Di-Alert 智能告警管理软件

版本号：v1.0.2303

目录

1. 产品概述

1.1. 告警运维管理面临的挑战

告警运维管理过程中将会面临以下挑战：

- 告警风暴干扰，严重影响故障处置的效率。
- 告警来源众多，缺乏统一的集成管理和处置能力。
- 告警无法及时触达相关人员，告警处理效率下降。

在混合云架构下，需要提供海量告警的统一管理能力。通过智能告警压缩收敛，有效抑制噪音，提高告警关联性、针对性。从而将告警事件运维提升至告警对象运维，结合多渠道的人机告警触达，提升告警协同处置的效率。

1.2. 产品简介

Di-Alert 提供混合云架构下海量告警的统一管理平台。通过智能算法结合对象配置信息对告警事件进行富化、等级映射、智能打标、压缩、收敛、关联、溯源等治理分析工作，将告警运维由传统的面向事件运维升级为面向对象运维，更精准地进行告警触达，提升告警事件处置效率，提高业务系统的连续对外服务等级。

1.3. 应用场景及行业

应用场景

统一告警管理

通过 REST API、Agent 主动采集、URL 回调等多种方式将监控系统的告警集成到 Di-Alert 告警平台统一管理。

告警抑制收敛

基于智能算法对海量的、持续的冗余消息进行告警压缩和去重，抑制告警消息的数量，减少告警的频率。

告警触达，团队协作

通过多种通知方式将告警通知给相关负责人处理，处理人可以在智能告警管理平台完成告警分派、升级、认领、处理、关闭的完整生命周期的告警集中管控流程。

适用行业

银行金融、政府医疗、商业地产、智能制造行业等

2. 技术特性

2.1. 技术概述

Di-Alert 的主要技术特点：

告警分散管理

通过不同监控工具的告警模块分别配置策略和通知机制，告警管理分散在各个监控工具之中。

告警统一管理

将不同监控工具或系统产生的告警接入统一的管理平台，实现告警的统一分派和通知，并能基于规则对告警进行去重和压缩。

告警智能管理

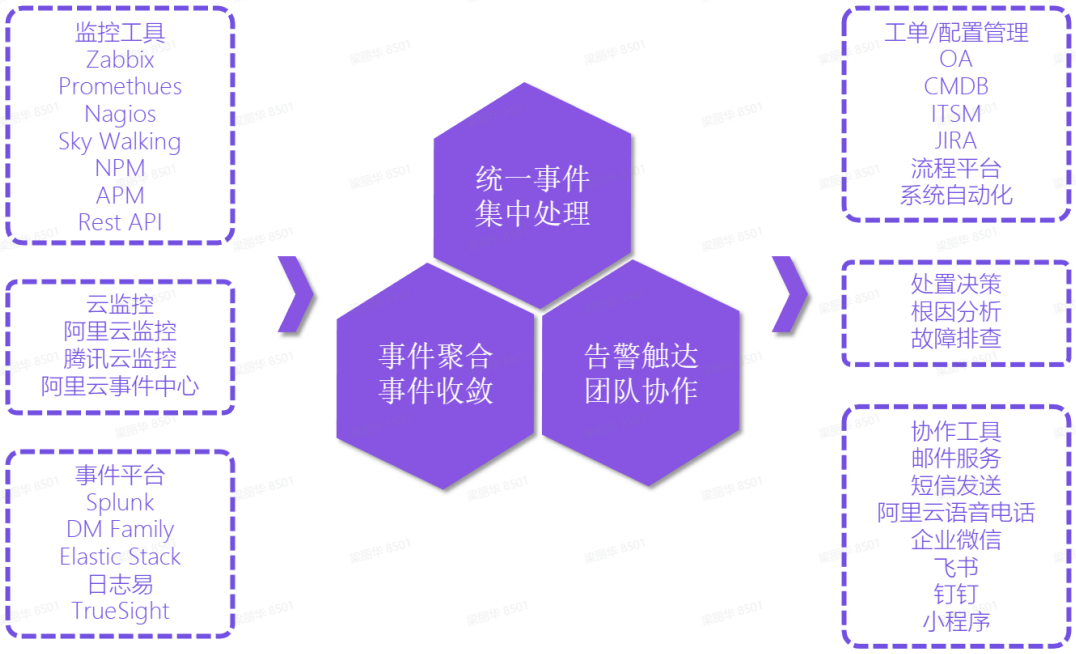
通过运用人工智能算法，无法人工参与的情况下，自动识别告警类别和新增类型，对复杂场景下的相识告警进行更高比例的压缩降噪。

根因告警定位

通过运用知识图谱技术和告警专业领域知识，能够自动推荐各个业务场景下海量告警信息中的根因告警。

告警自愈

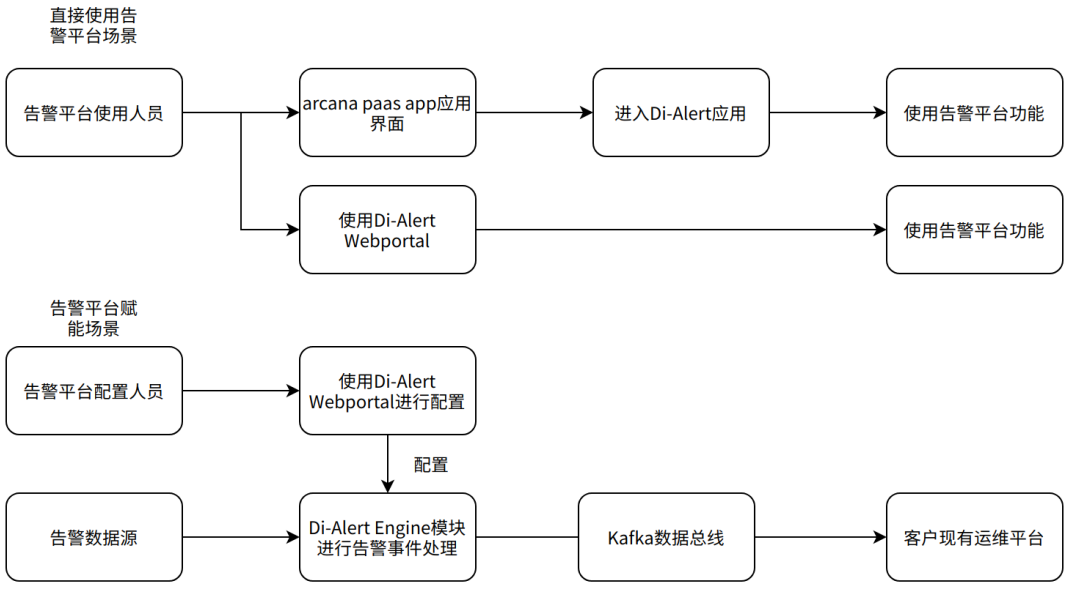
针对根因告警，通过结合告警故障知识库和运维自动化工具，对系统故障进行自动恢复。并通过不断的知识沉淀，提升自愈能力。



