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

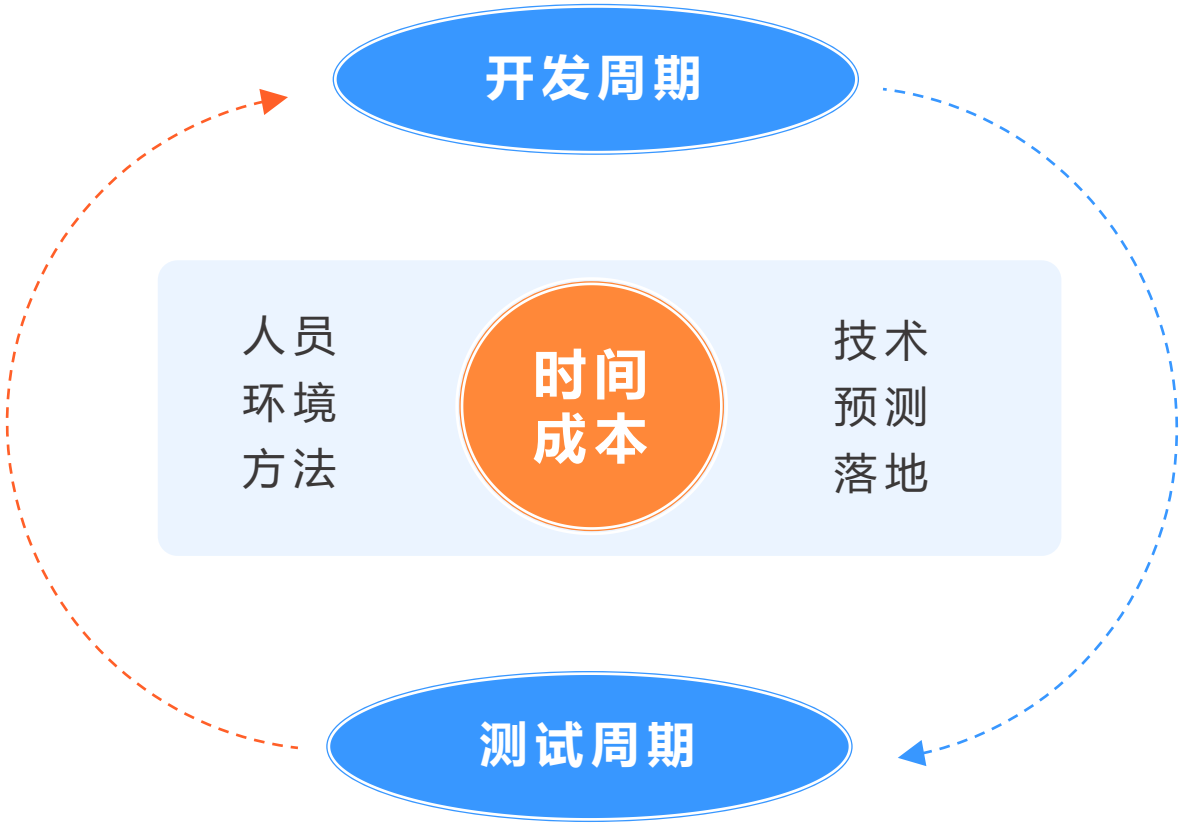
网站访问延时增高

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

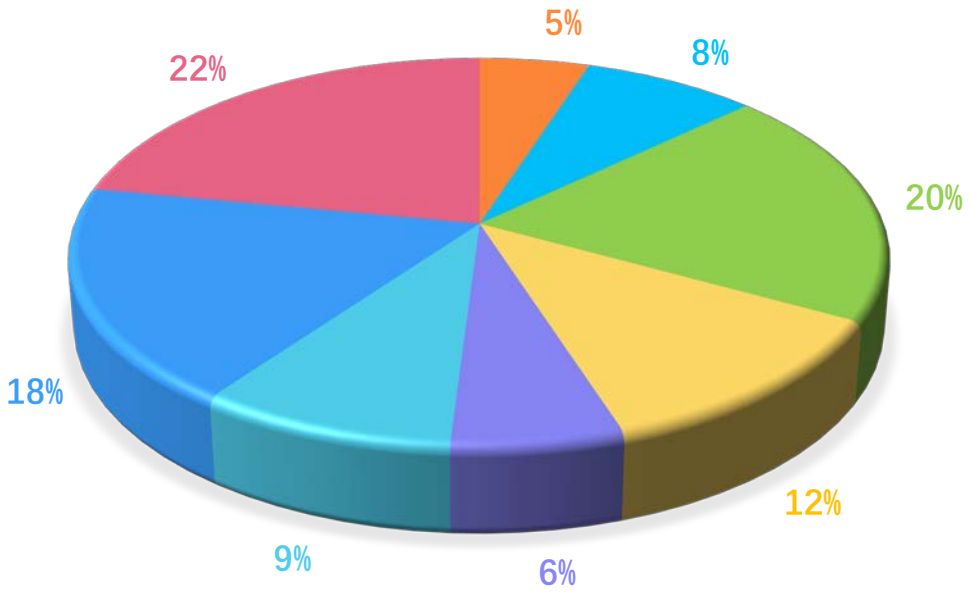
测试环境和
生产环境如何管理

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%

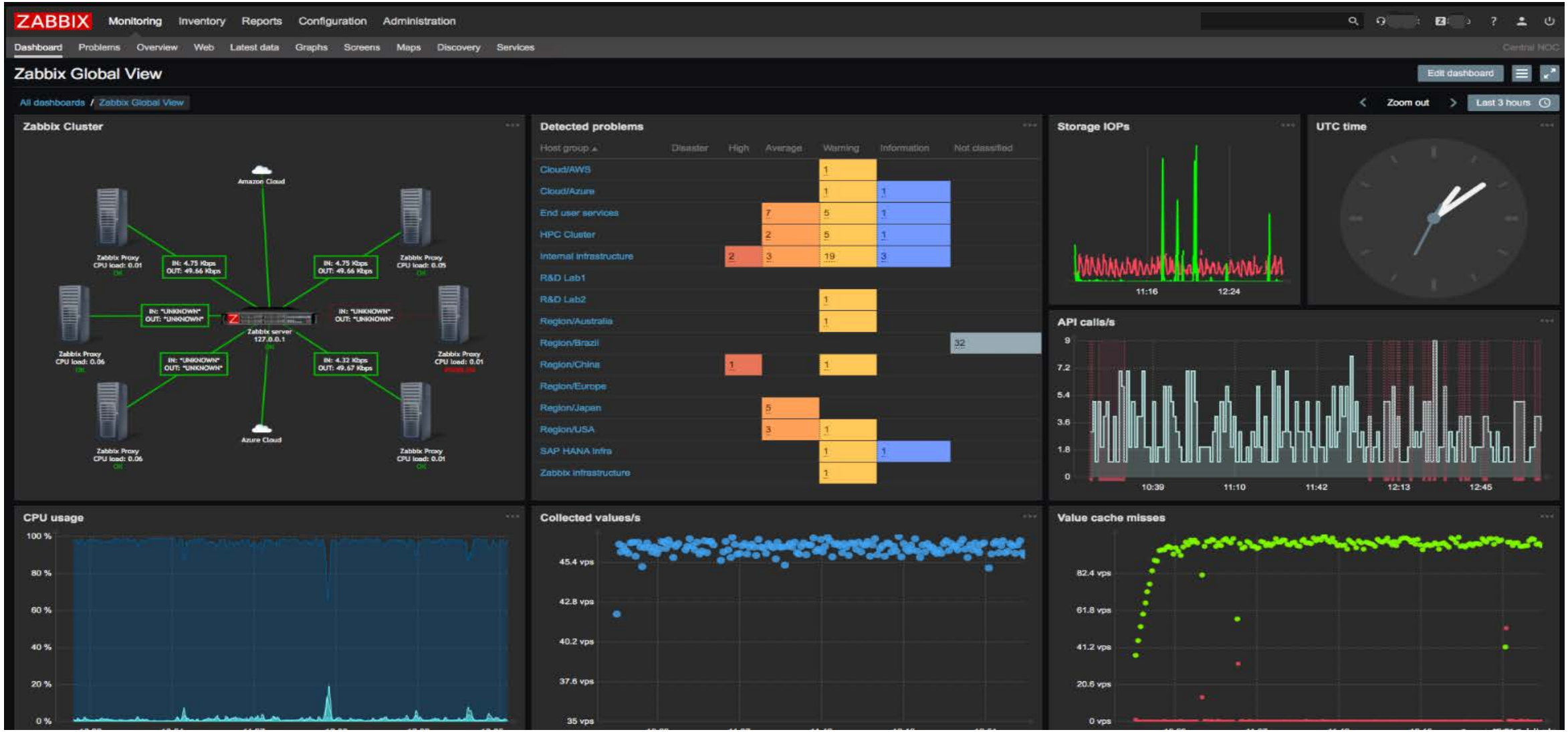
主机硬件配置
主机参数配置
主机网络配置
12%

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


ZABBIX
Monitoring
Inventory
Reports
Configuration
Administration
Dashboard
Problems
Overview
Web
Latest data
Graphs
Screens
Maps
Discovery
Services
Zabbix Global View
Edit dashboard
All dashboards / Zabbix Global View
Zoom out
Last 3 hours
Zabbix Cluster
Amazon Cloud
Azure Cloud
Zabbix server
127.0.0.1
Zabbix Proxy
Detected problems
Host group
Disaster
High
Average
Warning
Information
Not classified
Cloud/AWS
Cloud/Azure
End user services
HPC Cluster
Internal infrastructure
R&D Lab1
R&D Lab2
Region/Australia
Region/Brazil
Region/China
Region/Europe
Region/Japan
Region/USA
SAP HANA Infra
Zabbix infrastructure
Storage IOPs
11:16
12:24
UTC time
API calls/s
10:39
11:10
11:42
12:13
12:45
CPU usage
100 %
80 %
60 %
40 %
20 %
0 %
Collected values/s
45.4 vps
42.8 vps
40.2 vps
37.6 vps
35 vps
Value cache misses
82.4 vps
61.8 vps
41.2 vps
20.6 vps
0 vps

