

# SOFAShark

业务智能可观测平台  
产品简介

产品版本：AntStack Plus 1.13.1

文档版本：20230708



# 法律声明

蚂蚁集团版权所有©2022，并保留一切权利。

未经蚂蚁集团事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

## 商标声明

 蚂蚁集团 ANT GROUP 及其他蚂蚁集团相关的商标均为蚂蚁集团所有。本文档涉及的第三方的注册商标，依法由权利人所有。

## 免责声明

由于产品版本升级、调整或其他原因，本文档内容有可能变更。蚂蚁集团保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在蚂蚁集团授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过蚂蚁集团授权渠道下载、获取最新版的用户文档。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

# 通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[ ] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

# 目录

1.什么是业务智能可观测平台	05
2.功能架构	06
3.实现原理	08
4.应用场景	12
5.基本概念	15

# 1. 什么是业务智能可观测平台

业务智能可观测平台 BOS (Business-Intelligent Observability Service) 是一款具有可视化监测能力的金融级监控产品。基于日志、指标、链路等海量数据进行多维聚合，向用户提供业务监控、应用监控、云原生监控、基础资源监控、日志查询分析、分布式链路等多角度的可视化监测功能，有丰富的可视化大盘，并提供了告警订阅功能。该服务可以帮助运维、研发、SRE (Site Reliability Engineer) 等快速地发现、定位问题、分析问题、解决问题，为线上系统可用率提供有效保障。

BOS 支持的功能特性如下：

- **全方位实时监控**：提供业务、应用、基础资源、云原生等各种视角的监控能力，可实现关键指标秒级、普通指标分钟级的监控，具有高可靠、高时效、低延迟的特点。
- **灵活的报警规则**：可根据业务特征、时间段、重要程度等维度设置报警规则，实现不误报、不漏报。
- **便捷的自定义配置**：具有丰富的自定义产品配置功能，可便捷、高效地进行产品、报警配置。
- **开放的技术栈配置**：可实现 Kubernetes、SOFA 技术栈应用部署即监控，通过简单技术栈配置，即可接入并监控非标业务应用。
- **可视化大盘**：丰富的可视化大盘，帮助您定制个性化的监控大盘。
- **分布式链路**：提供应用拓扑和链路查询功能，观测应用及服务之间的复杂调用关系、性能指标、出错信息与关联日志，从而实现故障根因分析、服务治理、应用开发调试、性能管理、性能调优、架构管控、故障定责等运维开发工作。
- **日志查询和日志关联**：提供日志查询和日志关联功能。用户不仅可以对日志执行查询操作，还可以进行历史查询和上下文查询，以及查看 Error 指标关联的错误日志和链路关联业务日志，更加方便高效地进行问题分析定位。
- **低资源占用**：在可靠传输大量监控数据时，保证对宿主机的 CPU、内存等资源的极低占用率。
- **高可用**：提供万台设备的分钟级监控部署能力，故障自动恢复，集群可伸缩。
- **稳定高效的时序和数据存储**：在线持续聚合数据，保证数据容量可控，提供智能分级存储、存放策略。

## 2. 功能架构

BOS 通过采集各种指标、日志和链路等数据，并进行海量数据的清洗、计算。以此来支撑产品层的应用监控、业务监控、平台监控、基础设施监控、告警管理和分布式链路等能力。作为一个企业级产品，BOS 提供资源租户隔离、访问鉴权控制和监控配置模板等企业级特性。并且提供数据高可用、服务高可靠、双机房容灾部署等平台特性。

基于 BOS 丰富数据和强大功能，可以支撑容灾巡检、故障重放、弹性扩缩、微服务治理和全链路压测等场景。



### ● 应用监控

BOS 能同时监控容器应用和经典应用，并通过 LDC、IDC 和单机实例等多视角、多维度逐层下钻分析，实时展现服务实例、依赖的中间件和基础资源运行状态、使用趋势和告警信息，发掘应用故障所在的层级和对象，保证应用的流畅运行。