2.2. 技术架构

2.2.1. 架构图

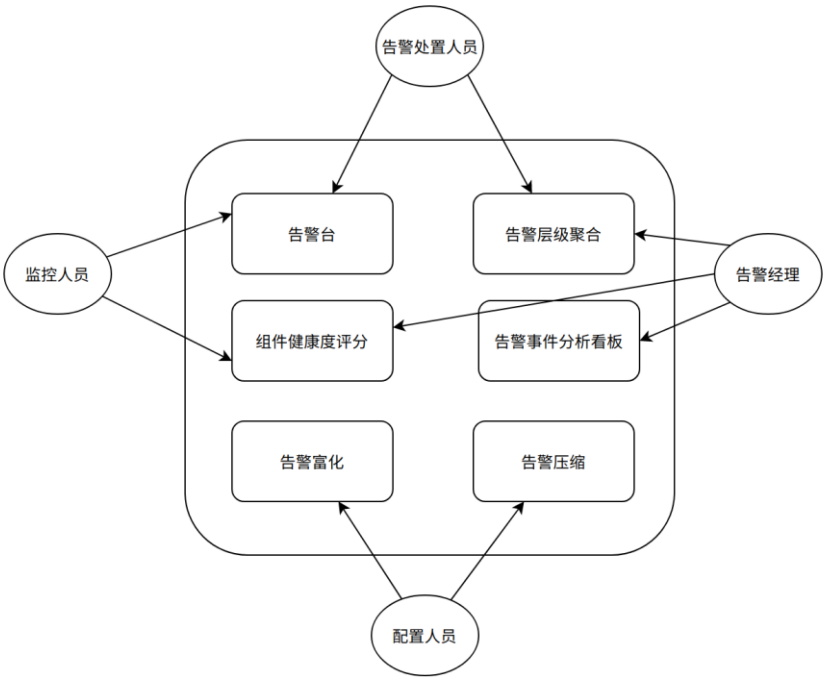
业务系统上下文及业务架构



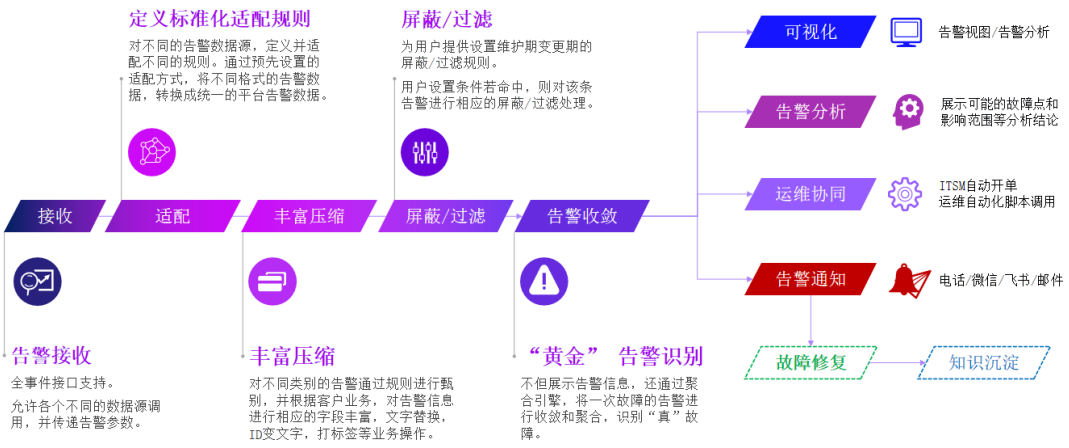
顶层业务视图及业务用例

- 目标用户角色：
  - 监控人员：负责告警 24 小时的监控，并对告警进行分派开单。

- 告警处置人员：查询被分派的告警、进行告警处置、并关闭告警。
- 告警经理：负责对告警进行分析，包括各组件的健康度情况、告警关联性收敛、告警有效性分析、告警处置效率分析等；
- 配置人员：o对告警平台进行配置，对监控人员、告警处置人员、告警经理进行告警平台的交付工作。

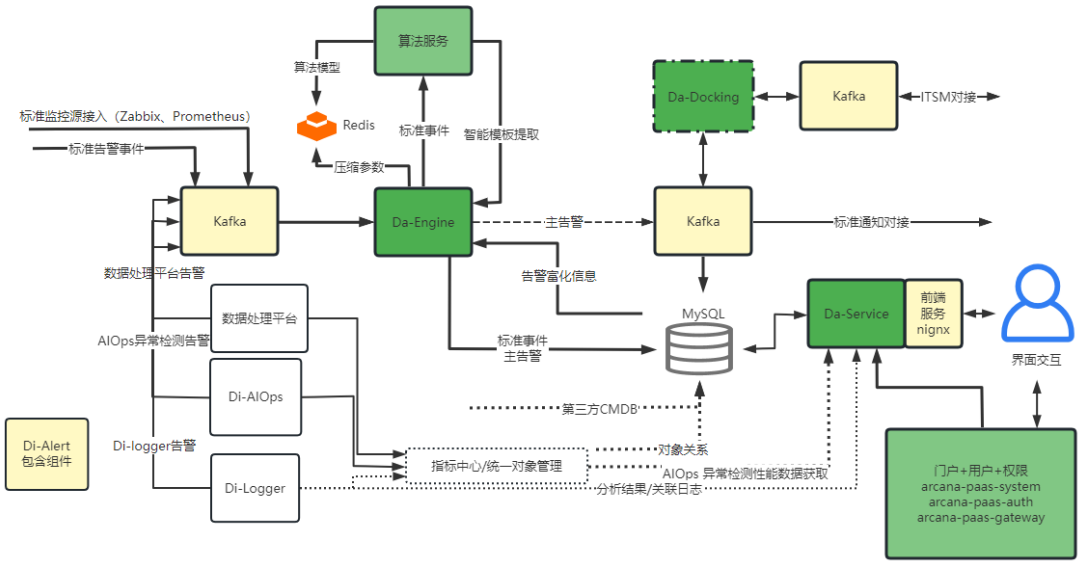


Di-Alert 技术架构图



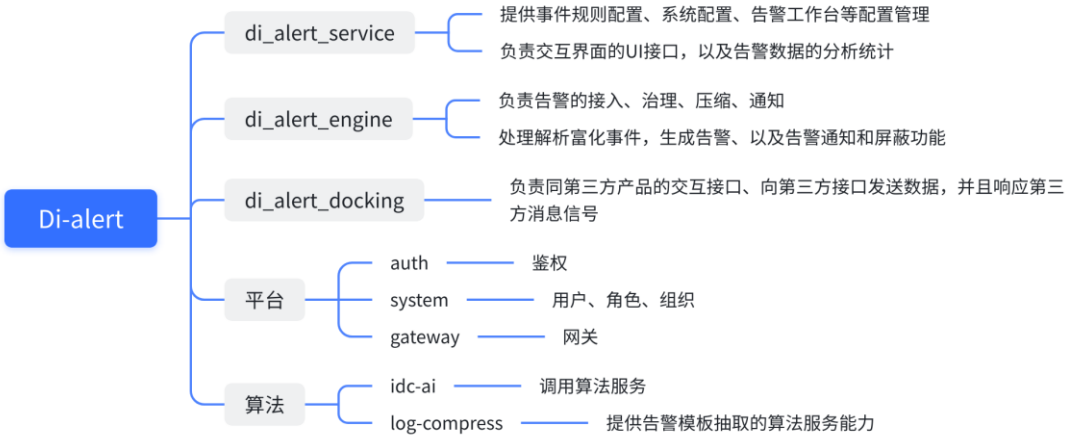
2.2.2. 数据流图

Di-Alert 与其他产品组合数据流：



各个微服务说明：

- Da-Engine： 负责告警的接入、治理、压缩、通知。
- Da-Service: 负责交互界面的 UI 接口，以及告警数据的分析统计。
- Da-Docking: 负责同第三方产品的交互接口、向第三方接口发送数据，并且响应第三方消息信号。
- 算法服务：提供告警模板抽取的算法服务能力。



