

如何在 Zabbix 中玩转 智能告警

ZABBIX 2019
Conference



何毅鹏

CTO 睿象云

运维危险预警

瞬时用户量访问急剧增大

网站访问延时增高

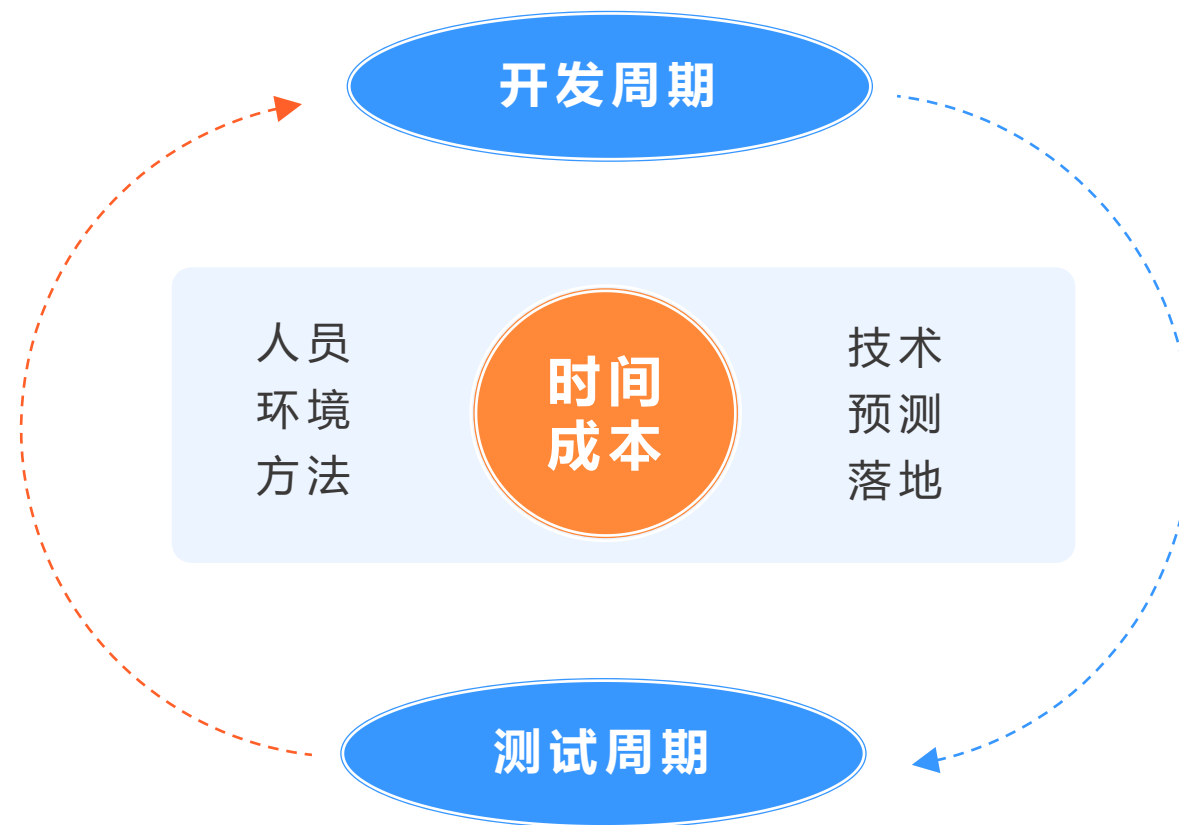
系统非常容易过载

服务端流量高

系统资源占用高



宏观根因分析



微观问题梳理



测试环境和
生产环境如何管理



影响线上性能
因素如何分析



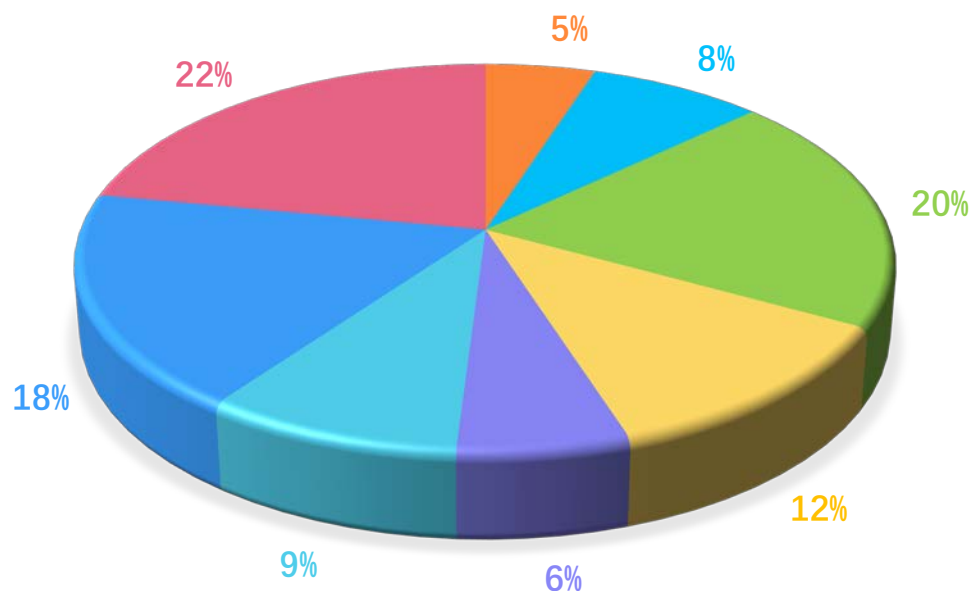
测试数据如何准备
生产数据如何清洗



测试关键指标
如何监控



影响线上性能因素分析



网络带宽
网络质量
BGP节点

5%

静态资源缓存
JS位置合理性
图片Flash视频大小

6%

DNS解析速度
静态资源CDN
视频资源CDN

8%

应用缓存
数据库缓存
缓存技术架构合理性

9%

