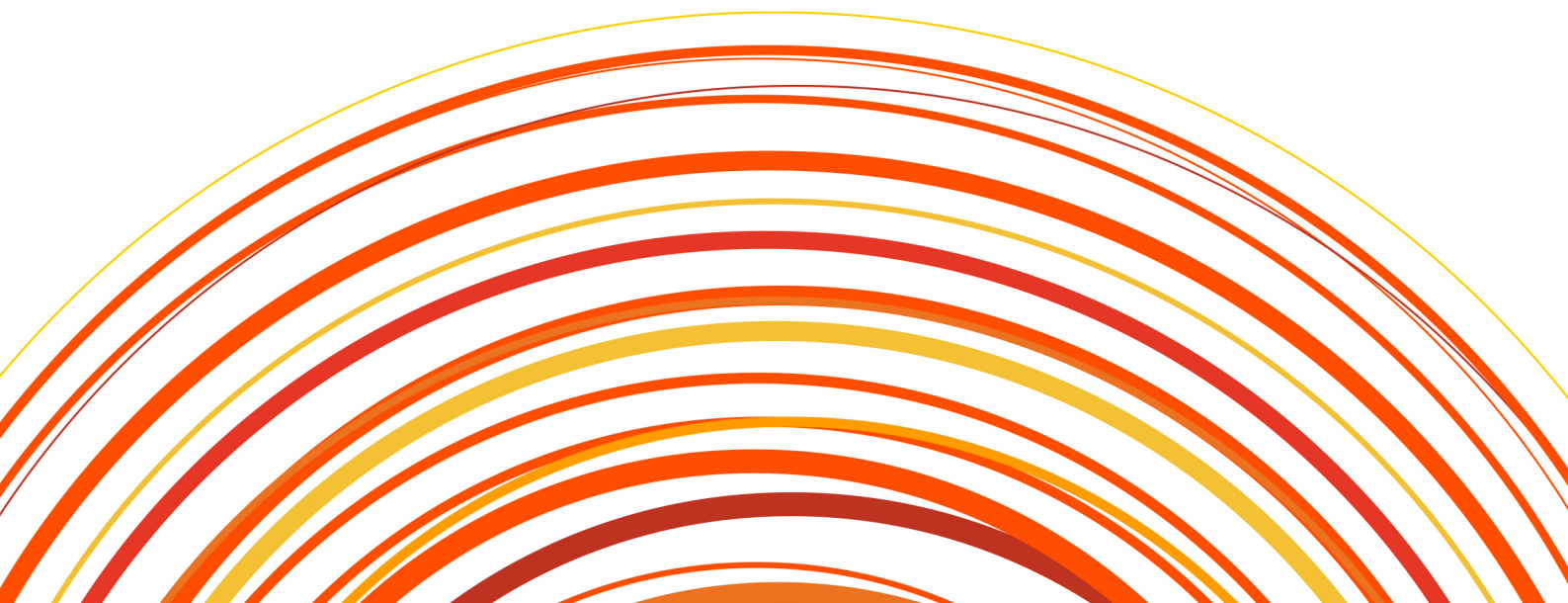




产品白皮书

上海驻云信息科技有限公司



前言

目前有一个新兴的概念在云计算时代下发展起来了，叫做可观测性，这并不是一个新的概念，在这个概念进入到计算机软件领域前，我们其实是通过监控这种方式去保障整体系统的稳定性，似乎计算机领域也很少有人提及可观测性。如果我们要完成对一个计算机系统的监控，那么监控的就是计算机所产生的数据，而监控前提是被监控对象要能够产生可被观测的指标等数据，如果指标或者数据少，即我们可观测的数据少，那么监控带来的价值和意义就会变得少。比如，我们仅仅能监控到一台服务器是否正常，那么只能判断这台服务器的状态，完全无法观察到上面的操作系统的状态，如果我们监控了操作系统的指标，那么我们仅仅能判断操作系统的状态，完全无法判断安装在这个操作系统之上应用的状态，如果要监控了应用，那就需要每个应用本身具备可观测性，否则我们可能也只能从操作系统的角度仅仅判断这个应用是不是在运行。所以监控是一个动作，而前提条件是被监控的对象要具备可观测性，而更多的可观测数据也就意味着我们能更好的掌控整个系统。

随着互联网的发展，我们即将面对更多的互联网设备接入（IOT 技术下的物联网，工业互联网），同时会有更多的新的云技术，数据技术出现，而这些设备和新的技术也需要具备可观测性，以及能够监控管理他们的监控产品。为了保障一个个如此复杂构建的系统，监控和可观测性也将不断的发展。

观测云作为驻云科技推出的云时代的可观测性平台也是随着历史的潮流和用户的需求应运而生。

目录

前言.....	2
概述.....	6
产品架构.....	7
产品优势.....	8
关键技术.....	9
功能介绍.....	10
数据采集.....	10
DataWay 数据网关.....	10
DataKit 采集器.....	11
场景.....	13
仪表板.....	13
笔记.....	14
查看器.....	15
视图变量.....	16
可视化图表.....	17
简单查询.....	17
表达式查询.....	18
DQL 查询.....	18
Json.....	19
链接.....	20
时序图.....	20
概览图.....	22
饼图.....	22
柱状图.....	24
SLO	25
排行榜.....	25
仪表盘.....	26
散点图.....	27
气泡图.....	27
表格图.....	28
矩形树图.....	28
漏斗图.....	29
中国地图.....	29
世界地图.....	30
蜂窝图.....	30
日志流图.....	31
对象列表图.....	31
告警统计图.....	32
文本.....	33
视频.....	33
图片.....	34
命令面板.....	34

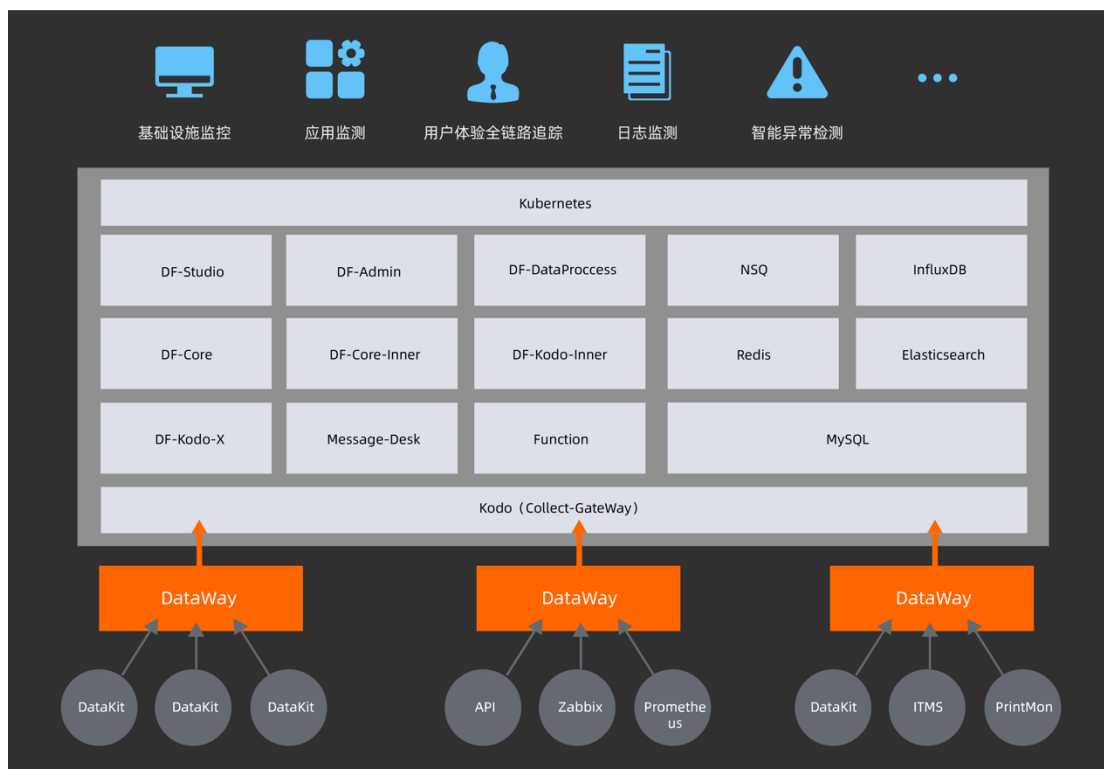
IFrame	35
组合图.....	35
事件.....	36
事件管理.....	36
未恢复事件.....	36
事件详情.....	37
事件聚合.....	38
基础设施.....	38
主机.....	38
容器.....	40
进程.....	41
自定义.....	42
指标.....	42
指标管理.....	42
指标字典.....	44
日志.....	45
日志管理.....	46
日志详情.....	47
Pipelines	48
生成指标.....	49
黑名单.....	50
备份日志.....	50
应用性能监测.....	50
服务.....	50
关系图.....	51
链路.....	52
用户访问监测.....	54
查看器.....	54
用户访问详情.....	58
追踪.....	59
可用性监测.....	60
可用性监测管理.....	60
自建节点管理.....	61
安全巡检.....	61
安全巡检管理.....	61
安全巡检事件详情.....	62
监控.....	63
监控器.....	63
SLO	66
工作空间管理.....	68
基本设置.....	68
API Key 管理.....	69
成员管理.....	69
SSO 管理	70

通知对象管理.....	71
内置视图.....	71
分享管理.....	72
付费计划与账单.....	73
按量付费.....	73
计费价格.....	74

概述

观测云是一款旨在解决云计算，以及云原生时代系统为每一个完整的应用构建**全链路的可观测性**的云服务平台。观测云是由驻云科技自 2018 年以来全力打造的产品，产品的目标是**为中国的广大基于云计算的开发项目组**提供服务，相较于复杂多变的开源产品，如 ELK, Prometheus, Grafana, Skywalking 等，观测云不单纯的只是提供一种监控类的产品，更重要的是提供整体可观测性的服务，我们除了在**底层存储和系统架构上是一体化的**基础上，也把所有关于云计算及云原生相关的技术栈进行了完整的分析和解构，任何项目团队可以非常轻松的使用我们的产品，无需再投入太多的精力去研究或者改造不成熟的开源产品，同时观测云是以服务方式，按需按量的方式收取费用，完全根据用户产生的数据量收取费用，无需投入硬件，同时对于付费客户，我们还会建立专业的服务团队，帮助客户构建**基于数据的核心保障体系**。

系统架构



产品架构



观测云平台架构总体分为四层：

- **数据采集层：**观测云的数据采集支持多种数据采集器，包括官方出品的 DataKit，以及开源的 Telegraf 和 Prometheus 等，同时用户也可以通过 WDF 和 DataWay API 开发自定义的采集器。观测云数据采集器能够采集云、基础设施、应用、指标、日志、链路、Web、App 和小程序等多种数据，满足实时、高频的数据采集需求。
- **数据网关层：**观测云的数据网关层基于自主研发的 DataWay 网关可实现数据代理上报和数据清洗的功能。
- **数据分析和处理层：**观测云的数据分析和处理层分为三大模块，观测云数据分析和洞察平台、观测云数据处理开发平台以及观测云管理后台。观测云基于时序数据存储引擎以及异常检测引擎实现对数据的实时洞察、关联分析、异常检测、原因追踪；观测云数据处理开发平台基于实时数据处理引擎和函数计算引擎实现数据处理函数的开发和在线发布。
- **API 网关层：**观测云基于 K8S 的微服务架构，通过 Inner API 提供的扩展性，满足企业开发自定义数据应用的需求。

产品优势

统一存储

观测云采用了统一的存储方案，底层采用了多模数据湖形态，我们将时序，日志，对象，链路，事件等数据结构进行了统一的存储，通过行协议（Line Protocol）经过统一的 Dataway 接口实现一致性高效低延时的写入，由自研的查询语言 DataFlux Query Language（DQL）进行统一的查询与分析。

强大而安全的数据采集方案

我们提供了自主研发的强大的数据采集端 DataKit，集成了全面数据采集能力，包括主机（云主机），容器，进程，中间件，数据库，消息队列，各种语言开发的应用，网络访问性能，黑盒拨测，安全巡检等。同时我们也兼容开源的主流数据采集方案，可以与 Datakit 实现快速的集成，如 Prometheus，Telegraf 等，与这些方案相比较，除了能够采集对应技术栈相应的指标数据，日志数据之外，最为强大的部分是可以有效的将所有的数据构建统一的关系，方便使用者可以快速的寻找指标与指标之间的关联关系。

全链路可观测性

基于强大的数据采集能力，观测云构建了从基础设施，容器，中间件，数据库，消息队列，应用链路，前端访问，系统安全，网络访问性能全链路的可观测性，基于我们的标准产品，当用户正确的配置了 Datakit 以后，可以很快的实现自己项目的完整可观测性的构建，同时基于行协议（Line Protocol），以及我们的场景构建能力，用户还可以自定义所需观测的指标方便的整合在一起，实现进一步的可观测性。

友好的用户界面

观测云整体作为一个面向可观测性的完整技术产品，本身存在着非常多的技术门槛，相较于开源的各种方案，我们从一开始就非常强调整如何有效的降低用户使

用产品的学习成本以及提升用户的易用性。因此从 DataKit 的安装部署，包括所有的可配置能力，观测云尽量选择降低用户的配置难度，以符合大部分程序员和运维工程师的习惯，同时提升整个 UI 的易用度和专业度，让使用者能很快了解产品的用户和其所带来的价值。

技术强大

观测云整个产品的构建过程中，我们积累类强大的技术体系和技术实力，除了拥有非常高性能的且完全可跨平台的 Datakit 以外，强大的数据处理能力的 DataWay 数据网关，拥有自主查询语言 DQL，自主研发的日志文本数据批处理脚本 pipeline，以及可实现完全安全巡检的脚本模型 Scheck，还有强大的算法开发平台 Function。

基于服务

观测云作为一种面向 Devops，帮助项目组构建完整可观测性的产品，除了提供产品本身的能力之外，我们也将为我们的商业客户提供全方位的服务，为每一个客户提供一个技术服务团队，在使用过程中，协助商业客户中每一个使用者，无论是程序员，测试工程师，还是运维工程师，能够有效的从使用观测云的过程中获得真正的收益。

关键技术

观测云作为云时代的系统可观测性平台，包含了四大关键技术：

1. 基于时序数据库和列式数据的数据存储技术

时序数据库和列式数据库具有高压缩比和优越的写入和查询性能，在数据写入端能够满足海量、高频的数据写入请求，同时在数据读取端能够实现灵活的多维度查询和关联分析

2. 基于 Elasticsearch 数据库的文本数据存储技术

Elasticsearch 数据库实现日志，对象，链路，事件等数据结构的统一存储，通过行协议（Line Protocol）经过统一的 Dataway 接口实现一致性高效低延时的

写入，由自研的查询语言 DataFlux Query Language (DQL) 进行统一的查询与分析

3. 独创的旁路数据采集技术

数据采集是大数据平台进行数据分析的初始环节，观测云的大部分数据采集器基于旁路技术实现数据采集的功能，能够在尽量不影响业务系统的前提下完成数据采集的任务

4. 数据一致性保证和系统的高可靠性

从数据采集到数据清洗到数据处理的整个链路上，观测云基于消息队列技术和多重尝试机制保证了数据的一致性，弥补了时序数据库和列数数据库的弱势。同时基于 k8s 以及阿里云高可用的时序数据库产品保证了整个系统的可靠性。

5. 云原生

整个平台在底层技术模块的选型以及整体架构上，100% 基于云原生产品实现，在保证功能的完整性和技术架构的可靠性的前提下实现了高性价比。

功能介绍

数据采集

观测云具有全域数据采集能力，支持机器数据、日志数据、链路追踪数据、业务数据、云平台数据、行业公开数据等多种数据源采集。观测云的数据采集具有实时性特点，除了官方开发的标准数据采集器 DataKit 外，也支持 Telegraf、Prometheus Exporter 等第三方数据采集器。

DataWay 数据网关

DataWay 是部署在用户环境中的数据网关，主要作用有两个：

- 1) 接收采集器发送的数据，然后上报到观测云中心进行存储；
- 2) 将采集的数据进行处理后再发送到观测云中心进行存储。

同时 DataWay 还拥有如下的高级功能：

1) 支持多路由配置，可指定数据采集器的上报路由，并针对不同路由做指定的数据处理。

2) 支持引入 Lua 脚本对数据进行处理后再上报到观测云中心。当有如下需求时可使用 Lua 脚本：

- 需要对采集的数据进行清洗，比如添加、修改、删除标签/指标，甚至删除整个指标集；
- 需要将第三方数据源（比如 MySQL、Postgres、SQL Server、API 请求、CSV 文件、JSON 文件）中数据合并到采集的数据点然后在上报观测云。

DataKit 采集器

DataKit 是一款驻云官方开发的实时数据采集器，支持上百种数据的采集，涵盖绝大部分数据类型。所有数据源均可在观测云控制台的「集成」中找到对应的配置教程及说明。

DataKit 采集数据后需发送到 DataWay 数据网关，由 DataWay 网关将数据最终上报到观测云中心进行存储。DataKit 需部署到用户自己的 IT 环境中，支持多个操作系统。用户可登录观测云控制台的「集成」—「DataKit」页面查看和使用的 DataKit 的安装指令。

集成 DataKit Function DCA 移动端

官方提供标准的 DataKit 采集器，用来从你的系统和应用程序中收集各种指标和日志类集成数据

Linux Windows MacOS Kubernetes 离线安装 DataKit 升级

在 Linux 上安装

前提：需使用 Linux 2.6.23 或更高版本，支持ARM、x86全架构安装

- 选择 DataWay 数据网关地址
 - OpenWay <https://openway.guance.com>
- 复制下面的安装指令到服务器中运行即可


```
DK_DATAWAY="https://openway.guance.com?token=tkn_297t...ic988" bash -c "${curl -L https://static.guance.com/datakit/install.sh}"
```

额外支持的安装变量如下，只需要在 DK_DATAWAY 前面追加即可，多个环境变量之间以空格分割

- DK_DATAWAY：指定 DataWay 地址，含 TOKEN
- DK_CLOUD_PROVIDER：支持安装阶段填写云厂商(aliyun/aws/tencent)
- DK_NAMESPACE：支持安装阶段指定命名空间(选举用)
- DK_GLOBAL_TAGS：支持填写全局 tag，如 project="abc",owner="张三" (多个 tag 之间以英文逗号分隔)
- DK_HTTP_LISTEN：支持安装阶段指定 DataKit HTTP 服务绑定的网卡 (默认 localhost)
- DK_HTTP_PORT：支持安装阶段指定 DataKit HTTP 服务绑定的端口 (默认 9529)
- DK_INSTALL_ONLY：仅安装，不运行
- DK_DEF_INPUTS：默认开启的采集器列表，格式范例：input1,input2,input3
- DK_UPGRADE：升级到最新版本 (注：一旦开启该选项，其它选项均无效)
- DK_INSTALLER_BASE_URL：可选择不同环境的安装脚本，默认 <https://static.guance.com/datakit>
- HTTPS_PROXY：通过 DataKit 代理安装

DataKit 支持通过 DCA 进行远程管理。DCA（DataKit Control APP）是一款桌面客户端应用，旨在方便管理已经安装和配置的采集器，支持查看集成列表、配置文件管理、Pipeline 管理、集成配置文档在线查看等功能。您可以通过 DCA 远程连接 DataKit，在线变更采集器，变更完成后保存更新即可生效。

在观测云工作空间，依次点击「集成」-「DCA」，即可下载安装包。下载完成后，可安装在您的电脑远程管理 DataKit。

【观测云】 退出

搜索

运行情况 采集器配置 Pipeline配置 帮助

keqi_... (10.1...) unknown

Wen... (10.1...) online

iz23... (172...) unknown

luho... unknown

重连Datakit 刷新

基本信息

版本: 1.1.9-rc1 系统类型: darwin/amd64
 运行时间: 1h22m25.22s 容器运行: 否
 发布日期: 2021-09-28 10:39:28 IO消耗统计: inputCh: 0/1024, highFreqInputCh: 0/2048
 分支: master

采集器运行情况

采集器	实例个数	数据类型	频率	平均IO大小	总次数	点数	首次采集	最近采集	平均采集耗时	最大采集耗时	崩溃次数	当前错误(时间)
cpu	1	M	2.91/min	1	494	493	3 hours ago	a few seconds ago	134.96µs	2.39ms	0	-
disk	1	M	2.91/min	7	3458	493	3 hours ago	a few seconds ago	610.08µs	43.68ms	0	-
diskio	1	M	2.91/min	2	990	494	3 hours ago	a few seconds ago	1.35ms	7.51ms	0	-
host_processes	1	O	0.10/min	491	8359	17	3 hours ago	2 minutes ago	29.00s	39.51s	0	-
hostobject	1	O	0.10/min	1	18	17	3 hours ago	2 minutes ago	72.24ms	118.83ms	0	-
mem	1	M	2.91/min	1	495	494	3 hours ago	a few seconds ago	198.71µs	22.53ms	0	-
net	1	M	2.91/min	8	4101	494	3 hours ago	a few seconds ago	12.06ms	96.31ms	0	-

场景

在观测云中，用户可以根据不同的视角构建不同的洞察场景仪表版、记录笔记以及自定义查看器，从而满足不同业务的场景需求和数据分析。

仪表板

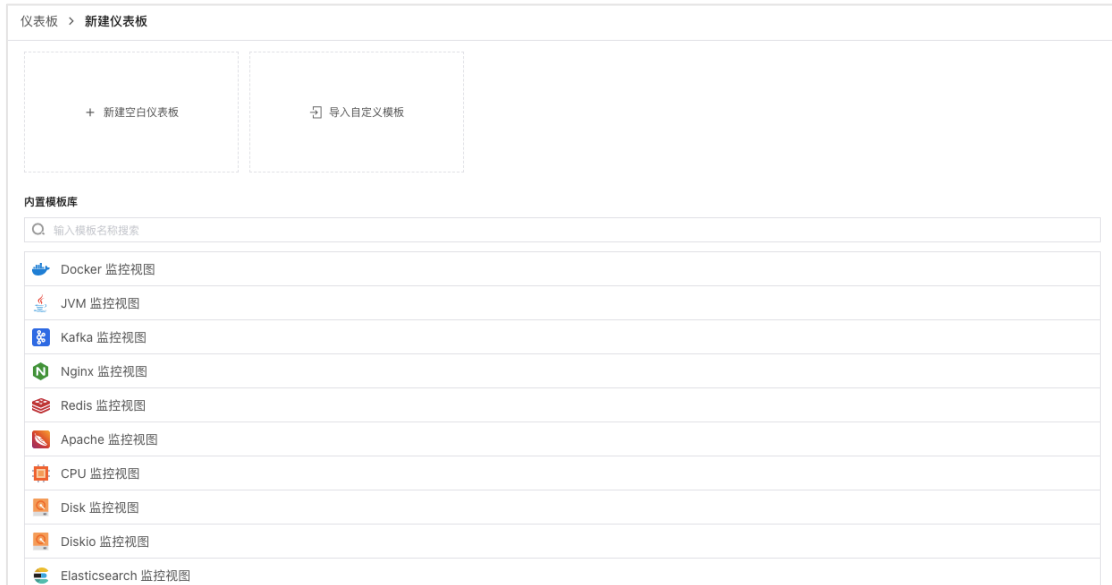
在场景下，支持创建多个仪表板来构建数据洞察场景，支持对已有场景进行修改、导出和删除，支持通过我的收藏、导入项目、我的创建、经常浏览进行仪表板过滤，支持通过标签对仪表板进行分组筛选。用户可以根据不同的业务需求构建不同的仪表板，如基础设施和应用监控、Nginx、JVM、Docker 监控等等。



新建仪表板

进入场景后，在「仪表板」，点击「+新建仪表板」，即可选择想要创建的仪表板模板。

- 空白仪表板：即创建一个空白的仪表板，后续可自定义设置仪表板中的图表。
- 自定义模板：导入自定义的视图模版。
- 内置模板库：系统提供的视图模板，无需配置，即选即用。



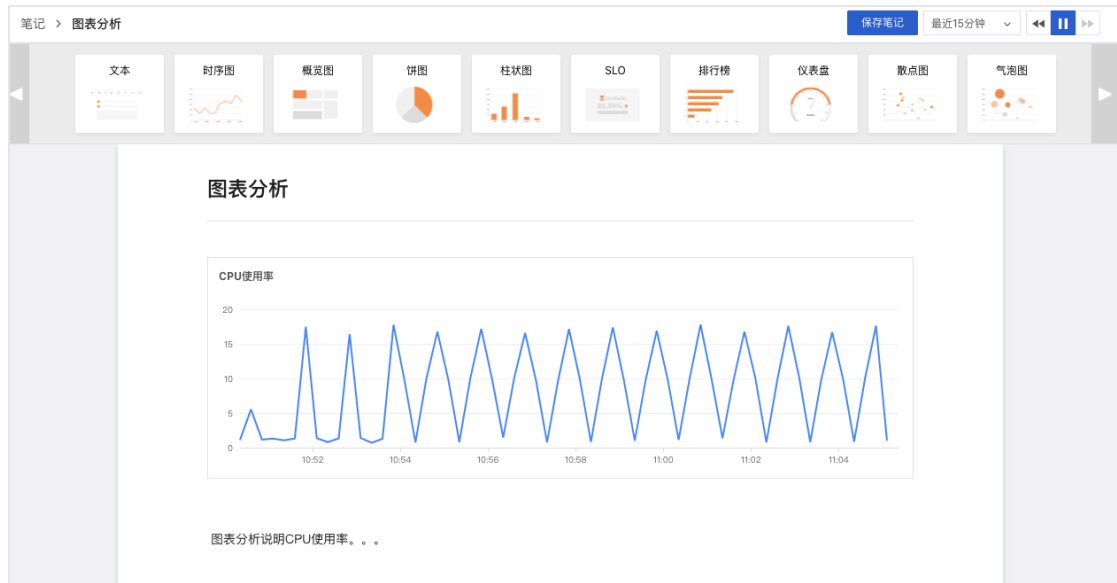
笔记

在场景下，可以创建多个笔记来进行总结报告，支持插入实时可视化图表进行数据分析，支持插入文本文档进行说明，结合图表和文档进行数据分析和总结报告；支持与工作空间所有成员共享笔记，留存异常数据分析，帮助回溯、定位、解决问题。