### ● 业务监控

BOS 提供了灵活的、基于业务场景的自定义业务监控，通过业务监控可将不同监控图表展示到同一个屏幕上，通过不同的大盘模板、统计模板等形式来展示可观测数据，例如，分钟级多 Key、TopN 等，让用户可以全面、深入地掌握业务数据。

- **中间件监控**

BOS 默认集成了对消息、Mesh、数据库等中间件的监控，并支持在应用监控中查看应用所调用各中间件的情况。

- **基础资源监控**

支持对物理机、虚拟机、Kubernetes 集群和原生容器等资源的监控。

- **日志管理**

BOS 提供日志查询和日志关联功能。用户不仅可以对日志执行查询操作，还可以进行历史查询和上下文查询，以及查看 Error 指标关联的错误日志和链路关联业务日志，更加方便高效地进行问题分析定位。

- **分布式链路**

分布式链路帮助运维人员、开发人员和架构师看清楚复杂的大规模微服务架构下的应用及服务之间的复杂调用关系、性能指标、出错信息与关联日志，从而实现故障根因分析、服务治理、应用开发调试、性能管理、性能调优、架构管控、故障定责等运维开发工作。

- **告警管理**

针对各资源对象，BOS 允许用户灵活地配置自定义告警规则，并支持多种订阅方式，如邮件、短信、钉钉等。当监控数据满足阈值条件时，第一时间通知对应的运维人员，帮助其发现异常及原因。

- **企业级特性**

在企业级特性层面，BOS 包含的能力如下：

- 提供多层级业务和资源隔离机制，比如租户、workspace 等，保证监控数据的安全性。
- 支持监控具有多 VPC 服务实例的应用，并以应用中心视角展示监控数据。
- 支持监控配置模板导入与导出，使测试环境的应用监控配置可在生产环境一键激活，避免了重复配置，也保证了发布流程的标准化和可控性。

## 3. 实现原理

### 监控的通用逻辑



- **定义数据源**：首先，需要建立元数据基本模型，元数据是监控系统的根基。例如：定义应用、部署实例、机房信息，单元化信息等。在 SOFAShield 场景下，这部分信息需要从 PaaS 侧自动获取。
- **数据采集**：通过安装在机器上的 Agent 采集监控数据，这部分可以是日志，也可以是通过各种方式获取到的指标。
- **数据清洗**：将采集得到的非结构化的数据，解析为监控系统可以处理的结构化信息。这部分解析能力需要是事先通过监控系统预设好的某种规则。例如，日志解析规则、Prometheus 协议规则等。

举个例子，有业务日志样例如下，希望通过监控获取每一分钟各商品各自创建了多少笔交易这一数据。

```
2012-11-11 11:11:11,2950211004,衣服,交易,创建,7,Y,  
2012-11-11 11:11:12,2950211005,衣服,交易,创建,8,Y,  
2012-11-11 11:11:13,2950211006,食品,交易,创建,9,Y,  
2012-11-11 11:11:14,2950211007,家居,交易,创建,11,Y,  
2012-11-11 11:11:15,2950211008,食品,交易,创建,7,N,  
.....
```

#### 说明

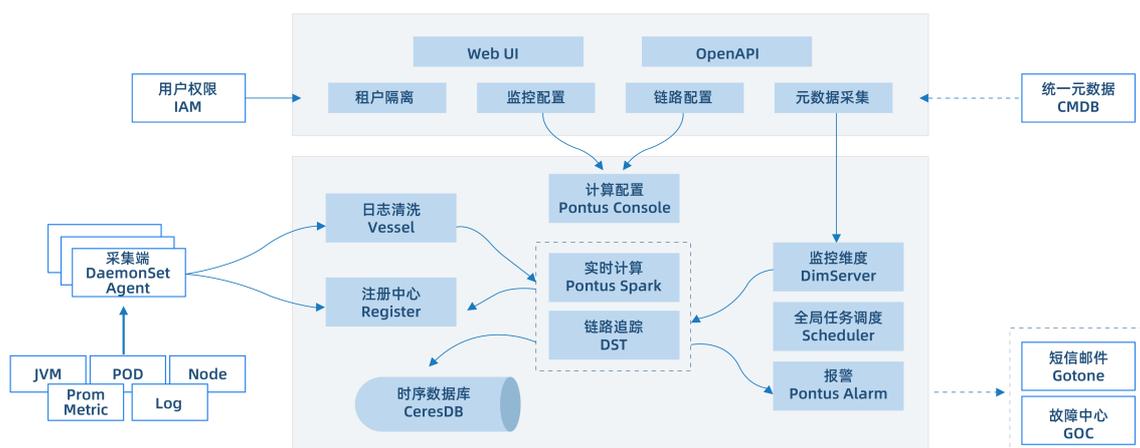
日志格式为：日志打印时间, 订单id, 商品, 服务名, 方法名, 耗时, 结果。