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

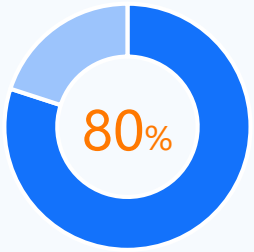
过程

每个告警处理过程平均至少需要流转2次

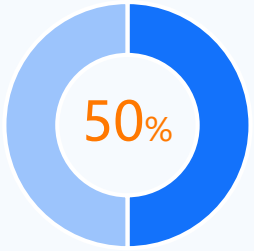
知识

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



建转运



IT架构重构

基础设施云化
运行环境容器化
业务系统微服务化

运维难度
提升4-5倍

更多的工具

更复杂的
规范和流程

更多的人员

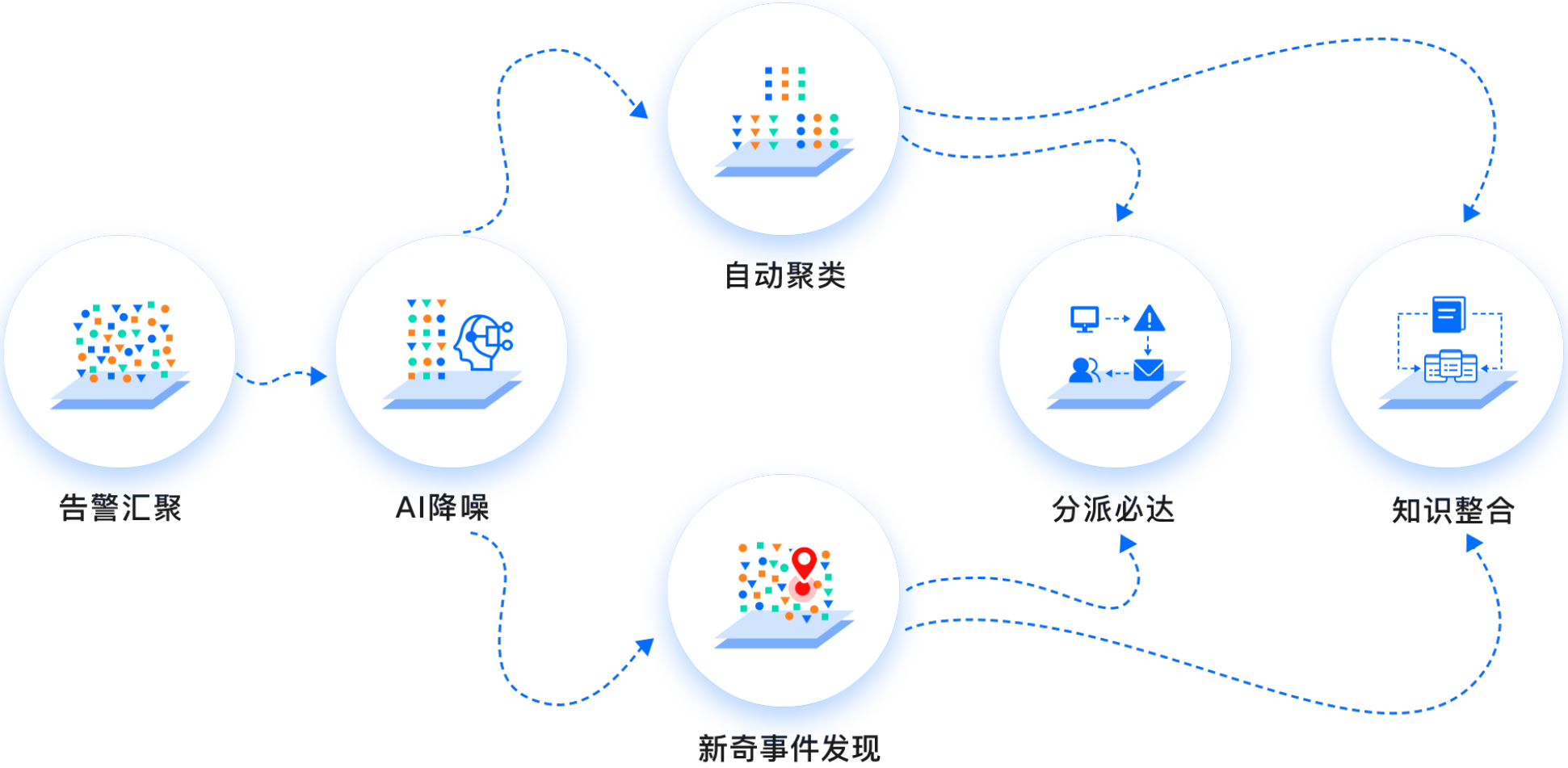
缺少统一管理
海量告警风暴

缺少升级机制
重要告警丢失

通知手段单一
知识缺少沉淀

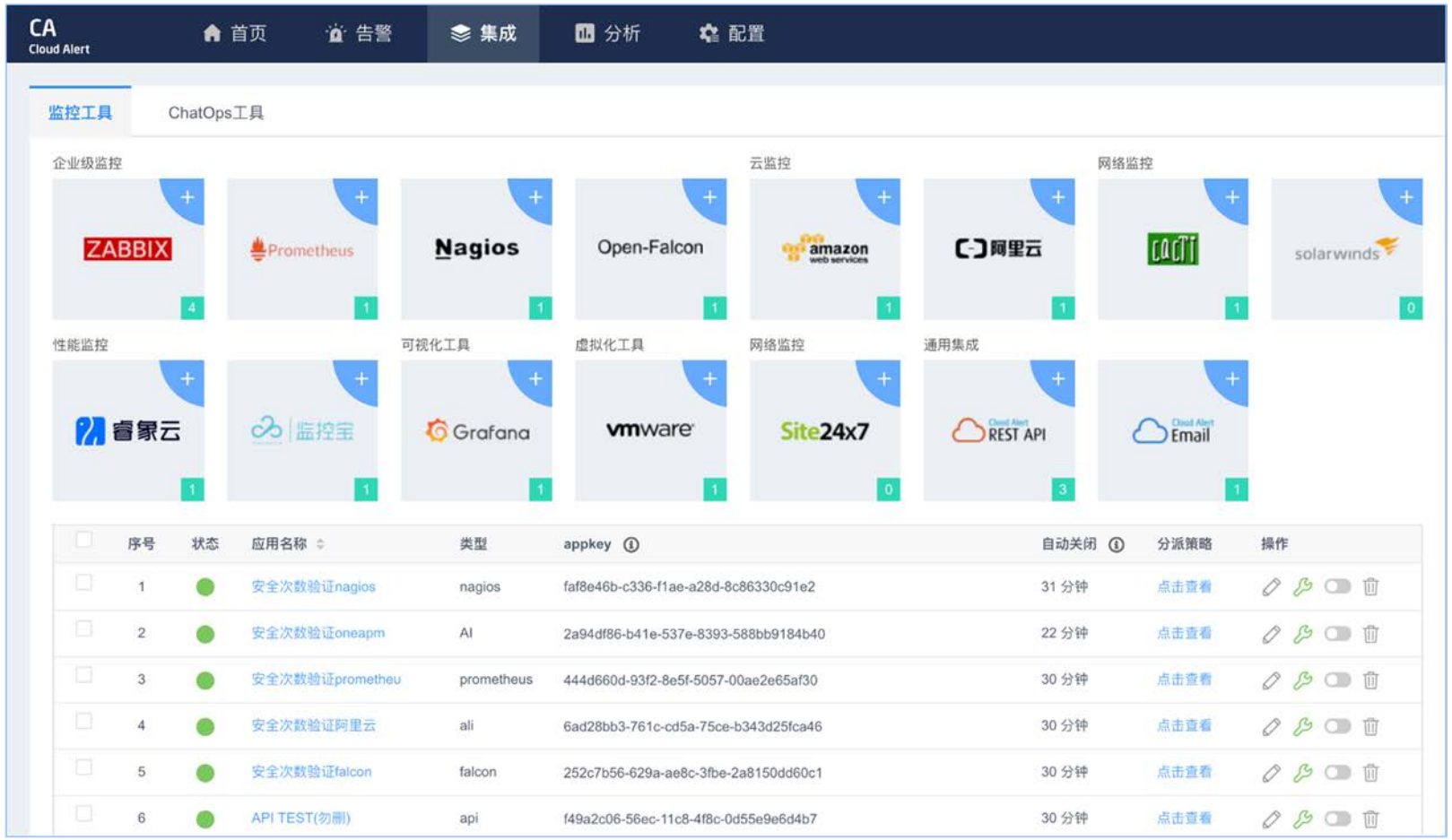
如何快速搭建统一的告警管理平台?