新建笔记

进入场景后，在「笔记」，点击「+新建笔记」，即可添加笔记进行编辑。



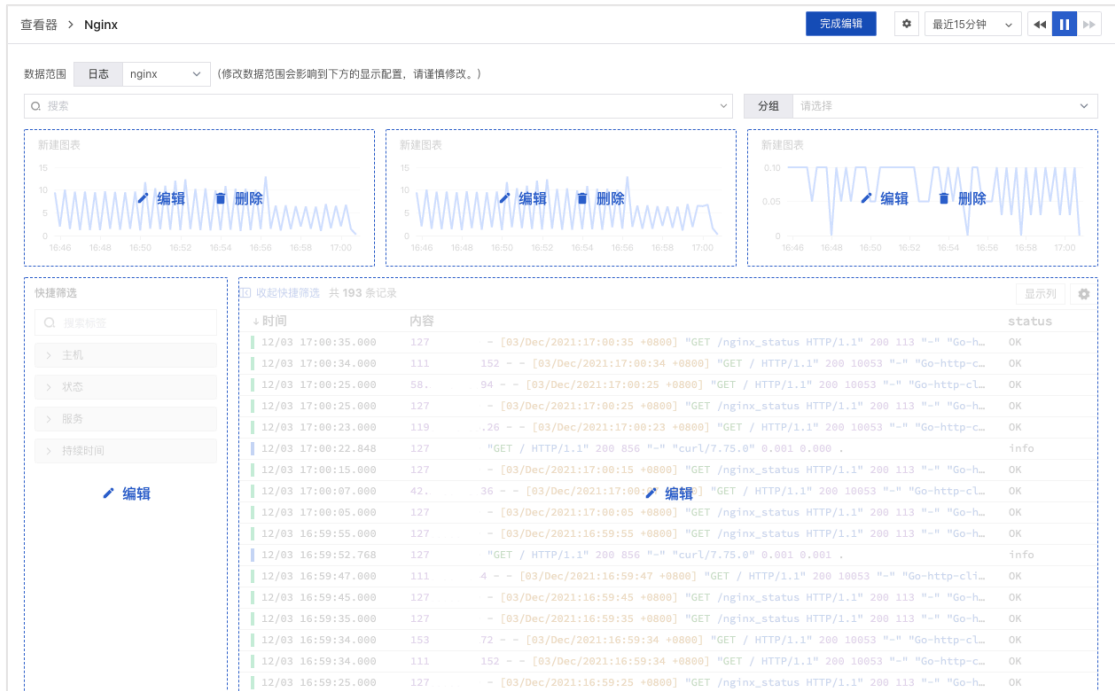
查看器

在场景下，可以与空间成员共同快速搭建多个自定义查看器，定制化查看需求，还可以将制作完成的查看器导出分享给他人，共享查看器模版。

查看器名称	最后修改时间	操作
日志 数据库	12/07 17:31	G ☆ ⋮
Nginx 中间件	12/03 17:03	G ☆ ⋮
MySQL 数据库	12/03 15:38	G ☆ ⋮

新建查看器

进入场景后，在「查看器」，点击「+新建查看器」并完成自定义查看器名称及标签后，即可创建一个新的查看器。支持导入自定义查看器模版，支持通过内置查看器模版库一键创建查看器。



视图变量

在仪表板中添加视图变量，进入视图变量配置页面，视图变量配置完成后，在图表中使用视图变量，即可完成图表的动态筛选。

数据来源	变量查询	默认值	变量名	显示名	是否隐藏	操作
指标	cpu	标签	*	host	主机名	<input type="checkbox"/>
DQL	SHOW_TAG_VALUE(from=["cpu"],keyin=["host"])	*	请输入变量名	请输入显示名	<input type="checkbox"/>	<input type="checkbox"/>
基础对象	分类	属性/标签	*	请输入变量名	请输入显示名	<input type="checkbox"/>
自定义对象	分类	属性/标签	*	请输入变量名	请输入显示名	<input type="checkbox"/>
自定义	请输入列表数据，多个用英文逗号分隔	*	请输入变量名	请输入显示名	<input type="checkbox"/>	<input type="checkbox"/>

+添加视图变量

保存 取消

对象视图变量支持属性映射功能，按照以下步骤设置完成后，即可在视图中查看设置的变量名，并在图表中显示，显示格式为“映射字段(原字段)”。

- 先定义一个基于对象类字段的视图变量
- 在“对象映射”选择对象分类需要映射的字段
- 在“图表查询”中以映射的标签作为分组
- 在“图表设置”中开启“字段映射”

视图变量		对象映射		属性映射		操作
数据来源	对象分类	属性映射				
基础对象	分类	属性/标签	→	属性/标签		■
自定义对象	分类	属性/标签	→	属性/标签		■
+添加映射						
		保存		取消		

可视化图表

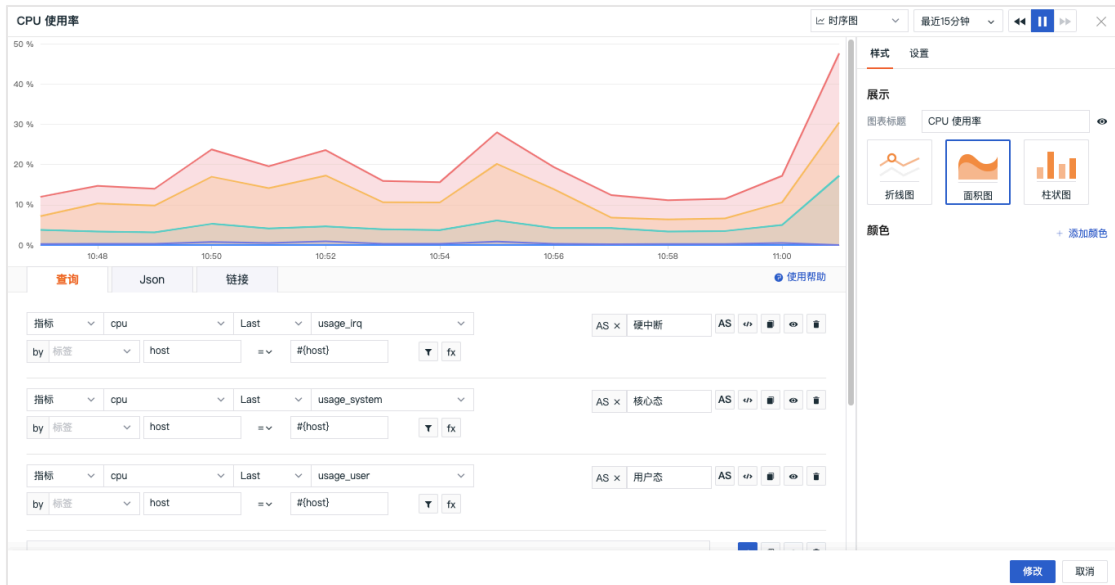
在图表添加页面中，可选择图表类型、查询方式以及进行图表设置，图表查询方式包括简单查询、表达式查询和 DQL 查询，图表类型包括时序图、概览图、饼图、柱状图、SLO、排行榜、仪表盘、散点图、气泡图、表格图、矩形树图、漏斗图、中国地图、世界地图、蜂窝图、日志流图、对象列表图、告警统计图、文本、视频、图片、命令面板、IFrame。用户可根据需要查询的内容选择对应的图表展现方式，支持分组和组合图展示。

可视化图表支持三种查询方式：简单查询、表达式查询和 DQL 查询。一个图表同时支持多条查询。

简单查询

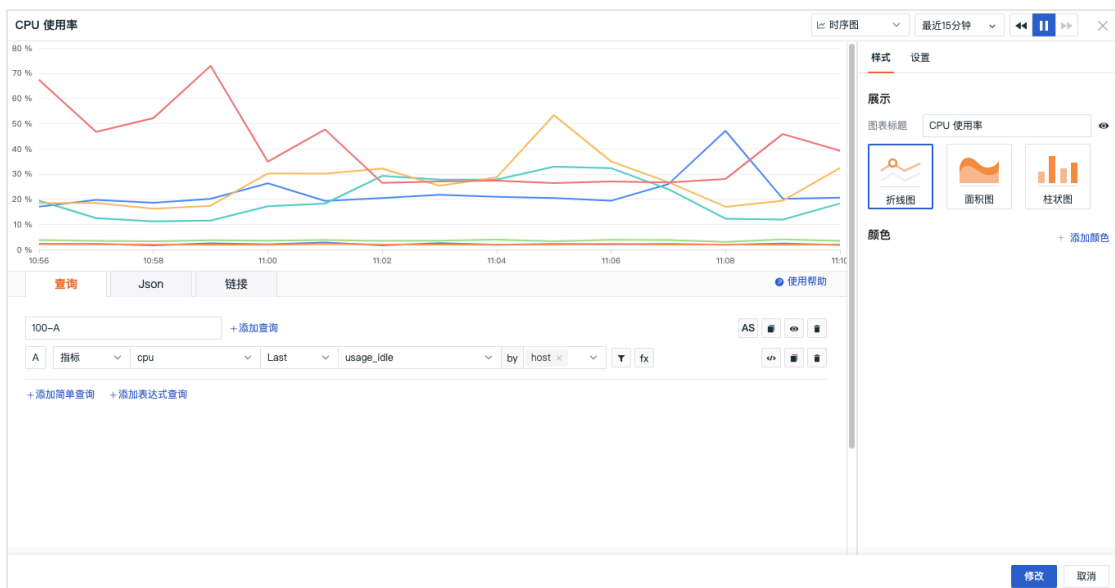
简单查询可选择不同数据源进行查询，并可通过函数、分组标签、label、筛选条件等调整图表展示。

- 数据源包括指标、日志、基础对象、自定义对象、事件、应用性能、用户访问、安全巡检、网络；
- 支持选择不同的标签进行分组显示，支持同时选择多个标签；
- 支持为查询添加多个 label 筛选或者筛选条件，对数据进行过滤；
- 支持为查询添加函数，对数据进行计算；
- 支持为查询修改别名；
- 支持切换到 DQL 查询，手动输入查询语句；



表达式查询

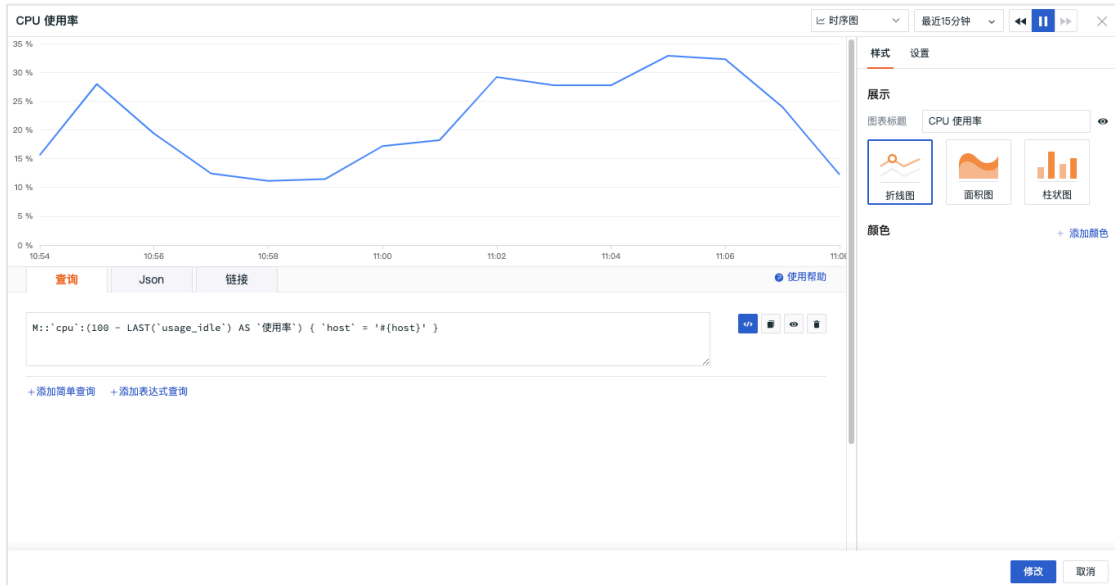
表达式查询基于简单查询的结果可进行表达式计算，并通过图表进行展示。



DQL 查询

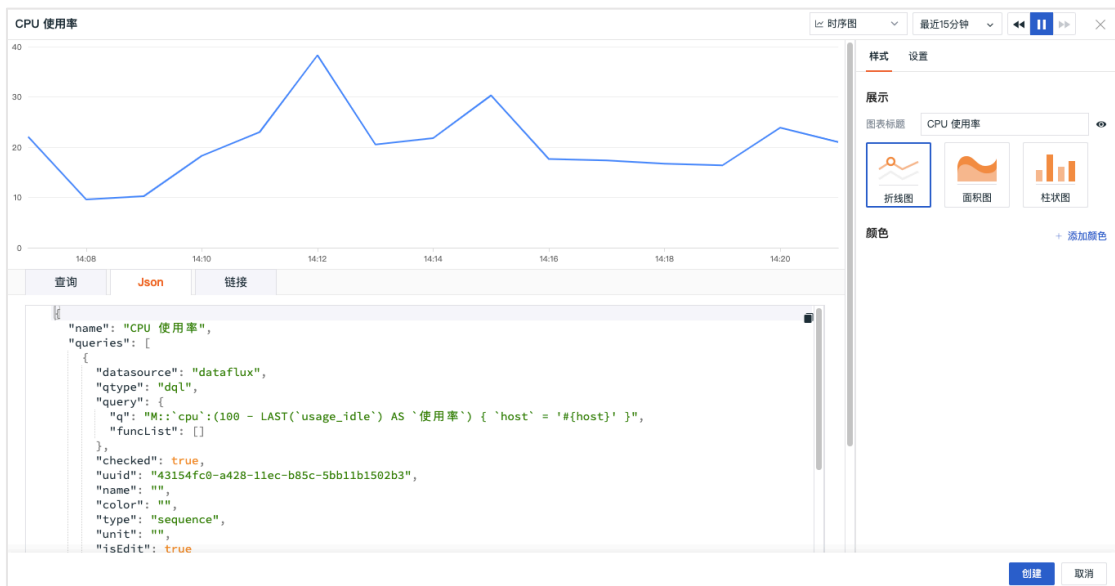
DQL 是专为观测云开发的语言，语法简单，方便使用，可在观测云控制台进行数据查询，也可通过客户端命令行进行数据查询。

在观测云控制台添加图表页面中，用户可切换「简单查询」到「DQL 查询」自行编写查询语句进行数据查询，同时可选择不同的图表类型进行查询结果展示。



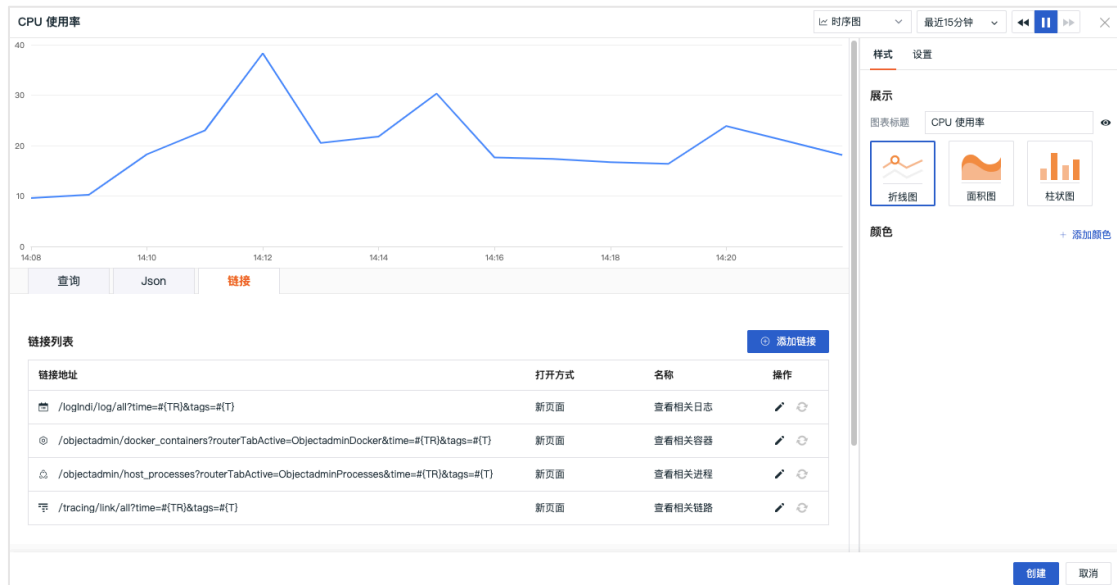
Json

在编辑图表时，每一个正确的查询都对应一个 json 文本，支持复制粘贴。支持编辑 Json 并和查询/设置联动，支持对输入的 Json 进行校验，若有错误则显示错误提示。



链接

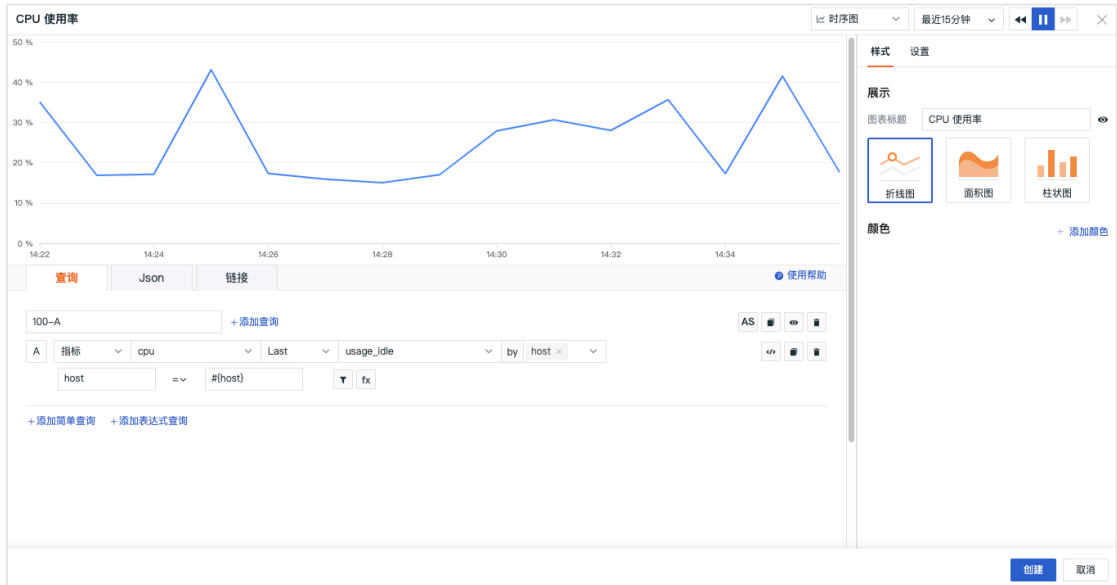
链接可以实现从当前图表跳转至目标页面，支持添加平台内部链接和外部链接，支持通过模板变量修改链接中对应的变量值将数据信息传送过去，完成数据联动。



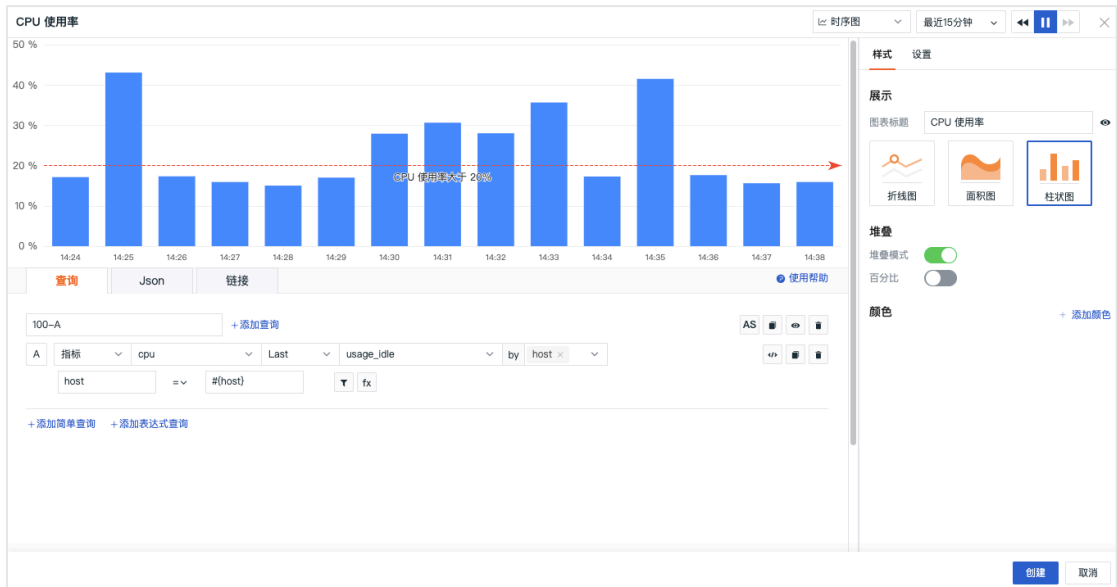
时序图

时序图一般用于显示数据在相等时间间隔下的趋势变化，同时也可以用来分析多组指标数据之间的作用及影响。图表类型支持折线图、柱状图和面积图。

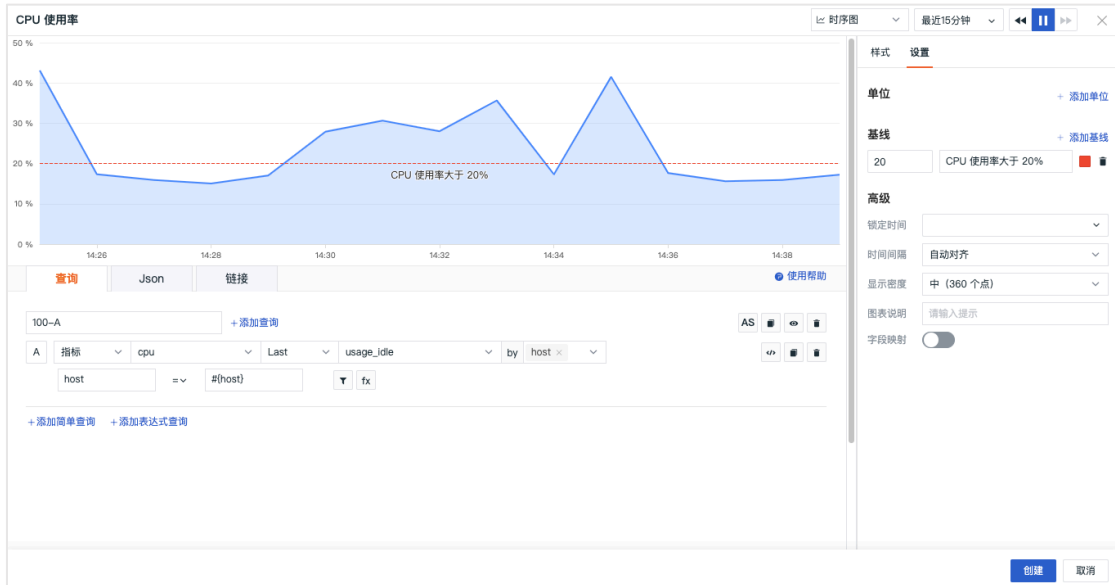
1) 折线图



1) 柱状图

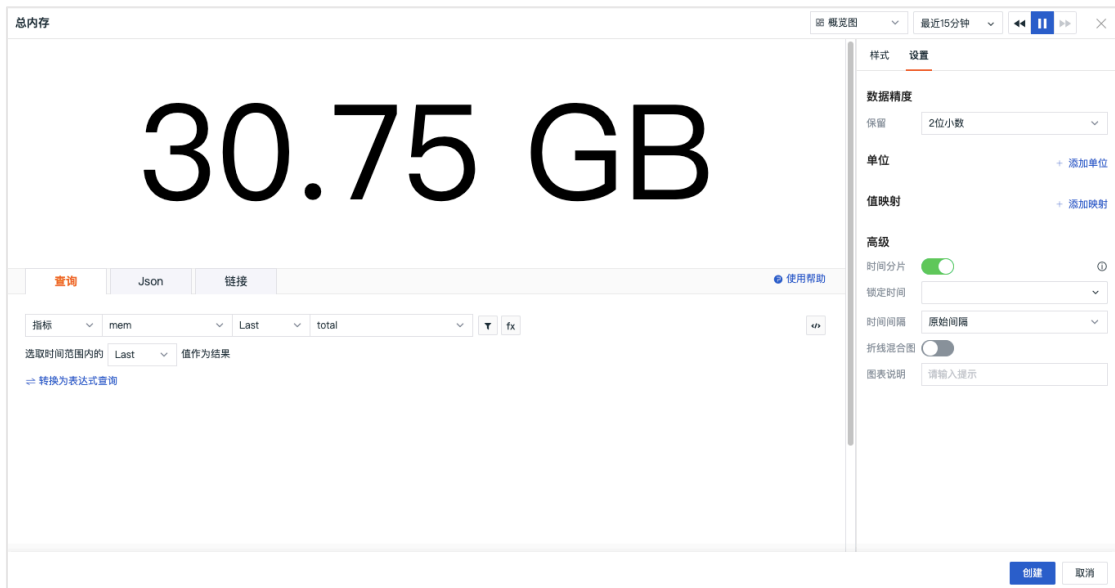


2) 面积图



概览图

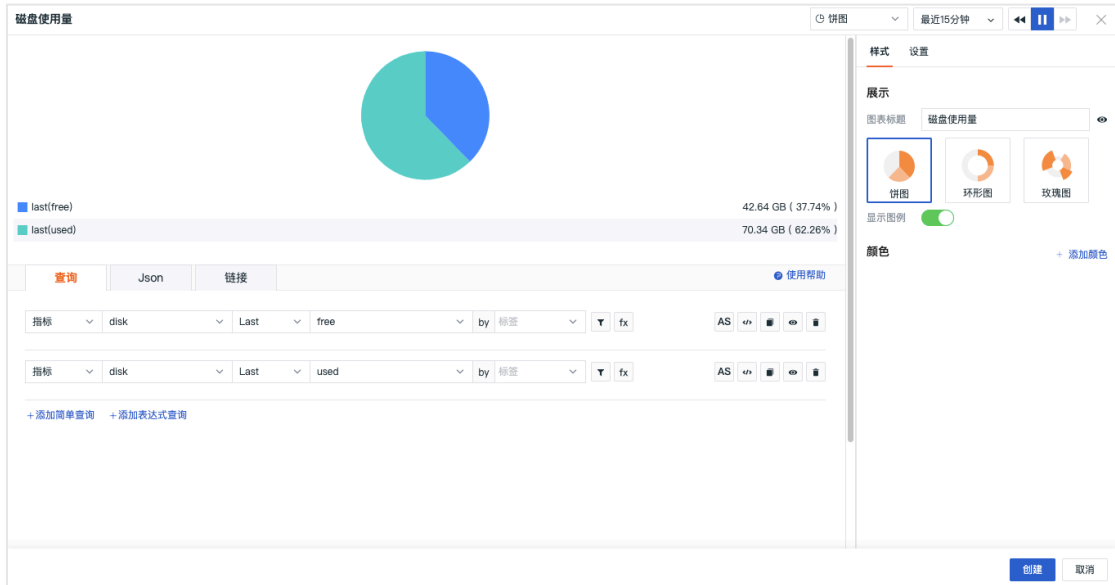
概览图可清晰显示一个指标的结果值。用户可进行阈值设置、颜色设置、映射值设置。同时支持与折线图混合显示，帮助用户在查询当前指标值的同时也能了解指标趋势。