负载均衡配置
防火墙策略
网络参数配置

20%

数据库配置
数据库读写分离技术
缓慢SQL语句

18%

主机硬件配置
主机参数配置
主机网络配置

12%

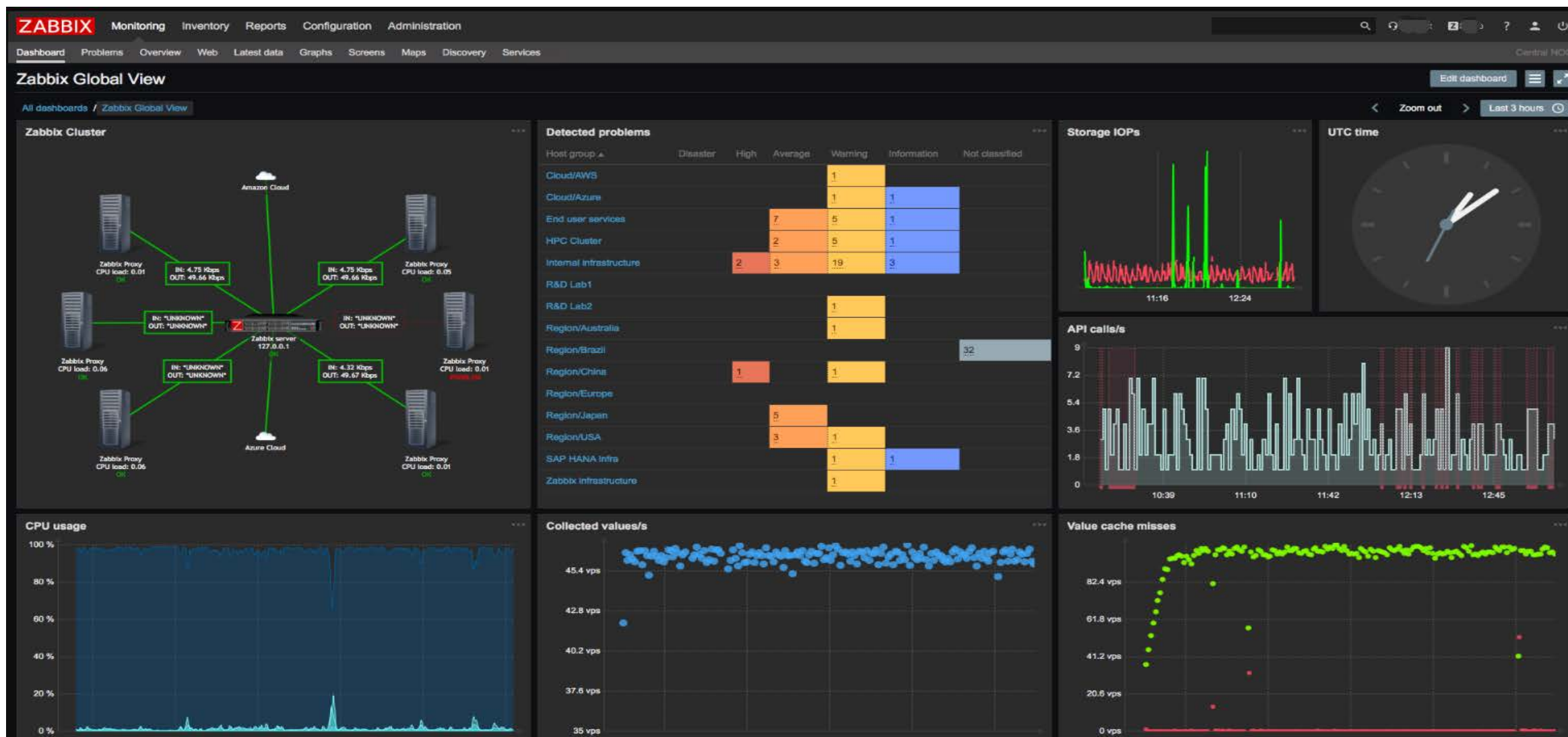
应用逻辑结构
应用参数配置
缓慢代码算法优化

22%

优化之路

- CDN系统 (第三方服务)
- 负载均衡系统 (Haproxy、LVS、Nginx、SLB)
- Web服务器/应用服务器 (PHP、Tomcat、Resin)
- 消息队列系统 (RabbitMQ、kafka、NSQ)
- 对象缓存系统 (Redis、Memcached、CouchBase)
- 数据库系统 (MySQL、MongoDB、ES)
- 运维支撑系统 (Zabbix)
- 日志采集分析系统 (ELK、Graylog、Loginsight)
- 服务器虚拟化 (Docker、Rancher)