- **数据统计**：由于监控系统面对的是海量集群，在获取结构化数据之后，需要对数据进行数据统计。统计方式可以有很多种，比如求行数、求和、求平均、最大/最小值等统计方法。
- **预警配置**：可在统计数据上定义类型丰富的预警规则，包括绝对值、同比、环比、最近 N 分钟求和等，支持定义多项规则和逻辑运算。

### 实现原理

RMS 的基本实现原理是在所有的应用主机上部署 Agent（代理），从而采集主机和应用的各类指标、日志和链路等数据，并将其存储在 CeresDB 中，通过在 PontusSpark 中进行分析计算，实现在不同产品场景中的可视化展现和告警通知。

#### RMS 实现原理示意图



## 采集层

### DaemonSet Agent (又称 Pontus-Agent) 日志采集代理

- 负责所有的数据的最终采集，包括原始日志拉取和指标型数据采集。
- 具有插件化的能力，统一本地调度能力，负责拉起插件和解析数据，解析完了之后做一次聚合计算。然后放入本地的缓存中，等待 Vessel 来拉取数据。
- 提供一次性的任务执行能力，主要用于性能分析。
- 启动时会和 Register 进行通信。通信之后会获取 Agent 运行所需要的所有配置，包含运行时采集配置，Vessel 建连的配置等。

### Register 注册中心

- 负责与 Agent 之间保持网络心跳，收集所有 Agent 的状态，版本透视等信息。
- 负责 Agent 与 Vessel 的配置生成与下发，即负责管控所有的采集配置。
- 负责管控 Agent 与 Vessel 之间的连接与会话 (session)，Register 感知 Vessel 集群负载，负责通知 Agent，应该和哪个 Vessel 地址进行建连。

### Vessel 流量清洗组件

- 抽象来看，Vessel 其实就是一个独立部署的 Agent，这个 Agent 通过 remote input 的形式，拿到了日志或者其他的数据。
- 一个 Vessel 服务可以托管 N 个 Agent，即从 N 个 Agent 中收集数据。
- Vessel 可以通过一系列的解析规则，最终将非结构化的数据变成结构化的数据并返回，也就是所谓的数据清洗。
- 所有上层组件（包括计算层与链路层组件）都是通过 Vessel 来获取数据。

## 计算层

### DimServer 维度数据服务 (又称元数据服务)

- 包括维度数据的读和写的服务。在这一层上无业务语义，业务语义为上层产品层注入。
- 计算和采集层都会用到维度数据（元数据），通过 DimServer 提供的 Java Client 来实现数据通讯。
- 为适配任意维度数据结构，DimServer 实现了维度数据 Table 化，即使用若干张宽表来处理所有可能的元数据表结构，这类宽表被称为维度表。

## PontusConsole 监控数据平台的管控端

- 主要负责内部运维性管控、系统配置，以及提供给产品使用的配置接口。
- 提供操作维度表、指标表的标准数据服务接口。

## Scheduler 全局任务调度器

- 不依赖任何中间件，实现全局任务调度能力，仅用于监控系统内部，实现功能自闭环。
- 负责根据配置信息定时生成并分发监控的计算任务。
- Scheduler 可以实现多机房部署，通过数据库维持高可用。

## PontusSpark 分布式计算引擎

- 功能强大的 Spark 计算集群，负责接收产品层的计算配置，并对数据进行离线计算和统计。
- 从 Register 中获取监控数据采集的 Vessel 地址，并通过 Vessel 获取必要的监控数据。