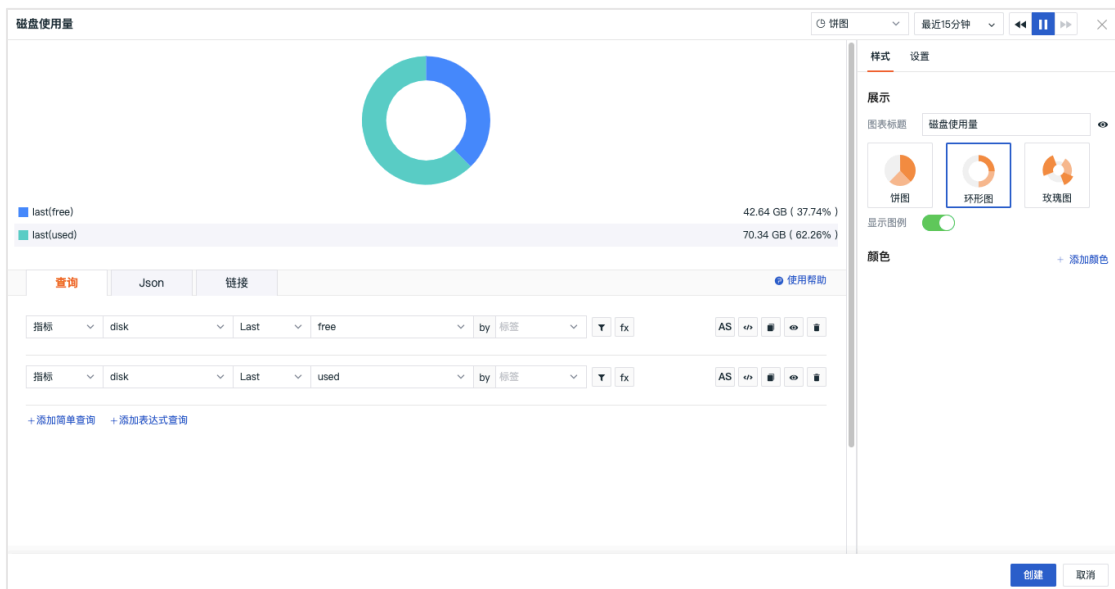
饼图

饼图一般适用于表现数据分组的对比情况。观测云支持三种饼图样式设定：

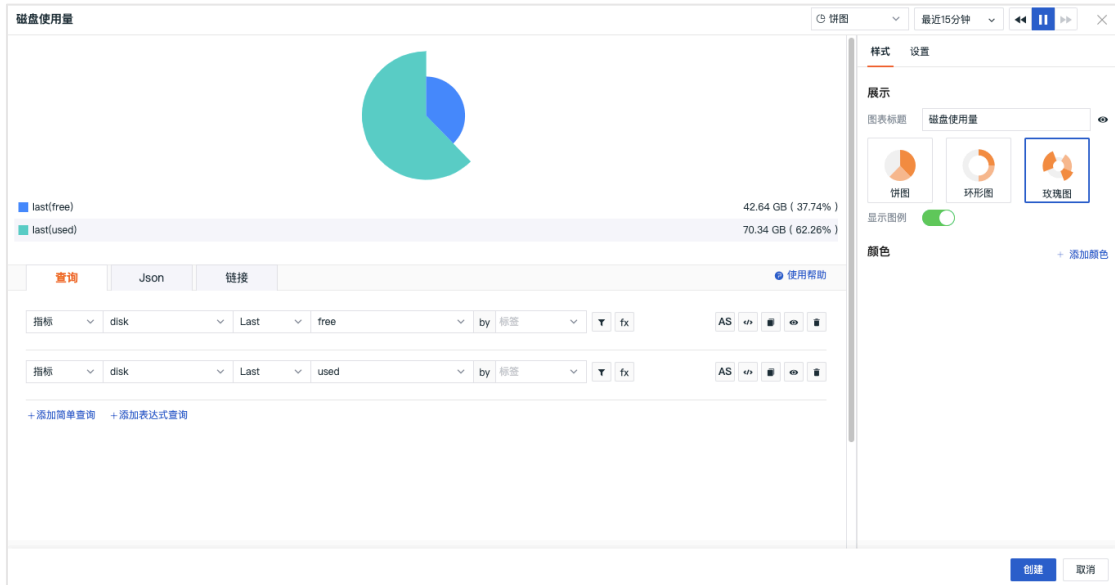
- 1) 饼图：显示数据分组的对比情况，更多用于样本指标较少的场景。



2) 环形图：更多适用于反映多个样本指标各部分所占比例。



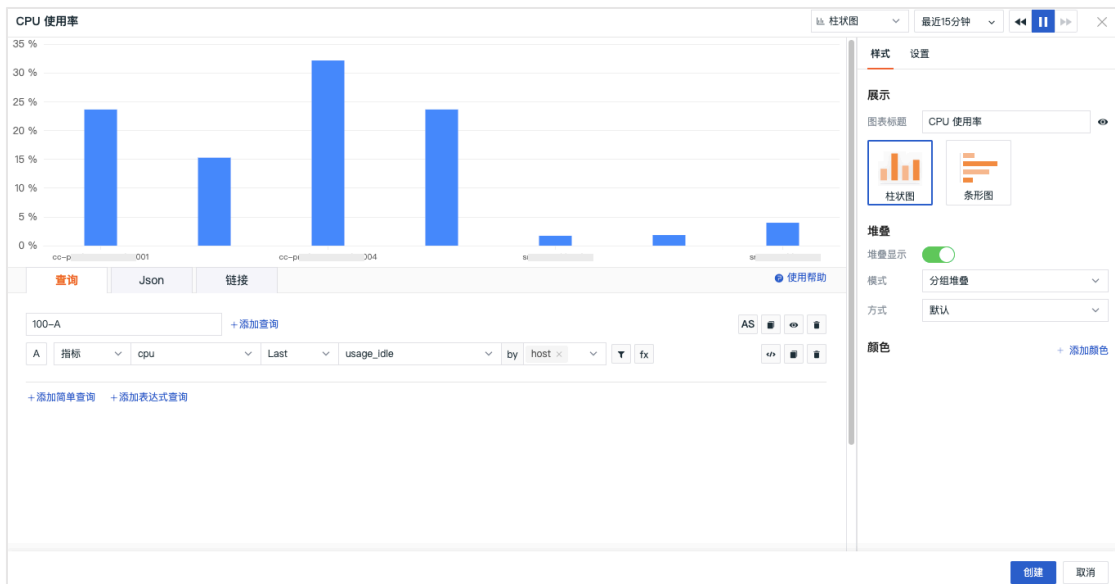
3) 玫瑰图：圆弧半径的大小表示数据的大小，适用于反映分类过多的场景，和数值大小相似的占比场景。



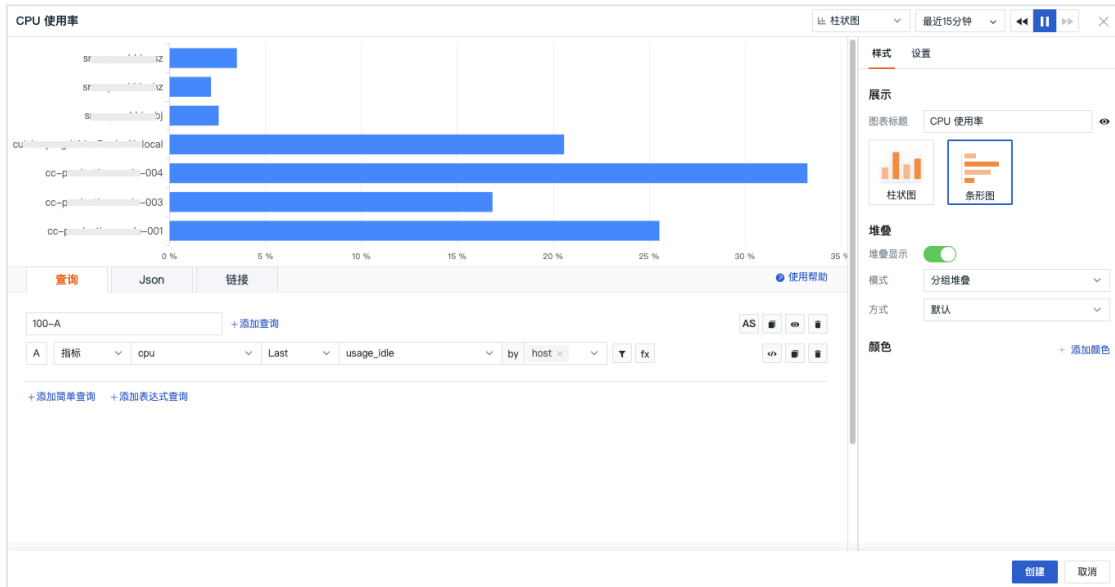
柱状图

柱状图一般适用于实现一段时间内的数据变化和各变量间的对比情况，支持两种图表样式。

1) 柱状图



2) 条形图



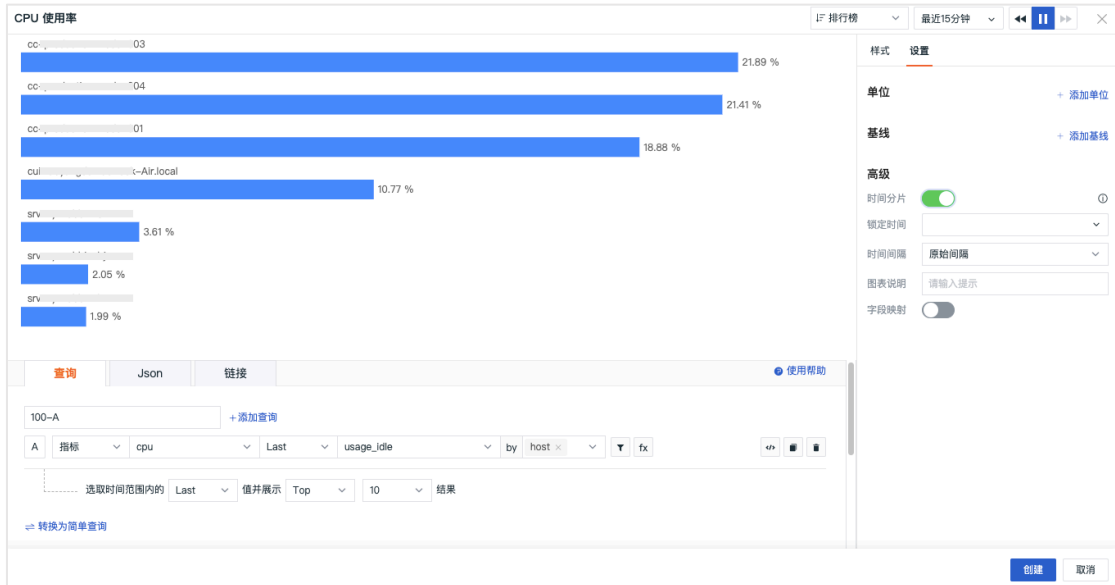
SLO

SLO 可直接选择设置的监控 SLO 进行 SLO 数据展示。



排行榜

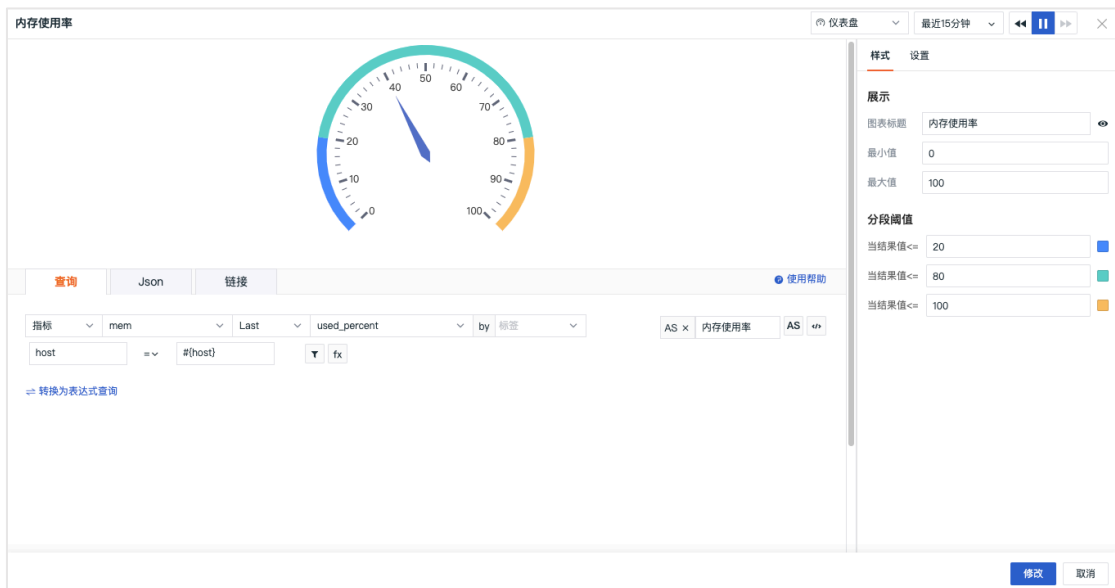
排行榜是对某一相关同类事物的客观实力反映,简洁的展示出 Top N 或者 Bottom N 的升降序排行。



仪表盘

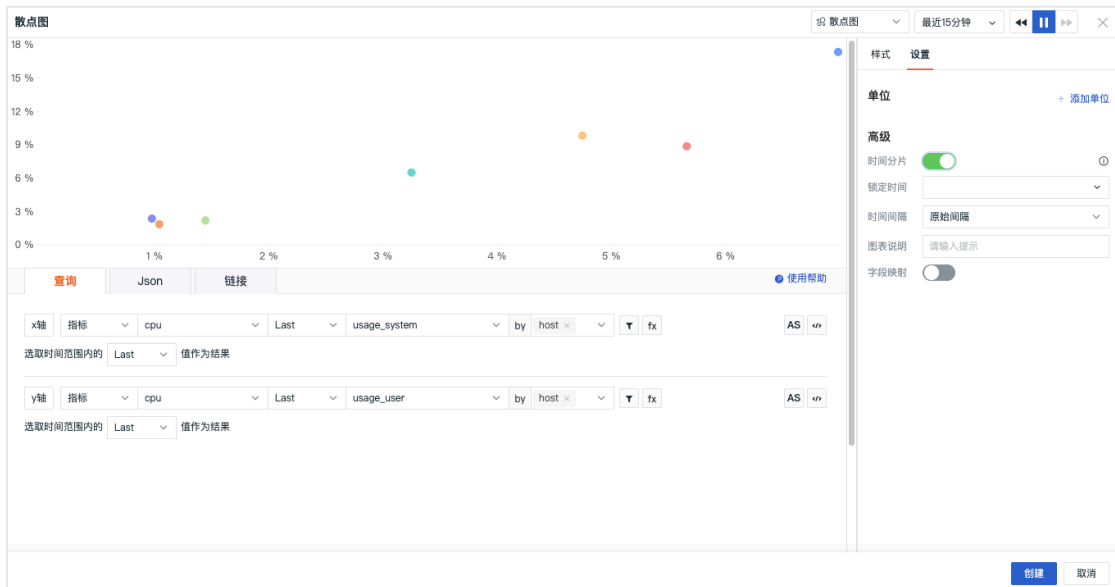
仪表盘可清晰展示指标数据值所在的范围。

- 1) 最小值：设置仪表盘的最小值，即表盘图中最左侧的数值；
- 2) 最大值：设置仪表盘的最大值，即表盘图中最左侧与最右侧数值之和；
- 3) 分段阈值：为数值设置分段临界值和表盘颜色。点击「+」和「-」可增加和删除对应阈值；



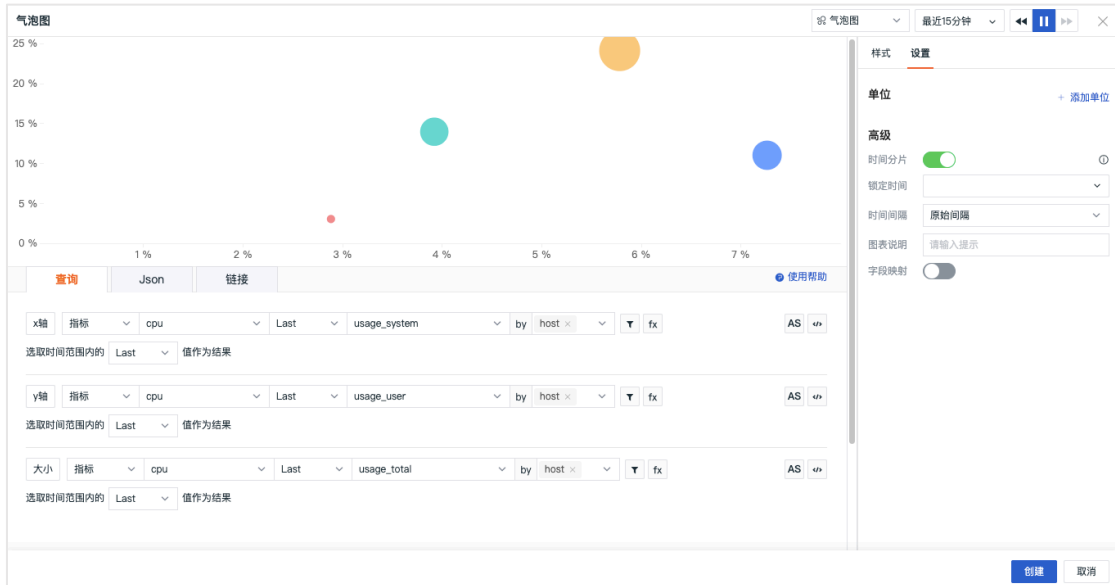
散点图

散点图表示因变量随自变量而变化的大致趋势，由此趋势可以选择合适的函数进行经验分布的拟合，进而找到变量之间的函数关系。可用来观察数据的分布和聚合情况。



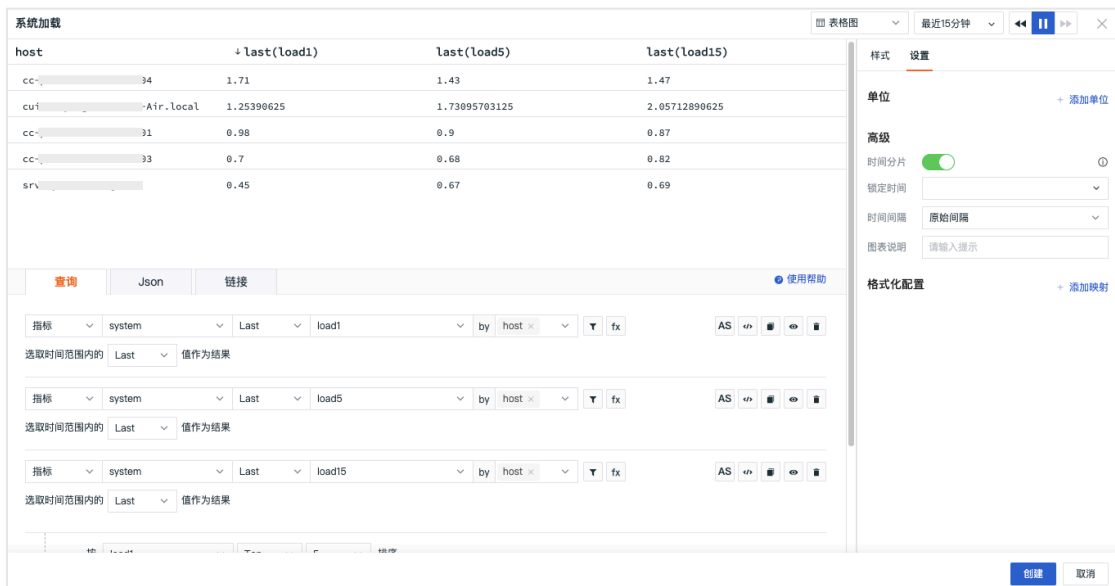
气泡图

气泡图可用于展示三个变量之间的关系，与散点图类似，分为横轴和纵轴，并加入表示大小的变量进行对比。表示因变量随自变量而变化的大致趋势，由此趋势可以选择合适的函数进行经验分布的拟合，进而找到变量之间的函数关系。可用来观察数据的分布和聚合情况。