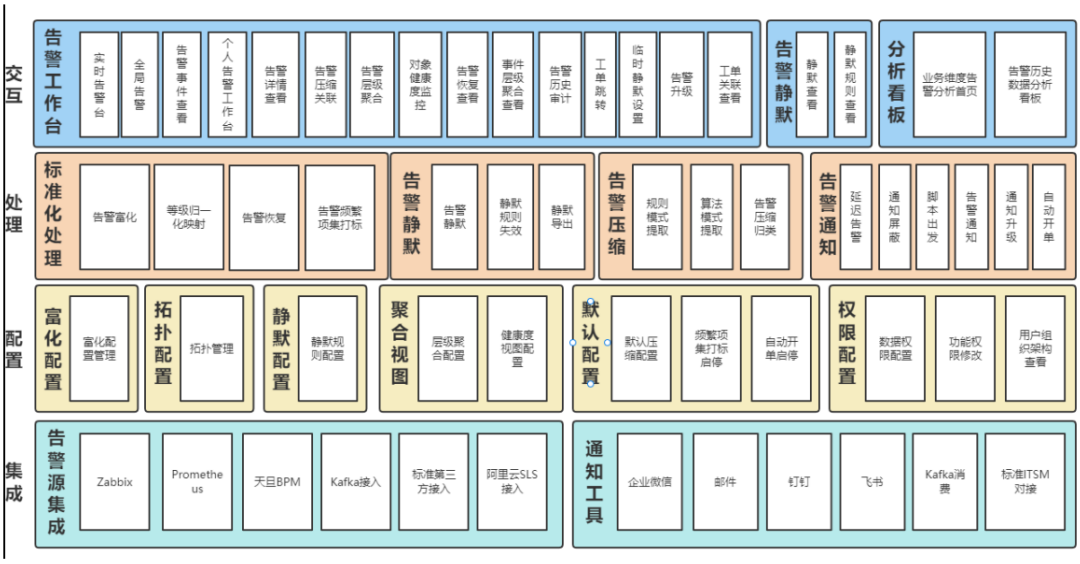
2.3. 系统性能

Di-Alert 的最低硬件配置要求是 4 核 16GB 内存的虚拟机，一台这样的虚拟机可支撑 20000 EPH 的告警量。用户根据每天的告警量估算硬件需求时，可参考这个指标。

3. 产品组成

3.1. 产品功能概览

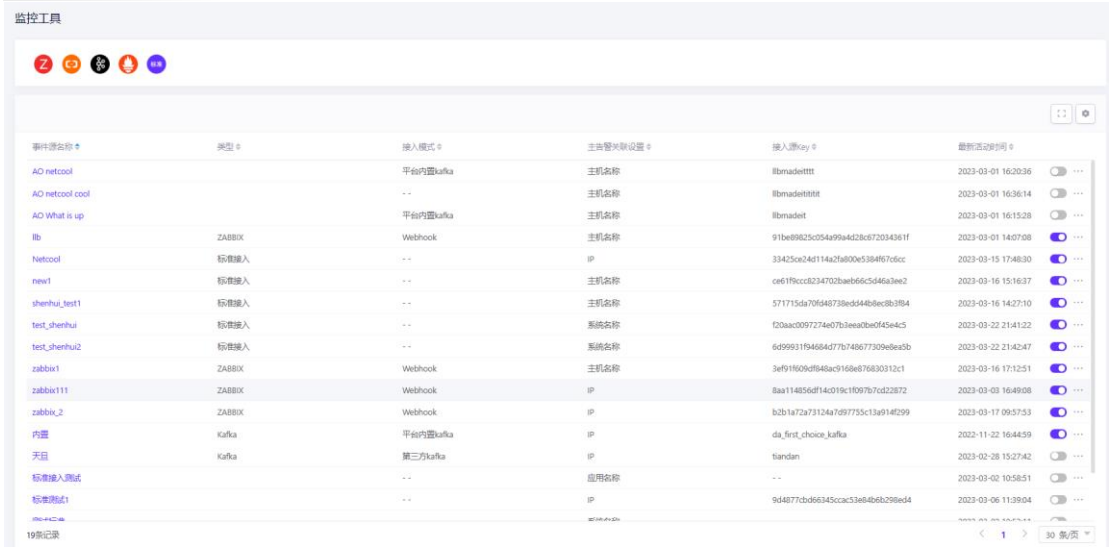
Di-Alert 产品功能如下所示：



3.2. 核心功能介绍

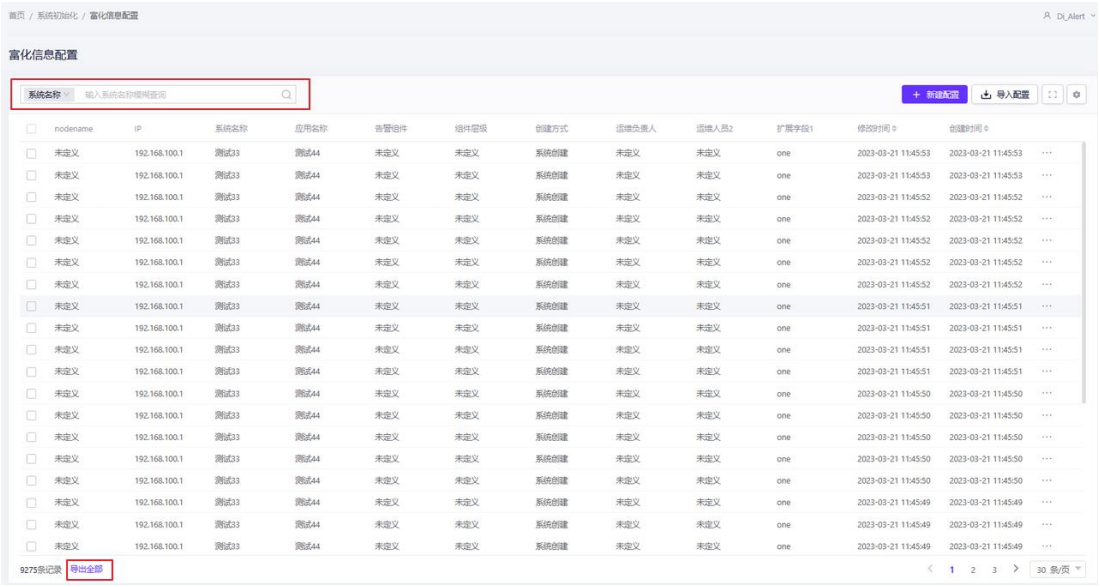
3.2.1. 告警源集成

Di-Alert 可接入多种监控工具的告警源并对接入的告警源进行统一管理。支持的监控工具有：Zabbix、Prometheus、阿里云事件、Kafka 消息队列、天旦 BPC 以及标准第三方数据；支持 API 方式，通过 HTTP Restful API 接口调用集成，快速接入其他监控工具。