Zabbix监控界面



再强大的工具
也会有短板

01

告警风暴的抑制能力

02

混合型多工具的告警接入

03

告警内容的快速分析

04

多渠道精准通知

05

告警流程的智能管理

为什么告警管理如此重要？



时间

告警每延迟**1**分钟，故障恢复时间将延迟**10-30**分钟



问题

每次告警风暴平均每分钟产生**100-1000**条告警



信息

每条告警平均与**5-10**个其他指标相关联



告警管理

人员

每个故障处理的平均参与人员为**5-8**人



过程

每个告警处理过程平均至少需要流转**2**次

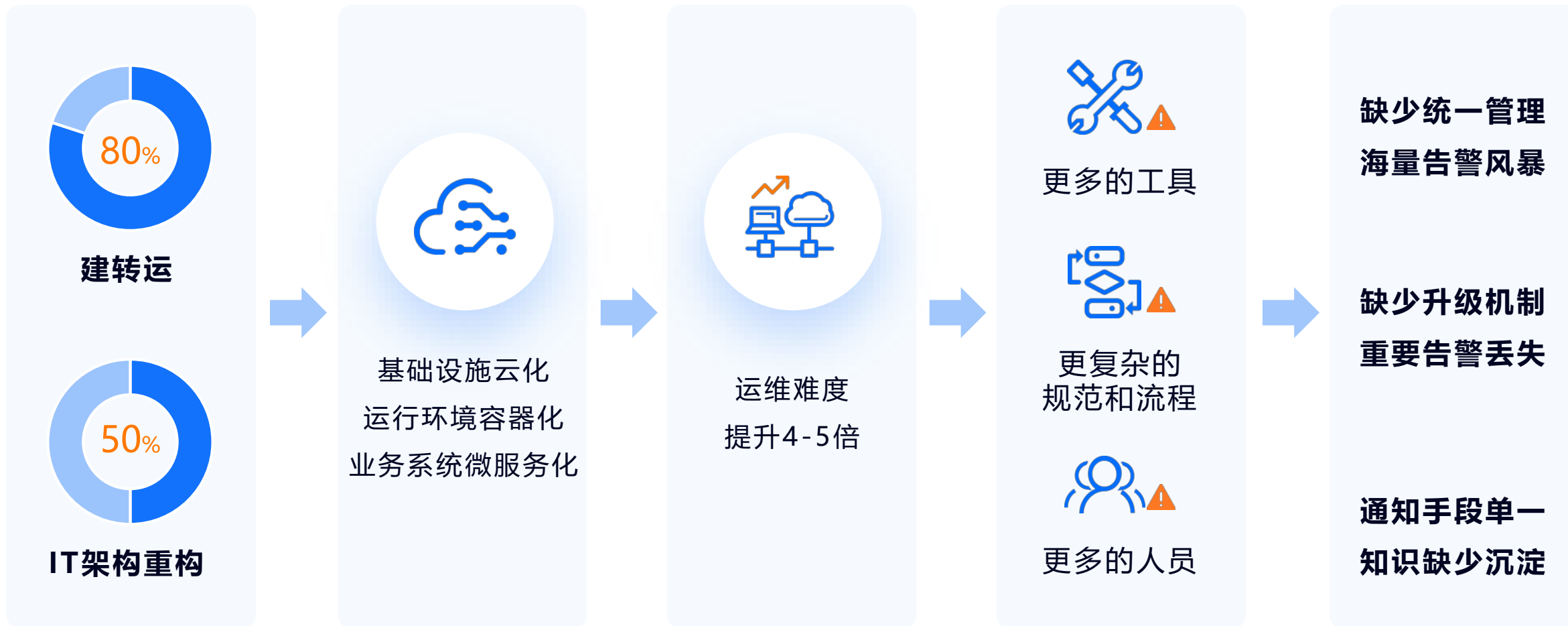


知识

每次故障排查需要花费**1-2**小时寻找过往经验



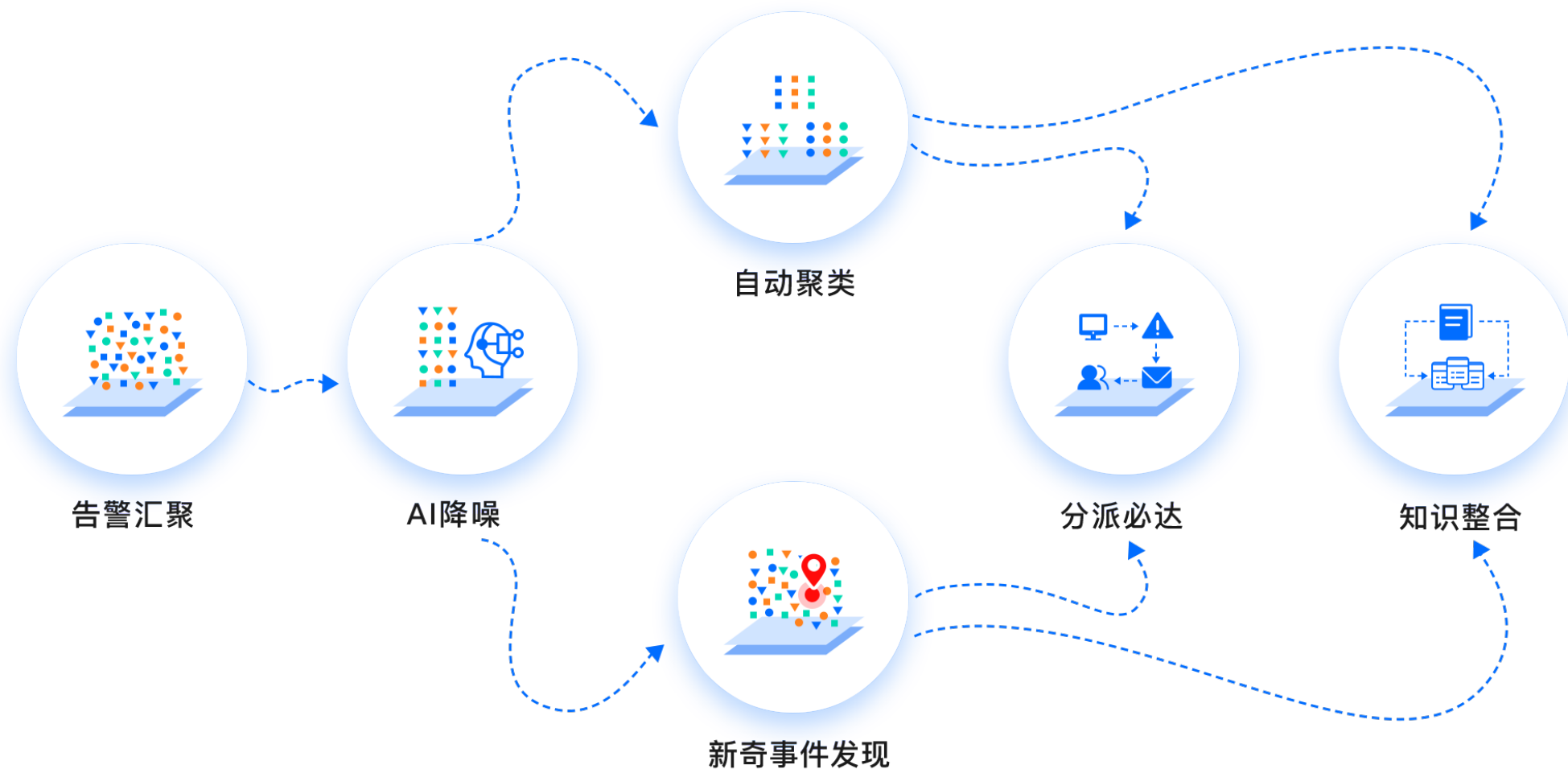
告警管理面临的挑战



如何快速搭建统一的告警管理平台?



智能告警平台 Cloud Alert 告警数据处理



告警汇聚 快速接入告警数据

- 通过配置即可对接主流监控工具/平台告警
- 通过 REST API 接入
- 通过 Email 接入

The screenshot shows the ZABBIX Cloud Alert (CA) interface. The top navigation bar includes 'CA Cloud Alert', '首页', '告警', '集成', '分析', and '配置'. The main content area is titled 'ChatOps工具' and displays a grid of integration options categorized by type: '企业级监控' (Enterprise Monitoring), '性能监控' (Performance Monitoring), '可视化工具' (Visualization Tools), '虚拟化工具' (Virtualization