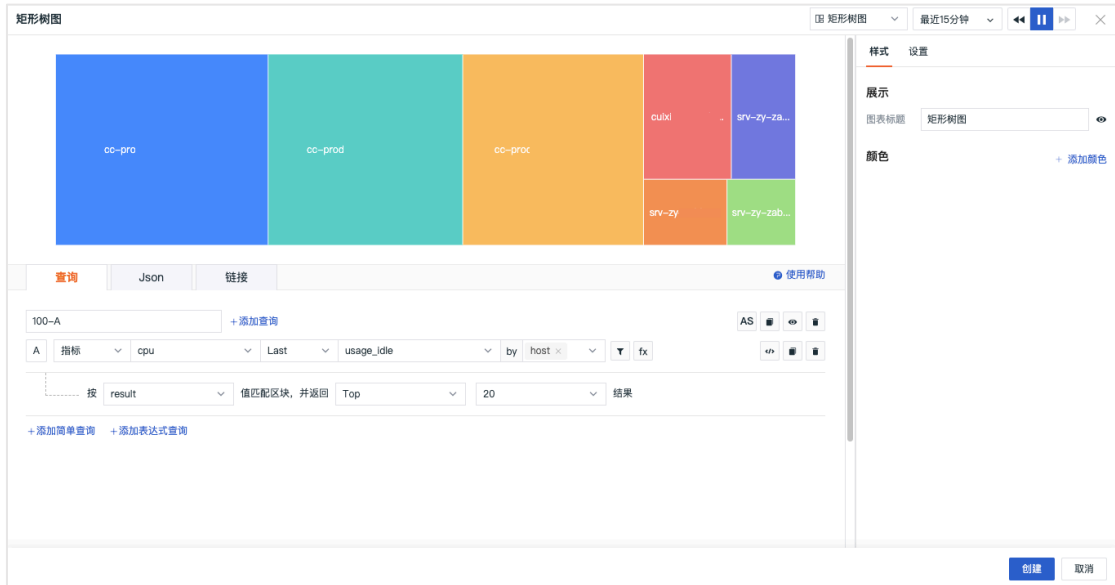
表格图

表格具有直观展示统计信息属性的特点，同时可以反映数据间的关系。用户可以通过链接设置当前图表的跳转目标页面，并通过模板变量将数据信息传送过去，完成数据联动。



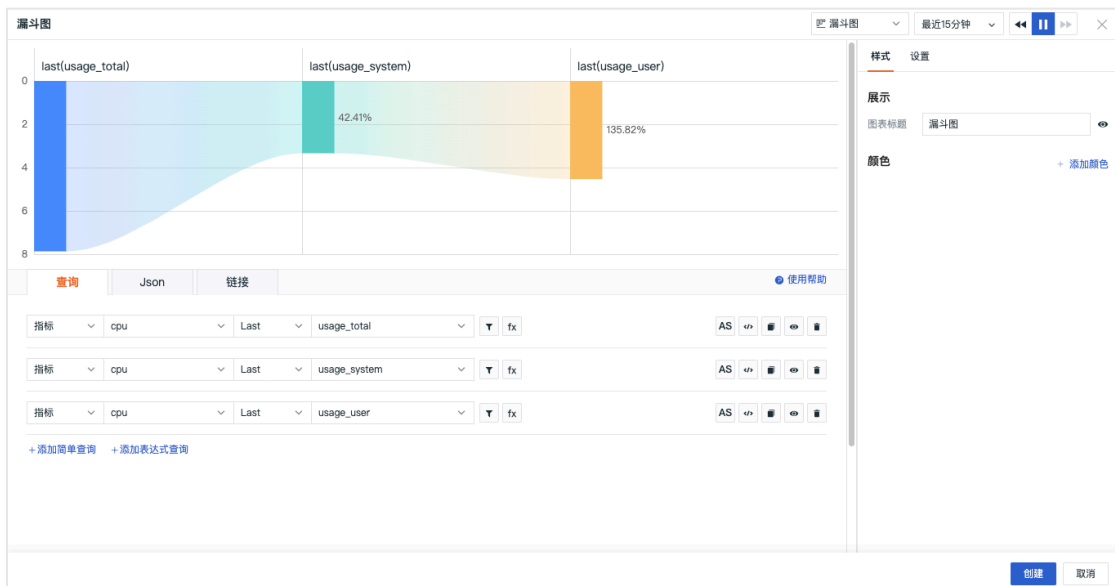
矩形树图

矩形树图用于展示不同分组下指标数据的占比分布可视化。



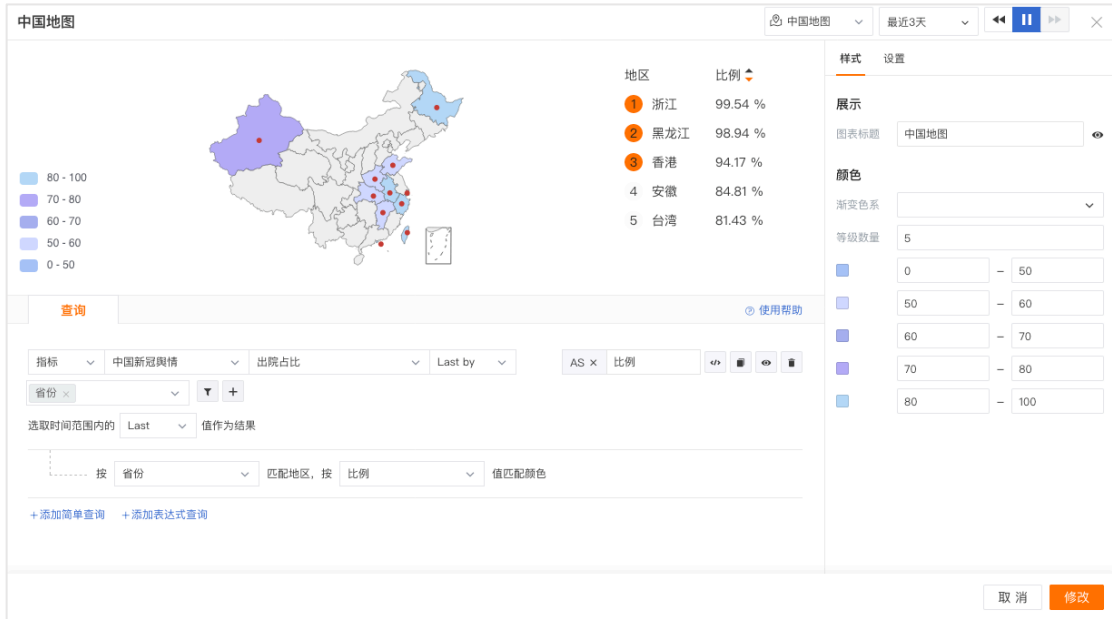
漏斗图

漏斗图一般适用于具有规范性、周期长、环节多的流程分析，通过漏斗图比较各环节的数据，能够直观地对比问题。另外漏斗图还适用于网站业务流程分析，展示用户从进入网站到实现购买的最终转化率，及每个步骤的转化率。



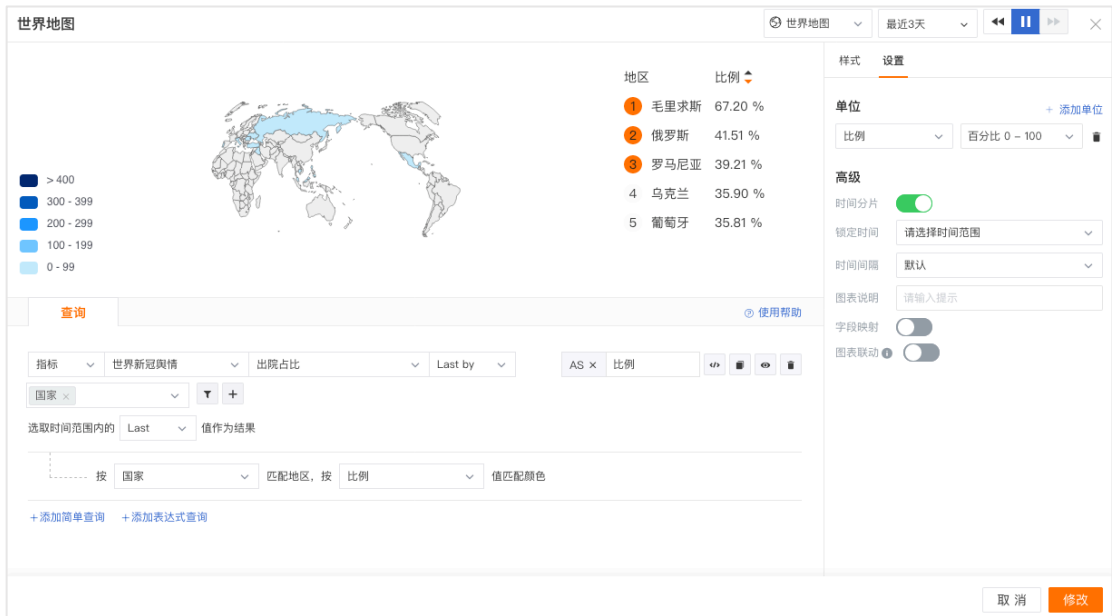
中国地图

观测云支持以中国地图的图表形式进行展示。用户可自定义显示的色块等级、范围和颜色。



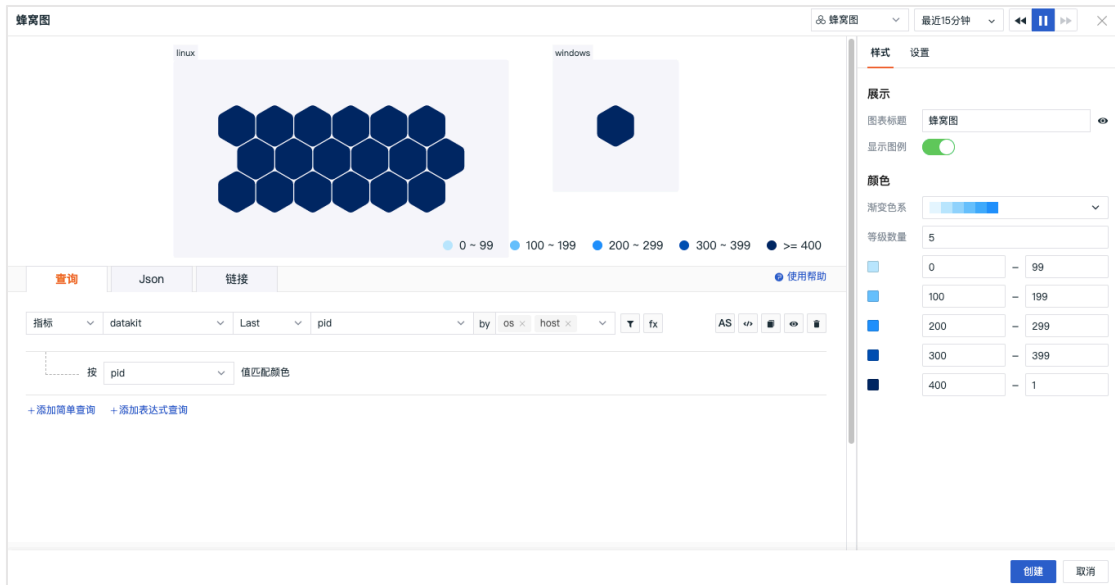
世界地图

观测云支持以世界地图的图表形式进行展示。用户可自定义显示的色块等级、范围和颜色。



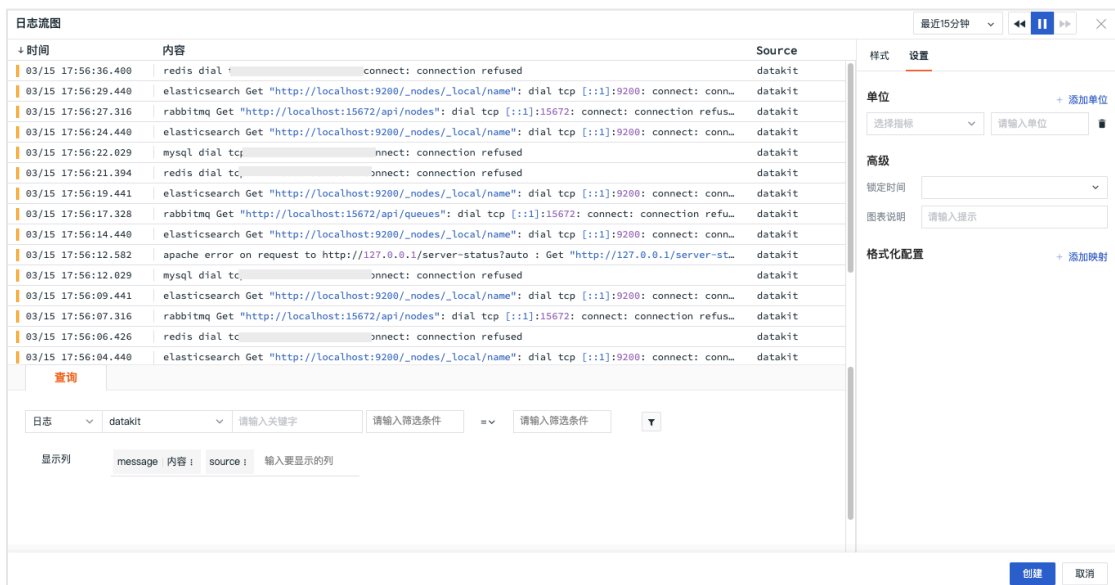
蜂窝图

蜂窝图展示不同分组下的数据情况，可用于对资产、基础设施的监控。



日志流图

观测云支持向视图添加日志流，可展示采集的日志数据，可通过标签筛选和关键字搜索对数据过滤后再进行展示。



对象列表图

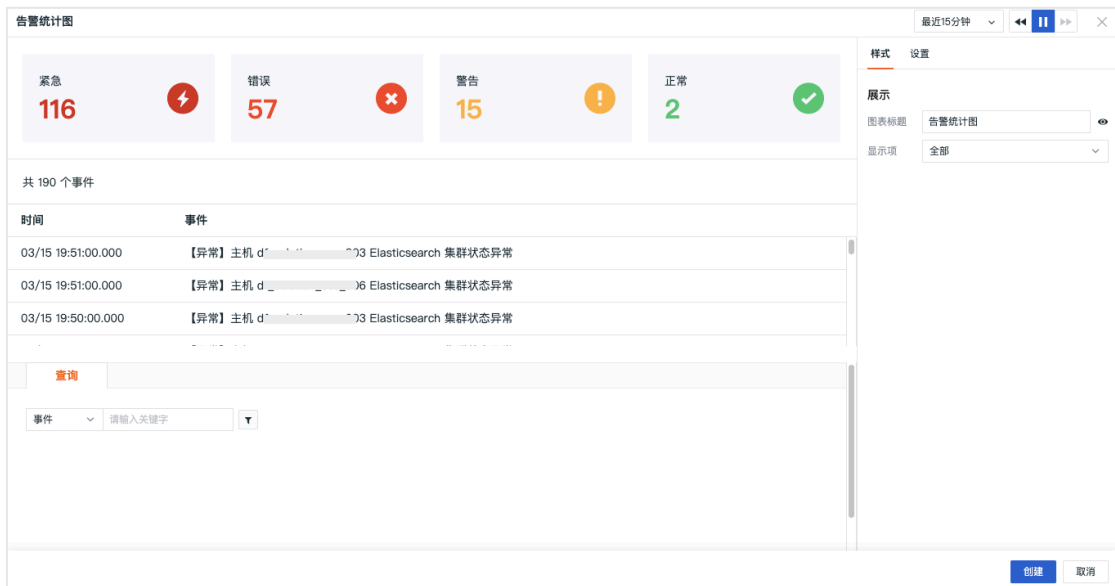
观测云支持向视图添加对象列表，可对数据进行筛选过滤，以查看相应对象分类下的数据。

名称	分类	Cpu_usage	Mem_used_pe...	Load	Os	Cloud_provi...	Region
whj...	HOST	14.34 %	73.33 %	3.81 %	darwin	-	-
da...	HOST	56.15 %	59.57 %	7.12 %	linux	-	-
izj...	HOST	5.94 %	49.82 %	0.23 %	linux	-	-
he...	HOST	24.68 %	73.65 %	2.51 %	linux	-	-
th...	HOST	12.38 %	65.25 %	4.62 %	darwin	-	-
te...	HOST	38.46 %	53.04 %	1.94 %	linux	aliyun	cn-hangzhou
Co...	HOST	4.98 %	73.09 %	2.36 %	darwin	-	-
pp...	HOST	15.26 %	85 %	0.28 %	windows	-	-
zy...	HOST	0.60 %	12.83 %	0 %	linux	-	-
my...	HOST	0.45 %	7.53 %	0.01 %	linux	-	-
ub...	HOST	1.25 %	30.48 %	0.13 %	linux	-	-
zh...	HOST	42.57 %	69.58 %	5.37 %	darwin	-	-
bu...	HOST	19.69 %	95.60 %	2.59 %	darwin	-	-
10...	HOST	0.45 %	30.08 %	0 %	linux	-	-
ub...	HOST	1.41 %	15.06 %	0.08 %	linux	-	-

告警统计图

支持向视图添加异常检测的告警事件，可通过标签筛选和关键字搜索对数据进行筛选过滤。告警统计图共分为两个部分，分别为统计图和告警列表。

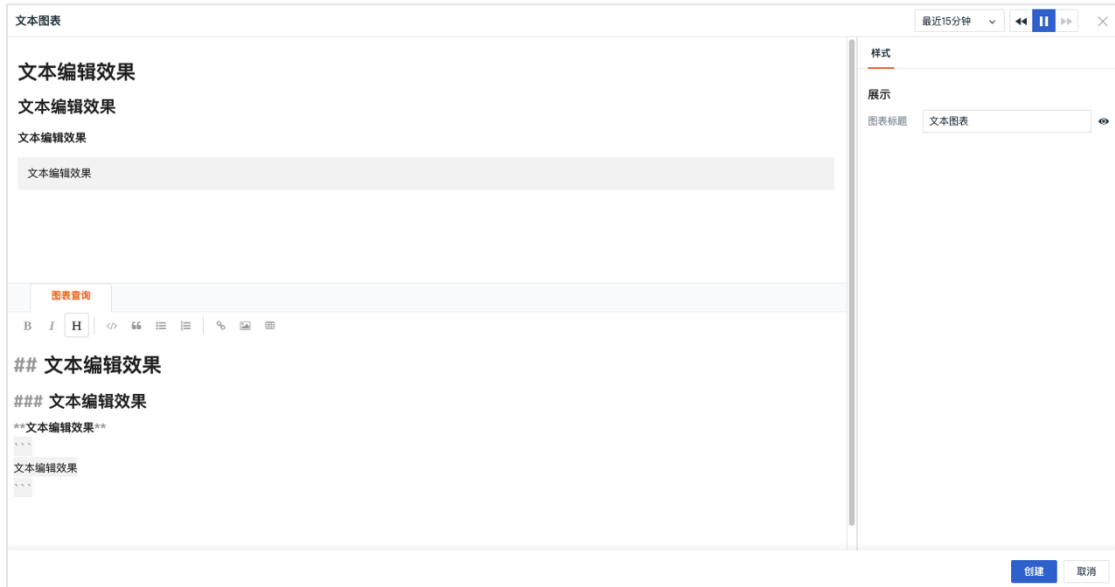
- 1) 统计图：将事件按等级分组并统计每个等级的事件数量，支持点击统计图跳转查询事件的详情；
- 2) 告警列表：显示所选时间范围内未恢复的告警事件。



文本

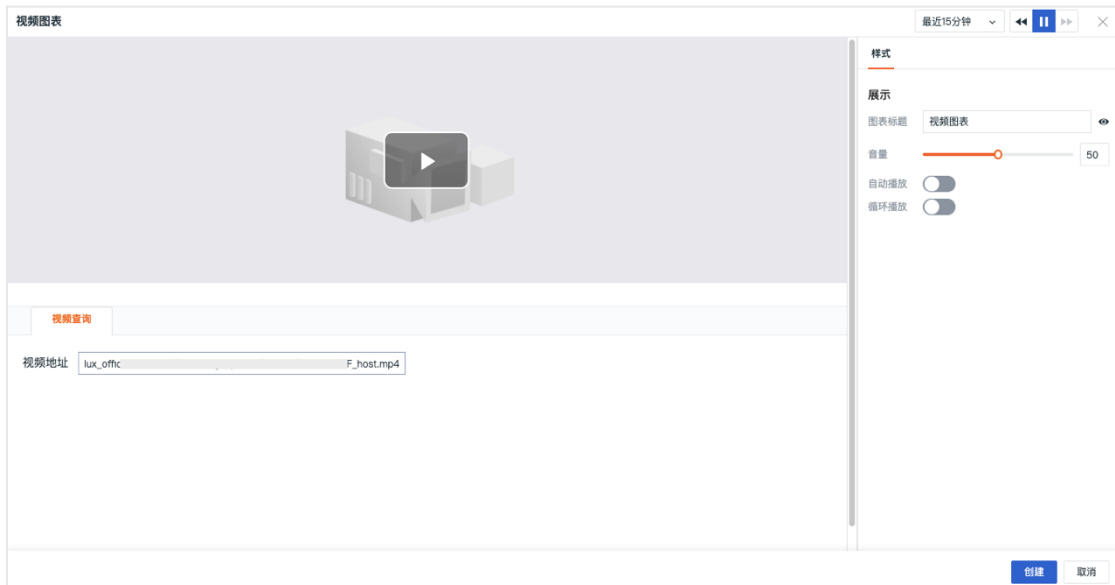
文本一般用于提示、说明，您可以在文本中添加文字、图像、超链接等。

此处的文本为 markdown 格式



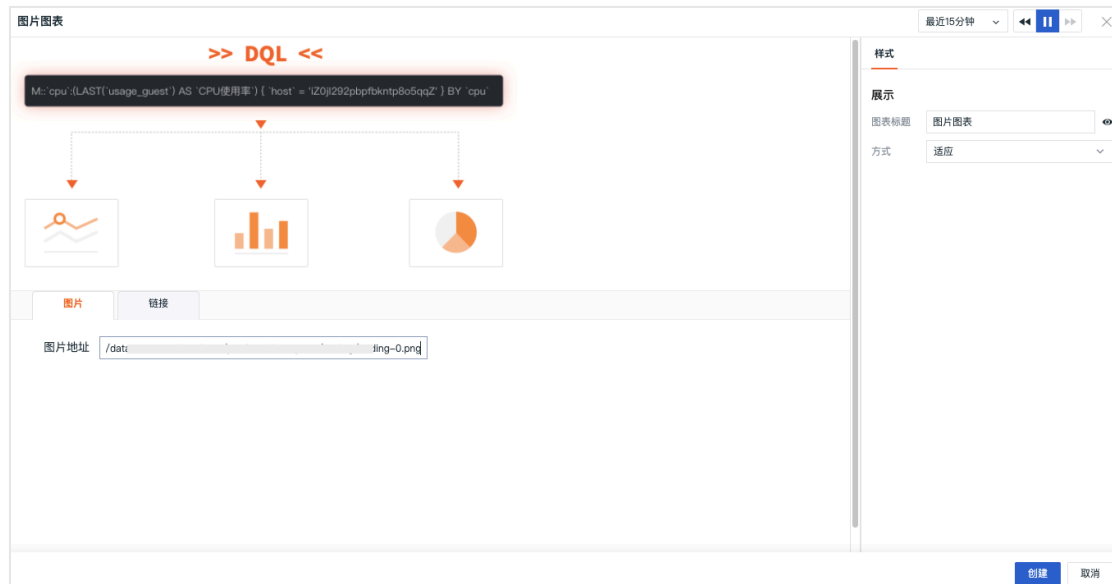
视频

DataFlux 中支持添加视频至视图中，可用于教程、说明等等。操作简单，只需要填入视频地址即可。



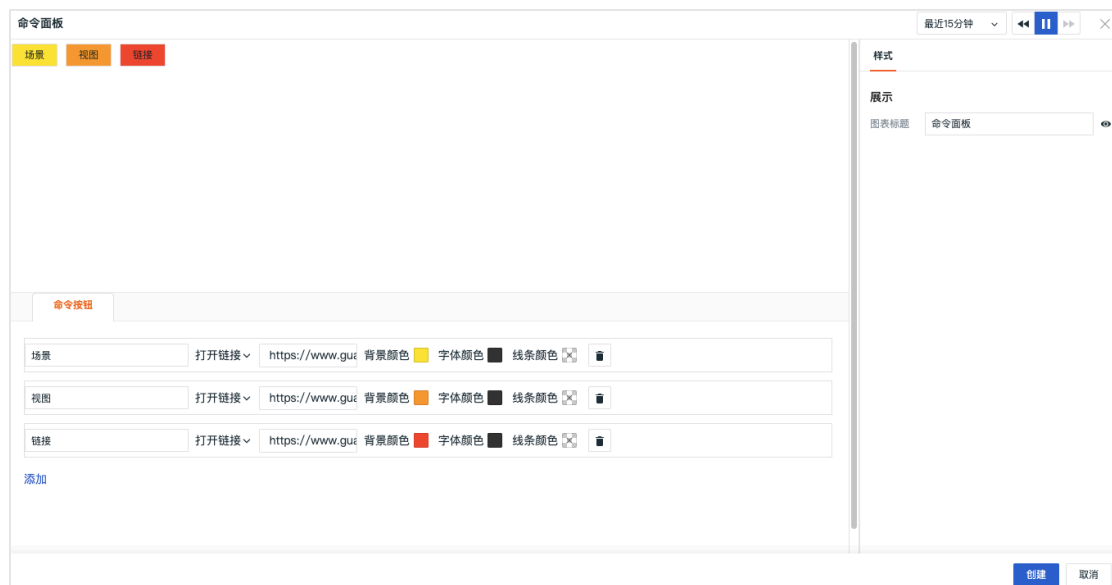
图片

图片一般用于展示图片，可以在图片中添加图片地址即可显示对应图片。



命令面板

命令面板由命令按钮组成，支持点击跳转到指定场景、视图、打开指定链接和执行指定命令，实现在视图中的交互动作。用户可通过拖拽按钮来调整位置进行排版。



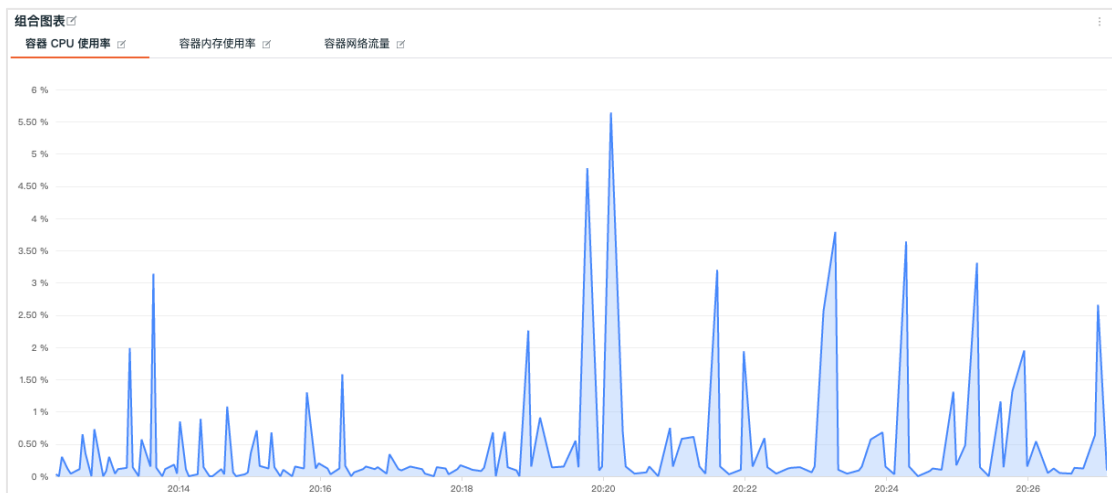
IFrame

IFrame 支持您配置 https 或者 http 链接地址，支持通过变量形式，实现 URL 地址参数调整。



组合图

组合图一般用于组合一个指标不同结果值的多个图表，帮助用户了解指标的对比结果，同时可以随意组合不同类型的图表。

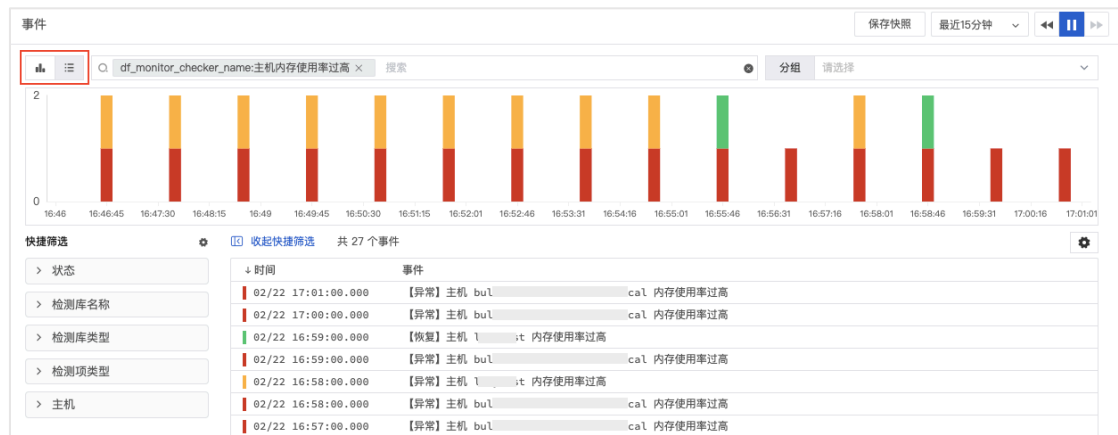


事件

事件包含配置异常检测规则后产生的所有事件。包括异常事件、无数据事件和未恢复事件。

事件管理

在所有事件列表，用户可进行搜索、多标签筛选和按检测项分组聚合统计，支持数据导出。系统根据选择的时间范围自动划分若干时间点，通过堆积柱状图展示不同状态事件的数量，帮助用户进行统计分析。