3.2.2.事件富化配置

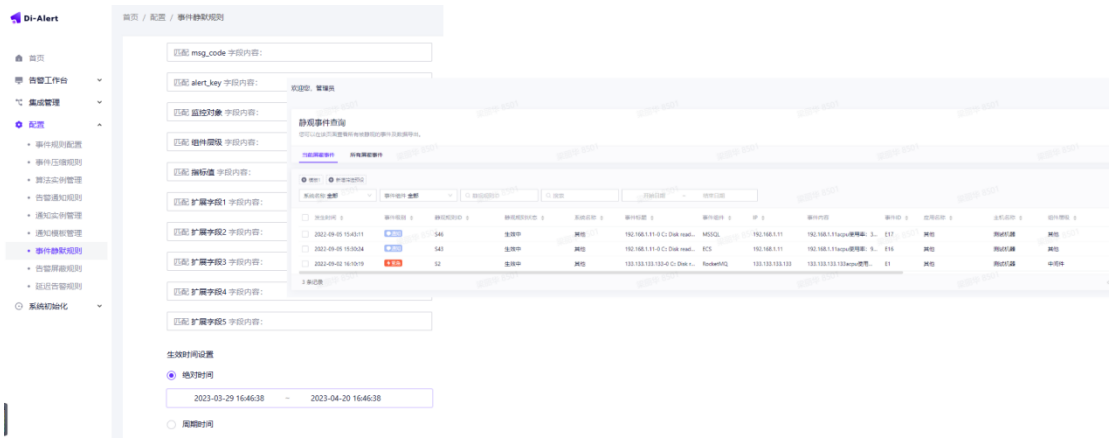
对接入的不同告警数据源，定义并适配不同的富化规则。通过匹配、转换、映射、提取等操作将不同格式的告警数据转换成统一的平台告警数据。



3.2.3.事件静默配置

事件静观规则是为用户提供在应用系统计划变更或者版本发布时，提前规避特定应用系统操作期间所产生的误报事件的屏蔽能力，主要是基于时间窗口和事件关键字段的提前屏蔽，用户可以根据自身需要进行配置和启用。

支持可配置临时静默规则、周期静默规则以及一次性运维告警静默规则，并且支持当前静默规则、静默事件审计。



3.2.4. 告警压缩

Di-Alert 提供基于 AI 算法和规则的事件压缩能力，对于海量的、持续冗余消息进行告警压缩和告警合并，减少告警消息的频率，提升运维工作的效率。

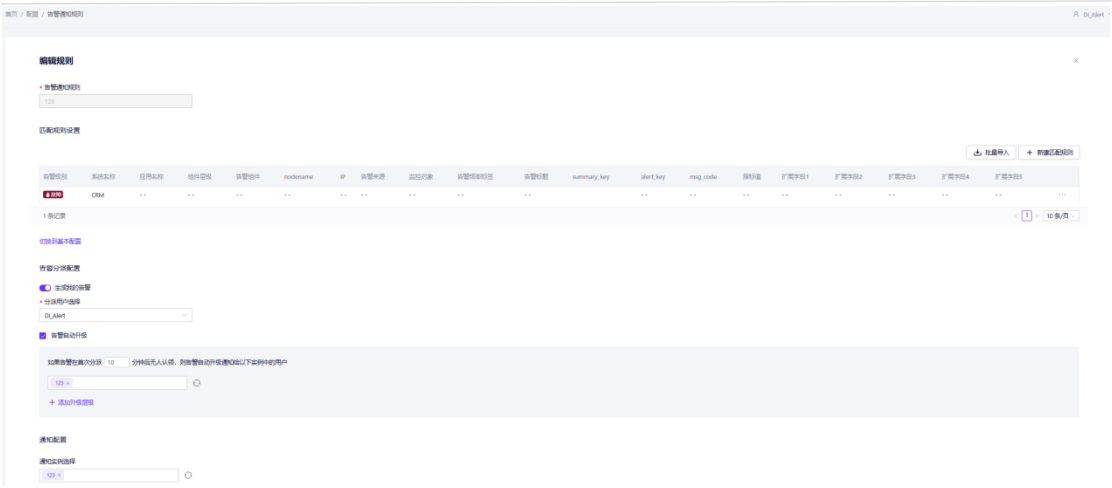
告警压缩支持按规则压缩和智能压缩两种方式：

- 规则压缩：可设置按照多个字段组合+时间窗口的方式进行组合压缩；如根据设备、字段、时间屏蔽，同步维护窗口。
- 智能压缩：使用 AI 算法对告警事件进行模板提取，对文本模式相似的告警在时间窗口内做抑制。

3.2.5. 告警通知

当告警事件触发告警时，告警运维负责人需要将告警信息或告警升级变更通知到对应的运维人员，确保运维人员及时查看和处理相关告警事件。

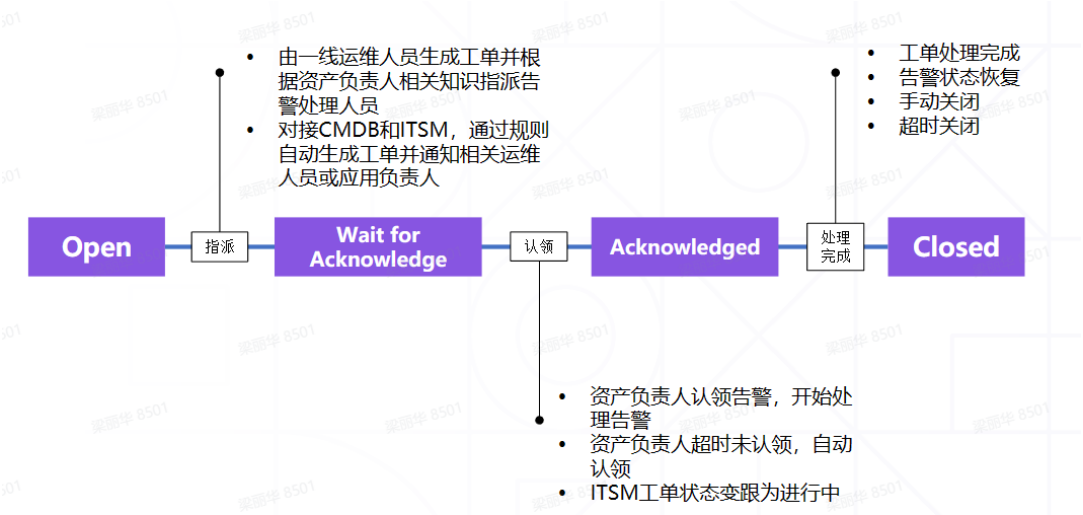
- 支持通知 CMDB 运维负责人、运维群组。
- 通知方式目前支持企业微信、钉钉、飞书、阿里云告警短信、邮件、触发脚本。
- 支持与 ITSM 对接，将告警事件与流程深度关联，基于告警快速生成工单。
- 支持自定义告警通知模板。
- 支持告警屏蔽和告警延迟，减少不必要的告警骚扰。



