云监控

用户指南

为了无法计算的价值 | 阿里云

用户指南

Dashboard

Dashboard概览

Dashboard 概览

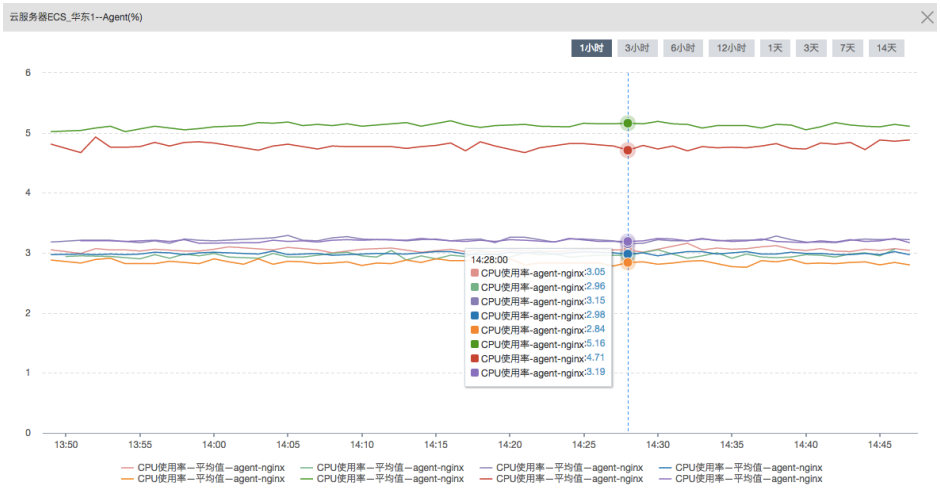
云监控推出 Dashboard 功能，旨在打造监控可视化一站式解决方案。既能满足您排查故障时查看监控细节，又能满足您总览大局时查看服务概貌。

应用场景

Dashboard 提供对云产品监控数据的自定义多维查询和展示，以下是几类比较常见的应用场景。

展示多个实例的监控数据走势

例如您的一个应用部署在多台 ECS 实例上，可以将部署了相同应用的多台 ECS 实例监控信息添加在同一张监控图表中，查看相关多台机器的监控数据变化趋势。 例如在一张图表中同时展示 ECS 多个实例各自的CPU使用率的时间序走势。



展示多个监控项的数据对比

例如在一张图表中展示 ECS 同一个实例的 CPU 使用率、内存使用率、磁盘使用率等多个指标。

展示机器的资源消耗排序

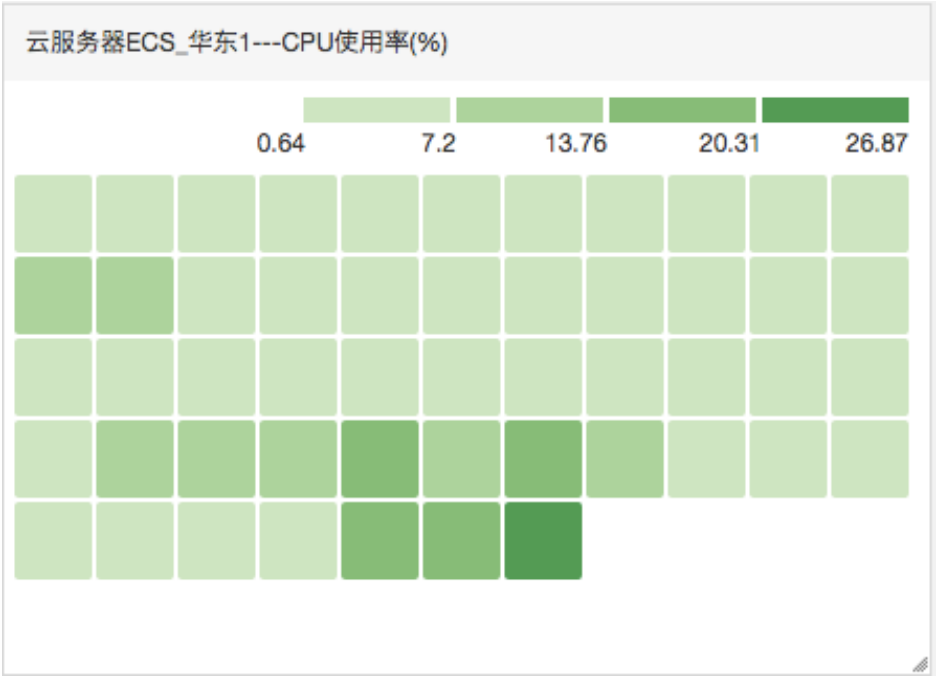
例如您有 20 台机器，通过表格展示可以查看 20 台机器的 CPU 使用率从大到小的排序。快速了解资源消耗情况，更合理的使用资源，减少不必要的花费。

云服务器ECS_华东1---CPU使用率(%)

时间	实例	平均值
2016-06-30 21:10:00	AY140612161618078becZ	26.91
2016-06-30 21:10:00	AY140612162025667fa4Z	25.9
2016-06-30 21:10:00	cmssiteprobehz121040130038	16.46
2016-06-30 21:10:00	AY140612161644758d2Z	15.5
2016-06-30 21:10:00	cmssiteprobehz121041117242	14.4
2016-06-30 21:10:00	cmssiteprobehz121041112148	13.68
2016-06-30 21:10:00	agent-proxy120027193019.hz	13.63
2016-06-30 21:10:00	cmssiteprobehz120026064126	12.91
2016-06-30 21:10:00	cmssiteprobehz120026216168.hz	12.56
2016-06-30 21:10:00	cmssiteprobehz121043105176.hz	12.23
2016-06-30 21:10:00	cmssiteprobehz121043107174	11.74

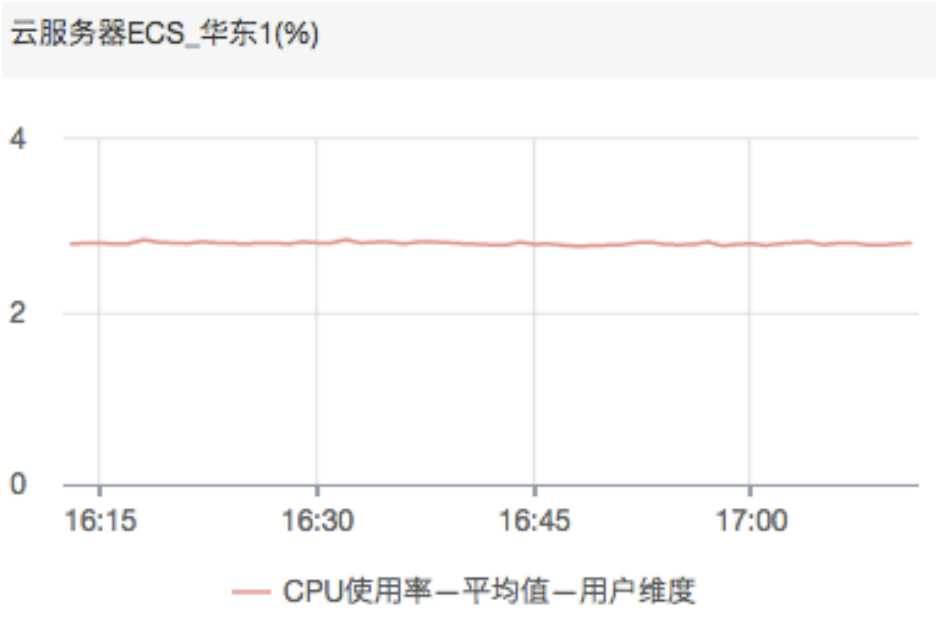
展示多个实例的监控数据实时分布

例如通过热力图，展示一组 ECS 实例的 CPU 使用率分布情况，知晓每台机器的 CPU 使用率和其他机器相比，处于什么水平。点击色块，可以查看该机器一段时间内的监控数据走势。