Tools), '云监控' (Cloud Monitoring), '网络监控' (Network Monitoring), and '通用集成' (General Integration). Each category contains several integration cards with logos and a plus sign, indicating they can be added. Below the grid is a table listing the configured integrations.

<input type="checkbox"/>	序号	状态	应用名称	类型	appkey	自动关闭	分派策略	操作
<input type="checkbox"/>	1	●	安全次数验证nagios	nagios	faf8e46b-c336-f1ae-a28d-8c86330c91e2	31 分钟	点击查看	
<input type="checkbox"/>	2	●	安全次数验证oneapm	AI	2a94df86-b41e-537e-8393-588bb9184b40	22 分钟	点击查看	
<input type="checkbox"/>	3	●	安全次数验证prometheu	prometheus	444d660d-93f2-8e5f-5057-00ae2e65af30	30 分钟	点击查看	
<input type="checkbox"/>	4	●	安全次数验证阿里云	ali	6ad28bb3-761c-cd5a-75ce-b343d25fca46	30 分钟	点击查看	
<input type="checkbox"/>	5	●	安全次数验证falcon	falcon	252c7b56-629a-ae8c-3f8e-2a8150dd60c1	30 分钟	点击查看	
<input type="checkbox"/>	6	●	API TEST(勿删)	api	f49a2c06-56ec-11c8-4f8c-0d55e9e6d4b7	30 分钟	点击查看	