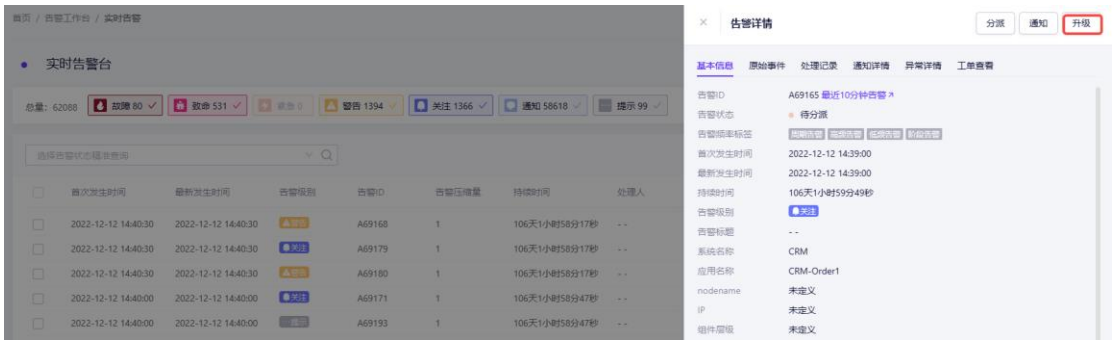
3.2.6. 告警周期管理流程

结合日常运维流程，提供覆盖告警生成、分派、认领、处理、关闭的完整生命周期的告警集中管控流程，让告警协同处理过程更加顺畅，告警处理过程有据可依。

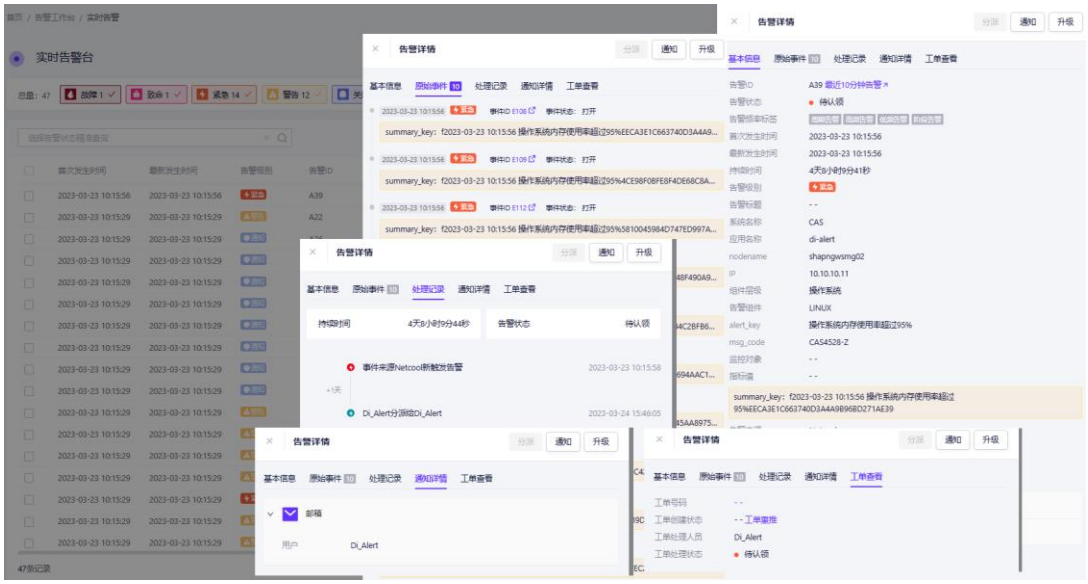
- 支持告警生成、分派、认领、处理、关闭等全生命周期管理事件。
- 支持自动创建工单。



- 支持按照时间和事件等级升级分派给其他人，不遗留关键事件的处理。

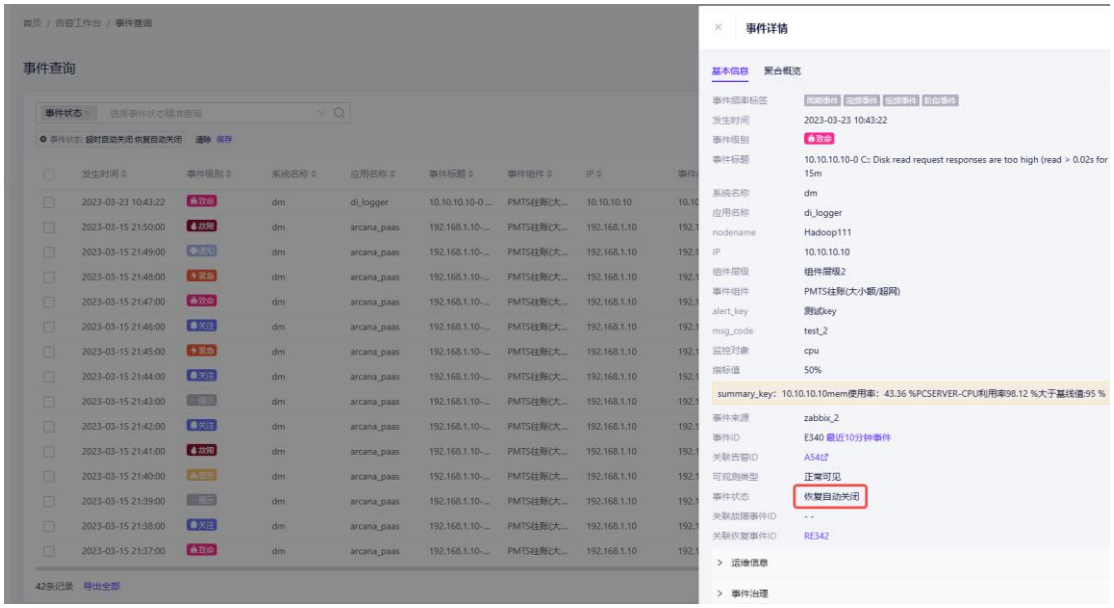


- 所有告警列表支持告警信息查看，支持被压缩的原始告警信息检索，方便用户检索告警相关的原始事件。并且支持查看告警处理记录、告警通知详情以及 ITSM 工单对接详情。