展示多个实例某一监控项的聚合数据

例如在一张图表中查看 ECS 多个实例的CPU使用率的平均聚合值，从而了解整体的 CPU 使用率水位，判断是否各个实例资源使用不均。



全景盯屏展示

Dashboard 支持全屏展示和自动刷新，可以将您的各类产品指标添加到监控大盘后在运维大屏上全屏展示。

管理监控大盘

用户可以创建监控大盘、修改监控大盘、删除监控大盘、查看监控大盘内的图表。

查看监控大盘

应用场景

云监控的Dashboard功能提供用户自定义查看监控数据的功能。用户可以在一张监控大盘中跨产品、跨实例查看监控数据，将相同业务的不同产品实例集中展现。

注意事项

- 云监控会为用户初始化ECS监控大盘，展示ECS部分监控数据。
- 支持对1小时、3小时、6小时的数据进行自动刷新，更长时间跨度的数据不支持自动刷新。

监控大盘参数说明

选择时间范围：点击监控大盘页面上方的时间选择按钮，可以快速选择大盘中图表展示的监控数据时间范围。时间选择的作用范围是监控大盘的全部图表。

自动刷新：开启“自动刷新”按钮后，当您选择查询“1小时”、“3小时”、“6小时”的查询时间

跨度时，可开启自动刷新功能，每分钟刷新一次。

- 监控项的单位展示在图表名称的括号内。
- 鼠标跟随显示所有图表相同时间的监控值。

操作步骤

1. 登录云监控控制台。
2. 点击左侧菜单的“Dashboard”选项，进入Dashboard页面。
3. 默认展示云监控初始化的“ECS全局监控大盘”。

点击监控大盘名称，拉下列表选择其他监控大盘。

点击页面右上角的“全屏”，可全屏查看监控大屏。

创建监控大盘

应用场景

当您的业务比较复杂，默认的ECS监控大盘无法满足您的监控可视化需求时，您可以创建新的监控大盘，自定义需要展示的图表。

注意事项

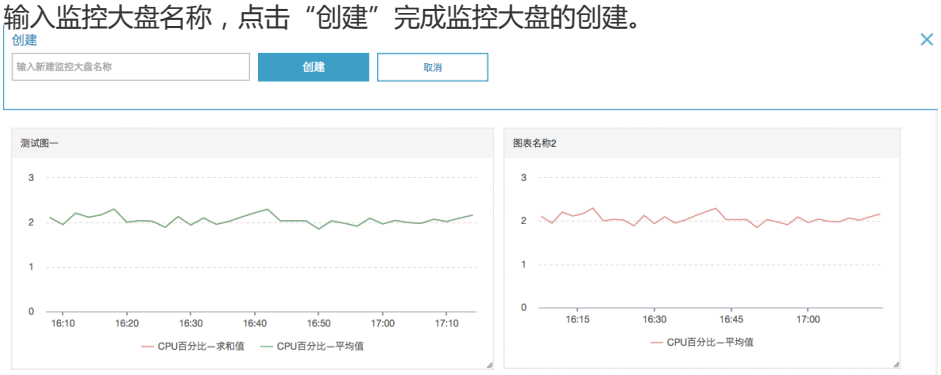
每张监控大盘最多创建20个图表。

操作步骤

1. 登录云监控控制台。
2. 点击左侧菜单的“Dashboard”选项，进入Dashboard页面。

点击页面右上角的“创建监控大盘”。

输入监控大盘名称，点击“创建”完成监控大盘的创建。



页面自动跳转到新创建的监控大盘页面，您就可以开始自由添加各种监控图表了。

切换监控大盘

应用场景

当您创建了多个监控大盘时，可通过切换监控大盘，查看不同大盘的监控图表。

操作步骤

1. 登录云监控控制台。
2. 点击左侧菜单的“Dashboard”选项，进入Dashboard页面。
3. 点击页面左上角的监控大盘名称，下拉显示您创建的所有监控大盘，通过选择不同的监控大盘名称，切换大盘展示

删除监控大盘

应用场景

当您的业务发生变更，不再需要某个监控大盘时，可以删除这个监控大盘。

注意事项

删除监控大盘时，会关联删除页面上设置的所有监控图表。

操作步骤

1. 登录云监控控制台。
2. 点击左侧菜单的“Dashboard”选项，进入Dashboard页面。
3. 点击页面右上角的“删除当前大盘”按钮，删除监控大盘。

修改监控大盘

应用场景

当您的监控大盘展示内容有变化，需要修改监控大盘名称时，可以通过此功能进行修改。

操作步骤

1. 登录云监控控制台。
2. 点击左侧菜单的“Dashboard”选项，进入Dashboard页面。
3. 鼠标悬浮在监控大盘名称上，右侧会出现“修改名称”四个字，点击“修改名称”进入编辑状态，即可修改大盘名称。

添加图表

应用场景

云监控为您初始化了用户维度的 ECS 监控大盘，如果您需要查看 其他数据，可以通过**添加图表**来设置。

注意事项

云监控会为您默认初始化 ECS 监控大盘。展示 CPU 使用率、网络流入速率、网络流出速率、系统磁盘 BPS、系统磁盘 IOPS、网络入流量、网络出流量7张监控图表。