未恢复事件

在未恢复事件列表，可以查看到空间内持续被触发的全部未恢复事件，及不同告警级别下未恢复事件的数据量统计、告警信息详情等。支持通过选择时间范围、搜索关键字，筛选等方式查询事件数据，支持通过窗口函数查看最近 6 小时内指标数据趋势，帮助快速在所有事件中定位到哪一时间范围、哪一功能模块、哪一行为触发的事件。



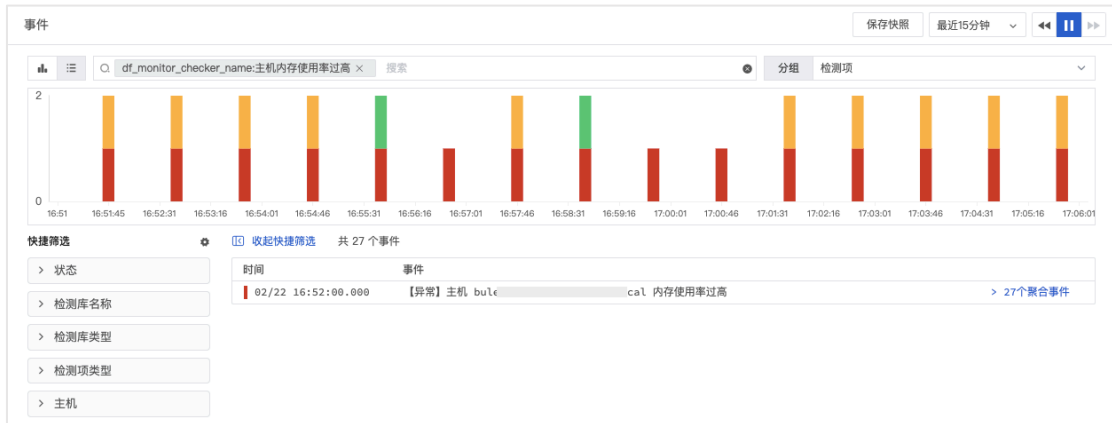
事件详情

点击事件列表可查看对应的事件详情，包括基础属性、状态&趋势、历史记录、关联事件和关联 SLO。



事件聚合

基于“检测项”分组，可点击查看「聚合事件」。在聚合事件详情页，可查看基于该检测项触发的全部事件，并查看不同检测维度下的状态分布、检测维度和指标监控。



基础设施

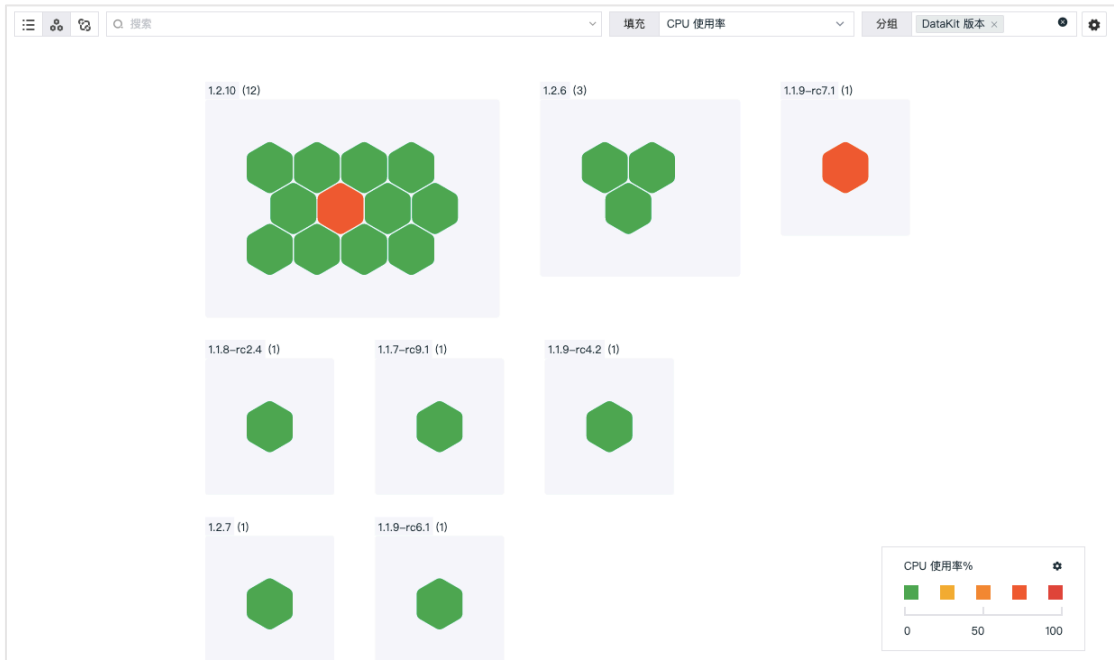
观测云支持查看工作空间内所有采集的基础设施数据，包括主机、容器、进程、自定义对象等。

主机

观测云支持采集主机数据，在「基础设施」的主机列表，支持对主机进行搜索、多标签筛选和分组聚合统计，支持数据导出，支持增加显示列。

主机	操作系统	CPU 使用率	MEM 使用率	CPU 单核负载
df_..._018	linux	7.99%	80.2%	0.02
sc_..._lab.cn	linux	2.06%	34.6%	0.06
df_..._008	linux	2.19%	73.87%	0.06
df_..._012	linux	6.15%	64.45%	0.23
df_..._003	linux	16.45%	59.82%	0.11
d1_..._006	linux	61.24%	49.71%	1.7
d1_..._002	linux	16.39%	69.04%	0.88
d1_..._004	linux	3.66%	21.07%	0.01

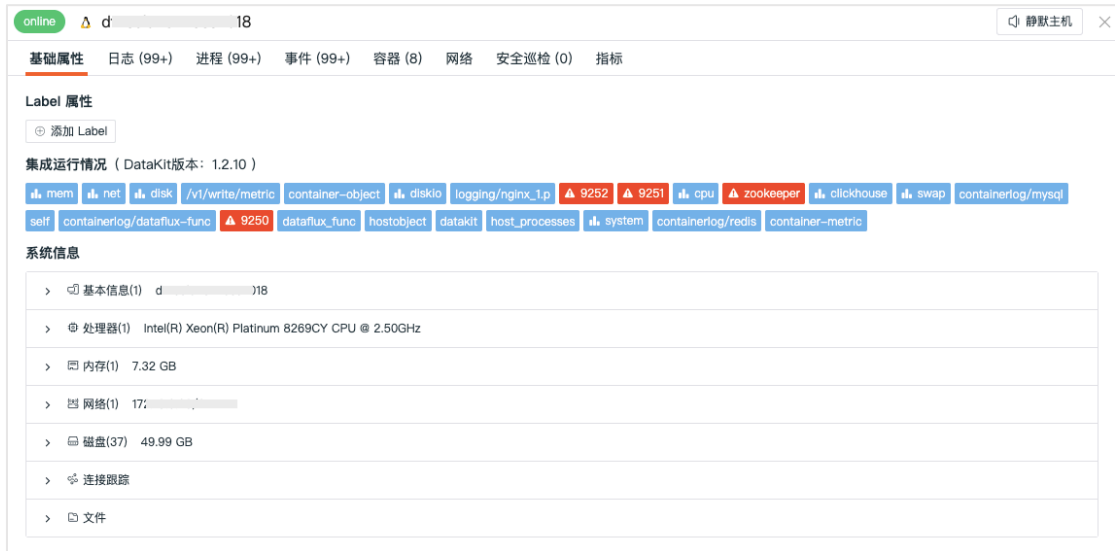
支持切换到主机分布图以可视化的方式显示主机列表。



支持切换到主机网络分布图以可视化的方式显示主机网络流量分布情况。

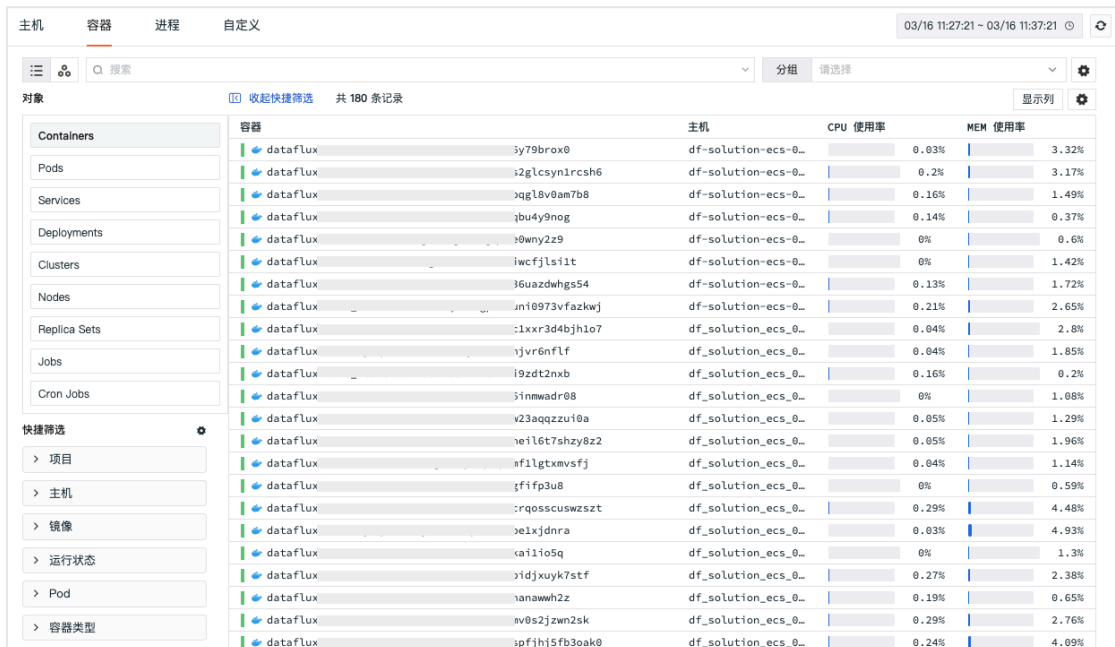


点击主机可侧滑查看主机详情、相关日志、相关链路、相关事件。在主机详情，可查看主机状态、主机名称、主机对应性能图表、关联的日志、进程、事件、容器、安全巡检、指标、网络性能监测数据以及主机的基础属性，包括 Label 属性、集成运行情况、系统信息、云厂商信息等；通过点击集成运行情况下的采集器，可查看对应的视图及报错信息。

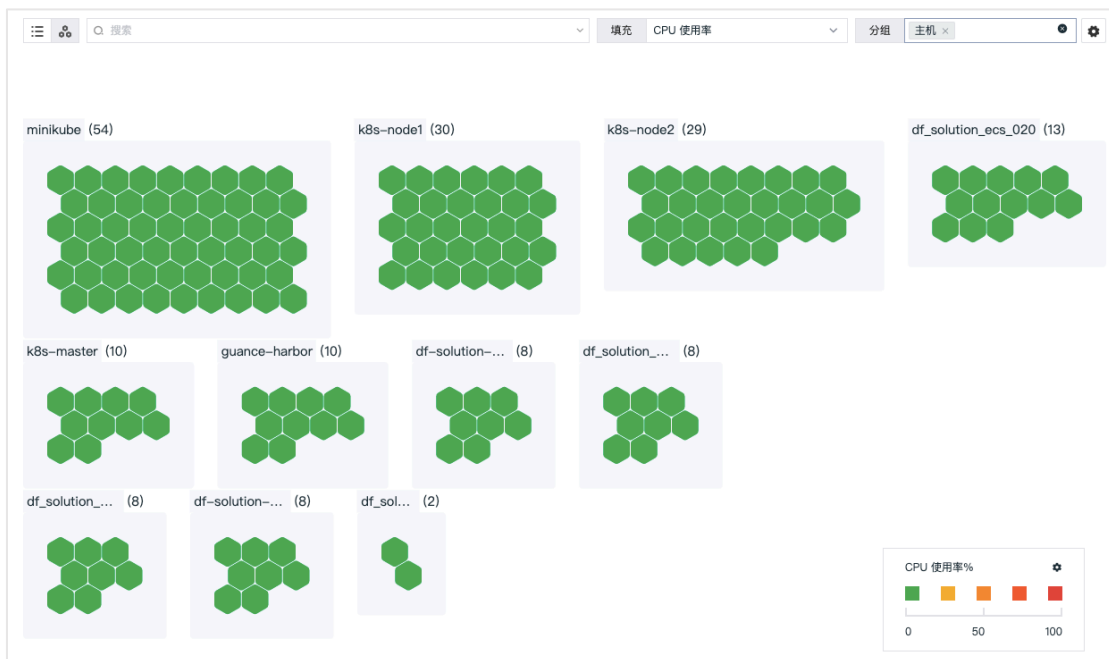


容器

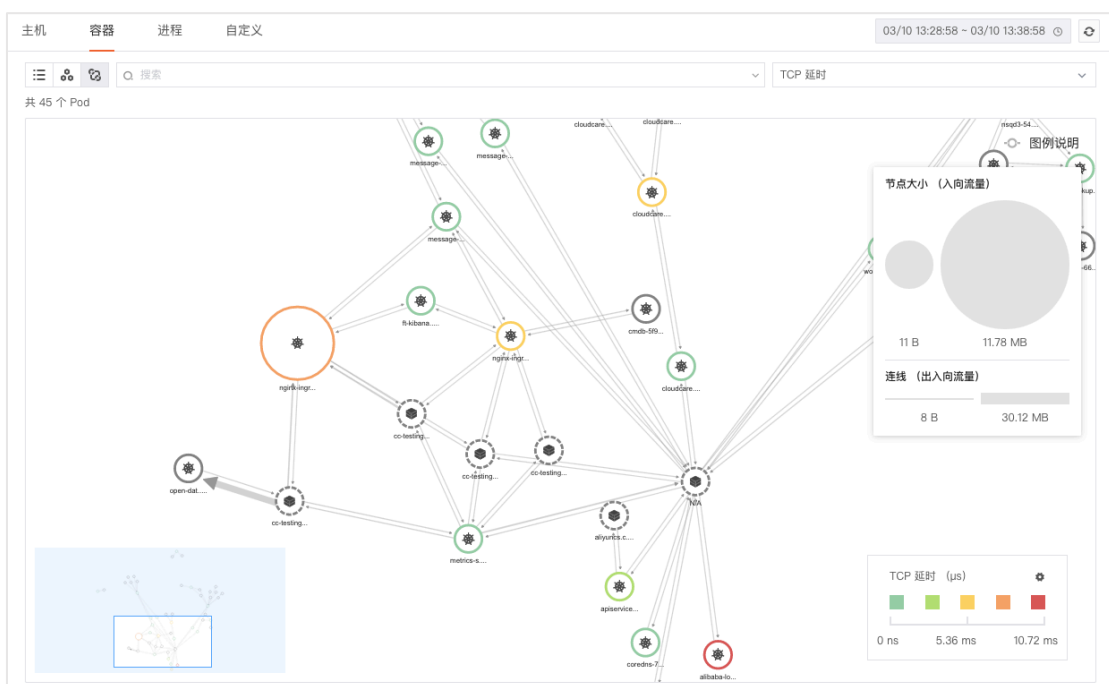
观测云支持采集容器数据。在「基础设施」的容器列表，支持以列表形式查看当前工作空间最近十分钟内采集的 Containers、Pods、Services、Deployments、Clusters、Nodes、Replica Sets、Jobs、Cron Jobs 数据，并对列表内数据进行检索、筛选和分组排行，点击容器可侧滑查看容器详情。



在「Container」/「Pod」列表页面，支持切换到容器分布图，对工作空间的 Containers 和 Pods 数据以分布图形式进行查看，并基于填充数据的大小，快速识别 Container/pod 的性能状态。



在「Pod」列表页面，支持切换到 Pod 网络分布图以可视化的方式显示 Pod 网络流量分布情况。



进程

观测云支持采集对象进程数据。在「基础设施」的进程列表，支持对进程进行搜索、多标签筛选和分组聚合统计，支持数据导出，支持增加显示列，点击进程可侧滑查看进程详情。

进程	用户	主机	CPU 使用率	MEM 使用率
/usr/bin/...	root	df_soluti...	0.08%	0.09%
/usr/bin/.../t/aegis_11_19/AlibabaYunDun	root	df_soluti...	1.88%	1.01%
ora_...	oracle	df_soluti...	0%	0.15%
ora_...	oracle	df_soluti...	0%	0.15%
/da... 2.0/dbhome_1/bin/tnslsnr LISTENER -i	oracle	df_soluti...	0.01%	0.05%
ora_...	oracle	df_soluti...	0.01%	1.24%
ora_...	oracle	df_soluti...	0%	0.09%
ora_...	oracle	df_soluti...	0%	0.07%

自定义

观测云支持自定义采集除了主机、容器、进程以外的其他对象数据，如阿里云 ECS 等。在「基础设施」的自定义列表，通过添加对象分类，可以创建新的对象分类，并自定义对象分类名称和对象字段。添加完自定义对象分类以后，可通过 API 的方式进行自定义数据上报，支持直接通过 API 的方式进行自定义数据上报。支持对上报的数据进行搜索和多标签筛选，支持数据导出，支持增加显示列，点击可侧滑查看详情。

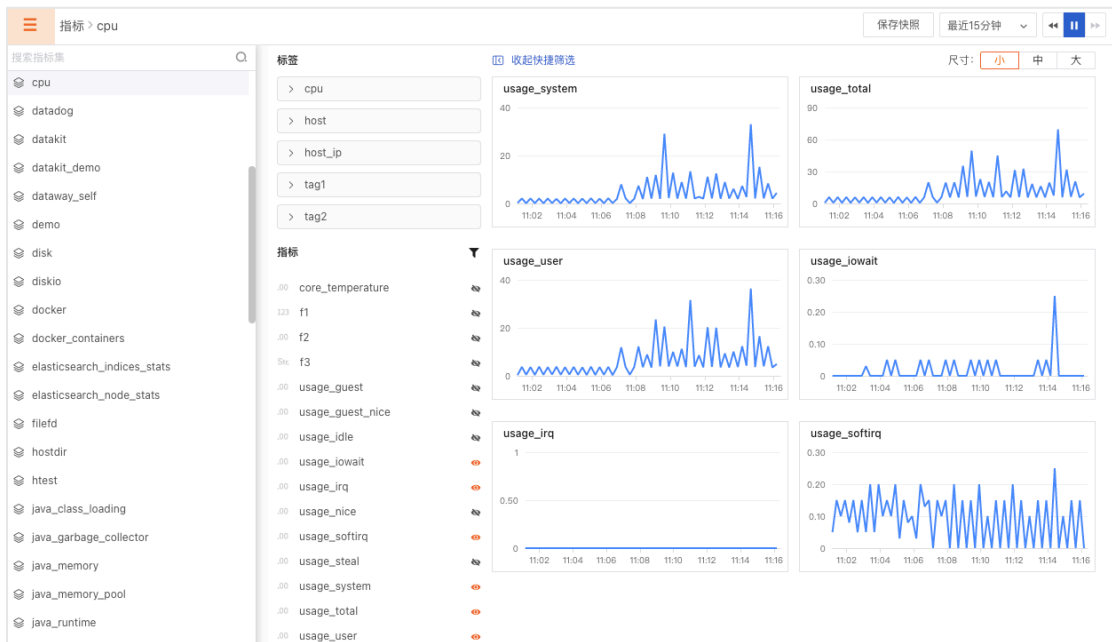
对象名	host	status	cpu	regionid	creat_time
iZm5ealqk5qliur...	i-m5ealqk5qliur...	Running	2	cn-qingdao	2021-07-01T05:2...