仅需 3 步 轻松接入 ZABBIX

- 第 1 步
切换到 Zabbix 脚本目录
- 第 2 步
获取 Agent 包
- 第 3 步
解压、安装

配置步骤

一、安装 Agent

1、切换到zabbix脚本目录 (如何查看zabbix脚本目录):

```
cd /usr/local/zabbix-server/share/zabbix/alertscripts
```

2、获取Cloud Alert Agent包:

```
wget https://download.aiops.com/ca_agent/zabbix/ca_zabbix_release-2.1.0.tar.gz
```

3、解压、安装。

```
tar -xzf ca_zabbix_release-2.1.0.tar.gz  
cd cloudalert/bin  
bash install.sh --
```


有序分派 不遗漏任何一条告警

制定灵活的分派条件

- 按照告警级别
- 按照告警内容
- 多种组合

制定灵活的人员策略

- 按照用户、组、排班、协作方式进行告警分派
- 设置认领超时，自动升级

The screenshot shows the ZABBIX Cloud Alert (CA) interface. The top navigation bar includes 'CA Cloud Alert', '首页', '告警', '集成', '分析', and '配置'. The main content area is titled '分派策略' (Distribution Strategy) and contains a table of strategies and a configuration panel.

序号	分派名称	关联应用
1	支付与会员, 订单管理, 商品和促销, Checkout	zabbix_app
2	信用卡, 购物车	zabbix_app
3	支付, payments, 购物车, 促销, SLIP	zabbix_app 或 zabbix_app 或 zabbix_app
4	购物车	my_alarm
5	基础运营	Zabbix_Conf
6	支付和订单_checkout	zabbix_app
7	支付和, VPS, 支付和, 支付和运营	zabbix_app
8	购物车, 购物车	zabbix_app
9	购物车, 支付, 支付, 支付, 支付	zabbix_app
10	支付, 支付, 支付, 支付	zabbix_app 或 zabbix_app 或 zabbix_app

The configuration panel for the selected strategy (row 7) shows the following settings:

- 分派条件 (Distribution Conditions):**
 - 或 (OR) zabbix_app
 - 且 (AND) 告警级别 (Alert Level) 在列表中 (In List) 严重 (Critical)
 - 且 (AND) hostgroups 在列表中 (In List) VG:zabbix Dept:PC:zabbix/develop Dept:PC
- 分派人 (Assignees):**
 - 立即 (Immediate):** 告警发生后, 立刻通知以下用户 (After alert, immediately notify the following users). Includes a search field for users.
 - 升级 (Escalation):** 如果告警从发生 30 分钟无人认领, 则告警升级分派给以下用户 (If no one claims the alert within 30 minutes of occurrence, the alert will be escalated and assigned to the following users). Includes a search field for users.

多种通知方式 提升告警到达率

灵活的通知策略

- 告警状态
- 通知时间
- 告警级别
- 延迟策略
- 通知方式
- 人员

The screenshot shows the 'CA Cloud Alert' configuration page. The '通知策略' (Notification Strategy) tab is active. The '新建通知策略' (New Notification Strategy) form includes the following settings:

- 告警状态 (Alert Status):** 发生时 (checked), 认领时 (checked), 关闭时 (checked), 全选 (checked).
- 告警级别 (Alert Level):** 提醒 (checked), 警告 (checked), 严重 (checked), 所有 (checked).
- 通知方式 (Notification Method):** 电话 (checked), 短信 (checked), 邮件 (checked), 微信 (checked).
- 时间设置 (Time Settings):** 任何时间 (selected), 工作时间, 非工作时间.
- 延迟策略 (Delay Strategy):** 立刻 (selected).
- 通知人 (Notification Person):** 何毅鹏, 李欣, 王宏伟 (all selected).

Below the form is a table of existing notification objects:

序号	通知对象	操作
> 1	何毅鹏	删除
> 2	刘源利	删除
> 3	葛福刚	删除
> 4	姜宇航	删除
> 5	郭晓雷	删除
> 6	董晓雷	删除

排班管理 制定专属告警响应机制

可视化排班管理

- 根据实际场景可按日、周、自定义周期排班，
- 自定义排班工作时间，严格划分工作时间与非工作时间
- 日历视图直观预览排班效果

CA Cloud Alert

首页 告警 集成 分析 配置

分派策略 通知策略 排班管理 压缩规则 团队管理 授权管理

新增排班

网络组_一线支持

分组1

增加值班人员

请选择

1. 何毅鹏

1. 刘远利

1. 李欣

设置排班周期

日

交班时间

00:00

排班时间

周一 周日 00:00 23:30

设置生效开始时间

2019-05-17 00:00

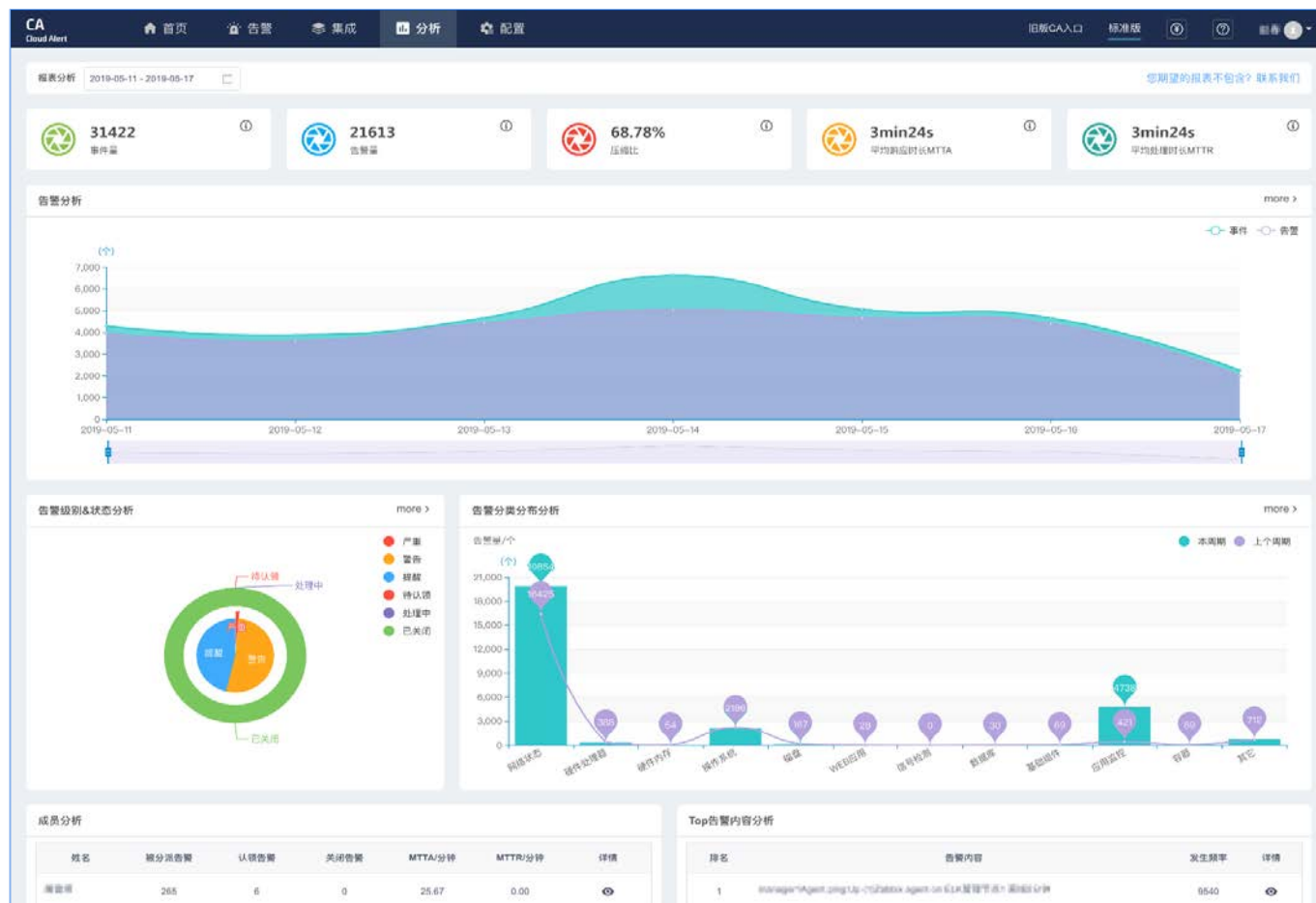
2019年 五月

周一	周二	周三	周四	周五	周六	周日
29	30	1	2	3	4	
6	7	8	9	10	11	
13	14	15	16	17	18	
				00:00 何毅鹏	00:00 刘远利	00:00 李欣
20	21	22	23	24	25	
00:00 何毅鹏	00:00 刘远利	00:00 李欣	00:00 何毅鹏	00:00 刘远利	00:00 李欣	00:00 何毅鹏
27	28	29	30	31	1	
00:00 刘远利	00:00 李欣	00:00 何毅鹏	00:00 刘远利	00:00 李欣	00:00 何毅鹏	00:00 刘远利
3	4	5	6	7	8	
00:00 李欣	00:00 何毅鹏	00:00 刘远利	00:00 李欣	00:00 何毅鹏	00:00 刘远利	00:00 李欣