折线图展示限制：1 个折线图最多可以显示 10 条线。

面积图展示限制：1 个面积图最多可以展示 10 块面积。

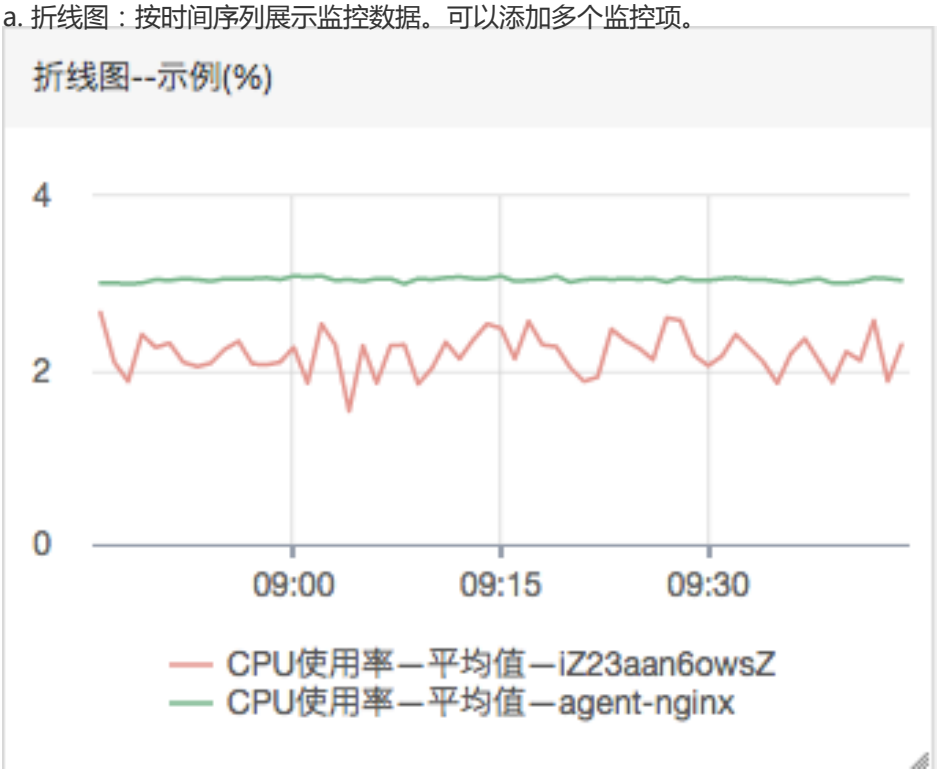
表格数据限制：最多展示 1000 条数据的排序结果。

热力图展示限制：1 个热力图最多展示 1000 个色块。

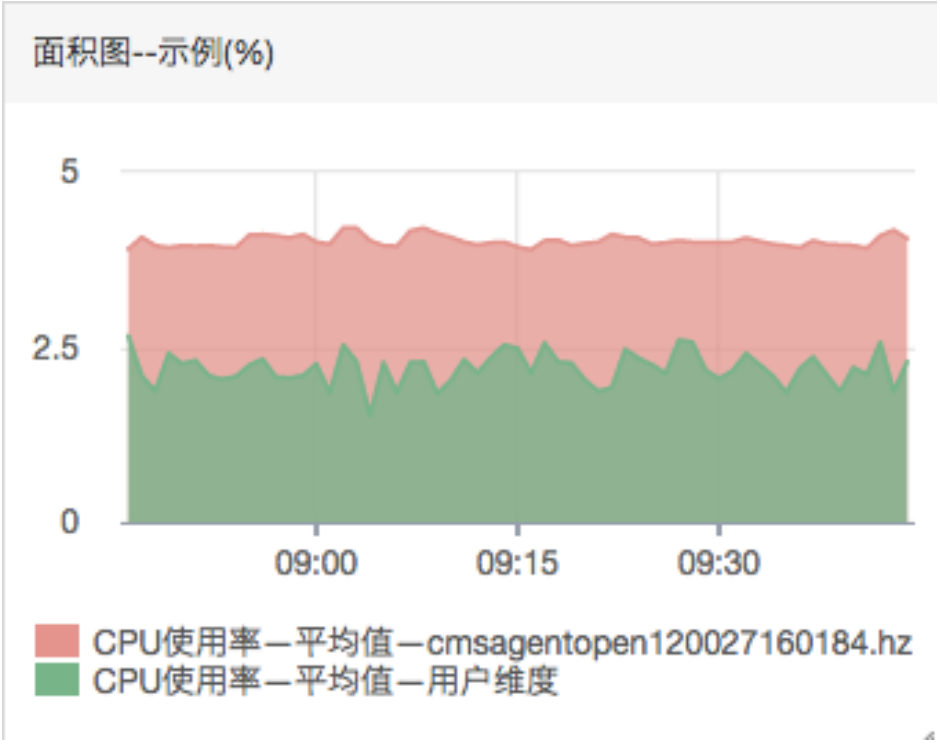
参数说明

选择图表类型：支持折线图、面积图、TopN表格、热力图、饼图。

a. 折线图：按时间序列展示监控数据。可以添加多个监控项。



b. 面积图：按时间序列显示监控数据，可以添加多个监控项。

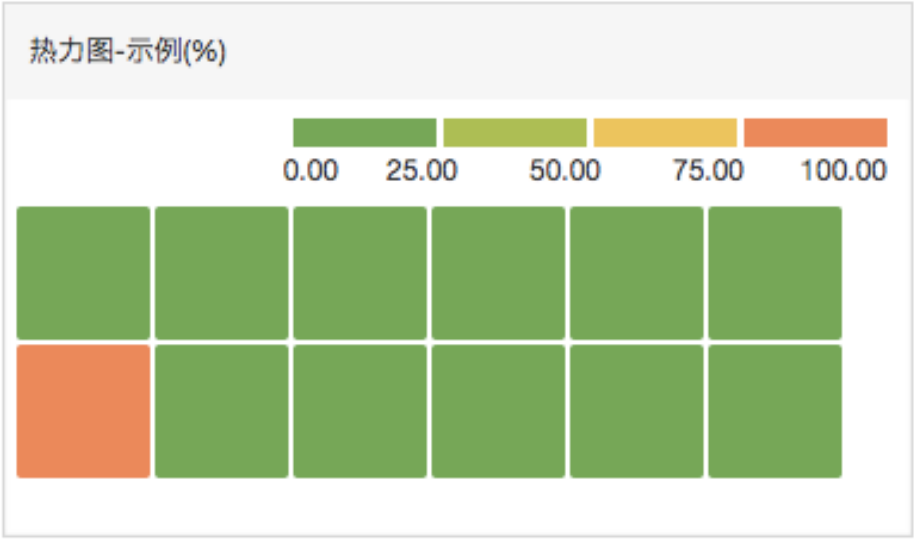


c. TopN表格：实时显示监控项数据值由大到小的排序。最多显示正序的1000条或倒序的1000条数据。例如 ECS 分组中所有机器 CPU 使用率从大到小的排序。只能添加一个监控项。

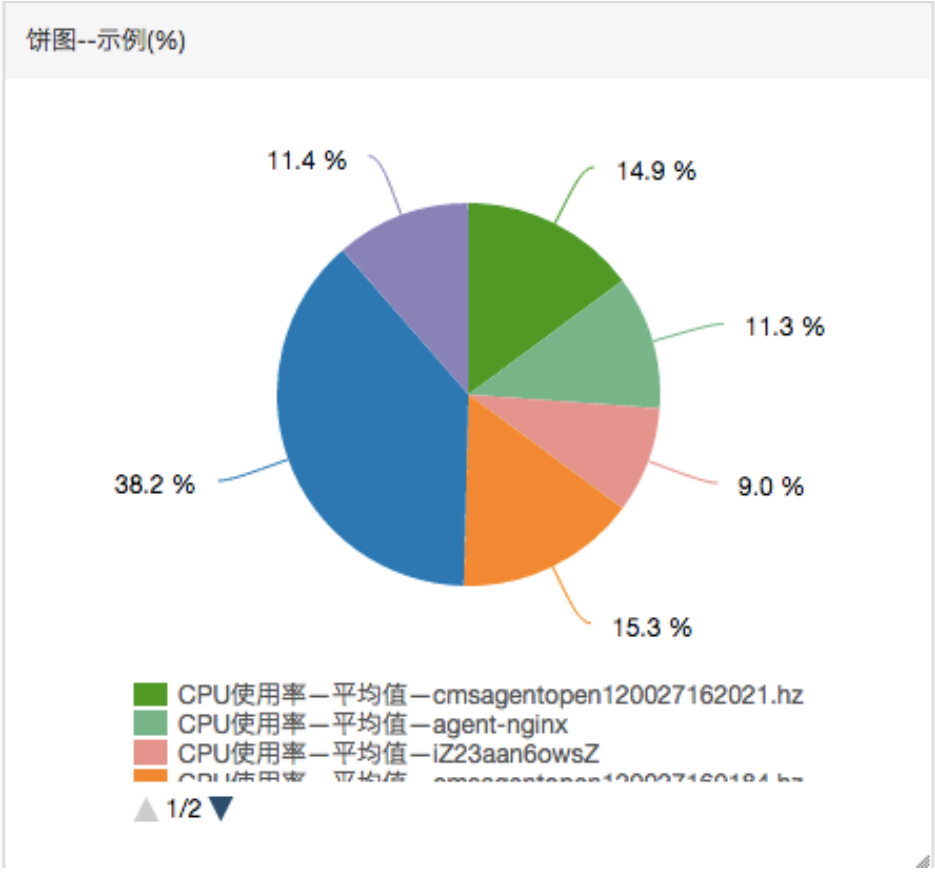
表格--示例(%)

时间	实例	平均值
2016-07-05 09:47:00	.hz	10.31
2016-07-05 09:47:00	.hz	4.47
2016-07-05 09:47:00	.hz	4.44
2016-07-05 09:47:00	.hz	4.15
2016-07-05 09:47:00	.hz	4.14
2016-07-05 09:47:00	.hz	4.1

d. 热力图：显示监控项的实时数据。用于展示多个实例指定监控项的实时监控数据分布与对比。例如展示多个实例 CPU 使用率的水位分布情况。只能添加一个监控项。



e. 饼图：显示监控项的实时数据。常用于数据的对比。只能添加一个监控项。



云产品监控：阿里云各个云产品的监控。

- 日志监控：用户通过日志监控自行添加的监控。
- 监控项：具体需要查看的监控指标名称，例如CPU使用率、内存使用率等。
- 统计方法：监控项对应的常见统计方法有最大值、最小值、平均值。既统计周期内监控数据的聚合方式。

