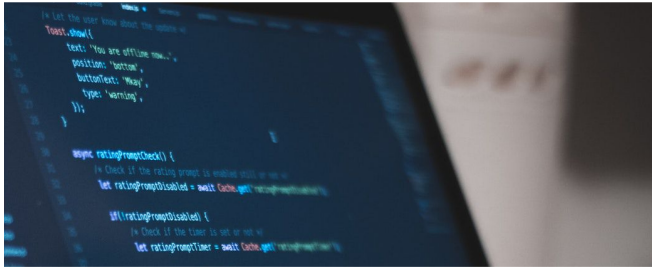


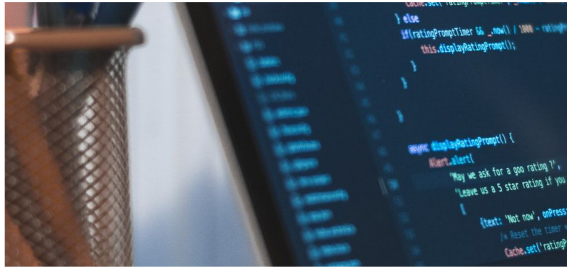
ZABBIX 2020 Conference CHINA

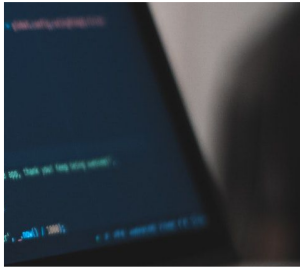
告警，不唯是告警

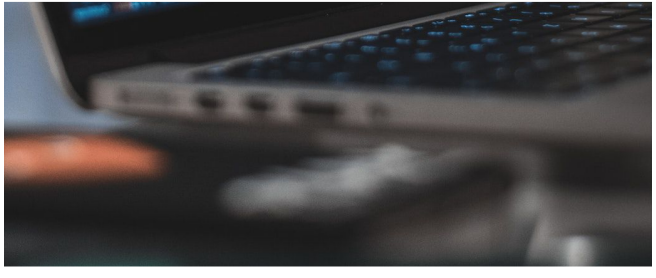
告警，不止于送达

告警，仅仅是开始

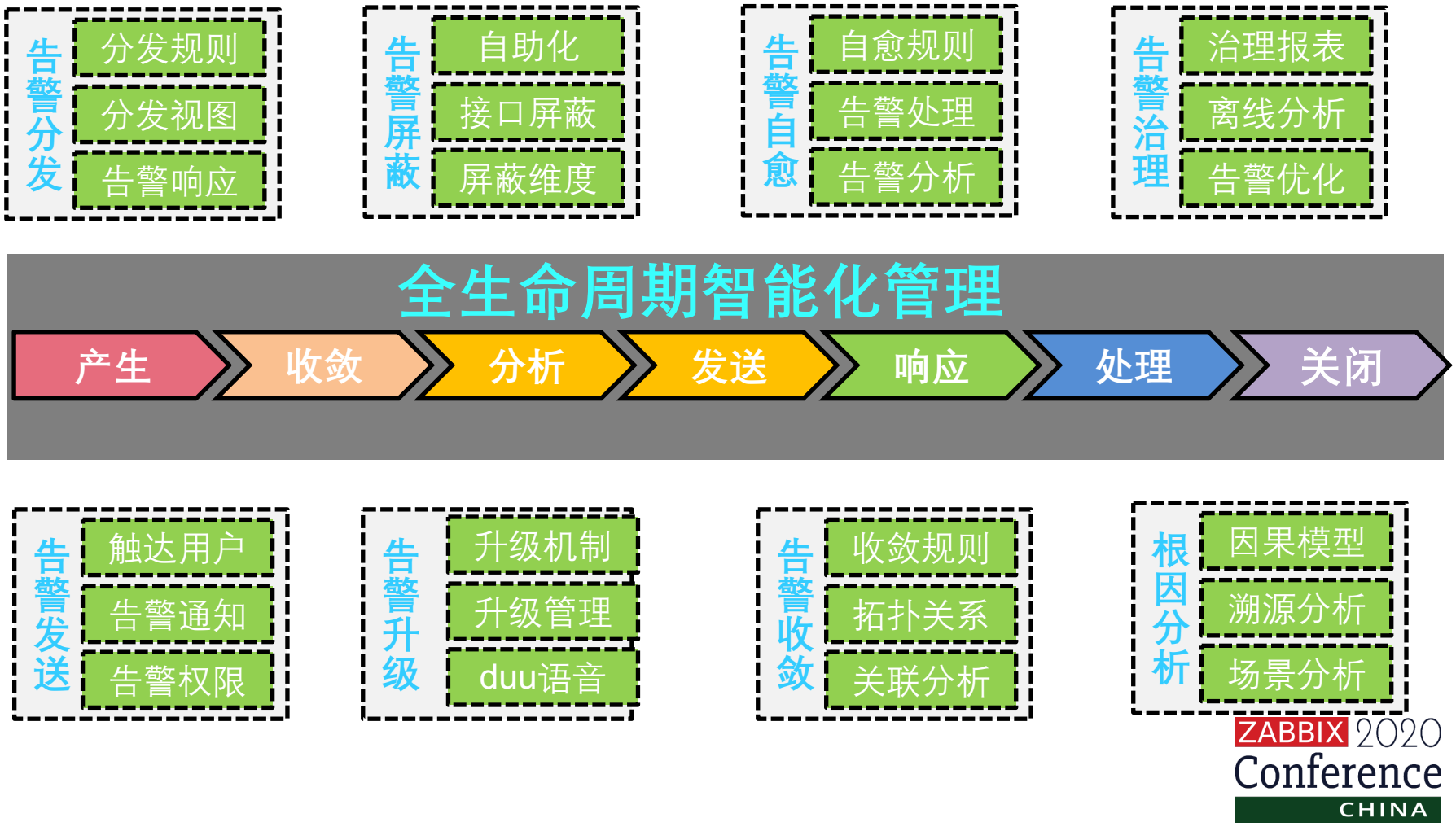