告警回溯 与多维分析

多维度统计和分析报表，
全面掌握系统运行状态

- 历史告警趋势
- 成员工作效率
- 告警Top分析
- 告警智能分类分析



智能告警算法框架

告警应用场景

告警分类

告警降噪

新奇事件发现

异常事件发现

根因定位

自然语言处理

文本分词

词性标注

命名实体识别

词向量

语义相似度

深度学习算法

循环神经网络
RNN

卷积神经网络
CNN

深度神经网络
DNN

双向循环神经网络
LSTM

多层感知机
MLP

词向量
Word2Vec

FastText

BERT

机器学习算法

主题模型
LDA

朴素贝叶斯
Naive Bayes

密度聚类
DBSCAN

频繁项集
FP-Growth

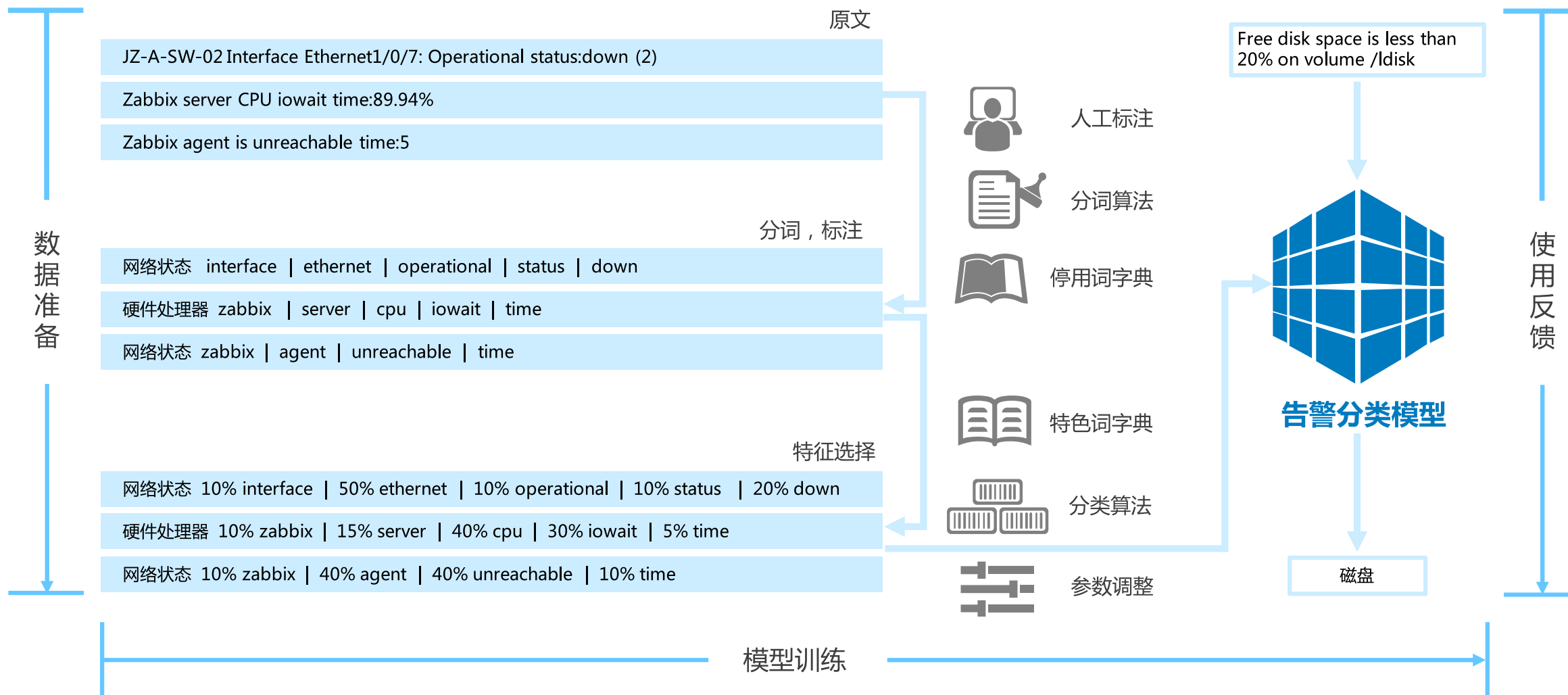
高斯混合
Gaussian Mixture

香农信息熵
Shannon Entropy

支持向量机
SVM

局部敏感Hash

告警智能分类



告警智能降噪 算法效果展示

可选 AI 智能降噪算法，
事中降噪

- 降噪比: 99%



知识整合

通用领域的知识

- 厂商手册、厂商知识库、博客、Stack Overflow等公开来源。需要使用到自然语言的命名实体识别、实体关系分析的一系列的手段进行知识的提取和整理。

企业内部知识

- 企业内部的工单、故障报告、监控数据、配置信息、端口调用信息、业务承载信息等。

Q: 运维知识图谱的最终形态应该是什么?

A: 通过汇聚通用领域知识和企业内部知识, 采用问答的方式完成知识图谱功能的使用。

知识问答 ©

The screenshot shows a search interface with a search bar containing 'HACS切换'. Below the search bar, there are three search results. The first result is titled 'NG3DCC-HA03 HACS切换有问题, 取消主动重启' and includes a brief description, analysis, and preventive measures. The second result is titled 'SUSE PPC 如何解析KDUMP' and includes a list of steps for troubleshooting. The third result is titled 'DGBOSS-ABM13/14 HA回切策略问题' and includes analysis and preventive measures. On the right side of the interface, there is a '热门问题' (Popular Questions) sidebar with a list of 10 items, including 'HACS', '高可用', 'HACS重启', 'HA', 'HACS切换', 'HA 切换', '高可用失效', 'HACS重启失败怎么办', '重启时间长', and 'HACS有问题'.