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



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 --
```

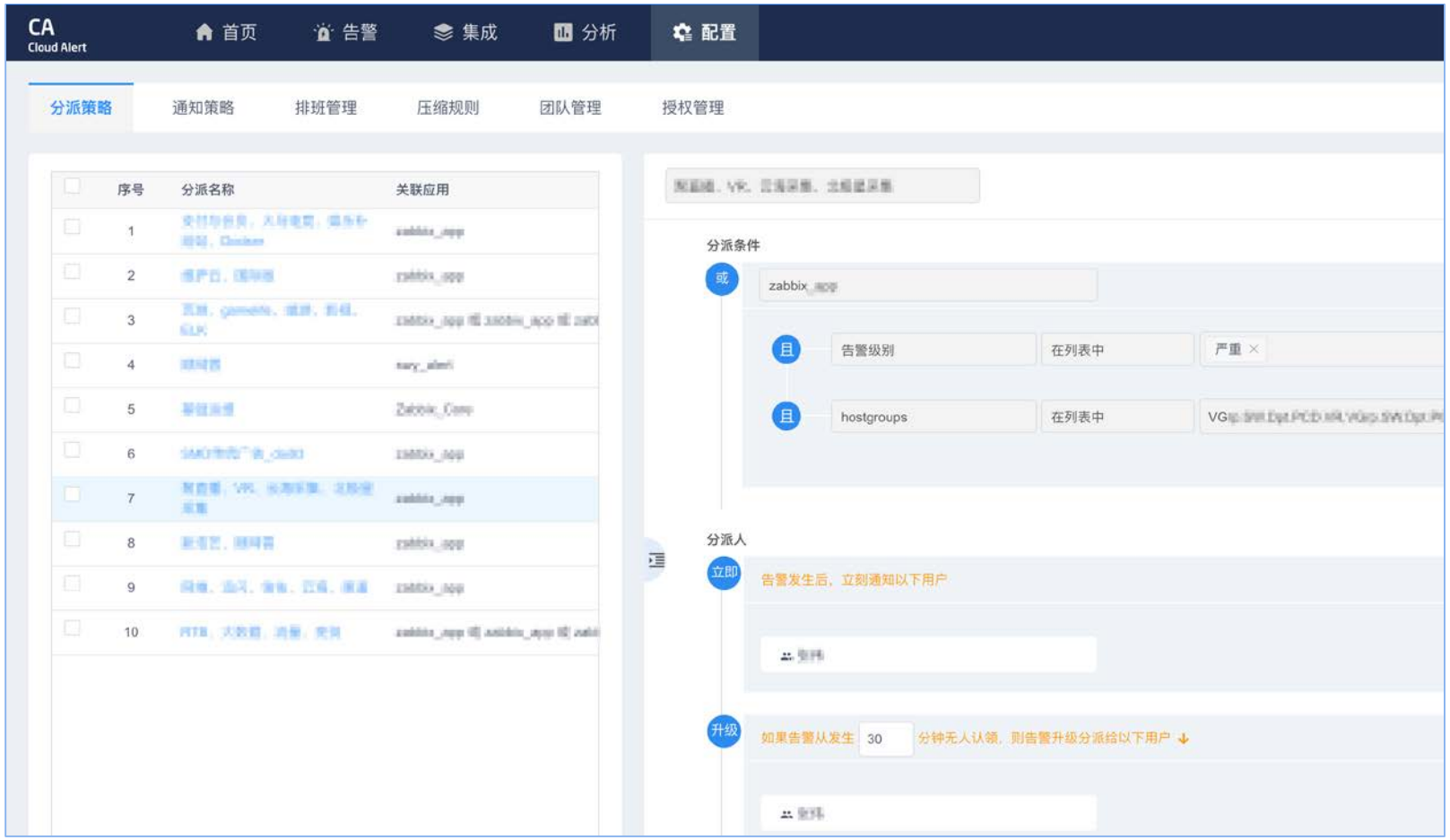
有序分派
不遗漏任何一条告警

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

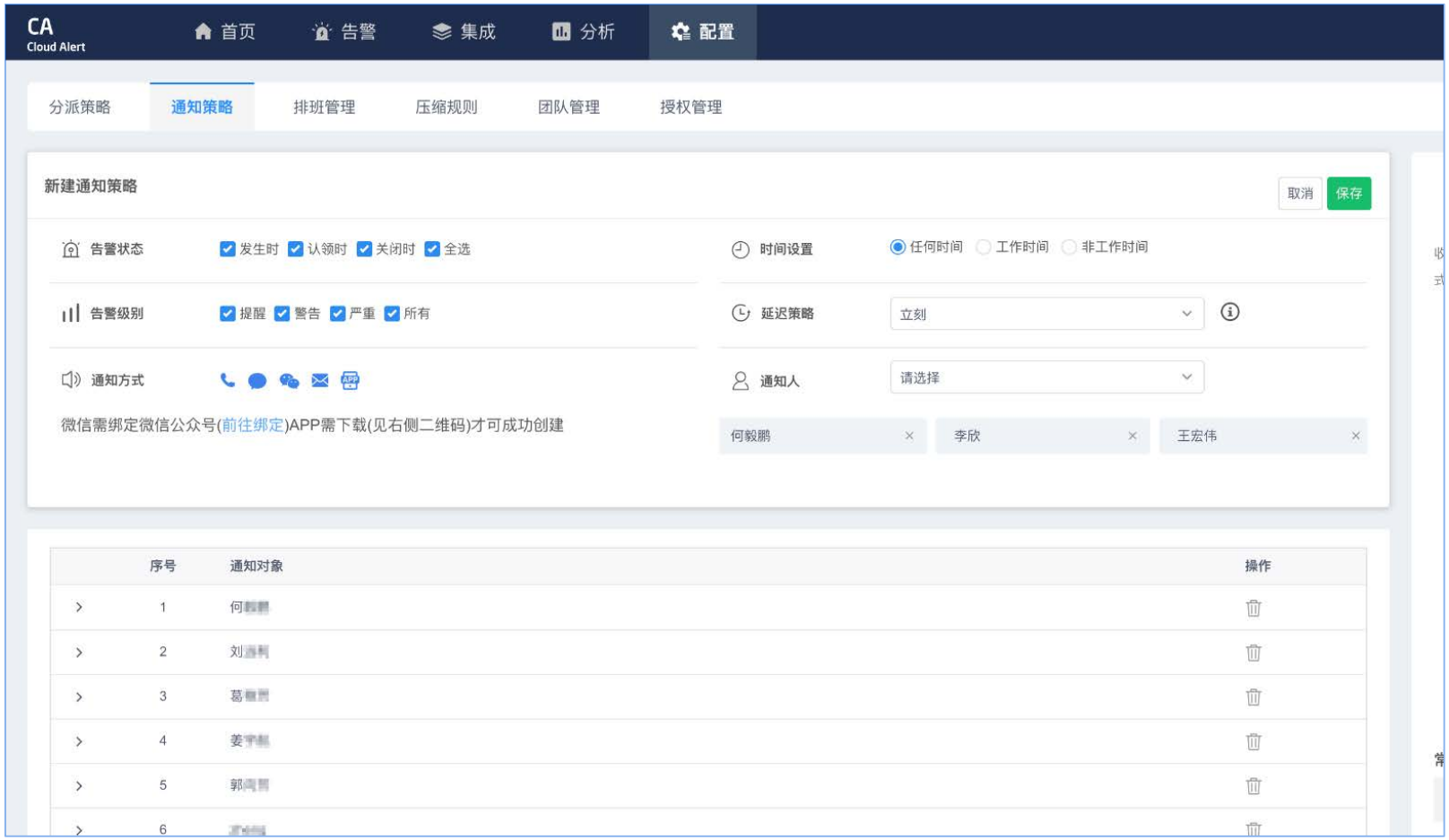
- 按照用户、组、排班、协作方式进行告警分派
- 设置认领超时，自动升级



多种通知方式 提升告警到达率

灵活的通知策略

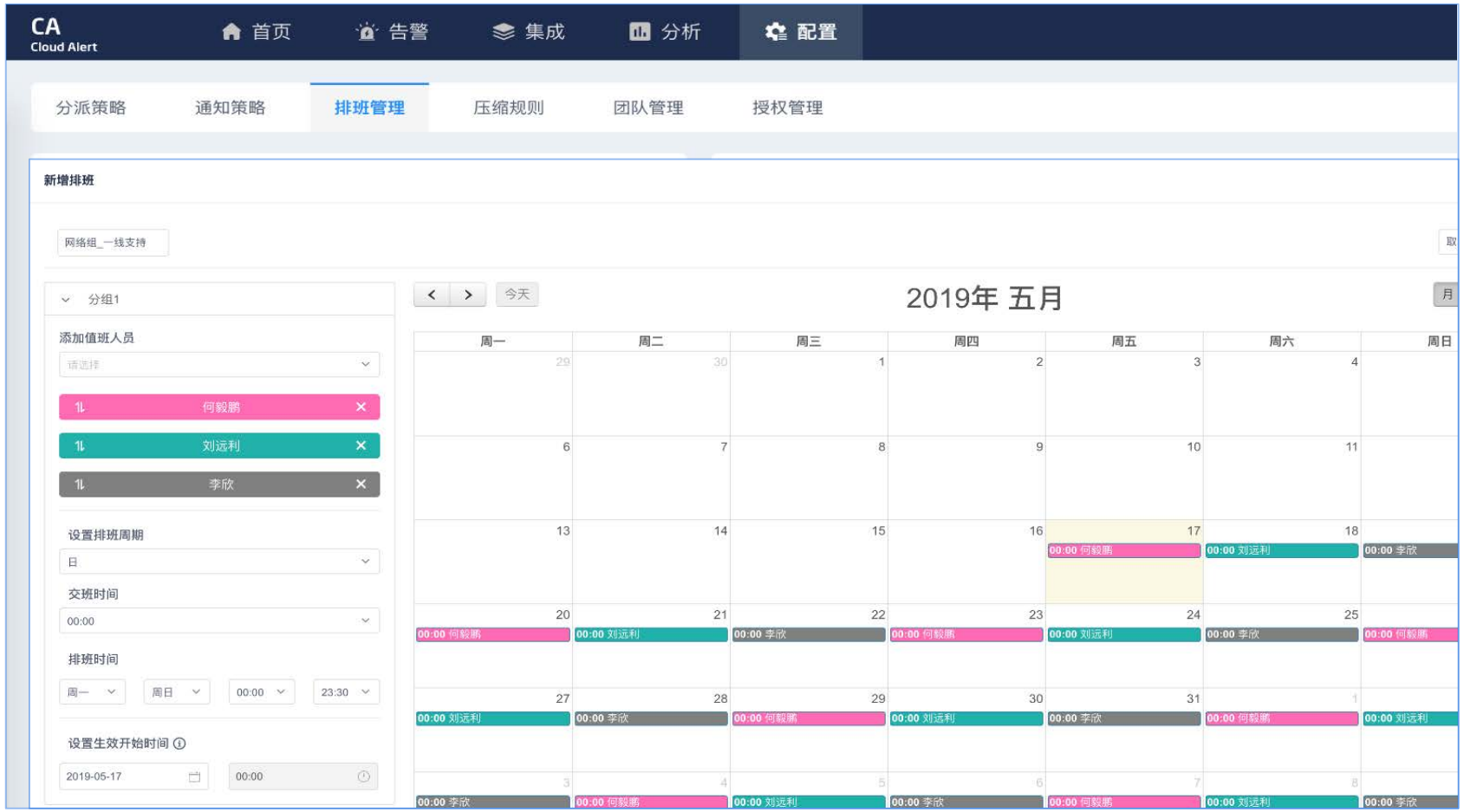
- 告警状态
- 通知时间
- 告警级别
- 延迟策略
- 通知方式
- 人员



排班管理
制定专属告警响应机制