智能报警中心建设-总览



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

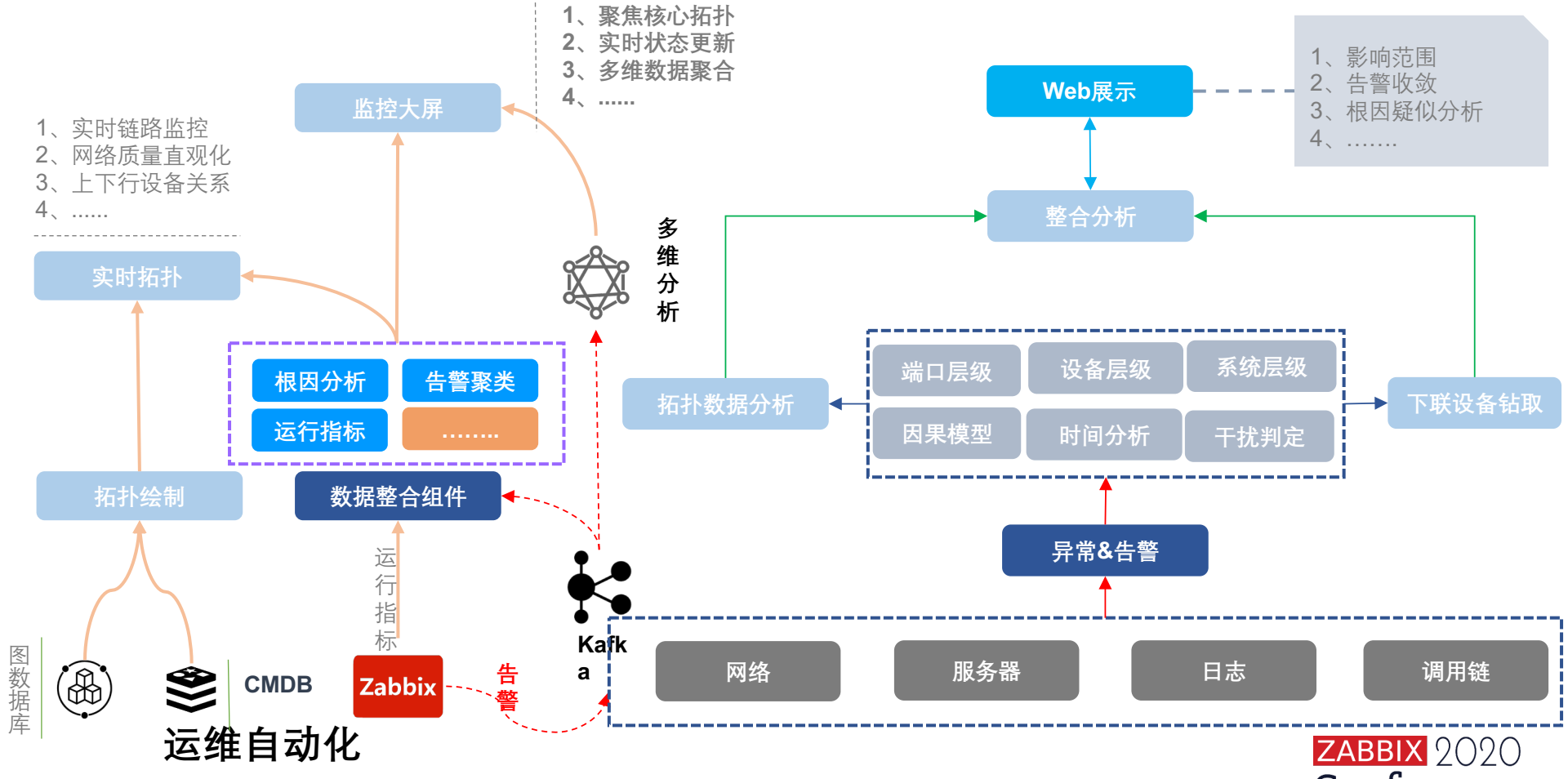
收敛规则

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

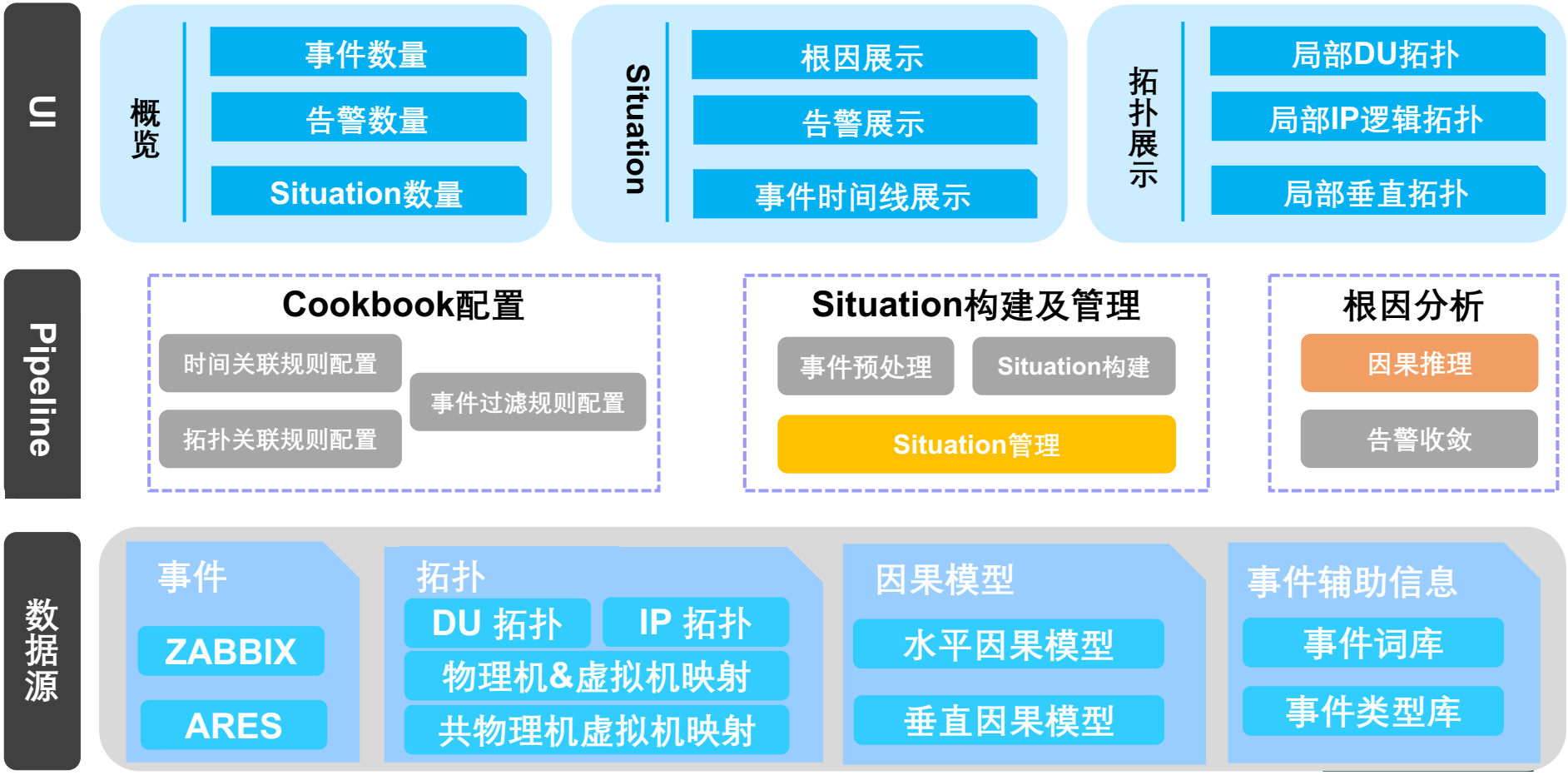
静默告警

根据用户的告警静默配置，自动屏蔽静默区间内告警

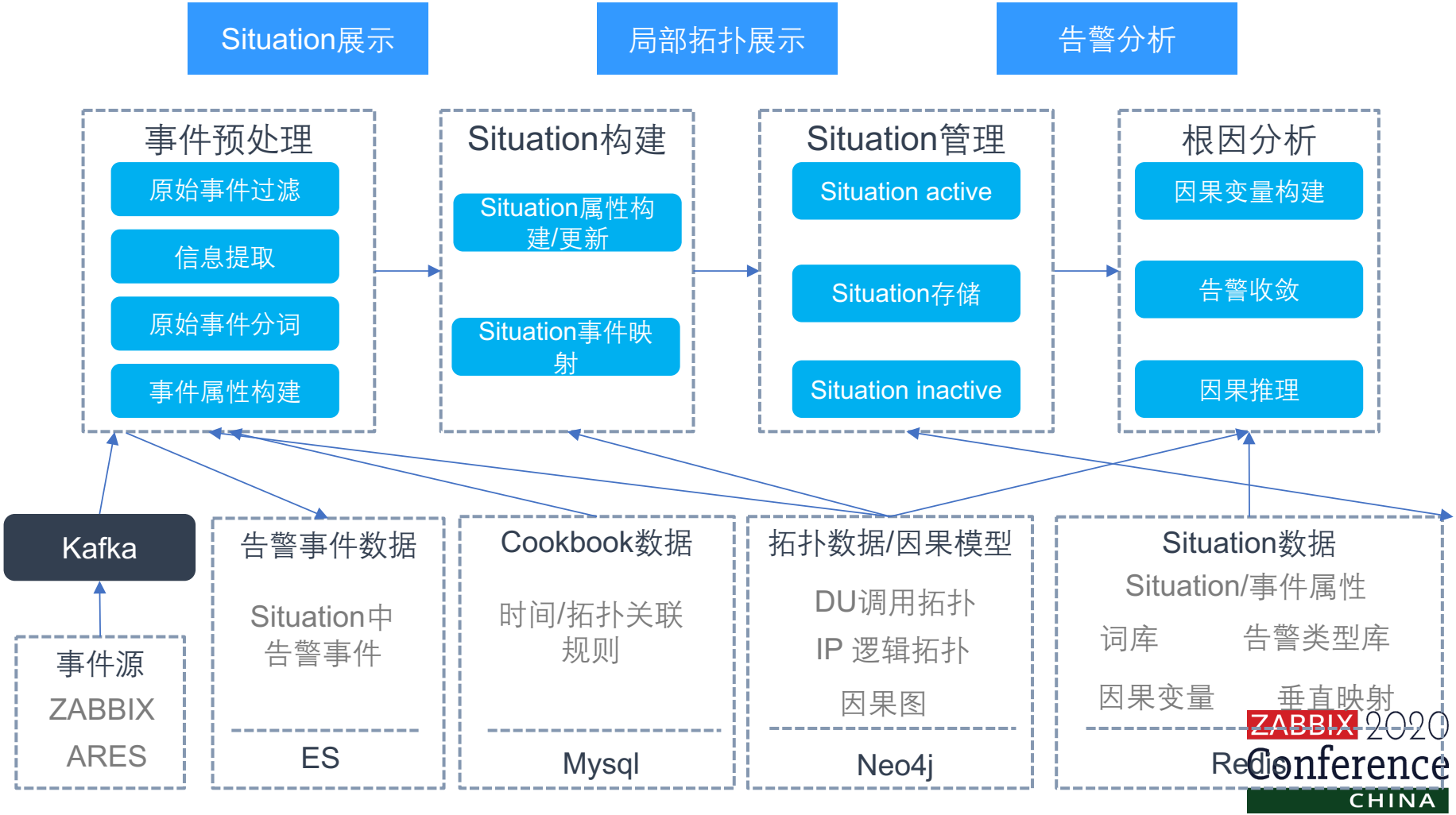