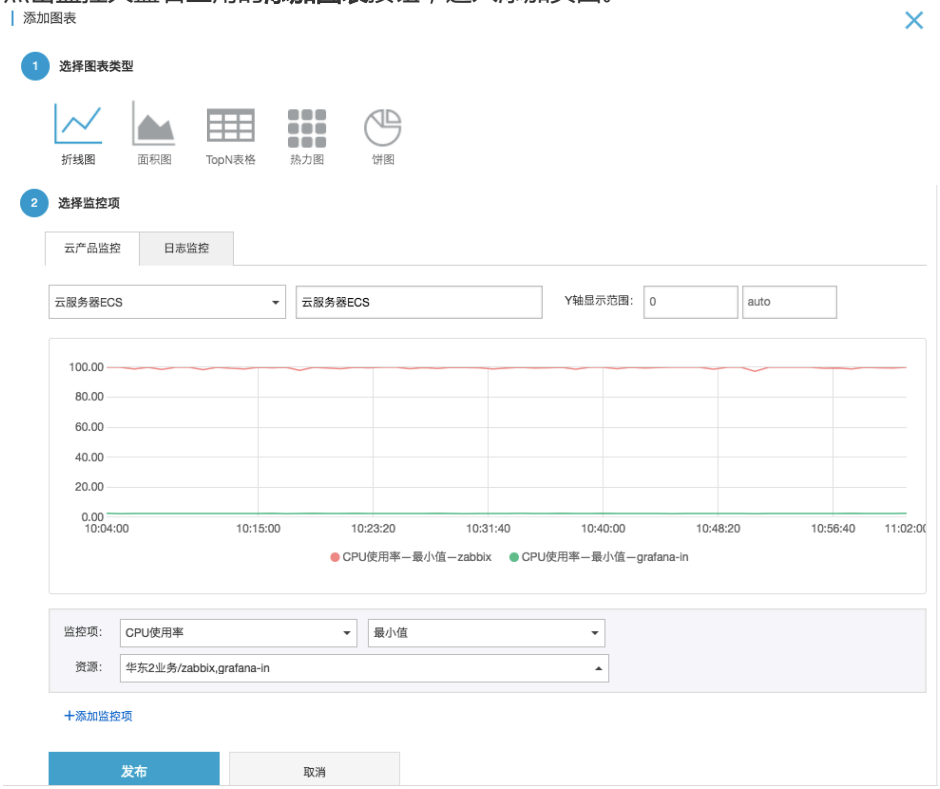
- 资源：通过应用分组或实例筛选需要查看哪些资源的监控数据。

操作步骤

登录云监控控制台。

点击左侧菜单的**Dashboard**选项，进入Dashboard页面。

点击监控大盘右上角的**添加图表**按钮，进入添加页面。



4. 选择图表的展现类型。
5. 选择需要查看的云产品并为图表命名。

选择需要查看的监控指标和统计方式。

a. 选择需要查看的监控项。

b. 选择监控数据的聚合方式，常见聚合方式为最大值、最小值、平均值。

如果还需增加监控项，请点击**添加监控项**，重复第6步。

点击**发布**，图表即可在监控大盘中看到。

拖拽图表右侧、下侧、右下侧，调整图表的高度和宽度（可选）。

添加日志监控

应用场景

当您配置好日志监控指标后，可以使用**添加日志监控**功能，在 Dashboard 中制作业务监控大盘

注意事项

折线图展示限制：1 个折线图最多可以显示 10 条线。

面积图展示限制：1 个面积图最多可以展示 10 块面积。

TopN表格限制：最多展示 Top1000 的结果。

热力图展示限制：1 个热力图最多展示 1000 个色块。

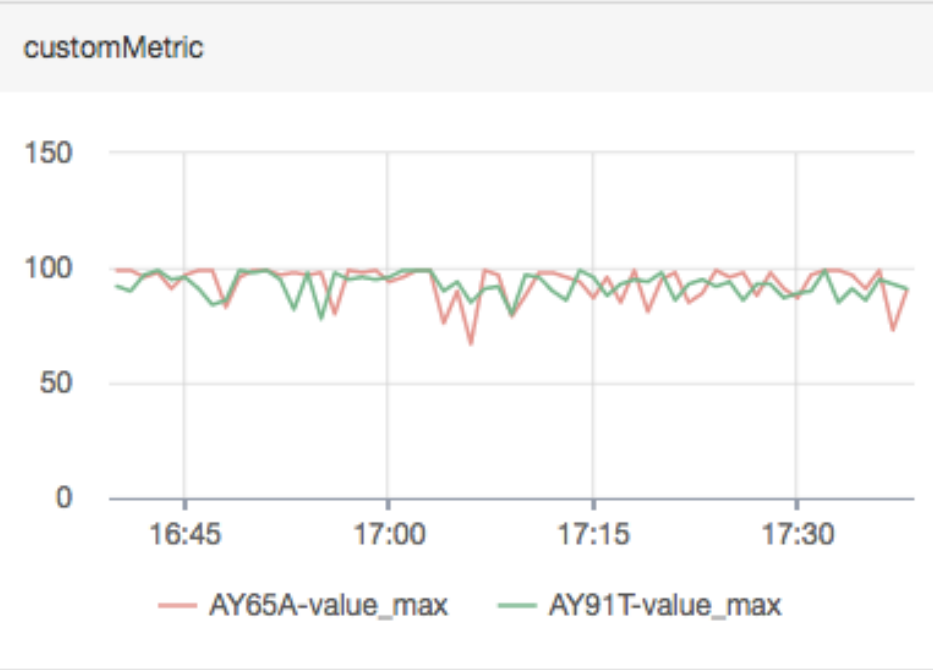
参数说明

图表名称：监控图表的名称，默认显示监控项名称。

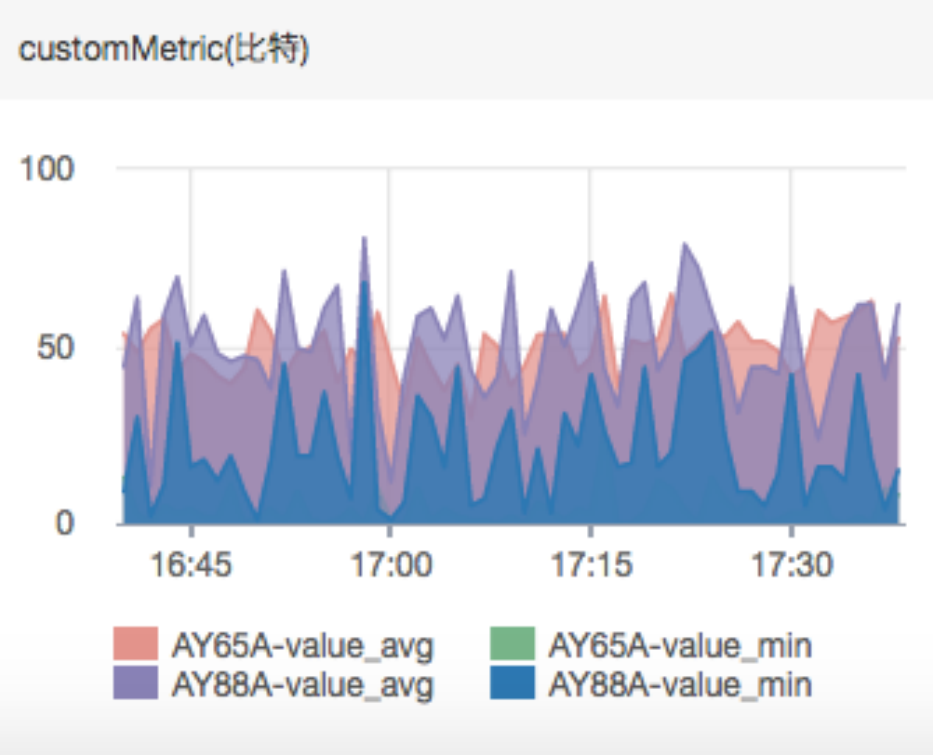
监控项：在日志监控中定义的监控项。

Filter：相当于 SQL 中的 where 条件，在日志监控中定义了Group By字段的监控项会显示此选项。

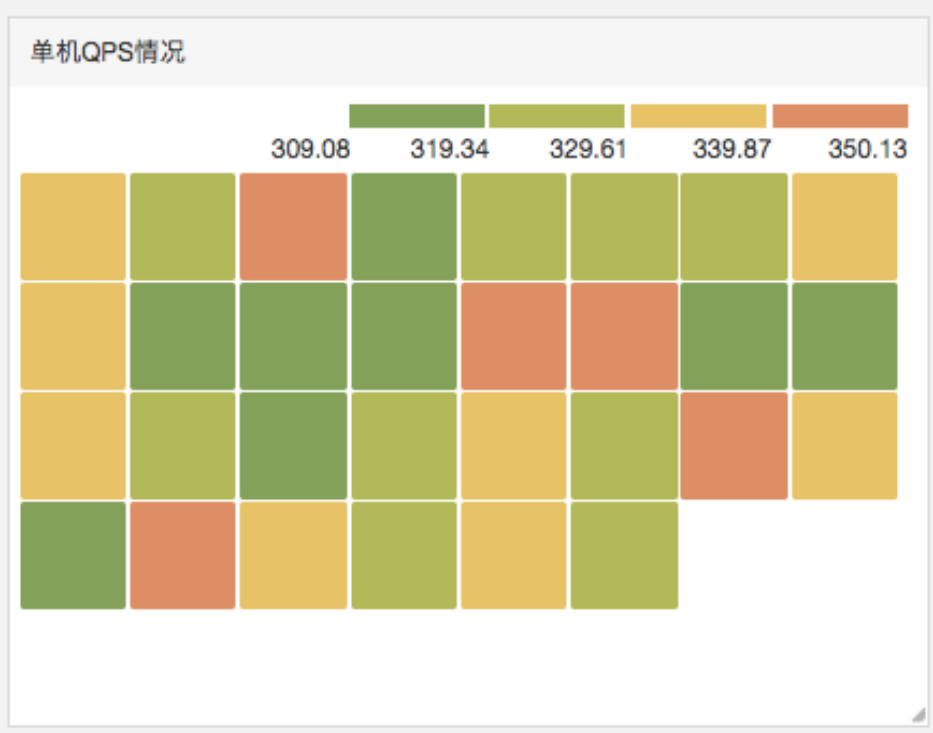
a. 折线图：按时间序列展示监控数据。



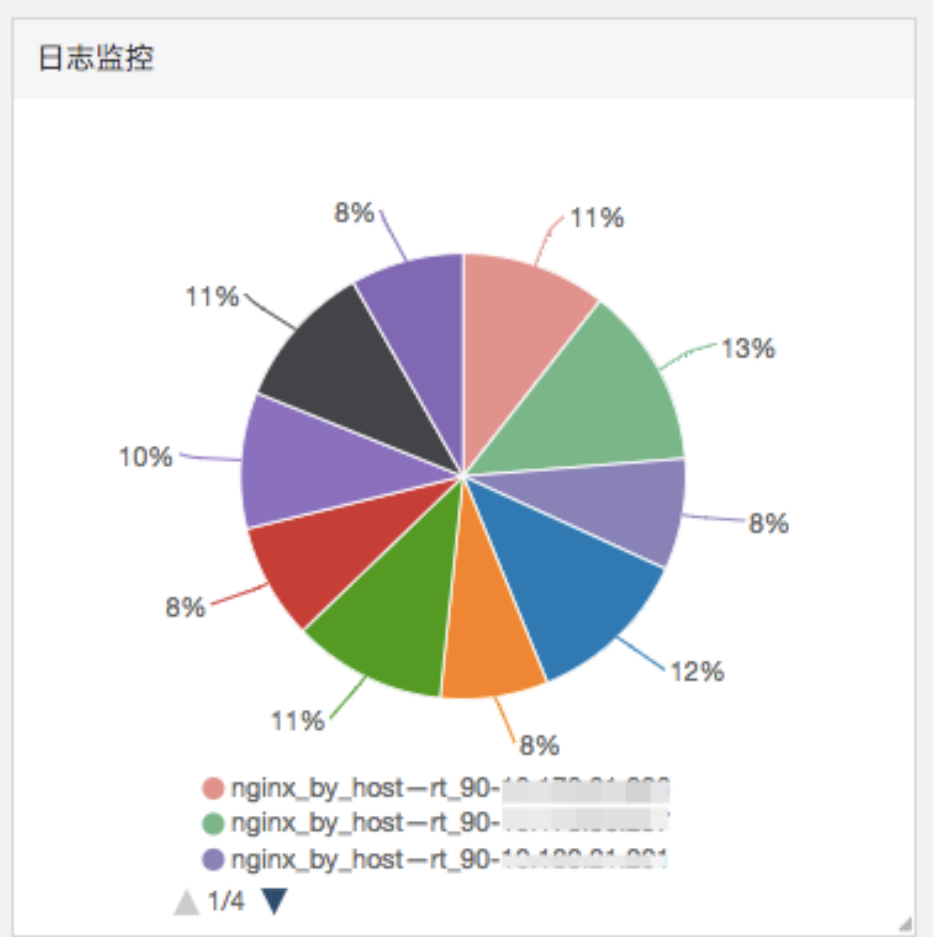
b. 面积图：按时间序列显示监控数据。



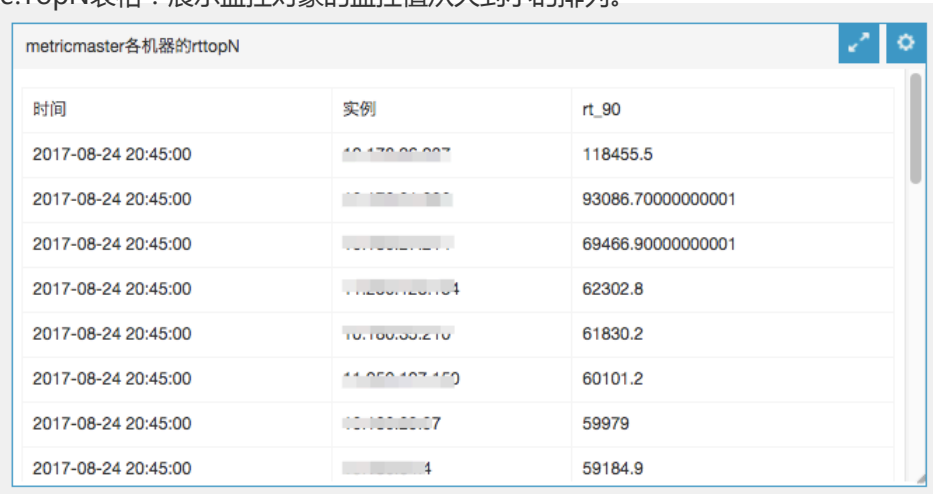
c. 热力图：展示指标的最新数据。常用于展示多个监控对象的监控值分布与对比。



d. 饼图：展示指标的实时数据。常用于数据的对比。



e.TopN表格：展示监控对象的监控值从大到小的排列。

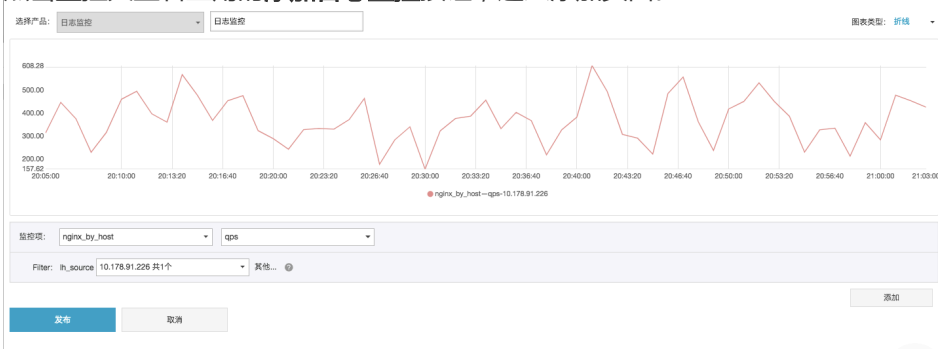


操作步骤

登录云监控控制台。

点击左侧菜单的**Dashboard**选项，进入Dashboard页面。

点击监控大盘右上角的**添加日志监控**按钮，进入添加页面。



4. 定义图表名称、图表类型。
5. 选择需要查看的监控项和过滤条件。
6. 点击发布，图表即可在监控大盘中看到。
7. 拖拽图表右侧、下侧、右下侧，调整图表的高度和宽度（可选）。

应用分组

应用分组概览

应用分组概览

应用分组提供跨云产品、跨地域的云产品资源分组管理功能，支持用户从业务角度集中管理业务线涉及到的服务器、数据库、负载均衡、存储等资源。从而按业务线来管理报警规则、查看监控数据，可以迅速提升运维效率。