- 告警自动关闭：支持告警恢复自动关闭、超时自动关闭和手动关闭等告警关闭策略，

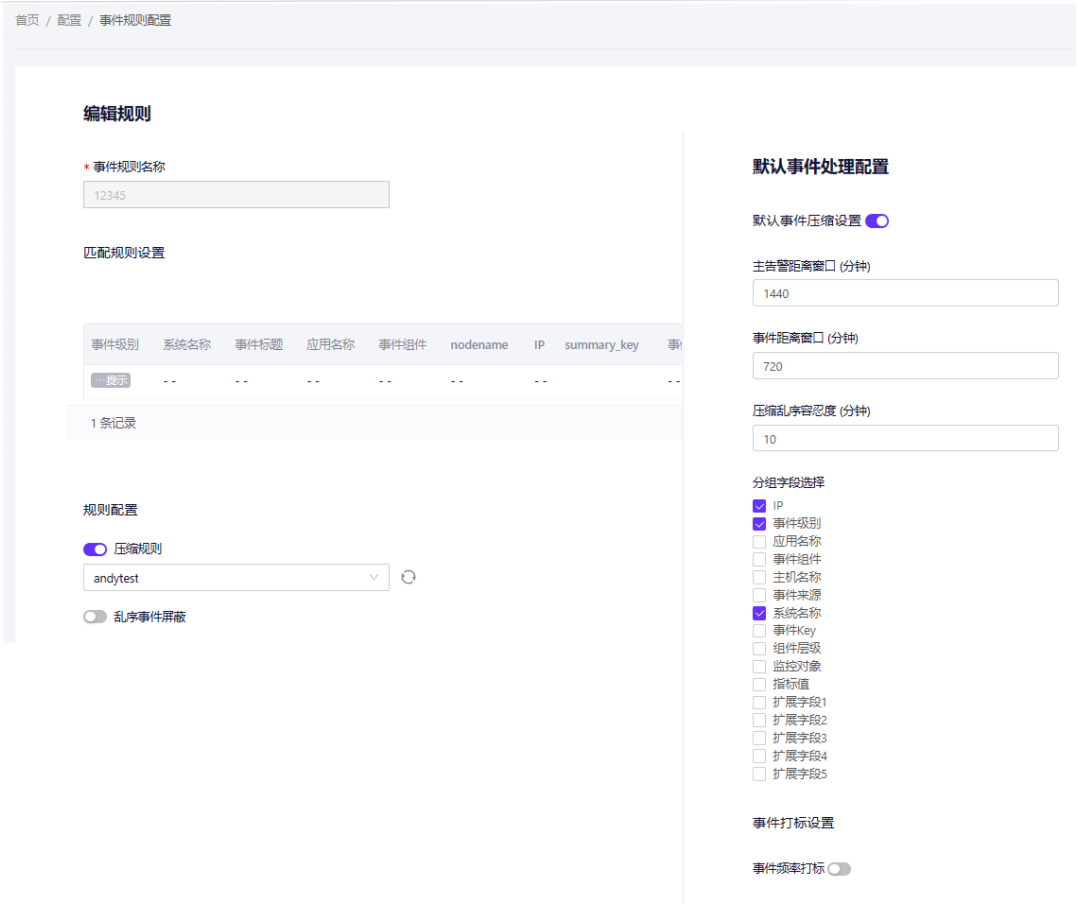
满足多种告警管理场景。



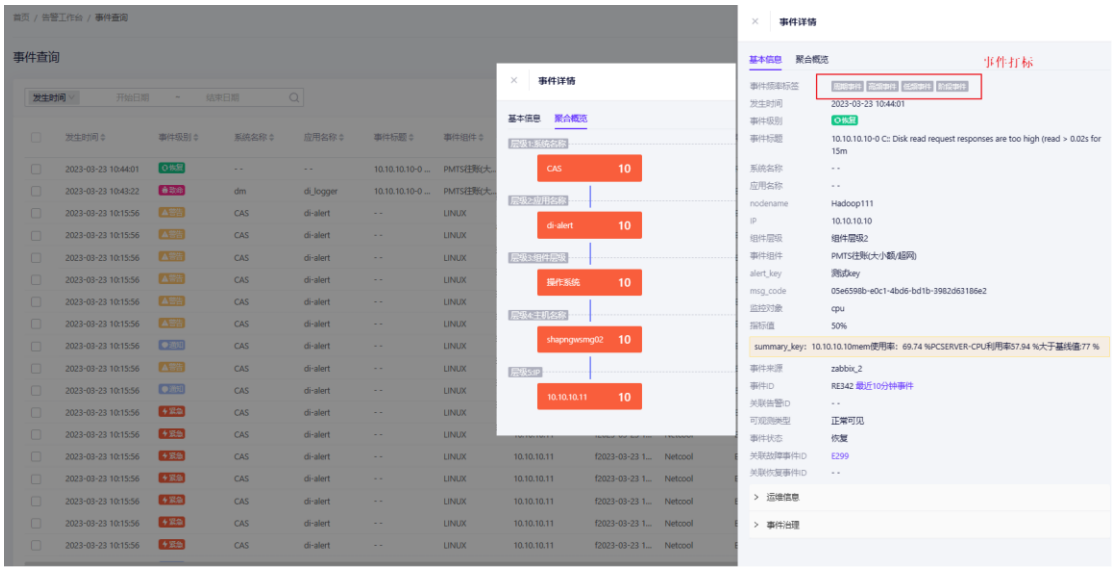
3.2.7.事件集中处置

Di-Alert 支持自定义事件规则和预置默认事件处理配置，将符合匹配条件的事件经过转换、映射、提取等操作转换成标准事件。

- 事件规则支持压缩、超时关闭配置。
- 支持对事件频繁项集进行打标启停，自动区分周期性事件、高频事件、低频事件和阶段事件。



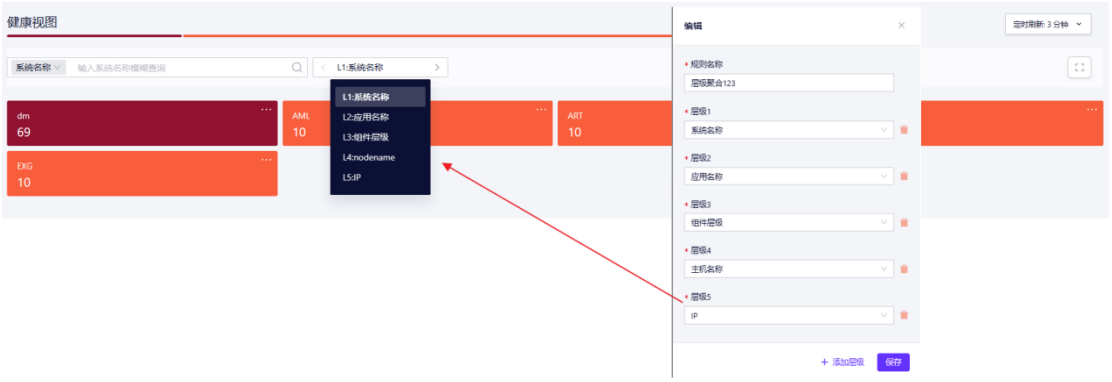
事件查询页面展示所有通过解析处理的标准事件，事件列表支持查看基本信息以及基于组件或自定义层级的聚合拓扑展示。