可视化排班管理

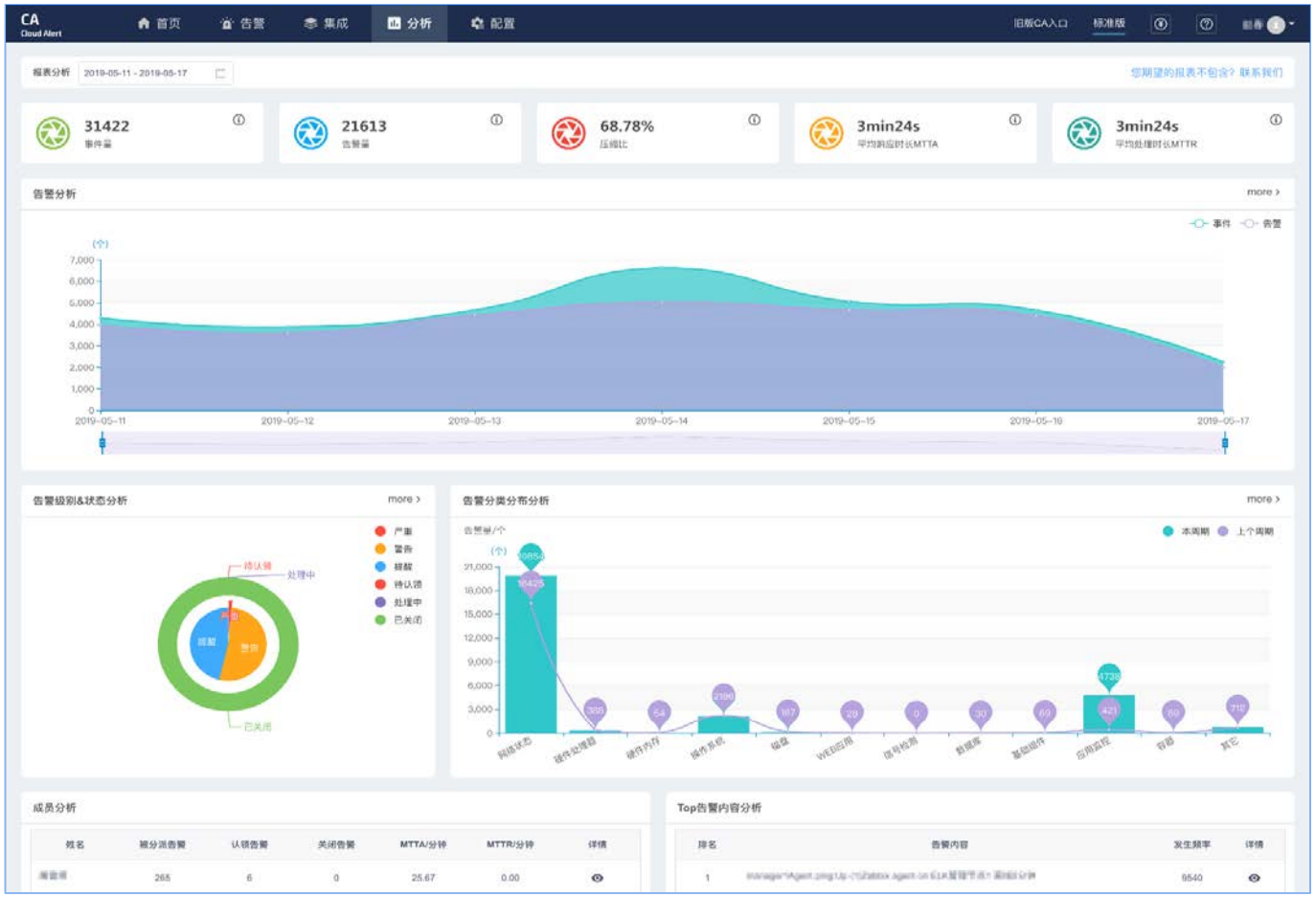
- 根据实际场景可按日、周、自定义周期排班，
- 自定义排班工作时间，严格划分工作时间与非工作时间
- 日历视图直观预览排班效果



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

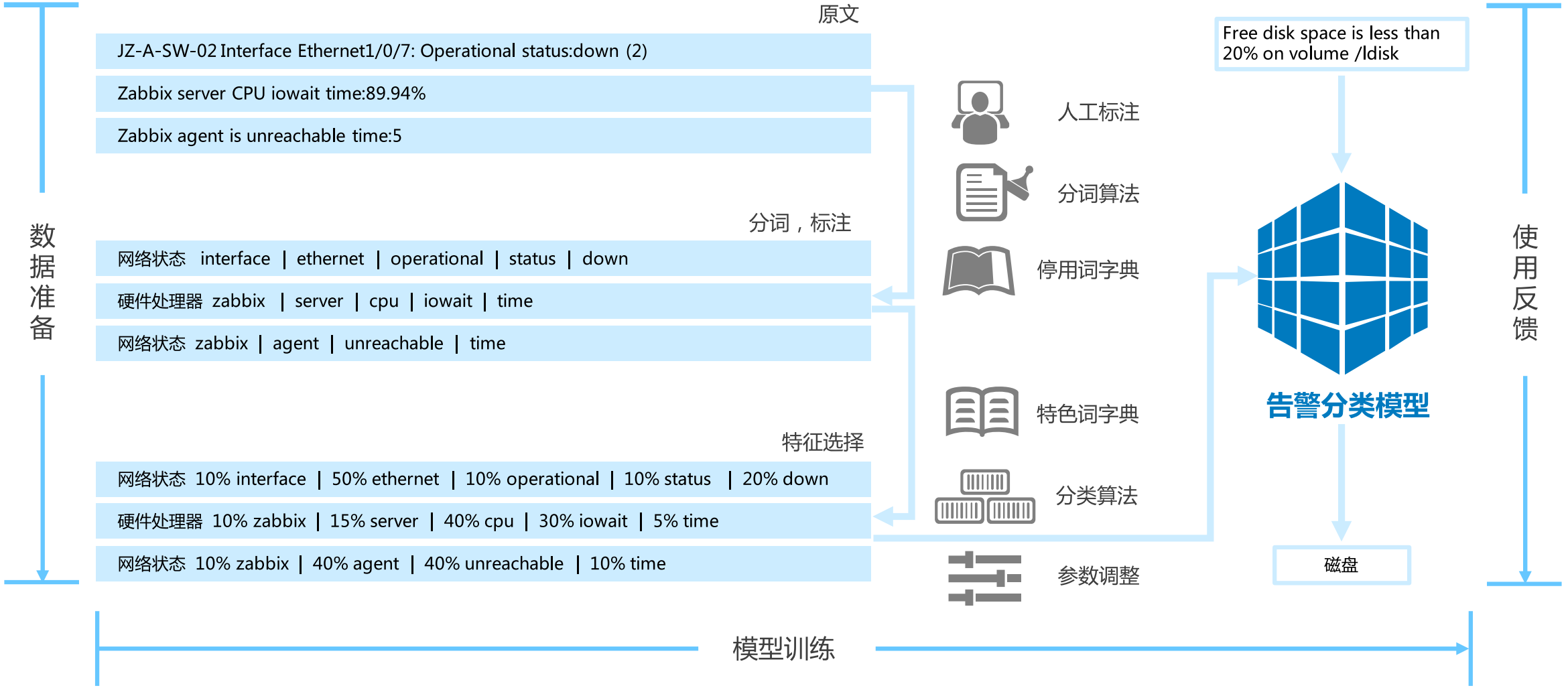
深度学习算法

- 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


数据准备
原文
JZ-A-SW-02 Interface Ethernet1/0/7: Operational status:down (2)
Zabbix server CPU iowait time:89.94%
Zabbix agent is unreachable time:5
分词，标注