应用场景

购买了多种云产品的阿里云深度用户，通过应用分组功能将同一业务相关的服务器、数据库、对象存储、缓存等资源添加到同一应用分组中。在分组维度管理报警规则，查看监控数据，可以极大的降低管理复杂度，提高云监控使用效率。

注意事项

- 一个云账号最多创建100个应用分组。
- 一个应用分组最多添加1000个资源实例。

创建应用分组

创建应用分组

应用场景

购买了多种云产品的阿里云深度用户，通过应用分组功能将同一业务相关的服务器、数据库、对象存储、缓存等资源添加到同一应用分组中。在分组维度管理报警规则，查看监控数据，可以极大的降低管理复杂度，提高运维效率。

注意事项

每个分组最多添加1000个资源实例。

创建分组时如果勾选了**初始化报警规则**，云监控会根据您组内资源的类型，检查5分钟内平均值是否超过阈值，通知方式为邮件和旺旺，通知对象为创建应用分组时选择的报警联系人组。

操作步骤

登录云监控**控制台**。

选择页面左侧菜单的**应用分组**，进入**应用分组**页面。

单击页面右上角的**创建应用分组**，进入编辑页面。

填写分组名称。

选择需要添加的产品。

默认初始化 ECS 和 RDS 产品，可以通过**添加产品**、**删除本产品**按钮选择该分组的产品范围。

在产品对应的实例列表中选择需要加入分组的实例。

选择接收报警通知的通知对象。

选择是否为分组初始化报警规则。

单击**确认**按钮，保存应用分组设置。

管理报警规则

您可以在应用分组内对报警规则进行创建、查看、修改、删除、启用和禁用6种操作。

注意事项

- 在应用分组内查看报警规则时，只能查询到作用在该分组上的报警规则。不支持查询作用在实例或全

部资源上的报警规则。

新建报警规则

登录云监控控制台。

选择页面左侧菜单的**应用分组**，进入应用分组页面。

选择需要创建报警规则的分组，单击分组名称或者**管理**，进入分组详情页面。

单击页面右上方的**新建报警规则**。

填写报警规则页面内容，完成创建。

删除报警规则

登录云监控控制台。

选择页面左侧菜单的**应用分组**，进入应用分组页面。

选择需要删除报警规则的分组，单击分组名称或者**管理**，进入分组详情页面。

单击页面上方的**报警规则**，进入分组的报警规则页面。

单击报警规则**操作**选项中对应的**删除**，删除单条报警规则。或者勾选多条报警规则后，单击列表下方的**删除**按钮，删除多条报警规则。

修改报警规则

登录云监控控制台。

选择页面左侧菜单的**应用分组**，进入应用分组页面。

选择需要修改报警规则的分组，单击分组名称或者**管理**，进入分组详情页面。

单击页面上方的**报警规则**，进入分组的报警规则页面。

单击报警规则**操作**选择项中对应的**修改**，修改单条报警规则。

禁用或启用分组的报警规则

当需要主动停止服务进行应用维护和升级时，可以禁用分组内的全部报警规则，避免因为人为主动变更而收到大量无用的报警通知。完成变更操作后可以再重新启用分组中的报警规则。