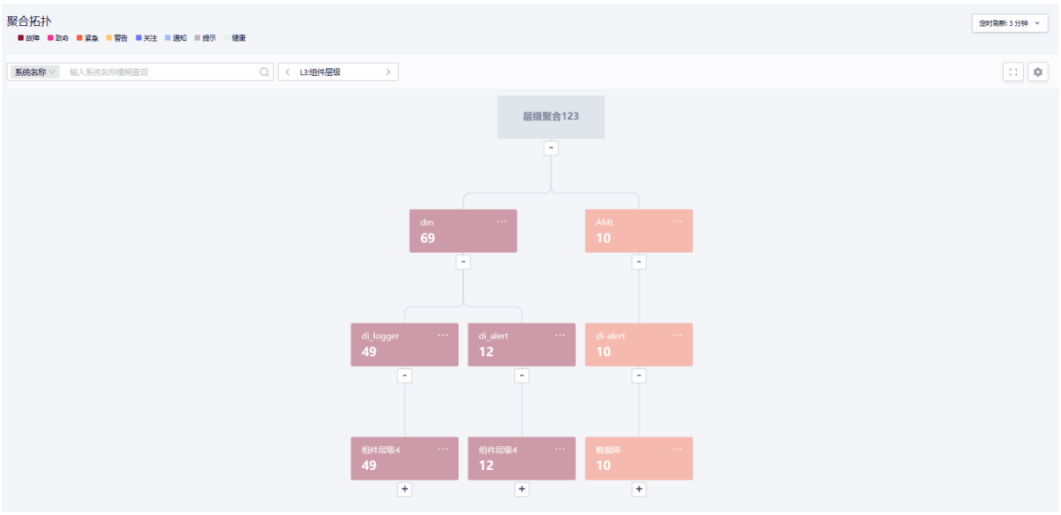
事件层级聚合展示

Di-Alert 提供事件层级聚合和对象健康度监控功能，根据业务运维需求自定义事件层级以及选择健康度评分标准，实现层级支撑逻辑快速实现故障定位，将小时级的根因告警

缩短至分钟级。



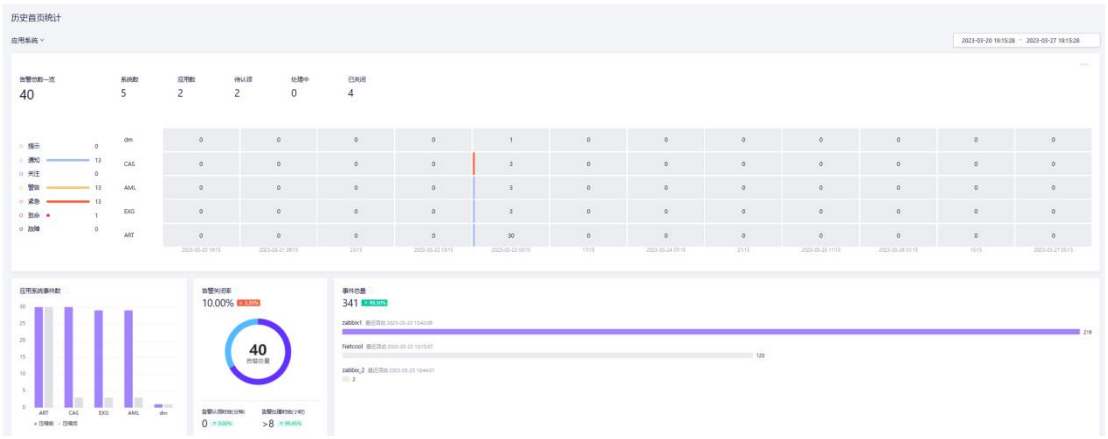
聚合拓扑指的是将告警时序与拓扑关系相结合，通过拓扑关系呈现同一层级下不同对象的传导关系。



3.2.8. 告警分析看板

Di-Alert 提供从业务维度告警分析和历史数据分析的看板，从告警视角触发的运维效率分析、评估能力。

主要统计告警关闭率、MTTA、MTTR，评估运维效率；统计应用系统、应用组件告警事件数量排名，评估系统稳定性。



4. 客户案例

案例一：助力某城市商业银行实现告警生命周期统一管理

【客户需求】

监控工具多，每天告警数量上千条，大部分是噪音或重复告警信息，人工无法及时处理；告警触发到故障处理之间的流程需要人工干预，无法自动化处置及记录处理流程。

【解决方案】

部署 ARCANA 数智平台+Di-Alert 智能告警管理软件。提供丰富的告警事件接入能力，并结合 CMDB 信息丰富告警事件的元数据能力。同时根据告警资产的相关信息，完成故障处理全流程生命周期覆盖。

【客户价值】

- 在一个平台查看所有监控工具告警，避免遗漏。
- 通过告警生命周期管理功能，能够快速生成告警通知相关系统负责人处理，并监控告

警处理状态。

- 使用智能告警管理工具前每日工单数量 500+，运维人员需要处理大量重复工单，重要故障无法快速响应，使用智能告警管理工具后每日工单数量 20+，故障恢复时间缩短 90%。

案例二：助力某省联社建设告警统一管理平台

【客户需求】

能够比较准确的收到应用告警，但并不能分析到基础资源，缺乏打通多层的问题发现。不能对事件进行分级，无法区分事件、告警、故障。

【解决方案】

- 建设统一告警中心，打通管理全域告警，并对于时间、告警和故障进行标准的级别管理和分类分级。
- 根据应用资产图谱的系统级的拓扑化溯源分析；通过统一故障处理中心，按照告警或人工上报升级为故障。

【客户价值】

- 能够方便简单的进行规则配置，完全覆盖目前 Zabbix 工具的告警规则；
- 聚合多平台告警统一管理，并分类、分层，帮助快速聚焦问题；
- CMDB 配置帮助在信息有欠缺的情况下，告警层面能够进行增强达到正确拓扑结构的告警压缩呈现。
- 智能算法方便使用，覆盖难以配置的复杂告警文本自动归类。
- 通过事件层级视图展示辅助排障，故障分析时间由原本 5-6 小时缩短为平均 30 分钟，分析时间减少 90%。