指标

「指标」提供了快速查看当前工作空间所有数据指标的能力，并支持对指标集进行搜索、筛选过滤等功能。

指标管理

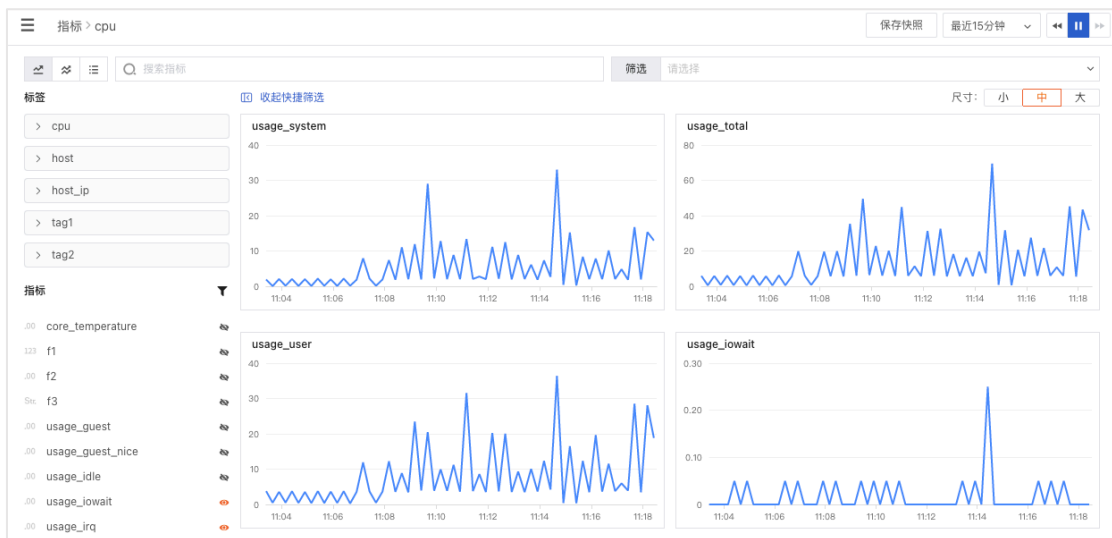
进入「指标」-「查看器」页面，左侧显示空间内所有采集的指标集，右侧展示对应的标签和指标内容。支持对指标集和指标进行搜索、筛选过滤等功能。



观测云支持三种指标浏览模式，平铺模式、混合模式、列表模式。

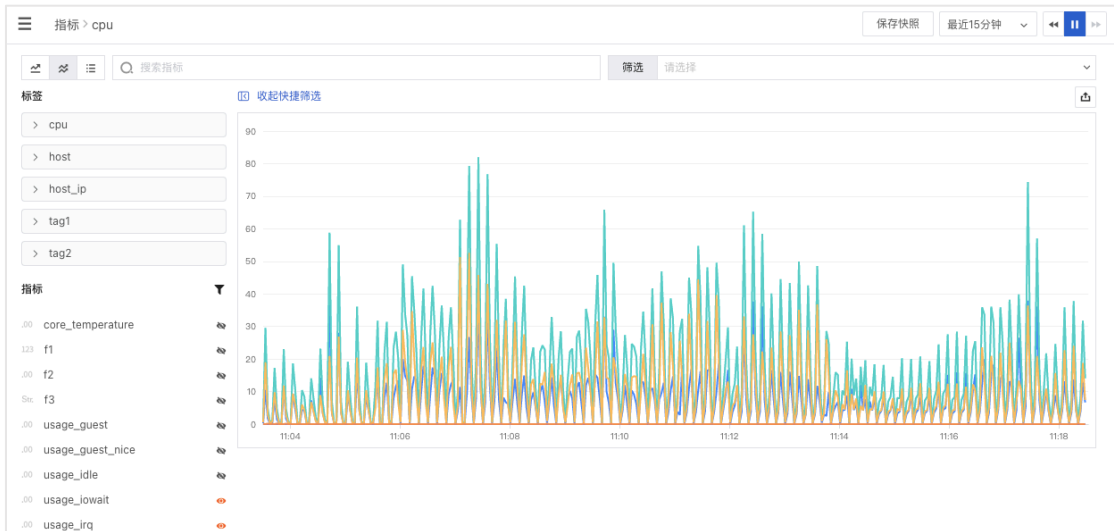
1) 平铺模式

该模式下支持同时显示多个图表，每一个指标为一个折线图，方便进行指标的对比分析。支持选择“小”、“中”、“大”三种图表尺寸查看方式，默认为“中”。



2) 混合模式

该模式下所选指标均显示在一个折线统计图中，可查看指标在一定时间内的数据走势。点击右上角导出按钮，即可导出图表到场景视图。



3) 平铺模式

该模式下展示所选指标采集的数据详情，可查看到数据采集时间以及所有的字段。点击右上角设置按钮，即可导出列表到 CSV 文件。

时间	cpu	usage_sys...	usage_total	usage_user	usage_iowa...	usage_irq	usage_sof...
2021/10/29...	cpu-total	0.55	1.16	0.55	0.05	0	0
2021/10/29...	cpu-total	18.21	31.05	12.84	0	0	0
2021/10/29...	cpu-total	2.17	6.31	3.99	0.05	0	0.10
2021/10/29...	cpu-total	15.13	36.07	20.94	0	0	0
2021/10/29...	cpu-total	1.61	4.89	3.12	0	0	0.15
2021/10/29...	cpu7	4.28	26.48	22.20	0	0	0
2021/10/29...	cpu6	4.67	28.15	23.37	0	0	0.10
2021/10/29...	cpu5	4.22	27.21	22.99	0	0	0
2021/10/29...	cpu4	4.64	27.72	23.08	0	0	0
2021/10/29...	cpu3	4.26	27.11	22.84	0	0	0
2021/10/29...	cpu2	5.19	28.38	23.09	0	0	0
2021/10/29...	cpu1	3.84	25.18	21.23	0	0	0
2021/10/29...	cpu0	4.56	26.27	21.70	0	0	0
2021/10/29...	cpu-total	4.45	27.06	22.58	0	0	0.03
2021/10/29...	cpu-total	13.48	40.98	27.50	0	0	0
2021/10/29...	cpu-total	3.44	8.37	4.93	0	0	0
2021/10/29...	cpu-total	11.97	25.88	13.91	0	0	0
2021/10/29...	cpu-total	0.13	0.63	0.43	0	0	0.08

指标字典

指标数据采集后，可以在观测云工作空间的「指标字典」查看所有采集的指标集及其指标和标签。

指标字典

Q 搜索

指标集名称
ClickHouseAsyncMetrics
ClickHouseMetrics
ClickHouseProfileEvents
acs_ecs_dashboard
aliyun-bss-sync
aliyun-es-INSTANCELOG
aliyun-es-SEARCHSLOW
aliyun-sls-slb-hz-logs
aliyun_acs_ecs_dashboard
conntrack
cpu

支持在详情页查看该指标集下所有可用的指标和标签，支持通过模糊搜索来查询指标集。支持对通过 DataKit API 直接上报的数据，手动设置指标的单位。

datakit

在指标页打开

指标 (18) 标签 (9)

Q 搜索

指标名	字段类型	单位
cpu_usage	float	-

指标名称: cpu_usage 保存 取消

字段类型: float

单位: 百分比 0 - 100

描述: 请输入描述信息

支持把所有的指标、日志、链路数据统一上报到工作空间，通过对采集的数据打上相同的标签进行关联查询和分析，发现并解决存在的潜在风险。

cpu

在指标页打开

指标 (12) 标签 (4)

Q 搜索

标签名	统计
cpu	1
cpu-total	
host	36
host_ip	6
project	1

日志

观测云拥有全面的日志采集能力，支持标准日志采集和配置自定义日志采集两种方式，能采集 Windows/Linux/macOS 主机多种系统日志以及 Nginx、Redis、Docker、ES 等多种应用日志数据。

日志管理

在「日志列表」页面支持对日志进行搜索和多标签筛选，支持数据导出，支持增加显示列，同时系统根据选择的时间范围自动划分若干时间点，通过堆积柱状图展示不同等级日志的数量，帮助用户进行统计分析。若对日志进行了筛选，柱状图同步展示筛选后结果。支持将当前的展示内容、时间范围、筛选条件保存到快照。

日志查看器支持三种查看模式：默认、近似文本、分组。

1) 默认查看器

支持基于采集的原始日志数据进行查看和分析。



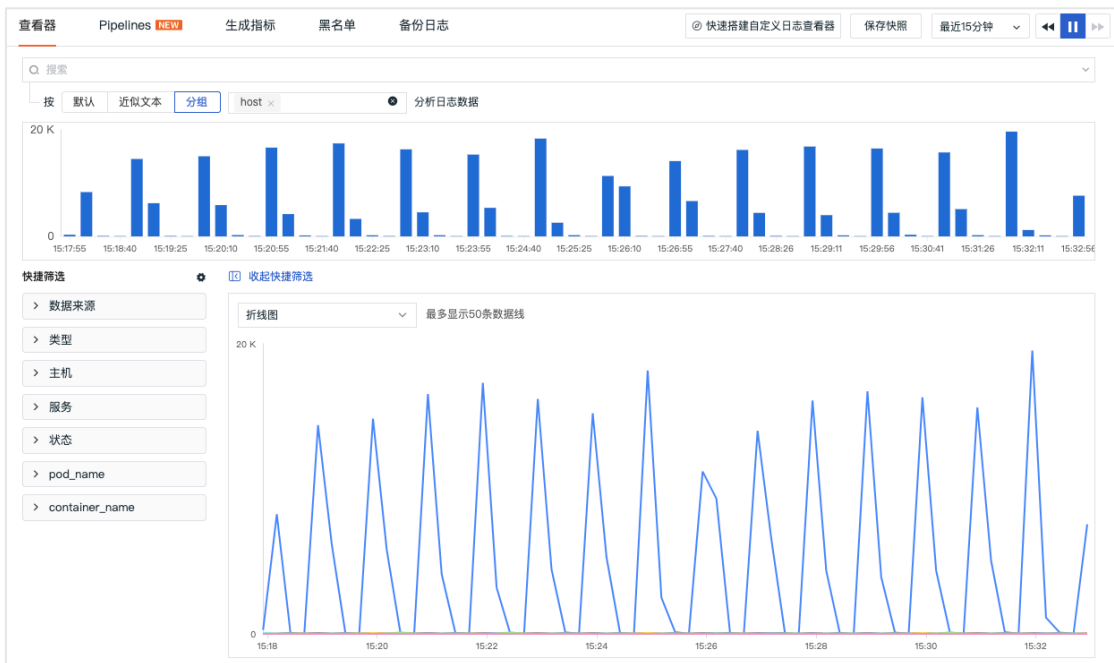
2) 近似文本查看器

支持根据右上方选择的时间范围固定当前时间段，并获取该时间段内 10000 条数据进行近似文本分析，将近似度高的日志进行聚合，并提取共同的 pattern 聚类，有利于发现异常日志和快速定位问题。



3) 分组查看器

支持对原始日志数据基于 1-3 个标签进行分组统计，以反映出日志数据在不同的分组下，不同时间的分布特征与趋势。

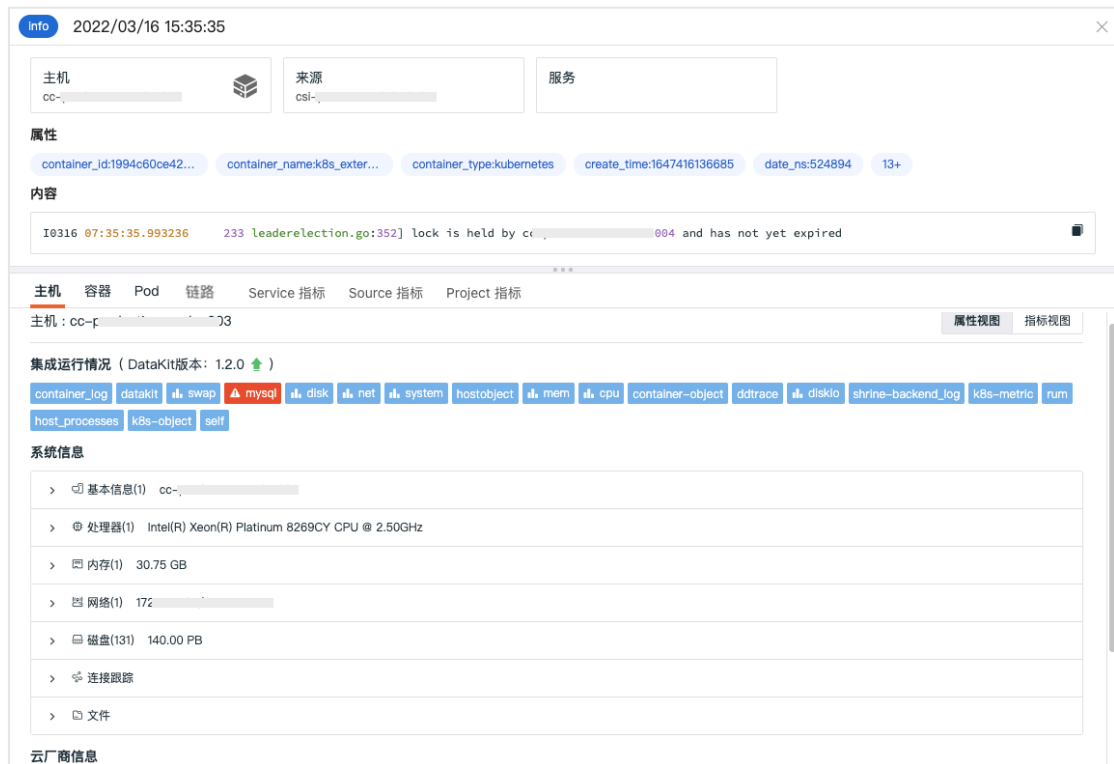


日志详情

点击想要查看的日志，即可查看对应的日志详情，包括日志关联的所有属性、日志内容等，同时支持查看关联的主机、容器、Pod、链路、指标（Service、Source、Project）。

注意：在日志详情页中查看关联的主机、容器、Pod、链路、指标等，需要匹配相关的字段“host”、“container_name”、“pod_name”、“trace_id”、

“service”、“project”、“source”，否则无法在日志详情查看到相关的页面。



Pipelines

Pipeline 支持对不同格式的日志数据进行文本解析，通过编写 Pipeline 脚本，可以自定义切割出符合要求的结构化日志，并把切割出来的字段作为属性使用。通过属性字段，我们可以快速筛选相关日志、进行数据关联分析，帮助我们快速去定位问题并解决问题。

自定义 Pipeline 管理

观测云支持用户创建自定义 Pipeline 脚本，在观测云工作空间「日志」-「Pipelines」，点击「新建 Pipeline」可创建一个新的 Pipeline 文件。支持多种脚本函数，可通过观测云提供的脚本函数列表直接查看其语法格式。

Pipeline 名称	状态	最后更新时间	操作
nginx.p	已启用	2022-02-23	🔴 ✎ 🗑️
datakit.p	已启用	2022-02-23	🔴 ✎ 🗑️

共 2 条

Pipeline 官方库

观测云提供 Pipeline 官方脚本库，内置多种日志解析 Pipeline。在观测云工作空间「日志」-「Pipelines」，点击「Pipeline 官方库」即可查看内置标准的 pipeline 官网文件库，包括如 nginx、apache、redis、elasticsearch、mysql 等。选择打开任意一个 pipeline 文件，如 nginx.p，可以看到内置的解析规则，如果需要自定义修改，可通过克隆创建一个新的 pipeline 文件。

注意：pipeline 官方库文件不支持修改。

nginx.p
🔗 克隆 ✕

1 * 过滤日志 🕒

nginx

根据所选日志来源自动生成同名 Pipeline

2 * 定义解析规则 🕒

```

1
2 #----- 警告 -----
3 # 不要修改本文件，如果要更新，请拷贝至其它文件，最好以某种前缀区分，避免重启后被覆盖
4 #-----
5
6 add_pattern("date2", "%{YEAR}[./]%{MONTHNUM}[./]%{MONTHDAY} %{TIME}")
7
8 # access log
9 grok(_, "%{NOTSPACE:client_ip} %{NOTSPACE:http_ident} %{NOTSPACE:http_auth} \\[%{HTTPDATE:time}\\]")
10
11 # access log
12 add_pattern("access_common", "%{NOTSPACE:client_ip} %{NOTSPACE:http_ident} %{NOTSPACE:http_auth} \\"
13 grok(_, "%{access_common} %{NOTSPACE:referrer}" "%{GREEDYDATA:agent}")
14 user_agent(agent)
15
16 # error log
17 grok(_, "%{date2:time} \\[%{LOGLEVEL:status}\\]" "%{GREEDYDATA:msg}, client: %{NOTSPACE:client_ip}, :
18 grok(_, "%{date2:time} \\[%{LOGLEVEL:status}\\]" "%{GREEDYDATA:msg}, client: %{NOTSPACE:client_ip}, :
19 grok(_, "%{date2:time} \\[%{LOGLEVEL:status}\\]" "%{GREEDYDATA:msg}")
          
```

取消

生成指标

观测云支持基于日志数据配置聚合规则产生新的指标数据，以便于进行更深入的数据分析。

查看器	Pipelines NEW	生成指标	黑名单	备份日志																		
<div style="display: flex; justify-content: space-between;"> 新建规则 </div> <table border="1"> <thead> <tr> <th>指标集</th> <th>指标</th> <th>聚合方式</th> <th>维度</th> <th>频率</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>nginx_custom</td> <td>city</td> <td>count</td> <td>city</td> <td>1分钟</td> <td>开关 删除 编辑 更多</td> </tr> <tr> <td>nginx_custom</td> <td>browser</td> <td>count</td> <td>browser</td> <td>1分钟</td> <td>开关 删除 编辑 更多</td> </tr> </tbody> </table>					指标集	指标	聚合方式	维度	频率	操作	nginx_custom	city	count	city	1分钟	开关 删除 编辑 更多	nginx_custom	browser	count	browser	1分钟	开关 删除 编辑 更多
指标集	指标	聚合方式	维度	频率	操作																	
nginx_custom	city	count	city	1分钟	开关 删除 编辑 更多																	
nginx_custom	browser	count	browser	1分钟	开关 删除 编辑 更多																	

黑名单

观测云支持黑名单功能，通过添加日志过滤规则，减少日志不必要的数据上报。

查看器	Pipelines NEW	生成指标	黑名单	备份日志						
<div style="display: flex; justify-content: space-between;"> 新建黑名单 </div> <table border="1"> <thead> <tr> <th>来源</th> <th>过滤条件</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>scheduler</td> <td>host in ["cc- 001"]</td> <td>删除 更多</td> </tr> </tbody> </table>					来源	过滤条件	操作	scheduler	host in ["cc- 001"]	删除 更多
来源	过滤条件	操作								
scheduler	host in ["cc- 001"]	删除 更多								

备份日志

观测云支持配置备份规则对符合规则的日志进行备份存储，备份周期按天进行备份，每天 00:00:00 开始备份前一天 00:00:00—23:59:59 的日志数据，查看日志备份的数据，需要选择备份数据时间范围。

日志备份 > 备份规则											
<div style="display: flex; justify-content: space-between;"> 新建规则 </div> <table border="1"> <thead> <tr> <th>名称</th> <th>搜索关键字</th> <th>过滤条件</th> <th>操作</th> </tr> </thead> <tbody> <tr> <td>nginx_backup</td> <td></td> <td>source: nginx</td> <td>删除 更多</td> </tr> </tbody> </table> <div style="text-align: right; margin-top: 5px;"> 共 1 条 < 1 > 跳至 <input type="text" value="1"/> 页 </div>				名称	搜索关键字	过滤条件	操作	nginx_backup		source: nginx	删除 更多
名称	搜索关键字	过滤条件	操作								
nginx_backup		source: nginx	删除 更多								

应用性能监测

观测云支持对链路数据进行分析和管理，追踪所有服务处理请求所花费的时间以及请求状态，可用于对应用程序的性能监控。支持关联用户访问监测、日志监测，支持通过采样的方式减少应用性能数据采集，节约存储空间。支持基于当前空间内的现有数据生成新的指标数据，便于依据需求设计并实现新的技术指标。

服务

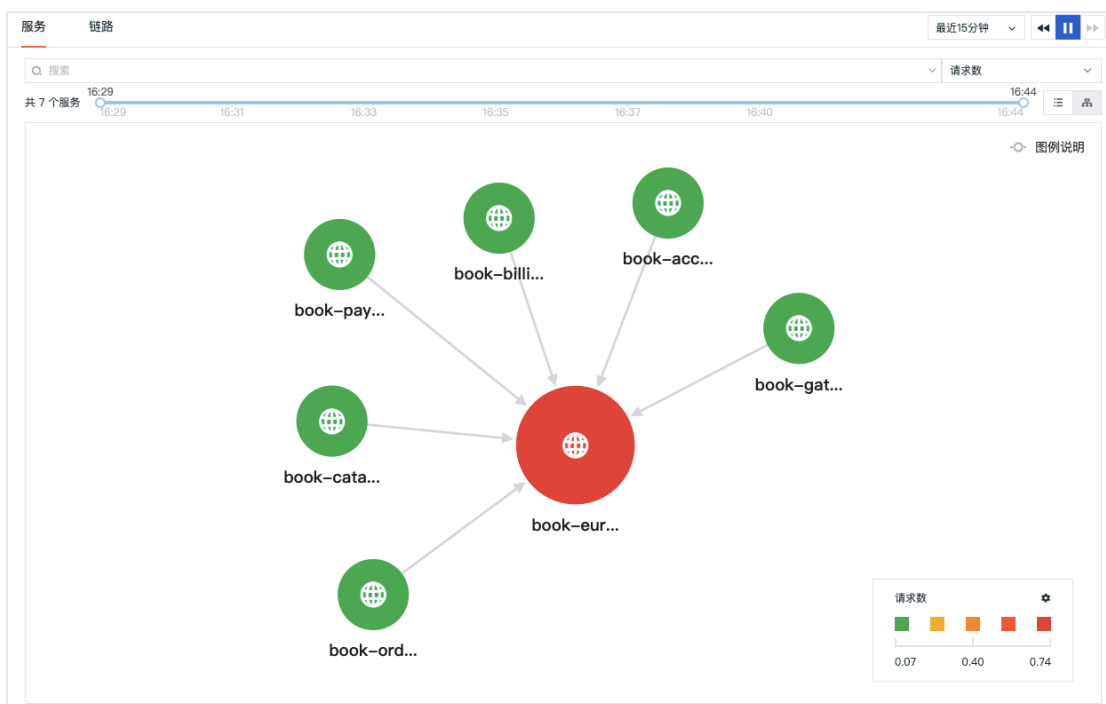
应用性能监测的“服务”展示工作空间内所有的链路服务列表，并可查看到所有服务的追踪指标：“平均每秒请求数”、“平均响应时间”、“P75 响应时间”、

“P95 响应时间”和“错误数”。点击服务名后会侧滑显示该服务的链路概览，可查看请求数、错误数、响应时间、响应时间分布等图表分析，还可查看和搜索服务所包含的资源性能指标，添加更多的性能指标显示列。

服务	服务类型	平均每秒请求数	平均响应时间	P75响应时间	P99响应时间	错误数
book-payment	web	0.07 req/s	< 0.01	2.03 ms	2.43 ms	0(0.00%)
book-order	web	0.07 req/s	< 0.01	2.08 ms	2.29 ms	0(0.00%)
book-gateway	web	0.07 req/s	< 0.01	1.88 ms	1.93 ms	0(0.00%)
book-eureka	web	0.74 req/s	< 0.01	1.67 ms	1.95 ms	0(0.00%)
book-catalog	web	0.07 req/s	< 0.01	1.9 ms	1.95 ms	0(0.00%)
book-billing	web	0.07 req/s	< 0.01	2.07 ms	2.63 ms	0(0.00%)
book-account	web	0.07 req/s	< 0.01	1.97 ms	2.53 ms	0(0.00%)

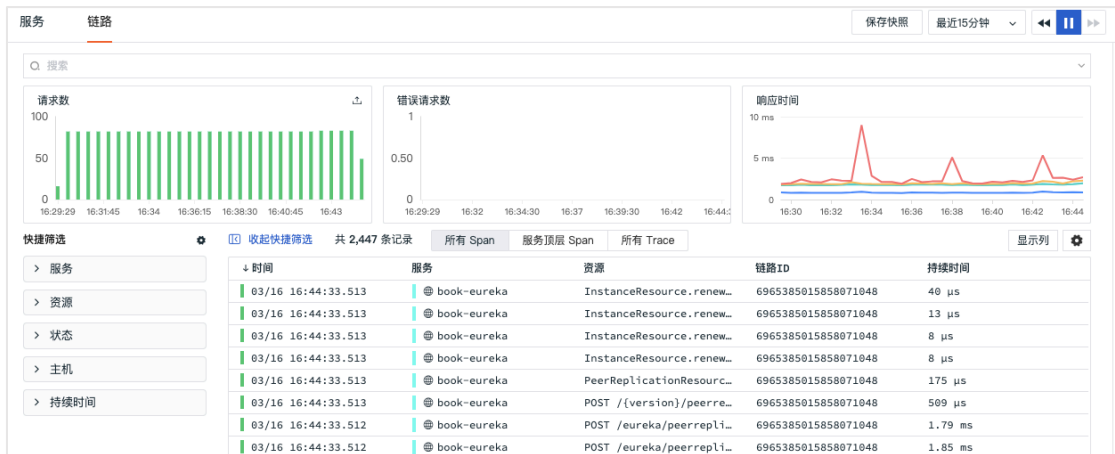
关系图

链路服务支持切换列表至关系图模式查看各个服务之间的调用关系。将鼠标悬浮在服务节点处时，你可以查看该服务的“请求数”、“P50 响应时间”、“P75 响应时间”、“P99 响应时间”和“错误数”。支持通过不同的性能指标进行筛选显示，并可自定义链路服务性能指标颜色区间。支持通过时间轴、高亮显示、节点尺寸、填充项、缩略图等方式调整分布图。



链路

应用性能监测的“链路”，支持统计所选时间范围内链路的“请求数”、“错误请求数”、“响应时间”，并展示服务的所有链路列表。观测云提供三种链路筛选查看列表，分别为“所有 Span”、“服务顶层 Span”和“所有 Trace”。支持对链路数据进行搜索、多标签筛选、数据导出、增加显示列等操作，支持将当前的展示内容、时间范围、筛选条件保存到快照。