禁用分组中全部报警规则

登录云监控**控制台**。

选择页面左侧菜单的**应用分组**，进入**应用分组**页面。

选择相应的分组名称，在**操作**中单击**更多**按钮。

4. 选择**更多**中的**禁用所有报警规则**，禁用分组中的全部报警规则。

启用分组中全部报警规则

登录云监控**控制台**。

选择页面左侧菜单的**应用分组**，进入**应用分组**页面。

选择相应的分组名称，在**操作**单击**更多**按钮。

选择**更多**中的**启用所有报警规则**，启用分组中的全部报警规则。

禁用分组中部分报警规则

登录云监控**控制台**。

选择页面左侧菜单的**应用分组**，进入**应用分组**页面。

选择相应的报警规则分组，单击分组名称或者**管理**，进入分组详情页面。

单击页面上方的**报警规则**，进入分组的报警规则页面。

单击报警规则**操作**选择项中对应的**禁用**，禁用单条报警规则。或者勾选多条报警规则后，单击列表下

方的**禁用**按钮，禁用多条报警规则。

启用分组中部分报警规则

登录云监控**控制台**。

选择页面左侧菜单的**应用分组**，进入**应用分组**页面。

选择需要创建报警规则的分组，单击分组名称或者**管理**，进入分组详情页面。

单击页面上方的**报警规则**，进入分组的报警规则页面。

单击报警规则**操作**选择项中对应的**启用**，启用单条报警规则。或者勾选多条报警规则后，单击列表下方的**启用**按钮，启用多条报警规则。

查看应用分组

概览

分组的详情页包含故障列表、报警历史、报警规则、组内资源、事件和分组内资源的监控数据六类信息。

应用分组列表

应用分组列表展示用户在云监控拥有的全部应用分组及各个分组的资源和健康度概况。

列表参数说明

- 分组名称：应用分组的名称。
- 健康状况：组内资源是否正在报警。组内所有资源均未发生报警时，为健康状态。只要有资源正在报警，则为不健康状态。
- 服务器总数：组内所有服务器数量总和，包括ECS 和其他非ECS的服务器。
- 资源类型总数：组内资源类型的数量，例如组内有云服务器 ECS，云数据库 RDS，负载均衡 三种资源类型，则资源类型总数为3。
- 不健康实例数：组内所有正在报警的实例数总和。例如您有2台ECS 、1台 RDS正在报警，则不健康实例数为3。

- 创建时间：应用分组的创建时间。
- 操作：目前支持管理、启用所有报警规则、禁用所有报警规则、删除组四种操作。

故障列表

故障列表显示您的分组下当前正在报警的所有资源。方便您快速总览全部不健康实例，及时处理故障。

注意事项

- 同一个资源的多个监控项同时报警时，故障列表里会显示多次显示该资源。列表中的每一行代表资源的一个正在报警的监控项。
- 禁用正在发生报警的规则后，规则对应的资源和监控项将不再出现在故障列表中。

列表参数说明

- 故障资源：正在发生报警的资源。
- 开始时间：首次发生报警的时间。
- 状态：提示用户相关资源正在报警。
- 持续时间：故障资源处于报警状态的总时长。
- 规则名称：故障资源对应的报警规则名称。
- 操作：点击“展开”可查询故障实例正在报警的监控项最近6小时的走势和报警阈值的对比。

报警历史

展示应用分组下所有报警规则的报警历史。

注意事项

- 最多支持连续查询3天的历史信息。如果查询起止时间间隔超过3天，会提示您重新选择时间。

列表参数说明

- 故障资源：正在发生报警的资源。
- 持续时间：故障资源处于报警状态的总时长。
- 发生时间：该条报警通知发生的时间。
- 规则名称：故障资源所属报警规则的名称。
- 通知方式：报警通知的发送渠道。包括短信、邮件、旺旺三种。
- 产品类型：故障资源属于哪种产品。
- 状态：报警规则的状态，包括报警、恢复、通道沉默三种状态。
- 通知对象：报警通知发送的联系人组。

报警规则

展示该应用分组下的全部报警规则。并且可以在报警规则列表中对指定规则进行禁用、启用、修改等操作。

注意事项

- 只展示该应用分组的报警规则。不展示创建报警规则时“资源范围”选择“全部资源”或“实例”的报警规则。

列表参数说明

规则名称：新建报警规则时，用户自定义的报警规则名称。

状态：描述报警规则关联的资源是否正在报警。

a. 正常状态：规则关联的资源全部正常。

b. 报警状态：规则关联的实例至少有一个实例正在报警。

c. 数据不足：规则关联的实例至少有一个实例数据不足且没有实例正在报警。

启用：报警规则是否被启用。

- 产品名称：组内资源归属的产品名称。
- 规则描述：简要描述报警规则的设置。

操作：包括“修改”、“禁用”、“启用”、“删除”、“报警历史”。

a.修改：修改报警规则。

b. 禁用：禁用报警规则。禁用后报警规则不再检查监控数据是否超过阈值。

c. 启用：启用报警规则。将禁用的报警规则重新启用后，报警规则将重新开始根据规则设置检查监控数据是否需要报警。

d. 删除：删除报警规则。

e. 报警历史：指定报警规则对应的报警历史。

组内资源

展示应用分组内的全部资源和资源的健康度。

列表参数说明

- 实例名称：资源的实例名称或者实例ID。
- 健康状况：资源对应的报警规则均未发生报警时，为健康状态。只要报警规则正在报警，为不健康状态。

事件

目前提供报警历史和增加、删除、修改报警规则的操作事件信息，方便用户追溯对报警规则的操作。

注意事项

- 事件信息可查询最近90天内的数据。

列表参数说明

- 发生时间：事件发生的时间。
- 事件名称：包括报警发生、报警恢复、创建报警、修改报警、删除报警。
- 事件类型：分为系统事件和报警事件。系统事件包括创建报警规则、删除报警规则、修改报警规则。告警事件包括报警发生和报警恢复。
- 事件详情：事件对应的详细信息。

监控图表

应用分组详情页下方展示分组内资源的监控详情。云监控会默认为用户初始化常用监控数据，如果需要展示更多监控数据或者改变图表的展现形式，可以对图表进行修改，自定义监控数据和图表展示类型。

注意事项

- 云服务器ECS的 操作系统监控指标需要安装云监控插件才能获取。

初始化的监控数据

应用分组为用户初始化以下数据，如果您想查看更多监控数据，可以点击“添加监控图表”添加更多监控指标。

产品类别	监控项	展现形式	备注
云服务器 ECS	CPU使用率、公网流出带宽	折线图	展示分组下所有服务器的聚合数据
云数据库 RDS 版	CPU使用率、磁盘使用率、IOPS使用率、连接数使用率	折线图	展示单个数据库实例的数据
负载均衡	流出带宽、流入带宽	折线图	展示单个负载均衡实例

			的数据
对象存储 OSS	存储大小、Get类请求数、Put类请求数	折线图	展示单个Bucket的数据
CDN	下行带宽、命中率	折线图	展示单个域名的数据
弹性公网 IP	公网流出带宽	折线图	展示单个实例的数据
云数据库 Redis 版	内存使用率、连接数使用率、QPS使用率	折线图	展示单个实例的数据
云数据库 MongodbDB 版	CPU使用率、内存使用率、IOPS使用率、连接数使用率	折线图	展示单个实例的数据

修改应用分组

修改应用分组

应用场景

当您的应用根据业务扩容、缩容或改进技术架构使用更多的云产品时，会涉及到对应用分组中资源的修改。

当您应用的运维、开发人员变动时，会涉及到修改应用组发送报警的通知对象，这是会涉及到修改应用组的通知对象。

注意事项

将资源从该分组移除后，之前设置在分组维度上的报警规则，将不再适用于被移除的实例。

新加入分组的实例，将自动关联您之前设置在分组维度上的报警规则。无需再为该实例单独创建报警规则。

操作步骤

登录云监控控制台。

选择页面左侧菜单的**应用分组**，进入应用分组页面。

在分组列表中选择需要编辑的应用分组，进入分组详情页面。

单击页面右上方的**修改组**按钮。

在编辑页面进行分组内容的修改。

单击**确认**按钮保存修改。

复制应用分组

应用场景

您可以通过复制组的功能，快速创建具有相同报警规则、监控图表的分组。简化配置分组的过程。使您不用对不同组重复配置相同的报警规则和监控图表。

操作步骤

登录云监控控制台。

选择页面左侧菜单的**应用分组**，进入**应用分组**的列表页面。

在应用分组列表页面选择一个需要复制的组，单击**操作**中**更多**，选择**复制组**。

在弹出的页面中对新组添加实例和通知对象，即可复制一个具有相同报警规则和监控图表的分组。

主机监控

主机监控概览

云监控主机监控服务通过在服务器上安装插件，为用户提供服务器的系统监控服务。目前支持Linux操作系统和Windows操作系统。

应用场景

无论您的服务器是阿里云服务器 ECS，还是其他云厂商的服务器或物理机，都可以使用主机监控服务。主机监控服务采集丰富的操作系统层面监控指标，您可以使用主机监控服务进行服务器资源使用情况的查询和排查故障时的监控数据查询。