网络状态 interface | ethernet | operational | status | down
硬件处理器 zabbix | server | cpu | iowait | time
网络状态 zabbix | agent | unreachable | time
特征选择
网络状态 10% interface | 50% ethernet | 10% operational | 10% status | 20% down
硬件处理器 10% zabbix | 15% server | 40% cpu | 30% iowait | 5% time
网络状态 10% zabbix | 40% agent | 40% unreachable | 10% time
人工标注
分词算法
停用词字典
特色词字典
分类算法
参数调整
Free disk space is less than 20% on volume /ldisk
告警分类模型
磁盘
使用反馈
模型训练

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

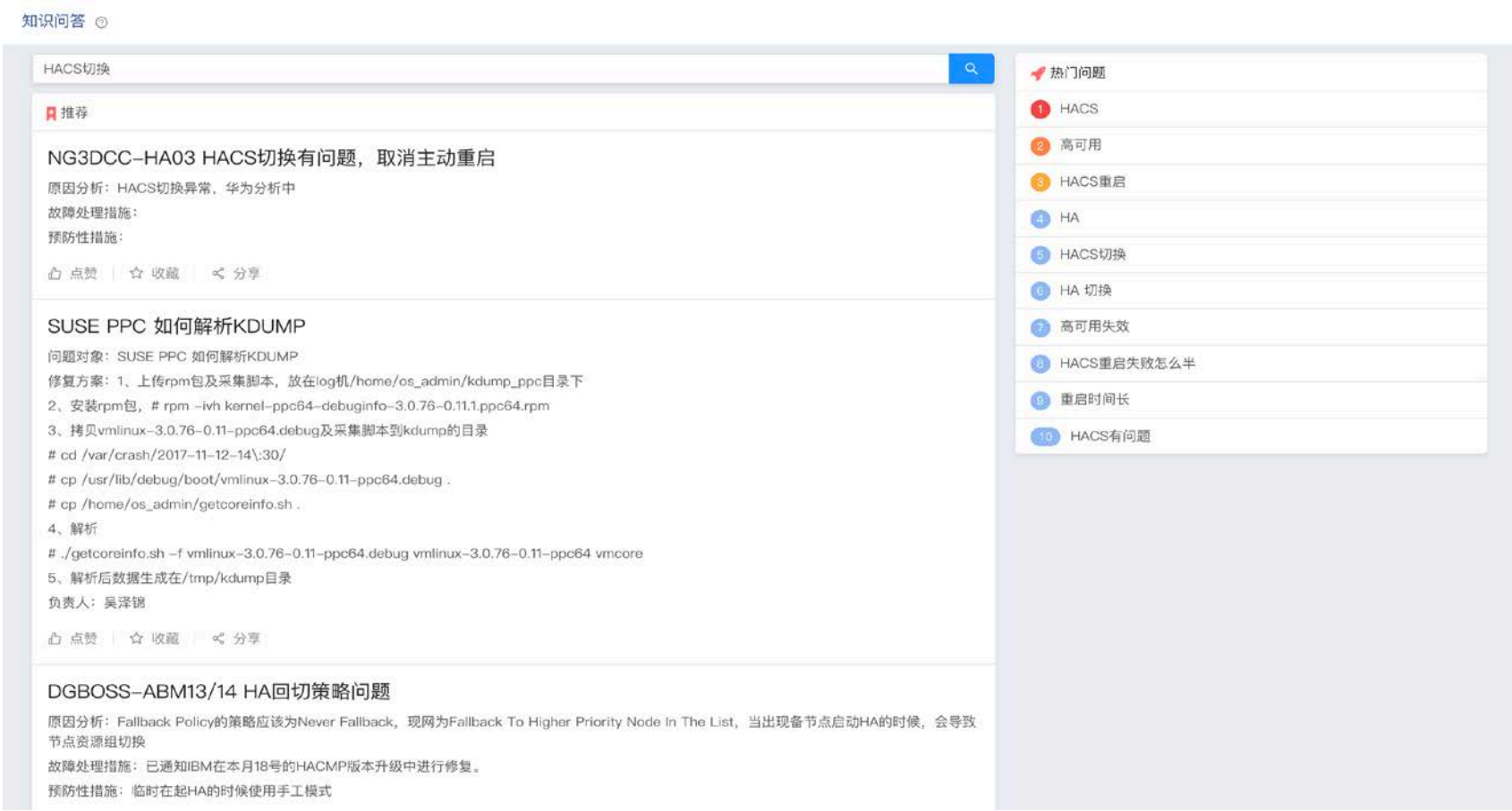
- 厂商手册、厂商知识库、博客、Stack Overflow等公开来源。需要使用到自然语言的命名实体识别、实体关系分析的一系列的手段进行知识的提取和整理。

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。



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

- 北京中关村银行 ZHONGGUANCUN BANK
- 安信信托 ANXIN TRUST
- 中汇支付 CNEPAY.COM
- 借贷宝

运营商

- 和 | 中国移动 China Mobile
- T··Systems·
- i-Café Mavin 顺网科技

制造业

- TCL
- Midea
- WEICHAI 潍柴

互联网

- 马蜂窝
- 皇包车 HUANG BAO CHE
- 云知声 Unisound
- 网宿科技

其它

- MEGVII 旷视
- Vanguard 华润万家
- 闲徕互娱 XIANLAIHUYL
- 汇通达 HUITONGDA

睿象云还能帮助您 ...

Cloud Insight
智能监控平台

5分钟，
搞定跨云监控

CI

Cloud Alert
智能告警平台

自动化场景录制
智能化业务质量分析

CA

睿象云

Cloud Test
业务可用性监测平台

自动化场景录制，
智能化业务质量分析

CT

Cloud Performance Test
云压力测试平台

十分钟搭建千万级真实压测场景

CPT

睿象云官网： www.aiops.com

咨询热线： 400-080-9810

Thank You!

ZABBIX 2019
Conference