## PontusAlarm 监控告警组件（又称 RMSAlarm）

- 主要负责将监控计算完成的告警信息以短信、邮件、钉钉等方式向外推送。
- 在 SOFAShark 输出的模式下，告警渠道主要通过 Gotone 服务提供。

## MonitorGateway 分布式链路追踪

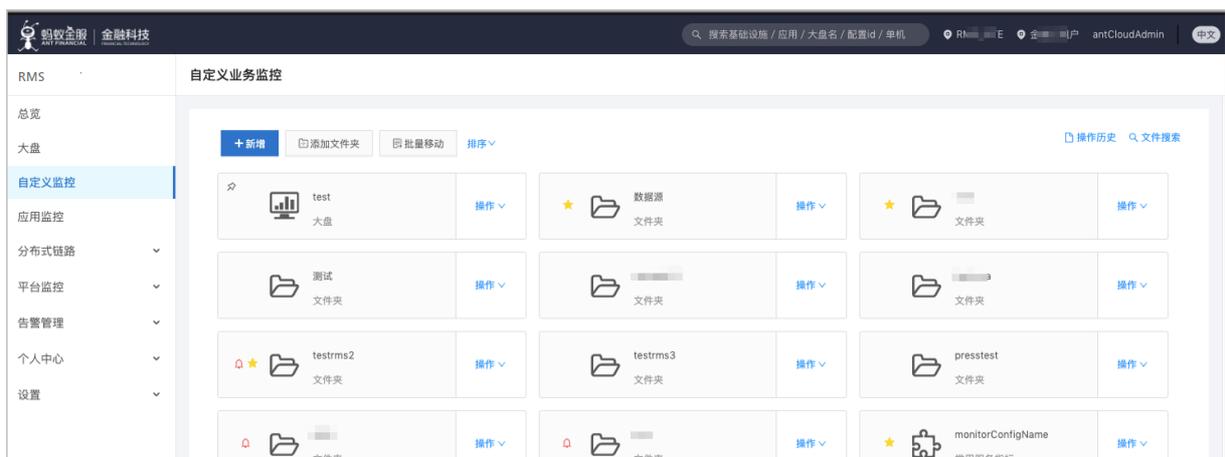
- 主要负责分布式链路处理的相关功能。
- 对于链路信息的收集，提供三种方式，分别为主动日志采集、SLS 日志采集以及链路日志上报。

## 数据层

主要是由时序数据库 CeresDB 来承载。CeresDB 是蚂蚁自研的时序数据库，时序引擎是一种存储和管理时间序列数据的分布式数据库，为时间序列提供高性能读写、预处理计算、可视化查询等功能。