智能报警中心建设-智能收敛分析



智能报警中心建设-收敛分析架构



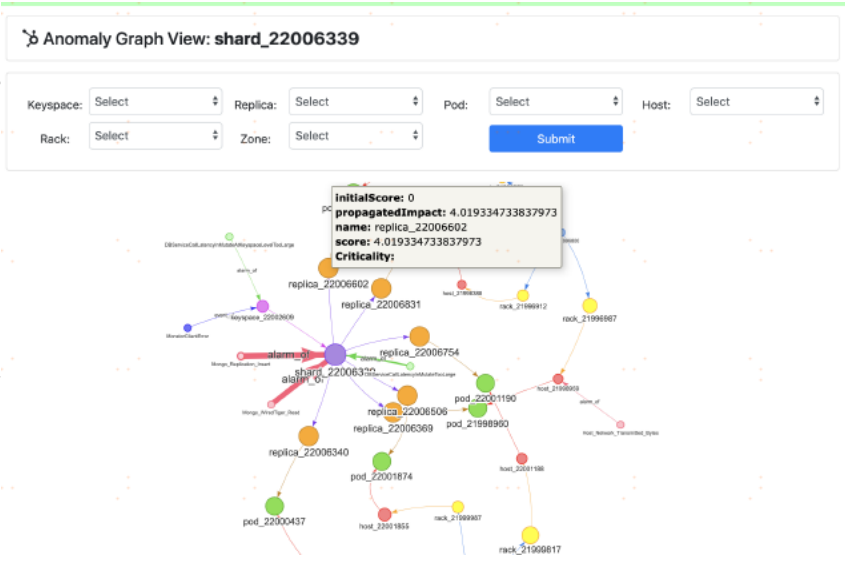
智能报警中心建设-收敛分析过程



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

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

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

$$s_{e(a,c)} = \sigma_{e(a,c)} \log(\frac{|\mathbf{C}|}{|\mathbb{C}_a|})$$

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

$$\mathbf{cs}_c = \sum_{a \in \mathbb{A}_c} \rho_a \mathbf{s}_{e(a,c)}$$

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

$$\mathbf{p}_c = \begin{cases} \beta \mathbf{cs}_c & \text{if } |\mathbb{V}_c| = 1 \\ \gamma \frac{\sum_{\hat{c} \in \mathbb{V}_c} \mathbf{cs}_{\hat{c}}}{|\mathbb{V}_c|} & \text{if } |\mathbb{V}_c| > 1 \end{cases}$$

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