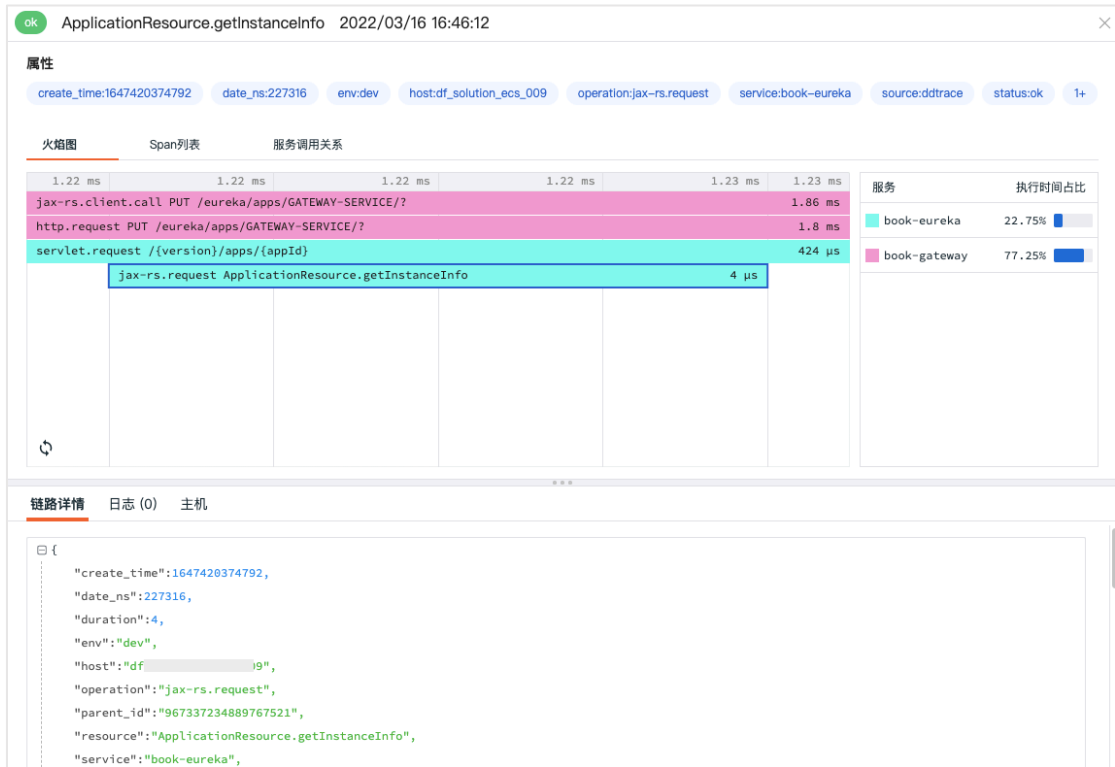


链路详情

点击链路列表可查看所属的链路详情，包含链路所有相关的「标签」、「火焰统计图」、「span 列表」以及与该链路关联的主机、日志和进程等数据。支持进行关键字搜索和多标签筛选，点击日志和进程内容可直接跳转到日志/进程详情页面，可结合日志/进程详情可对链路性能进行关联分析。

1) 火焰图

火焰图用于清晰展示整条链路中每个 span 的流转和执行时间。同时显示对应的服务列表及响应时间。



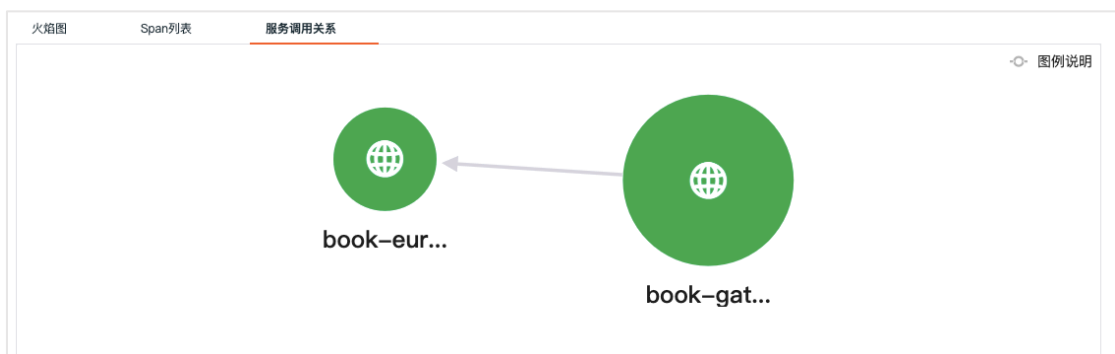
2) span 列表

展示该条链路中所有的 span 列表,包括“服务名”、“span 名”、“span 个数”、“执行时间”以及“执行时间占比”。点击「span 名」即可查看对应的 span 详情信息。

资源	Span数量	持续时间(平均)	执行时间	执行时间占比(%)
book-eureka	4	124.5 μ s	424 μ s	22.75%
book-gateway	2	1.83 ms	1.44 ms	77.25%

3) 服务调用关系图

用来查看各个服务之间的调用关系。



用户访问监测

观测云支持采集 Web、Android/iOS 和小程序用户访问数据，并提供了应用查看器、概览、性能分析、资源分析、错误分析等场景，帮助你快速监测用户的使用行为和遇到的问题。支持通过采样的方式减少用户访问数据采集，节约存储空间。支持基于当前空间内的现有数据生成新的指标数据，便于依据需求设计并实现新的技术指标。

查看器

观测云应用性能查看器支持对应用中的用户访问数据进行搜索、筛选和导出查看分析。支持自定义添加/删除显示列，点击会话或页面数据可查看详情。支持将当前的展示内容、时间范围、筛选条件保存到快照。

观测云用户访问监测查看器包括 session（会话）、view（页面）、resource（资源）、action（操作）、long_task（长任务）、error（错误）。

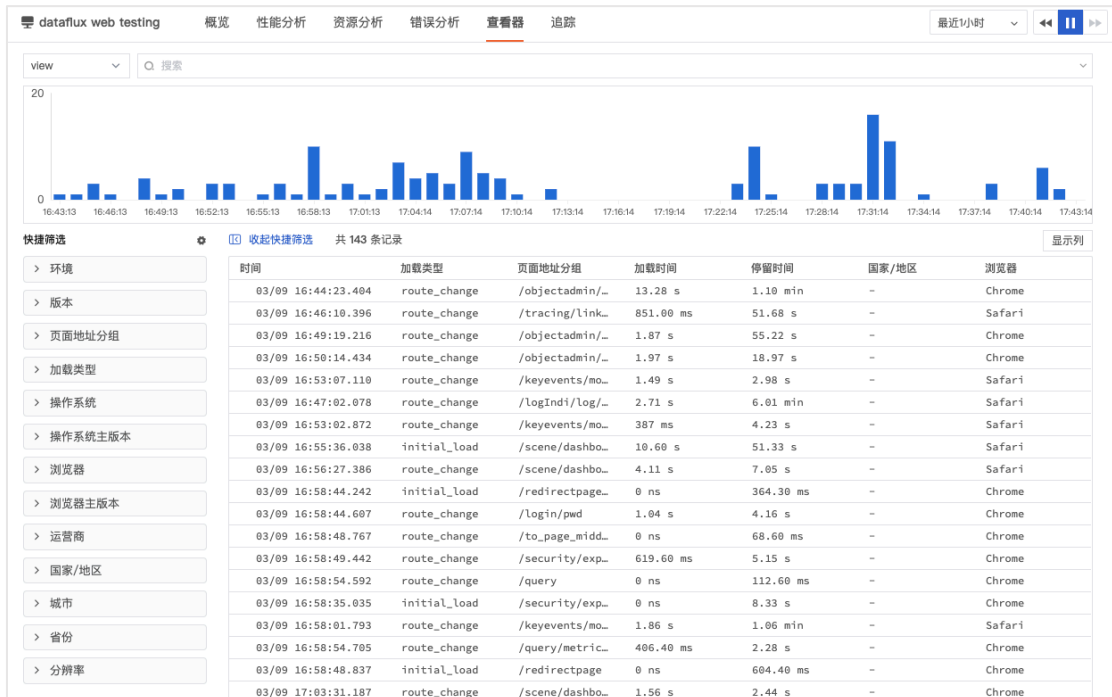
session 查看器

通过左上角的数据类型筛选栏，选择「session 查看器」即可查看对用户访问时的会话数据进行查询和分析，包括用户访问时的会话时长（即用户从打开一个应用到关闭的时间）、会话类型、页面访问数量、操作数量、错误数、用户最初访问页面和最后浏览页面等。



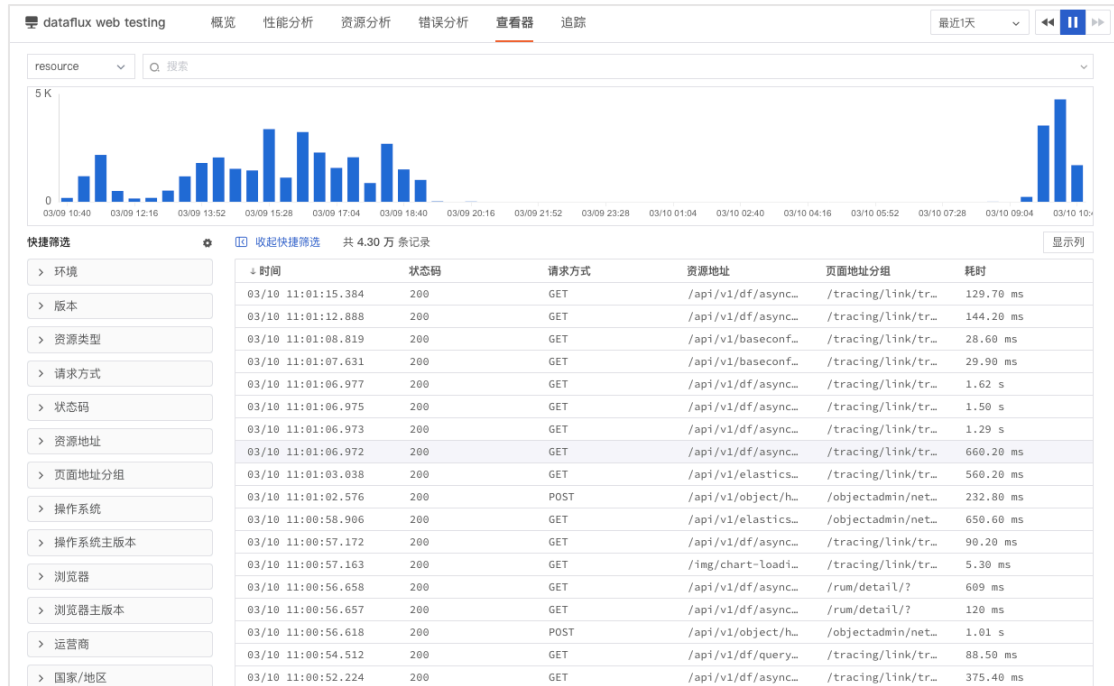
view 查看器

通过左上角的数据类型筛选栏，选择「view 查看器」即可对用户访问时的页面性能数据进行查询和分析，包括用户访问时的页面地址、页面加载类型、页面加载时间、用户停留时间等。



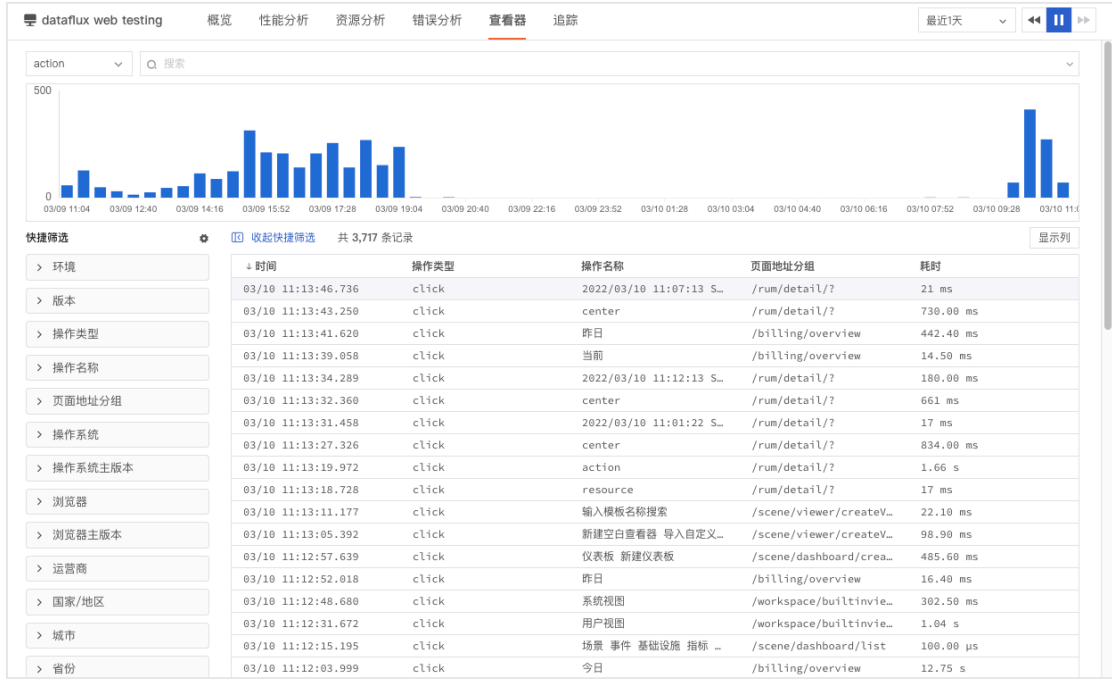
resource 查看器

通过左上角的数据类型筛选栏，选择「resource 查看器」即可对用户访问时的资源加载性能进行查询和分析，包括用户访问时的资源地址、状态码、请求方式、资源加载时间等。



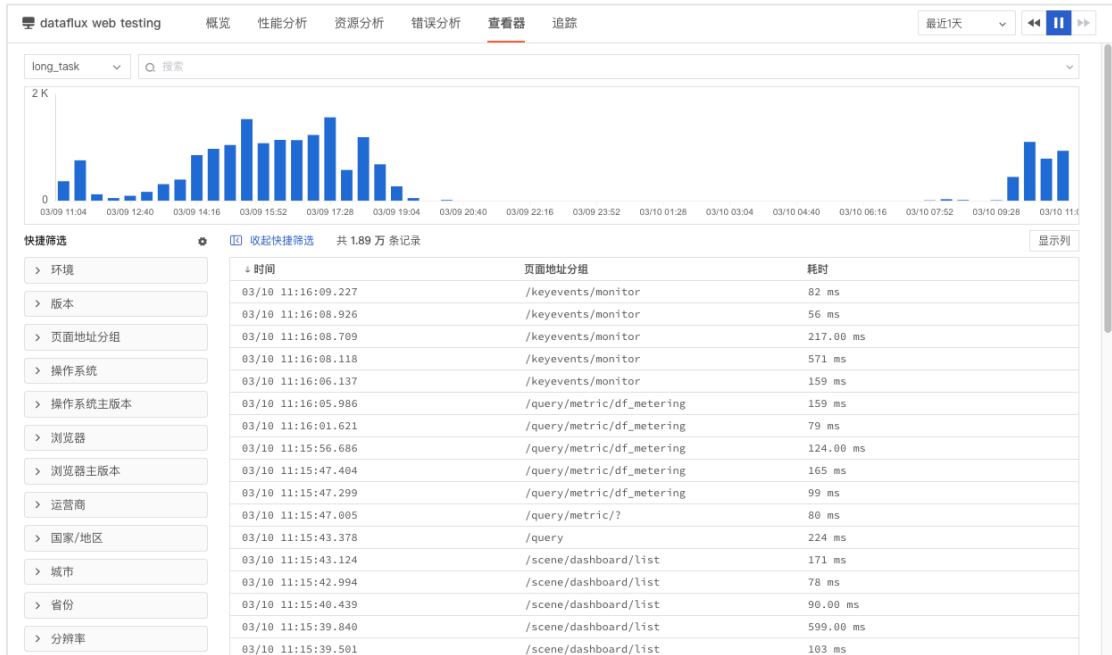
action 查看器

通过左上角的数据类型筛选栏，选择「action 查看器」即可对用户访问时的操作行为进行查询和分析，包括用户访问时的操作类型、操作内容、操作时间等。



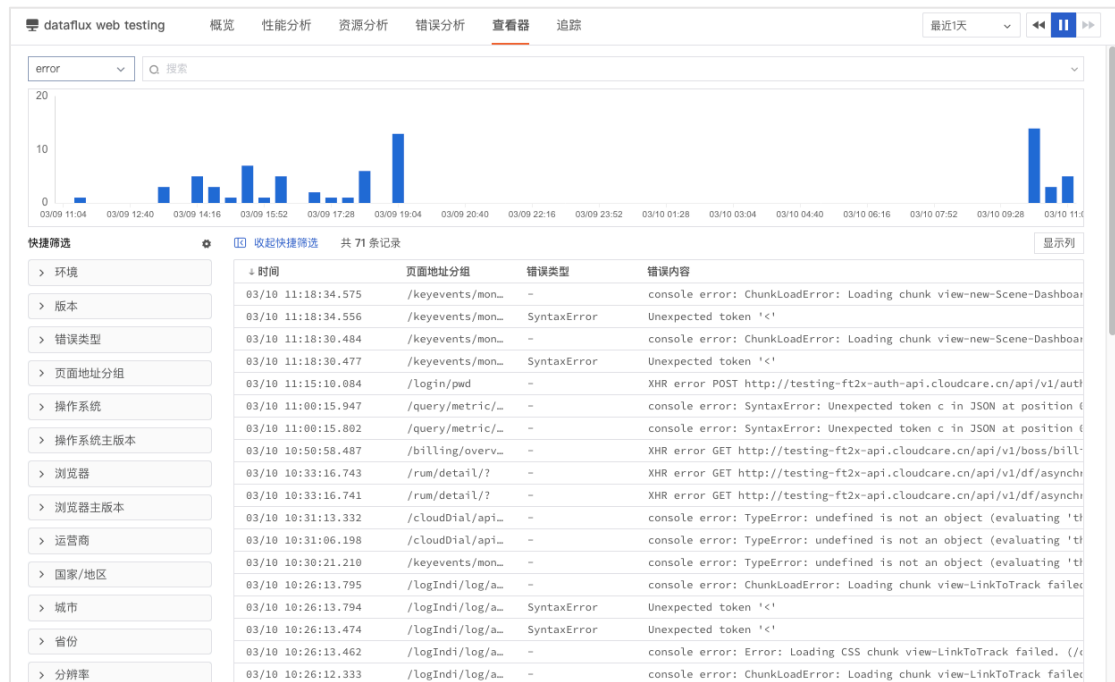
long_task 查看器

通过左上角的数据类型筛选栏，选择「long_task 查看器」即可对用户访问时的资源加载性能进行查询和分析，包括用户访问时的资源地址、状态码、请求方式资源加载时间等。



error 查看器

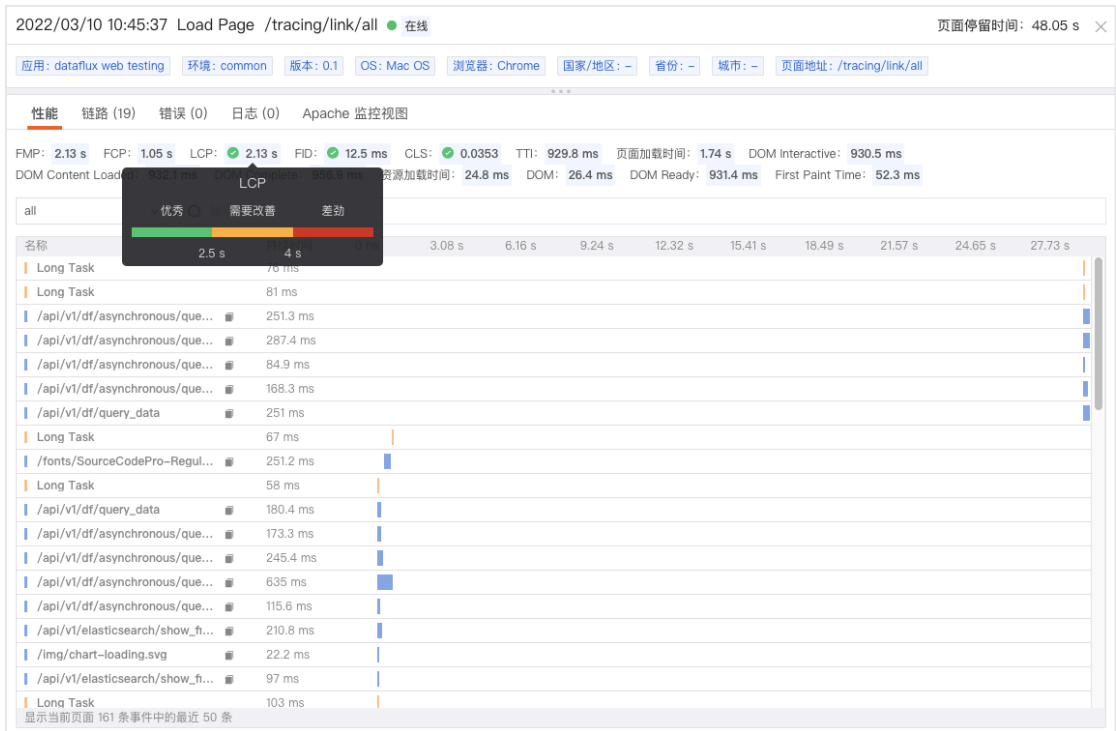
通过左上角的数据类型筛选栏，选择「error 查看器」即可对用户访问时发生的代码错误进行查询和分析，包括用户访问时的页面地址、代码错误类型、错误内容等。



用户访问详情

在查看器中，点击数据列表即可查看该用户访问的详情，包括性能、链路、错误和日志等。

- **性能:** 查看到用户访问指定应用时前端的页面性能，包括页面加载时间、内容绘制时间、交互时间、输入延时等。
- **链路:** 查看用户访问时向后端应用发出的每一个请求，包括发生时间、请求的链路和持续时间。点击请求，可跳转至对应链路的详情页。
- **错误:** 查看出现在该次用户访问时的错误数据信息、错误类型和错误发生时间。点击错误信息，可跳转至对应错误的详情页。支持 Sourcemap 的功能来还原混淆的代码，方便错误排查时在源码中 debug，定位代码问题。
- **日志:** 可以基于当前用户访问查看关联日志。支持对日志进行关键字搜索和多标签筛选。点击日志，可跳转至对应日志页。



追踪

观测云支持用户通过「用户访问监测」新建追踪任务，对自定义的链路追踪轨迹进行实时监控。通过预先设定链路追踪轨迹，可以集中筛选链路数据，精准查询用户访问体验，及时发现漏洞、异常和风险。

1 新建追踪

* 名称

标签

追踪ID

2 引入方式

NPM 引入 CDN 同步引入 CDN 异步引入

初始化 SDK 后，使用 `addRunGlobalContext(track_id,'value')` 添加追踪 ID。

```
import { datafluxRun } from '@cloudcare/browser-run'
datafluxRun.addRunGlobalContext('track_id','rtrace_XXXXXXXXXXXXXXXXXXXXXXXXXXXX');
```

详细步骤请参考: [追踪配置示例](#)

可用性监测

观测云提供开箱即用的云拨测解决方案，利用覆盖全球的监控网络，通过 API 拨测快速实现网络站点的可用性监测，结合地域、运营商、时间等维度，周期性的对 URL 站点质量进行监测，发现潜在问题，定位问题产生原因，提升用户体验。

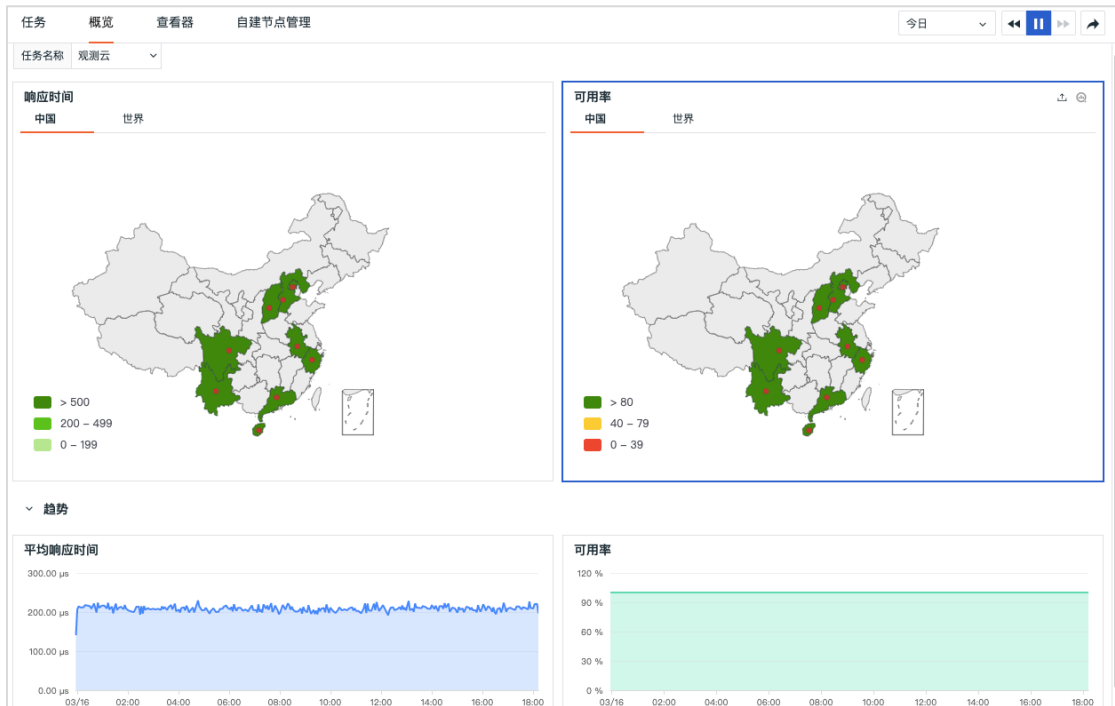
可用性监测管理

在可用性监测，点击「新建」即可添加一条新的云拨测地址。



名称	拨测地址	类型	任务状态	操作
观测云-自建	https://www.guance.com/	http	启动	<input checked="" type="checkbox"/>
观测云	https://www.guance.com/	http	启动	<input checked="" type="checkbox"/>