## 产品层

产品层（应用名为 monitorprod）承载了 RMS 的所有页面以及用户交互、配置逻辑，是监控对客的主要门户。如下图所示：



产品层负责与用户权限系统打通，读取用户身份信息。同时，产品层也负责打通 PaaS 元数据，将元数据同步至 DimServer。

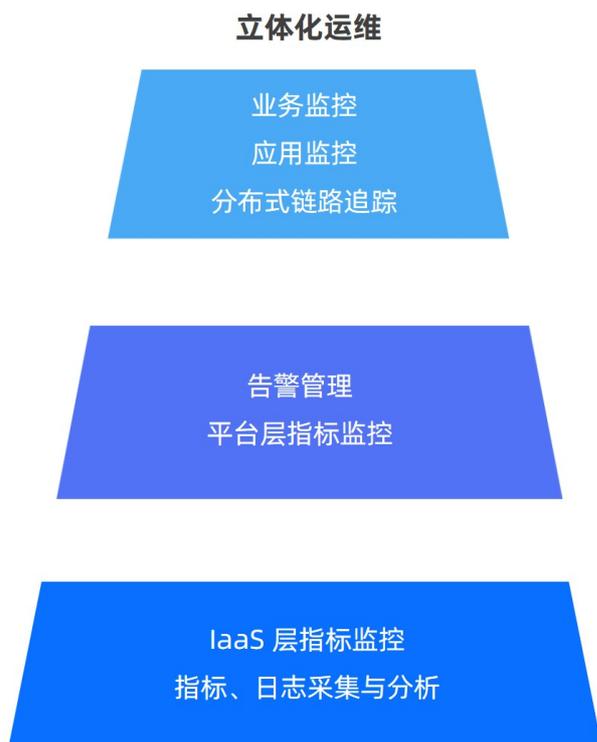
② 说明

PaaS 元数据，是指通过 PaaS 系统发布的描述应用的基本信息，例如应用 IP、机房、单元化等信息。

## 4. 应用场景

### 立体化运维

深度对接 Kubernetes、SOFA 等技术栈应用服务，一站式收集基础设施、中间件、应用运行时数据和业务数据，通过指标监控、日志分析、链路追踪、告警订阅等功能，对应用性能、运行状态和资源使用等提供立体化运维分析，及时发现并定位应用、资源及平台的问题。



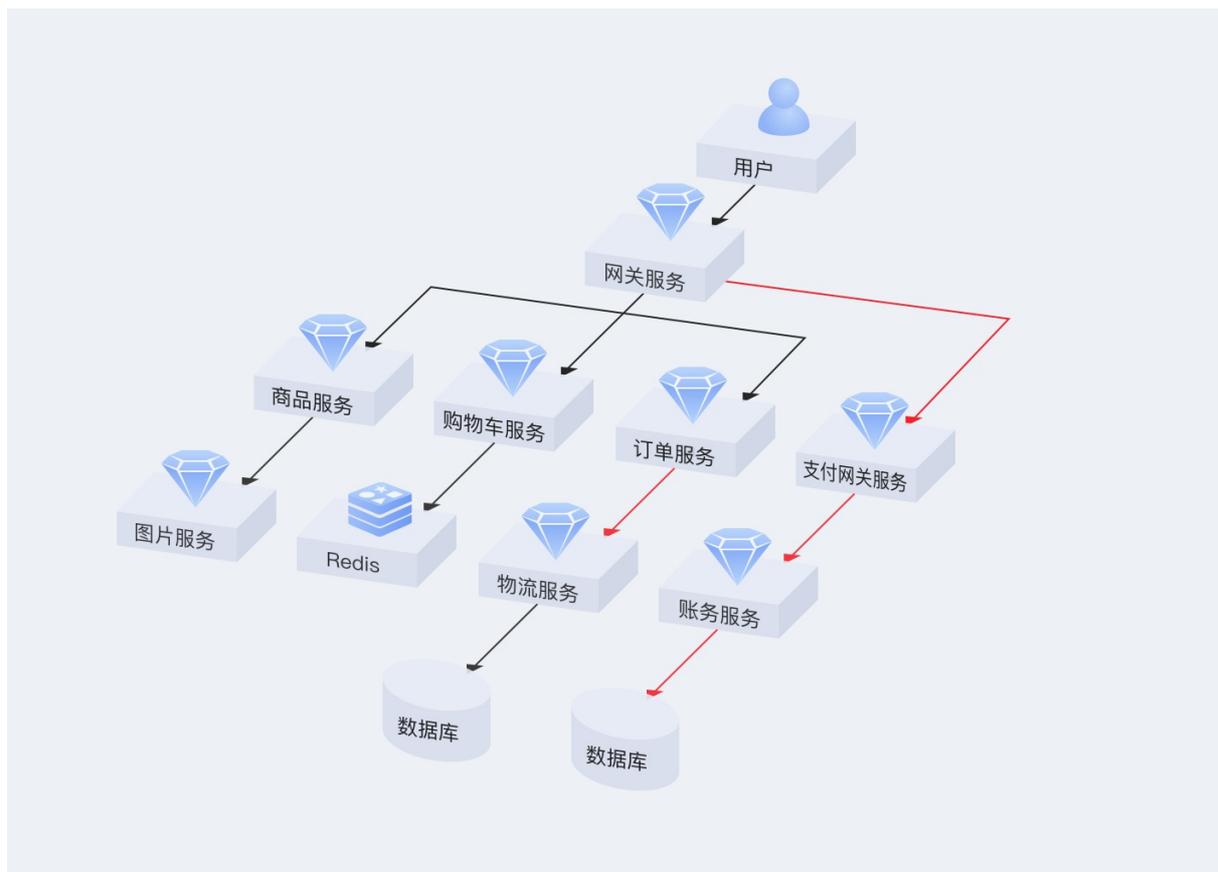
- **一站式分析**：在应用总览中可查看应用错误指标趋势、应用链路、应用指标和系统指标等，提供一站式的应用分析能力。
- **全方位监控**：覆盖基础设施、云数据库、云中间件、应用等多个维度监控，提供一站式运维能力。
- **故障关联分析**：以应用为中心，覆盖组件、实例、主机、云资源等多维度关联分析，迅速找到异常故障点。