HACS切换

推荐

NG3DCC-HA03 HACS切换有问题, 取消主动重启

原因分析: HACS切换异常, 华为分析中
故障处理措施:
预防性措施:

点赞 | 收藏 | 分享

SUSE PPC 如何解析KDUMP

问题对象: SUSE PPC 如何解析KDUMP
修复方案: 1、上传rpm包及采集脚本, 放在log机/home/os_admin/kdump_ppc目录下
2、安装rpm包, # rpm -ivh kernel-ppc64-debuginfo-3.0.76-0.11.1.ppc64.rpm
3、拷贝vmlinux-3.0.76-0.11-ppc64.debug及采集脚本到kdump的目录
cd /var/crash/2017-11-12-14/:30/
cp /usr/lib/debug/boot/vmlinux-3.0.76-0.11-ppc64.debug .
cp /home/os_admin/getcoreinfo.sh .
4、解析
./getcoreinfo.sh -f vmlinux-3.0.76-0.11-ppc64.debug vmlinux-3.0.76-0.11-ppc64 vmcore
5、解析后数据生成在/tmp/kdump目录
负责人: 吴泽锦

点赞 | 收藏 | 分享

DGBOSS-ABM13/14 HA回切策略问题

原因分析: Fallback Policy的策略应该为Never Fallback, 现网为Fallback To Higher Priority Node In The List, 当出现备节点启动HA的时候, 会导致节点资源组切换
故障处理措施: 已通知IBM在本月18号的HACMP版本升级中进行修复。
预防性措施: 临时在起HA的时候使用手工模式

热门问题

- 1 HACS
- 2 高可用
- 3 HACS重启
- 4 HA
- 5 HACS切换
- 6 HA 切换
- 7 高可用失效
- 8 HACS重启失败怎么办
- 9 重启时间长
- 10 HACS有问题

数以万家的企业选择了 Cloud Alert

累计接入告警 **2.3亿** 条 每周处理告警 **198万** 条

金融类



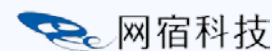
运营商



制造业



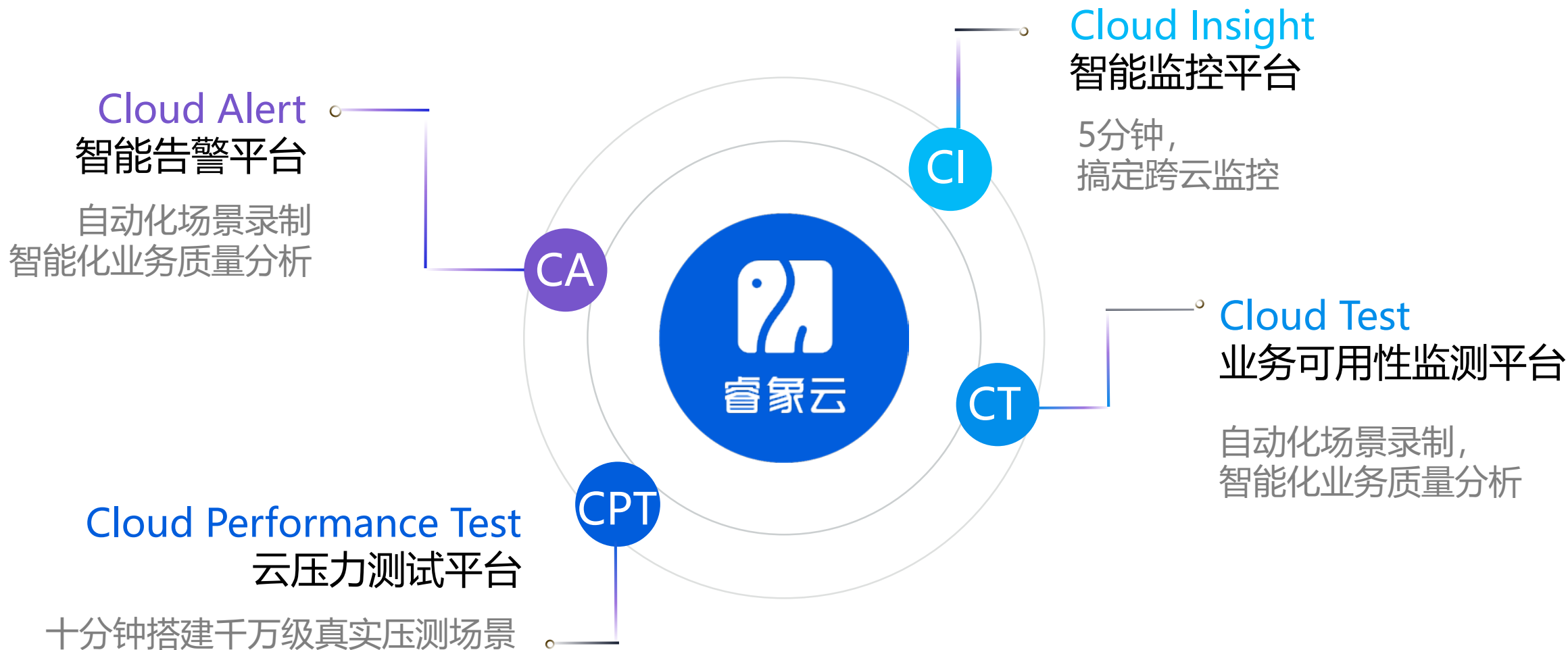
互联网



其它



睿象云还能帮助您 ...





睿象云官网: www.aiops.com

咨询热线: 400-080-9810



Thank You!

ZABBIX 2019
Conference