添加完成拨测地址后，可以在概览页面从地理和趋势两个维度分析当前拨测任务的响应时间和可用率。



可用性监测查看器支持对云拨测的数据进行查看、搜索、筛选、数据导出和添加显示列。支持通过堆积柱状图对拨测数据按照选择的时间范围进行统计，支持将当前的展示内容、时间范围、筛选条件保存到快照，点击列表数据即可查看拨测结果详情。



自建节点管理

观测云支持在全球范围内自建新的拨测节点，创建自建节点后，通过“获取配置”获取指定节点的配置信息，并在 DataKit 中进行配置，配置完成后即可在拨测中选择使用。

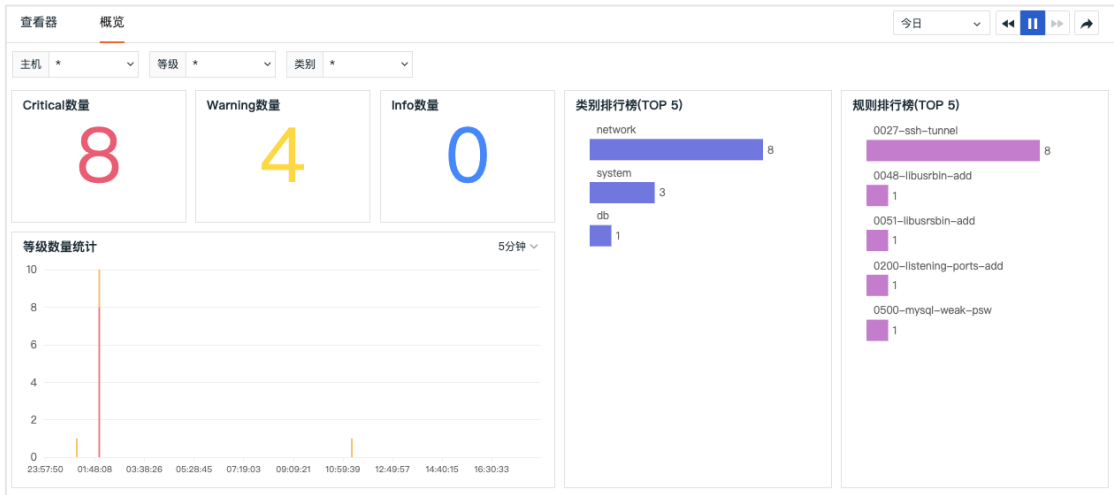
节点	地理位置	运营商	操作
China-Shanghai-telecom	China,Shanghai	telecom	🗑️
Afghanistan-Shahrak-telecom	Afghanistan,Shahrak	telecom	🗑️

安全巡检

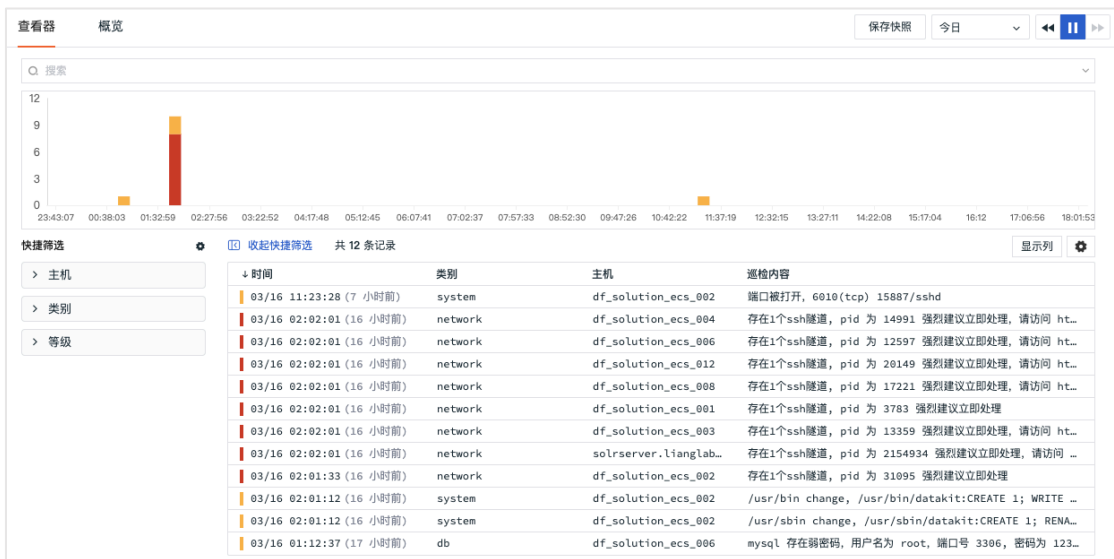
观测云支持通过「安全巡检」及时监控、查询和关联全部巡检事件。在及时发现漏洞，异常和风险的同时，帮助提高巡检质量、问题分析和问题处理的能力。支持基于当前空间内的现有数据生成新的指标数据，便于依据需求设计并实现新的技术指标。

安全巡检管理

在「安全巡检」-「概览」，支持通过筛选主机、安全巡检等级、安全巡检类别来查看不同主机发生安全巡检事件的概览情况，包括不同等级安全巡检事件发生的数量及可视化图表分析，不同类别和规则的安全巡检事件排行榜。



在「安全巡检」-「查看器」，支持对上报的安全巡检事件进行查看、搜索、筛选、数据导出和添加显示列。支持通过堆积柱状图对拨测数据按照选择的时间范围进行统计，支持将当前的展示内容、时间范围、筛选条件保存到快照，点击列表数据即可查看安全巡检的详情。



安全巡检事件详情

点击想要查看的巡检事件，在划出详情页中，可查看对本次安全巡检事件的处理建议，包括安全巡检事件发生的理论基础、风险项、审计方法、补救措施等，同时可查看关联的巡检事件以及主机等。

critical
(6 分钟前) 存在ssh隧道
✕

主机
df_solution_ecs_002

类别
network

规则
0027-ssh-tunnel

属性

category:network create_time:1647426121786 date_ns:12463 host:d...02 level:critical rule:0027-ssh-tunnel version:1.0.8

内容

存在1个ssh隧道, pid 为 23280 强烈建议立即处理

建议 关联巡检 (5) 主机

理论基础

SSH隧道即SSH端口转发, 在SSH客户端与SSH服务端之间建立一个隧道, 将网络数据通过该隧道转发至指定端口, 从而进行网络通信。SSH隧道自动提供了相应的加密及解密服务, 保证了数据传输的安全性。如果主机存在未知的ssh隧道, 主机会面临数据泄露的危险, 所以应该在审计范围内。

风险项

黑客渗透,数据泄露,网络安全,挖矿风险,肉机风险

审计方法

验证主机进程列表, 是否存在cmdline 为 sshd: root@notty的 进程。可以执行以下命令验证:

```
ps -ef | grep -v grep | grep "sshd: root@notty"
```

补救

如果存在 未知的cmdline 为 sshd: root@notty的 进程, 请执行 kill -9 隧道pid, 关闭危险进程。

监控

观测云拥有强大的异常检测功能, 支持内置检测库和自定义检测库。配合告警和关联事件, 能帮助您快速发现问题、定位问题、解决问题。同时, “观测云”支持 SLO (Service Level Objective) 监控, 精准把控服务水准和目标。

监控器

监控器模版

观测云内置多种监控器模版, 开箱即用, 包括 Docker、Elasticsearch、Redis、主机检测库等监控模版, 开启后, 即可接收到相关的异常事件告警。

监控器
SLO NEW
静默管理

+ 新建监控器
+ 从模板新建

批量操作 ▾
导入监控器
分组管理

分组 Docker 检测库 × 🔍 搜索监控器名称

监控器名称	分组	状态	操作
Docker 容器状态检测	Docker 检测库	已启用	🟢 ✎ 🗑️ 🔇
Docker 容器内存使用率过高	Docker 检测库	已启用	🟢 ✎ 🗑️ 🔇
Docker 容器 CPU 使用率过高	Docker 检测库	已启用	🟢 ✎ 🗑️ 🔇

自定义监控器

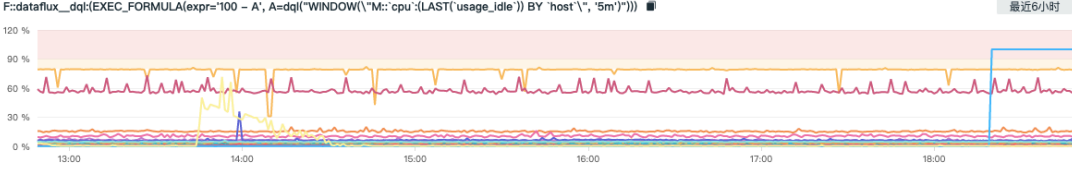
观测云支持多种自定义监控器，允许用户自定义配置检测和触发条件，并通过设置告警第一时直接接收告警通知。

检测规则	说明
阈值检测	基于设置的阈值对指标数据进行异常检测
日志检测	基于工作空间内的日志数据进行异常检测。
突变检测	基于历史数据对指标的突发反常表现进行异常检测，多适用于业务数据、时间窗短的场景。
区间检测	基于动态阈值范围对指标的异常数据点进行检测，当数据超出设定的区间范围后，产生告警并通知用户，多适用于趋势稳定时间线的场景。
水位检测	基于历史数据对指标的持续反常表现进行异常检测，可避免突发检测的毛刺告警。
安全巡检	基于工作空间内安全巡检数据进行异常检测，用于监控工作空间内系统、容器、网络等存在的漏洞、异常和风险。
应用性能指标检测	基于工作空间内应用性能监测数据进行异常检测，通过设置阈值范围，当指标到达阈值后触发告警
用户访问指标检测	基于工作空间内用户访问监测数据进行异常检测，通过设置阈值范围，当指标到达阈值后触发告警
进程异常检测	基于工作空间内进程数据进行异常检测，支持对进程数据的一个或多个字段类型设置触发告警
可用性监测数据检测	基于工作空间内可用性监测数据进行异常检测，通过对一定时间段内拨测任务产生的指定数据量设置阈值（边界）范围，当数据量到达阈值范围后即可触发告警

触发规则

在异常检测库“新建检测规则”即可自定义添加一个新的检测规则。在检测规则添加规则名称、选择检测指标、配置触发条件、添加事件名称和内容、选择检测频率，完成检测规则的配置。无数据状态支持「触发无数据事件」、「触发恢复事件」、「不触发事件」三种配置，支持通过模版变量的方式添加事件名称和内容。

F::dataflux_dql(EXEC_FORMULA(expr='100 - A', A=dq("WINDOW('M':cpu:(LAST('usage_idle')) BY 'host'\", '5m'))) # 最近6小时



* 规则名称

* 分组

关联仪表盘

检测指标

Result + 添加查询 AS

A 指标 Last by host

[转换为简单查询](#)

选取 内的数据

触发条件

紧急 当 Result > 90 90 %

重要 当 Result >= 请输入值

警告 当 Result between 80 - 90 80 %-90 %

正常 1 个检测周期内无异常事件产生。

无数据 若检测指标出现无数据情况，则

* 事件名称

模板变量示例: [{{ df_status }}](#) [{{ df_monitor_checker_name }}](#) [{{ Result }}](#) [如何使用模板变量](#)

* 事件内容

>等级: {{status}}

>主机: {{host}}

>内容: 系统 CPU 使用率为 {{ Result | to_fixed(2) }}%

>建议: 基础设施-进程-选择主机-CPU 使用率 (排序) 查看是否为异常导致

模板变量示例: [{{ df_status }}](#) [{{ df_monitor_checker_name }}](#) [{{ Result }}](#) [如何使用模板变量](#)

检测频率

触发告警

观测云支持对异常检测的结果设置触发告警，支持包括「空间成员」、「邮件组」、「钉钉机器人」、「企业微信机器人」、「飞书机器人」、「Webhook 自定义」和「短信」等多种通知方式。可在工作空间“管理”-“通知对象”种进行配置。



触发事件

观测云支持用户基于监控器查看相关事件。



SLO

观测云 SLO 监控是围绕 DevOps 各类指标，测试系统服务可用性是否满足目标需要，不仅可以帮助使用者监控服务商提供的服务质量，还可以保护服务商免受 SLA 违规的影响。支持导出仪表板和查看关联事件。

名称	监控器	达标率 (7天)	剩余额度 (7天)	目标	操作
Ruoyi08-System服务SLO	1	100 %	1小时 40 分钟	99%	
Ruoyi08-中间件服务SLO	1	100 %	1小时 40 分钟	99%	
Ruoyi08-前端用户体验SLO	3	100 %	1小时 40 分钟	99%	

新建 SLO

在监控「SLO」-「新建 SLO」，即可自定义创建新的 SLO 任务。

SLO > 新建 SLO

名称

目标 ■ 目标 % ■ 最低目标 %

SLI

异常通知对象

通知沉默 时间范围内，相同告警不发送通知

检测频率

描述

注意：SLO 配置一旦保存，SLO 名称、目标、检测周期将不可更改。

字段	说明
名称	SLO 任务名称。最多支持 64 个字符输入。
目标	SLO 目标百分比(0-100%)，支持选定两个目标，包括“目标”和“最低目标”： <ul style="list-style-type: none"> 目标：当 SLO 百分比 < 目标百分比，且 \geq 最低目标百分比时，被认定为 不健康 SLA 最低目标：当 SLO 百分比 < 最低目标百分比时，被认定为 不达标 SLA
SLI	衡量系统稳定性的指标。支持自定义添加一个或多个监控器作为测量指标
异常通知对象	告警通知对象，支持空间成员、邮件组、企业微信机器人、钉钉机器人、飞书机器人、短信等通知方式。
通知沉默	通知沉默时间范围内相同告警不发送通知。若同一个事件不是非常紧急，但是告警通知频率高，可以通过设置通知沉默的方式减少通知频率。 注意：通知沉默设置后事件会继续产生，但是通知不会再发送，产生的事件会存入事件管理

检测频率	SLO 检测频率，即以一定时间范围为周期，监测 SLO 任务中监控器是否出现异常事件。目前支持 5 分钟、10 分钟两种检测频率。
描述	描述性信息，最多支持 256 个字符。

工作空间管理

工作空间管理是针对当前工作空间进行的设置，管理和操作。在加入工作空间并被分配到权限后，可以通过「管理」，对该空间的基本信息、成员、权限、内容和付费计划进行变更。

基本设置

在工作空间「管理」-「基本设置」，可查看当前观测云版本、工作空间名称和 ID、数据权限、成员数量、安全操作审计等信息，支持管理员修改空间名称、备注、数据存储策略、删除指标集等操作。

基本设置
API Key 管理
成员管理
SSO管理
通知对象管理
内置视图
分享管理

基本信息

当前版本: 商业版 [查看详情](#)

工作空间名称: 观测云 [✎](#)

工作空间 ID: wksp_c00b: 383ae77 [■](#)

Token: tkn_297b45 4c988 [■](#) 更换

数据权限: 所有数据

成员数: 4 个

备注: DataFlux [✎](#)

安全

操作审计 查看

危险操作

变更数据存储策略 变更

存储策略变更后，之前的存储数据仍需按照旧的存储策略滚动删除。[了解详情](#)

删除指定指标集 删除指标集

指标集删除后，数据将无法恢复

API Key 管理

观测云支持通过调用 Open API 接口的方式来获取和更新观测云工作空间的数据，在调用 API 接口前，需要先创建 API Key 作为认证方式。在观测云工作空间「管理」-「API Key 管理」，点击右上角「新建 Key」，输入 Key 名称，即可创建。

注意：API Key 管理支持管理员及以上可编辑。



The screenshot shows the 'API Key 管理' (API Key Management) page. At the top, there are navigation tabs: '基本设置', 'API Key 管理' (selected), '成员管理', 'SSO管理', '通知对象管理', '内置视图', and '分享管理'. Below the tabs is a search bar with the text '搜索'. Underneath, it says '共 2 个' (Total 2 items). On the right side, there is a blue button labeled '新建 Key'. The main content is a table with the following data:

名称	Key ID	Key	新建时间	操作
2	wsak_b7693e3b48274a8aaf8ef4284c579553	*****8upv	2022/01/24 18:11:59	🔍 🗑
1	wsak_afe7735d0a104c79affcd92ead071fc5	*****UEc8	2022/01/24 18:11:55	🔍 🗑

成员管理

在观测云中“拥有者”拥有当前工作空间的最高操作权限，可以在当前工作空间的付费计划与清单进行版本升级，账号充值、转移等操作，可对工作空间内的所有成员进行统一管理，可转移角色给到其他工作空间成员。“成员管理”显示当前工作空间的所有成员信息，可通过邮箱邀请成员加入工作空间，支持编辑和删除空间成员，支持设置成员权限，分别为“管理员”、“标准成员”和“只读成员”。

- 管理员：可以对工作空间的基本设置、成员管理、通知对象管理进行操作；可以对数据的采集、禁用/启用、编辑、删除等进行管理
- 标准成员：具备查看、编辑、存储、分享工作空间数据的权限
- 只读成员：仅能够对工作空间的数据进行查看，无权对数据进行修改、编辑、储存等其他操作

注意：若当前工作空间升级到商业版，升级到“管理员”需要拥有者在费用中心验证通过才能生效。

邮箱	姓名	角色	操作
ch...	GCY	拥有者	
ca...	CXY	管理员	
jd...		标准成员	
lhr...		只读成员	

SSO 管理

观测云支持基于 SAML 协议的 SSO 管理,支持企业在本地 IdP(身份提供商)中管理员工信息,无需进行观测云和企业 IdP 之间的用户同步,企业员工即可通过指定的角色登录访问观测云。

身份提供商	访问角色	备注	操作
okta	标准成员	-	

新建 SSO

在观测云工作空间「管理」-「SSO 管理」-「新建身份提供商」,即可为员工设置 SSO 单点登录。

- 身份提供商: 用来标识 SSO 登录验证的身份提供商信息。
- 元数据文档: IdP(身份提供商)提供的 XML 文档。
- 用户白名单: 邮箱列表,用于校验用户提供的公司邮箱是否能够登录到观测云的工作空间。
- 访问角色: 观测云的系统权限角色,目前此处只支持[只读成员]、[标准成员]。
- 登录地址: 基于用户上传的元数据文档生成的观测云 SSO 的登录地址,一个登录地址有且只能访问一个工作空间。
- 备注: 用户针对身份提供商可以自定义添加的描述信息。

SSO > 新建身份提供商

类型 SAML

身份提供商

元数据文档

用户白名单

共 0 个 (CSV 示例: 白名单.csv)

访问角色

备注

通知对象管理

观测云支持添加钉钉机器人、企业微信机器人、Webhook 自定义和邮件组等通知对象进行告警通知。在工作空间进入「管理」 - 「通知对象管理」，点击「新建通知对象」，选择「钉钉机器人」/「企业微信机器人」/「飞书机器人」/「Webhook 自定义」 / 「邮件组」 / 「短信」，在对应页面输入所需信息，点击「确认」即可。

基本设置 API Key 管理 成员管理 SSO管理 通知对象管理 内置视图 分享管理

名称	类型	操作
Function	Webhook自定义	<input type="button" value="编辑"/> <input type="button" value="删除"/>
DQL	企业微信机器人	<input type="button" value="编辑"/> <input type="button" value="删除"/>
DataKit	邮件组	<input type="button" value="编辑"/> <input type="button" value="删除"/>
DataFlux	钉钉机器人	<input type="button" value="编辑"/> <input type="button" value="删除"/>

内置视图

内置视图显示当前工作空间的所有视图模版，包括系统视图和用户视图两种类型，支持在场景中应用内置视图，支持在基础设施手动绑定内置视图。



分享管理

观测云支持当前空间管理员和标准成员进行图表分享和管理。图表分享可用于在观测云以外的平台代码中插入图表进行可视化数据展示和分析。

1) 图表分享

在「场景」中编辑仪表板即可分享图表，完成图表分享后，通过「管理」-「分享管理」-「图表分享」可以查看当前空间内的图表分享列表，并进行查看图表，查看嵌入代码和取消分享。

图表名称	来源	时间范围	分享人	操作
容器 CPU 使用率	容器	最近1天	pe-...	查看 分享 取消
容器 CPU 使用率	容器	最近15分钟	pe-...	查看 分享 取消
CPU 平均每核负载	基础设施Windows主机监控视图	最近15分钟	pe-...	查看 分享 取消
内存使用率	基础设施Windows主机监控视图	最近15分钟	pe-...	查看 分享 取消

2) 快照分享

在场景、日志等查看器保存快照后，可在「快照」进行分享，分享快照后，通过「管理」-「分享管理」-「快照分享」可以查看快照分享列表，包括快照名称、分享方式、分享人、有效期、时间范围、查看快照和查看分享链接。

快照名称	分享方式	分享人	有效期	时间范围	操作
datakit-1.14-15:55	公开分享	chi...om	2022-03-18 19:28:35	2022/01/14 15:42:13-2022/01/14 15:57:13	

付费计划与账单

在「付费计划与账单」页面，可查看当前工作空间的使用版本和各个项目的使用情况。若你当前使用的是免费版，可以进行版本升级，点击「升级」，进入版本选择，观测云分成免费版、商业版、独占合作版。免费版用户支持在线升级到商业版，升级以后不可回退。升级商业版以后可以查看账单列表，工作空间拥有者角色可以进入费用中心、更换绑定账号、充值等操作。

商业版

[进入费用中心](#)
[更换绑定账号](#)
[充值](#)

账户名	现金账户余额	代金券余额
*****	*****	*****

使用统计 当前 昨日

DataKit 数量: 0	日志类数据数量: 0	Trace数量: 0
时间线数量: 0	备份日志数据数量: 0	PV 数量: 0
任务调度次数: 2,880	API 拨测次数: 0	短信通知次数: 0

账单列表 2022-03

累计消费金额: ¥0 (DataKit: ¥0 时间线: ¥0 日志类数据: ¥0 备份日志数据: ¥0 应用Trace: ¥0 用户访问: ¥0 任务调度: ¥0 短信: ¥0 API 拨测: ¥0)

账期	账号	产品明细	出账模式	原价	应付金额	现金支付	代金券抵扣	扣费金额	欠费
暂无数据									

按量付费

观测云支持按需购买，按量付费的计费方式。按照 DataKit 数量、时间线数量、日志类数据数量、备份日志数据数量、任务调度次数、用户访问 PV 数量、应用性能 Trace 数量、API 拨测次数、短信发送次数等多个维度进行价格统计。

- **DataKit 数量:** 当前工作空间下，一天内有数据上报的 datakit 的数量。
- **时间线数量:** 当前工作空间，上报的指标数据中基于标签可以组合而成的所有组合数量。
- **日志类数据数量:** 当前空间下，日志类数据的统计数量，日志类数据数量包括日志、云拨测（用户自建节点产生的云拨测数据）、安全巡检和事件的数据数量总和，默认计费单位为“百万条”。

- 备份日志数据数量：当前空间下，备份日志数据的统计数量，默认计费单位为“百万条”。
- 应用性能 Trace 数量：当前空间下，统计应用性能监测 trace_id 的数量，默认计费单位为“百万个”。
- 用户访问 PV 数量：当前空间下，统计一天内所有页面浏览产生的 PV 数量，默认计费单位为“千个”。
- API 拨测次数：当前空间下，统计一天内所有的 API 拨测产生的任务调用次数，默认计费单位为“万次”。
- 任务调度次数：当前空间下，统计一天内所有的 Func 平台调用的次数，涉及到任务的调用即会进行次数统计，如异常检测的规则数量、生成指标的规则数量等，默认计费单位为“万次”。
- 短信发送次数：当前空间下，统计一天内所有发送出去的短信的次数，默认计费单位为“次”。

观测云计费项分成全量统计和增量统计：

- 时间线、备份日志数据这两个计费项按照全量计费（即当前工作空间下，统计数据保存策略范围内所有的数据 / 数量。）
- DataKit 、日志类数据、应用性能 Trace、用户访问 PV 、API 拨测、任务调度、短信按照增量计费（即当前工作空间下，统计一天内产生的数据 / 数量。）

计费价格

观测云计费价格分成两种计费模式：一种是基于数据统计的基础计费模式，另外一种是基于数据统计及数据存储策略的梯度计费模式。日志类数据、应用性能 Trace、用户访问 PV 这三个计费项采用梯度计费模式，其他计费项采用基础计费模式。

基础计费模式

观测云提供两种基础计费模式，可在费用中心切换选择。一种是统计“DataKit+时间线”数量的计费模式，另外一种仅是统计“时间线”数量的计费模式。其他

计费项备份日志数据数量、API 拨测次数、任务调度次数、短信发送次数为通用计费项。

梯度计费模式

观测云提供基于数据统计及数据存储策略的梯度计费模式，包括日志类数据、应用性能 Trace、用户访问 PV 这三个梯度计费项。