混合云监控解决方案

云监控通过插件采集用户服务器监控数据，该插件支持安装在非ECS服务器上，解决您云上、云下双重环境的基础监控问题。

企业级用户的监控解决方案

主机监控提供应用分组功能，支持将阿里云不同地域的服务器分配在同一分组中，真正从业务角度管理服务器。同时提供分组维度的报警功能管理能力，一次规则设置可以作用全组，极大提升您的监控运维效率和管理体验。

注意事项

支持Linux操作系统和Windows操作系统，不支持UNIX操作系统。

插件对服务器的消耗：安装包大小75M，安装后200M，内存消耗64M，CPU消耗1%以下。

安装插件需要root权限。

TCP状态统计, 类似于Linux下 netstat -anp 命令,当TCP连接过多时,会消耗比较多的CPU时间,所以默认关闭。

a. 对于Linux操作系统，您可以将cloudmonitor/config/conf.properties配置文件的netstat.tcp.disable改为false来开启采集。修改配置后请重启插件。

b. 对于Windows操作系统，您可以在C:\”Program Files”\Alibaba\cloudmonitor\config的配置文件中，将netstat.tcp.disable改为false来开启采集。修改配置后请重启插件。

监控能力

云监控会提供CPU、内存、磁盘、网络等三十余种监控项，满足服务器的基本监控运运维需求。查看支持的全部监控指标。

报警能力

云监控对以上所有监控项提供报警功能，您可以选择在单台服务器、应用分组、全部资源三个角度设置报警规则。从业务角度的不同角度出发使用报警功能。

您可以直接在主机监控列表中使用报警功能，也可以将服务器添加到应用分组后，在分组中使用报警功能。

进程监控

进程监控

进程监控默认为您采集最近一段时间内活跃进程消耗的 CPU 使用率、内存使用率，以及进程的文件打开数。如果您添加了进程关键字，还会采集包含关键字的进程个数。

查看活跃进程消耗

插件会每分钟统计一次1分钟内消耗 CPU Top5 的进程，记录 Top5 进程的 CPU 使用率、内存使用率和打开文件数。

进程的 CPU 使用率与内存使用率， 参考 Linux top 命令。CPU 使用率为多核使用情况。

当前进程打开文件数，参考 Linux lsof 命令。

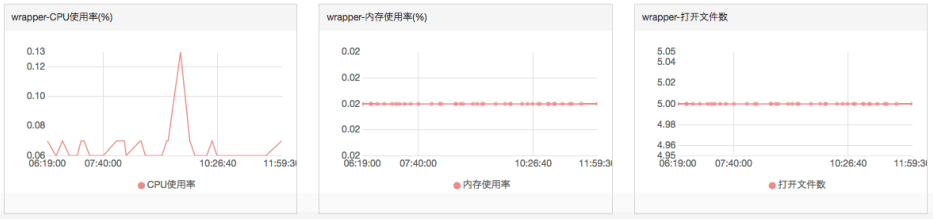
注意事项

如果您的进程占用了多个 CPU，会出现 CPU 使用率超过 100% 的情况。这里的采集结果为多核的总使用率。

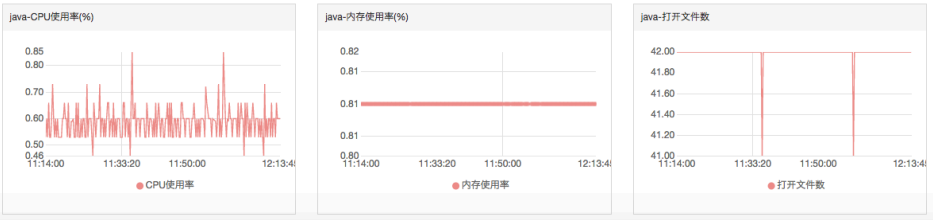
如果您查询的时间范围内，Top5 的进程不固定，进程列表中会展示这段时间内全部进入过 Top5 的进程，列表中的时间表示该进程最后一次进入 Top5 的时间。

只有进入 Top5 的进程才会采集进程的 CPU 使用率、内存使用率和打开文件数，所以如果该进程在查询的时间范围内未持续进入 Top5，会出现监控图中数据点不连续的情况，数据点的密集程度则表明了该进程在服务器上的活跃程度。

a. 如下图所示的 wrapper 进程，未持续进入服务器 CPU 消耗最高的 Top5 进程，所以监控图中的数据点稀疏、不连续，有数据点的时间表示该进程在Top5内。



b. 如下图所示的 java 进程，在监控图中数据点非常密集、连续，表明该进程持续排入 CPU 消耗最高的 Top5 进程内。



监控指定进程数

您可以通过进程数监控，采集关键进程的数量，及时获取关键进程的存活状态。

添加指定进程监控

注意事项

- 添加进程时，可以写进程的精确路径，也可以只填写进程关键字。可参考 Linux ps aux|grep ‘关键字’ 命令。

Windos机器添加指定进程时，请不要带”.exe”后缀，否则可能导致无法匹配进程名称。

举例如下：
机器当前运行如下几个进程
/usr/bin/java -Xmx2300m -Xms2300m org.apache.catalina.startup.Bootstrap
/usr/bin/ruby
nginx -c /ect/nginx/nginx.conf
假设用户配置了6个关键字，则采集结果分别如下：
配置关键字为：ruby，采集进程数：1，命中进程名称。
配置关键字为：nginx，采集进程数：1，命中进程名称与参数。
配置关键字为：/usr/bin，采集进程数：2，命中路径(两个进程包含这个路径)。
配置关键字为：apache.catalina，采集进程数：1，命中部分参数。
配置关键字为：nginx.conf，采集进程数：1，命中部分参数。
配置关键字为：-c，采集进程数：1, 命中部分参数。

操作步骤

登录云监控控制台。

通过选择左侧菜单的主机监控，进入主机监控页面。

点击需要添加监控的机器名称或点击操作中的**监控图表**，进入机器的监控详情页。

点击页面上方的**进程监控**，进入进程监控页面。

鼠标放置在进程数监控图表时，点击**添加进程监控** 按钮，增加需要监控的进程。

删除指定进程监控

登录云监控控制台。

通过选择左侧菜单的主机监控，进入主机监控页面。

点击需要添加监控的机器名称或点击操作中的**监控图表**，进入机器的监控详情页。

点击页面上方的**进程监控**，进入进程监控页面。

鼠标放置在进程数监控图表时，点击**添加进程监控** 按钮，进入已添加的进程列表页。

在列表中点击**删除**来删除对应进程即可。

设置报警规则

您在配置好指定进程的监控后，可以为进程配置报警规则，在进程数变化时收到报警通知。

1. 登录云监控控制台。
2. 通过选择左侧菜单的主机监控，进入主机监控页面。
3. 选择需要添加进程监控的报警的机器，点击操作中的**报警规则**，进入报警规则页面。
4. 点击页面上方的**新建报警规则**，进入报警规则创建页面。
5. 在规则描述中选择**进程数**，然后配置相应的报警阈值。如果机器上配置了多个进程，每个进程数量不一样，可以点击**添加报警规则**一次为多个进程配置报警。

监控项说明

主机监控的监控项分为插件采集的监控项和ECS 原生自带的监控项两部分，插件采集频率为15秒一次，ECS 基础监控数据采集频率为1分钟1次。

注意事项

您在查看ECS基础监控和操作系统监控数据时，可能会存在数据不一致的情况，主要有以下原因：

- 统计频率不同。监控图表中提供的数据均为统计周期内的平均值，基础监控统计频率是1分钟，操作系统统计频率是15秒，所以如果监控数据波动比较大时，会出现基础监控数据比操作系统监控数据小的情况，因为数据被削峰填谷了。
- 数据统计视角不同：基础监控的网络流量统计计费维度数据，除去了ECS和SLB之间不计费的网络流量。操作系统监控的网络流量，记录每张网卡实际的网络流量。所以会出现操作系统监控的网络数据大于基础监控网络数据的情况（即出现插件采集的数据比实际购买的带宽或流量大的情况）。