5. 部署方案

5.1. 部署规模与资源需求

- **环境要求**

  硬件：Intel x86 64 位芯片架构

  操作系统：标准 64 位 Linux（推荐 CentOS7.x 版本）

  内核版本：3.x 和 4.x

  浏览器：Google Chrome、Microsoft Edge（推荐）

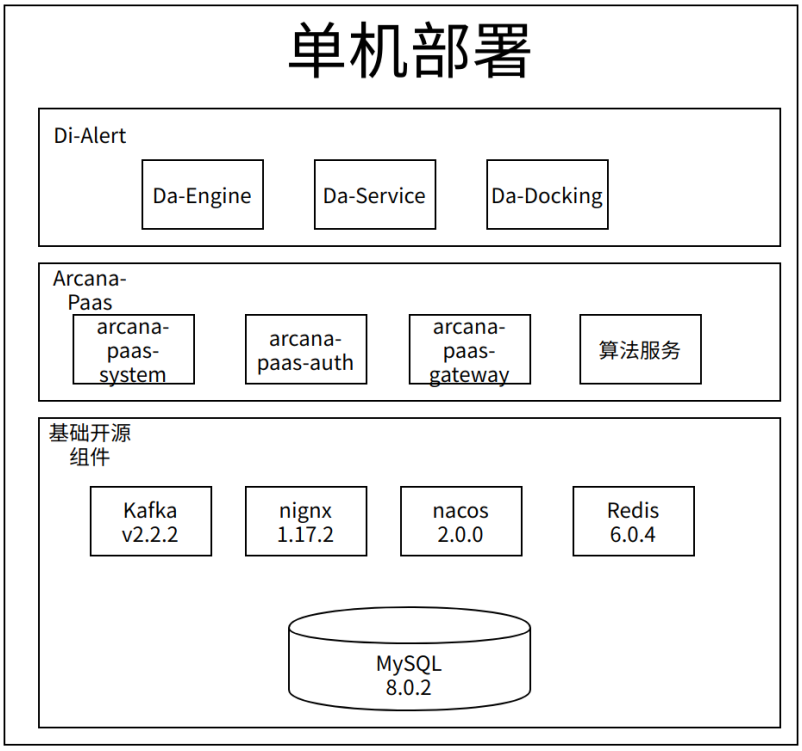
- **CPU 资源需求**

参考以下性能指标：

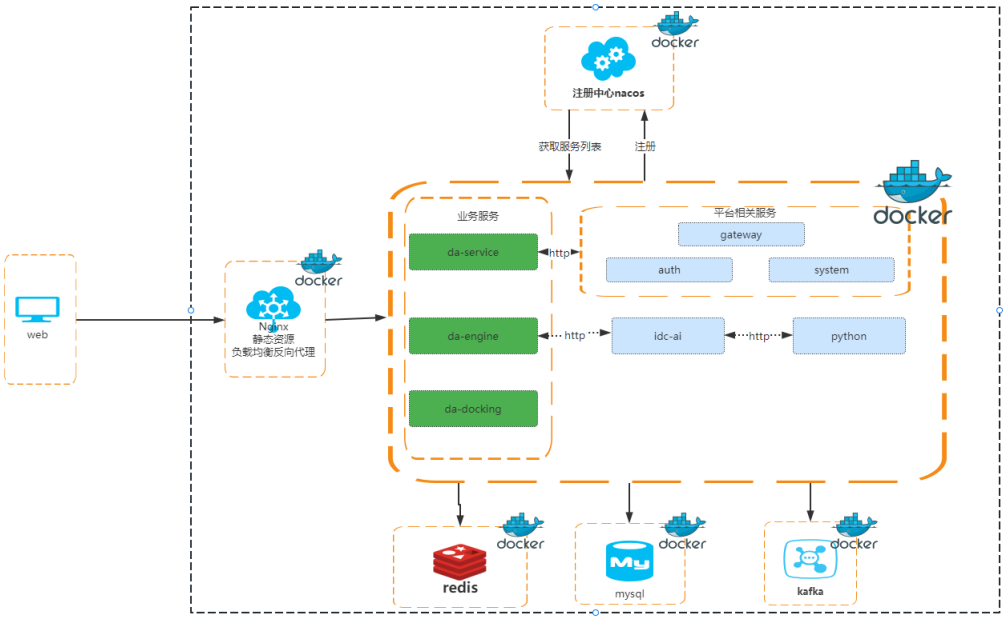
基线套餐	支撑的告警量	部署节点数	单节点配置	备注
单机最简套餐	20000 EPH	1	4C16G	单节点部署
最简集群套餐	50000 EPH	2	4C8G	集群高可用部署
标准集群套餐	60000 EPH	2	4C16G	集群高可用部署
高配集群套餐	200000+EPH	2	8C32G	集群高可用部署

5.2. 部署方案

- **单机部署方案（Docker 部署）**



- **单机部署下各组件调用方式**



- **集群部署方案（非 Docker 部署）**

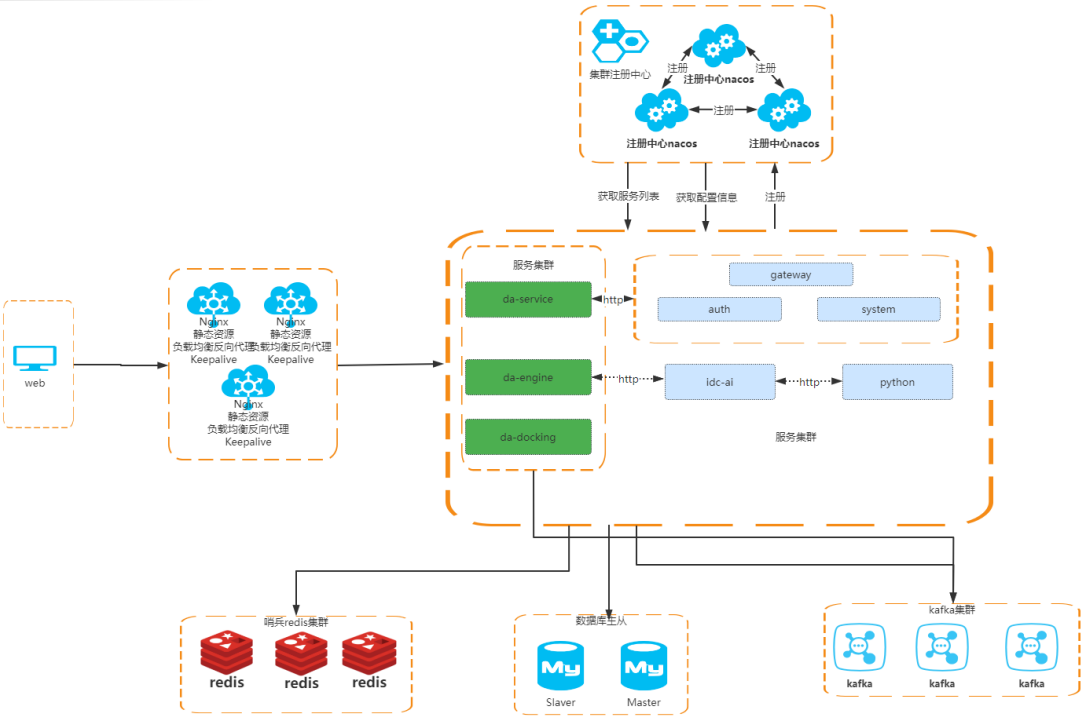
产品自研微服务均属于可扩展集群服务。开源组件满足集群部署最小方案进行集群部署架构设计。

集群部署资源为单节点部署资源*3。

注意：大部分微服务组件在 2 节点构成下即可实现集群高可用，但 Kafka、Redis 由于存在多副本仲裁机制必须需要使用 3 节点配置。为了平衡各服务器的容量，推荐使用三节点部署方案。

高可用集群部署

- **集群部署下各组件调用方式**


集群注册中心
注册
注册中心nacos
注册
注册
注册中心nacos
注册中心nacos
获取服务列表
获取配置信息
注册
服务集群
da-service
http
gateway
auth
system
da-engine
http
idc-ai
http
python
da-docking
服务集群
web
Nginx
静态资源
负载均衡反向代理
Keepalive
Nginx
静态资源
负载均衡反向代理
Keepalive
Nginx
静态资源
负载均衡反向代理
Keepalive
哨兵redis集群
redis
redis
redis
数据库主从
Slaver
Master
kafka集群
kafka
kafka
kafka