### 问题分析与快速定位

在分布式场景下，服务调用错综复杂，问题分析与定位非常困难，分布式链路跟踪系统能迅速定位到有问题的服务，协助快速解决问题节点。

- **完整的应用调用拓扑关系**：自动发现该服务的历史调用，以及对所有中间件的调用，绘制整个系统调用关系的拓扑图。
- **快速定位不健康应用**：在调用关系拓扑中，对不健康应用进行显式标识，便于快速发现有问题的应用并进行分析。
- **服务性能详情**：调用拓扑中的应用都可以单独进行下钻分析，可以从吞吐量、错误率、响应时间等指标出发，对应用性能进行详细分析。

#### 问题分析与快速定位示意图

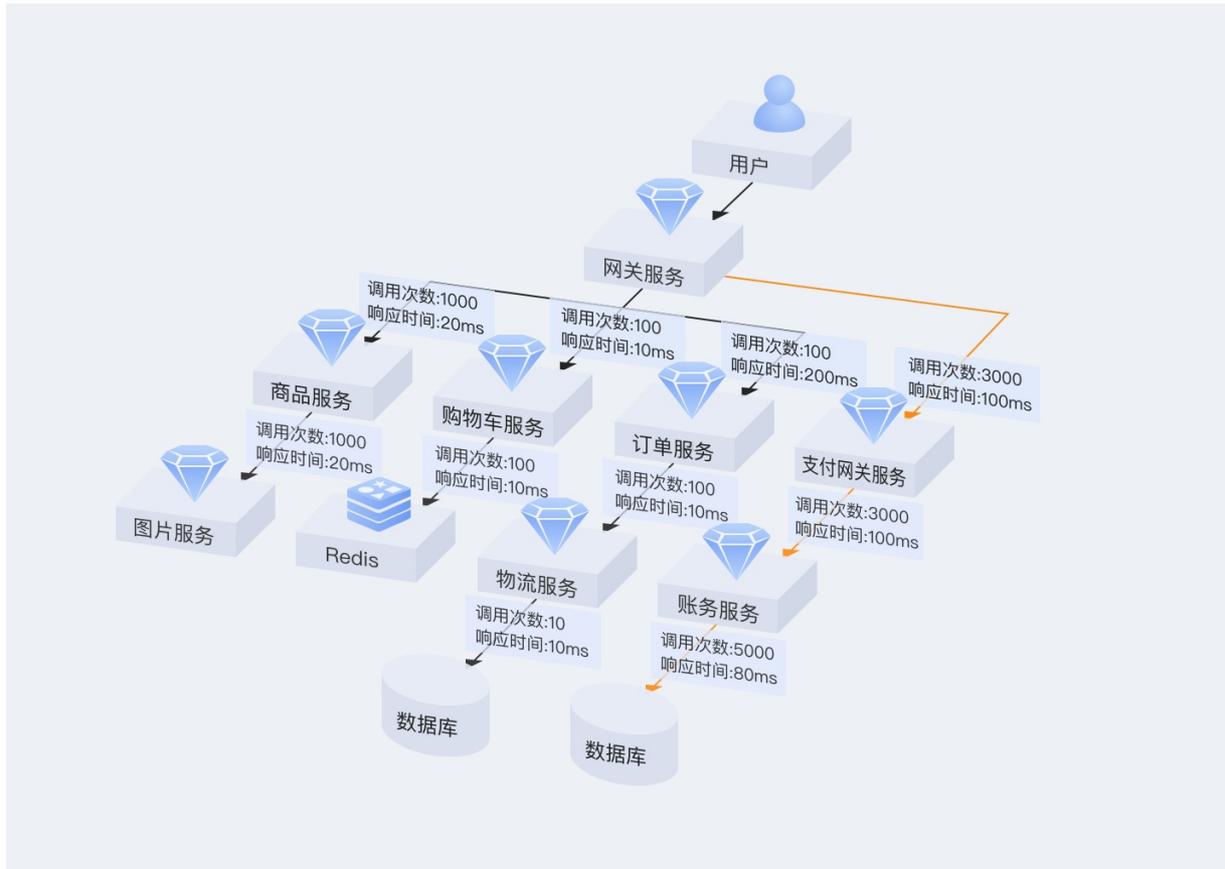


## 应用性能优化

在调用关系拓扑中，可以对各个应用的调用次数以及耗时情况进行分析，找到负载较高以及负载较少的应用，从而对资源进行合理利用。

- **调用链路聚合汇总：**对所有的调用信息进行聚合汇总，对各个应用的调用情况以及响应情况进行分析。
- **关键路径：**快速发现整个系统调用拓扑中，关键应用的路径。
- **优化不合理调用：**及时发现某些不合理的调用并进行处理，如频繁进行数据库操作等。

性能优化示意图



## 5. 基本概念

基本概念表中的基本概念按中文拼音进行排序。

### 报表 (Report)

指包含单个或多个数据源的视图，集中展示各数据源的监控结果。

### 大盘 (Dashboard)

指包含多个报表的一个页面。

### 单机视角

从应用实例（单机）维度进行指标数据的聚合，从单机的空间分布和时间分布上对应用监控指标数据进行对比分析。

### 订阅

订阅后，通知组内的成员会收到监控告警通知。

### 服务指标

服务指标将应用相关的 Error、Service、SAL、CAL、DAL 等服务指标进行聚合透出，从 IDC（机房）、LDC（单元化）、单机的空间分布和时间分布上进行对比分析，一个入口总览分析应用相关的所有监控数据。

### IDC 视角

从 IDC（机房）维度进行指标数据的聚合，从单机的空间分布和时间分布上对应用监控指标数据进行对比分析。

### 监控产品 (Monitoring Products)

指为实现自定义监控而提供的一些工具，可用于配置监控指标、生成数据源。

### 监控对象

由一个或者多个维度描述的被监控目标，比如说一个容器就可以用单个容器的维度描述。一个应用的一个逻辑 Zone 就需要用两个维度来描述 (App + Zone)。监控对象实际上是监控数据的归属。

### 框架配置

基于 SOFA/SOFABOOT 框架开发的应用，PV、Service、SAL、SQL、Cal、CE Thread 等监控项会自动基于默认框架下的日志路径采集指标，仅需开启监控即可。

### LDC 视角

从逻辑机房（LDC）维度进行指标数据的聚合，从单机的空间分布和时间分布上对应用监控指标数据进行对比分析。

### 配置模板

BOS 提供监控配置模板功能，支持将应用和自定义监控告警以配置模板 (JSON 文件) 导出，然后一键导入其他环境，如该环境已部署同名应用，则监控告警配置即生效，帮助投产运维更加高效便捷和一致。

### 数据源 (Data Source)

指通过监控产品配置的监控指标。

### 通知人 (Notificant)

指报警消息的接收人，接收渠道为手机短信。

### 通知组 (Notification Group)

每个通知组可包含一个或多个通知人。在管理通知时，可通过通知组订阅，将报警内容发送给通知组内所有的通知人。

### 预警（Alert）

指通过配置的报警规则，触发报警通知。

### 指标

一个被监控对象数量特征的概念和数值。通常可以用若干个指标来描述一个监控对象随时间变化的情况，达到监控谁发生了什么事的最佳效果。

### 自定义监控配置

非 SOFA/SOFABoot 框架开发的应用，需为每个监控项配置采集日志路径和列值，比如 Error、Dal。如果是 SOFA/SOFABoot 框架开发的应用，但不希望使用默认日志路径监控的，也可以切换到自定义监控配置。