插件采集指标

CPU 相关监控项

以下为CPU使用率相关监控指标，可参考Linux的top命令来理解各项指标含义。

监控项名称	监控项含义	单位	说明
Host.cpu.idle	当前空闲CPU百分比	%	当前CPU处于空闲状态的百分比
Host.cpu.system	当前内核空间占用CPU百分比	%	指系统上下文切换的消耗,该监控项数值比较高，说明服务器开了太多的进程或者线程
Host.cpu.user	当前用户空间占用CPU百分比	%	用户进程对CPU的消耗
Host.cpu.iowait	当前等待IO操作的	%	该项数值比较高说明有

	CPU百分比		很频繁的IO操作
Host.cpu.other	其他占用CPU百分比	%	其他消耗，计算方式为（Nice + SoftIrq + Irq + Stolen）的消耗
Host.cpu.totalUsed	当前消耗的总CPU百分比	%	指以上各项CPU消耗的总和，通常用于报警

内存相关监控项

以下为内存相关监控项，可参考free命令来理解各项指标含义。

监控项名称	监控项含义	单位	说明
Host.mem.total	内存总量	bytes	服务器的内存总量
Host.mem.used	已用内存量	bytes	用户程序使用的内存 + buffers + cached，buffers为缓冲区占用的内存空间，cached为系统缓存占用的内存空间
Host.mem.actualused	用户实际使用的内存	bytes	计算方法为（used - buffers - cached）
Host.mem.free	剩余内存量	bytes	计算方法为（内存总量-已用内存量）
Host.mem.freeutilization	剩余内存百分比	%	计算方法为（剩余内存量/内存总量*100%）
Host.mem.usedutilization	内存使用率	%	计算方法为（ Actual used/total*100%）

系统平均负载监控项

以下为系统平均负载相关监控项，可参考Linux top命令来理解各项指标含义。监控项数值越高代表系统越繁忙。

监控项名称	监控项含义	单位
Host.load1	过去1分钟的系统平均负载，Windows操作系统没有此指标	无
Host.load5	过去5分钟的系统平均负载，Windows操作系统没有此指标	无
Host.load15	过去15分钟的系统平均负载，Windows操作系统没有此指标	无

磁盘相关监控项

- 磁盘使用率与inode使用率可参考Linux df命令。
- 磁盘读写指标可参考Linux iostat命令。

监控项名称	监控项含义	单位
Host.diskusage.used	磁盘的已用存储空间	bytes
Host.disk.utilization	磁盘使用率	%
Host.diskusage.free	磁盘的剩余存储空间	bytes
Host.diskussage.total	磁盘存储总量	bytes
Host.disk.readbytes	磁盘每秒读取的字节数	bytes/s
Host.disk.writebytes	磁盘每秒写入的字节数	bytes/s
Host.disk.readiops	磁盘每秒的读请求数量	次/秒
Host.disk.writeiops	磁盘每秒的写请求数量	次/秒

文件系统监控项

监控项名称	监控项含义	单位	说明
Host.fs.inode	inode使用率,UNIX/Linux系统内部使用inode号码来识别文件，磁盘还未存满，但inode已经分配完时会出现无法在磁盘新建文件的情况，Windows操作系统没有此指标	%	inode数量代表文件系统文件数量，大量小文件会导致inode使用率过高

网络相关监控项

- 以下为网络相关指标，可参考Linux iftop。TCP连接数的采集，可参考Linux ss命令。
- TCP连接数会默认采集 TCP_TOTAL（总连接数）、ESTABLISHED（正常连接状态），NON_ESTABLISHED（非连接的状态连接数，ESTABLISHED以外的所有状态），如果您需要获取各个状态连接数的数量，请按如下说明操作：

Linux操作系统
您可以将cloudmonitor/config/conf.properties配置文件的netstat.tcp.disable改为false来开启采集。修改配置后请重启Agent。

Windows操作系统
您可以在C:\”Program Files”\Alibaba\cloudmonitor\config的配置文件中，将netstat.tcp.disable改为false来开启采集。修改配置后请重启Agent。

监控项名称	监控项含义	单位
Host.netin.rate	网卡每秒接收的比特数，即网卡的上行带宽	bits/s
Host.netout.rate	网卡每秒发送的比特数，即网卡的下行带宽	bits/s
Host.netin.packages	网卡每秒接收的数据包数	个/秒
Host.netout.packages	网卡每秒发送的数据包数	个/秒
Host.netin.errorpackage	设备驱动器检测到的接收错误包的数量	个/秒
Host.netout.errorpackages	设备驱动器检测到的发送错误包的数量	个/秒
Host.tcpconnection	各种状态下的TCP连接数包括LISTEN、SYN_SENT、ESTABLISHED、SYN_RECV、FIN_WAIT1、CLOSE_WAIT、FIN_WAIT2、LAST_ACK、TIME_WAIT、CLOSING、CLOSED	个

进程相关监控项

- 进程的CPU使用率、内存使用率可参考Linux top命令，CPU使用率为多核使用情况。
- Host.process.openfile 可参考Linux lsof命令。
- Host.process.number 可参考Linux ps aux |grep ‘关键字’ 命令。

监控项名称	监控项含义	单位
Host.process.cpu	某个进程消耗的CPU百分比	%
Host.process.memory	某个进程消耗的内存百分比	%
Host.process.openfile	当前进程打开文件数	个
Host.process.number	指定关键字的进程数	个

ECS自带监控项

如果您的主机是ECS服务器，以下监控项为购买ECS后，不需要安装插件就可以提供的监控项。指标采集粒度为1分钟。

监控项名称	监控项含义	单位
ECS.CPUUtilization	CPU使用率	%
ECS.InternetInRate	公网入流量平均速率	bits/s
ECS.IntranetInRate	私网入流量平均速率	bits/s
ECS.InternetOutRate	公网出流量平均速率	bits/s

ECS.IntranetOutRate	私网出流量平均速率	bits/s
ECS.SystemDiskReadbps	系统磁盘每秒读取字节总数	Bytes/s
ECS.SystemDiskWritebps	系统磁盘每秒写入字节总数	Bytes/s
ECS.SystemDiskReadOps	系统磁盘每秒读取次数	个/秒
ECS.SystemDiskWriteOps	系统磁盘每秒写入次数	个/秒
ECS.InternetIn	公网流入流量	bytes
ECS.InternetOut	公网流出流量	bytes
ECS.IntranetIn	内网流入流量	bytes
ECS.IntranetOut	内网流出流量	bytes

主机监控插件介绍

安装位置

- Linux：位于/usr/local/cloudmonitor。
- Windows 64位 位于 C:\” Program Files (x86)” \Alibaba\cloudmonitor。
- Windows 32位 位于 C:\” Program Files” \Alibaba\cloudmonitor。

进程信息

主机监控插件安装后，会在您的服务器上运行以下两个进程：

- /usr/local/cloudmonitor/jre/bin/java
- /usr/local/cloudmonitor/wrapper/bin/wrapper

端口说明

- 监听 TCP localhost 32000端口， 用于进程守护。
- 访问 TCP localhost 32000端口， 用于进程守护。
- 访问 TCP 远程 3128、8080、443端口。 用于心跳与监控数据上报，非阿里云机器使用443端口，阿里云机器使用3128或8080端口。
- 访问 HTTP 远程 80端口，用于云监控插件升级。

插件日志

- 监控数据采集日志位于/usr/local/cloudmonitor/logs 。
- 启动，关闭，进程守护等日志位于 /usr/local/cloudmonitor/wrapper/logs 。
- 可以通过修改/usr/local/cloudmonitor/config/log4j.properties配置来调整日志级别。

资源占用情况

- /usr/local/cloudmonitor/wrapper/bin/wrapper进程占用1M左右内存，基本不消耗CPU。
- /usr/local/cloudmonitor/jre/bin/java进程占用70M左右内存和单核1-2%的CPU。
- 安装包70M, 安装完成后约占用200M磁盘空间。
- 日志最多占用40M空间，超过40M会进行清除。
- 每15秒发送一次监控数据，约占用内网网络带宽10KB。
- 每3分钟发送一次心跳数据，约占用内网网络带宽2KB左右。

外部依赖

- 云监控Agent使用JAVA语言编写，内置JRE 1.8。
- Java service wrapper 用于进程守护、开机启动、Windows服务注册等。
- iproute ss命令 用于采集TCP连接，如果当前系统没有，需要用户自己安装。

安装说明

手工安装可参考插件安装文档。

非阿里云主机安装方法

1. 登录云监控主机监控页面。
2. 点击页面右上角的 “ **如何添加主机** ” 文档，复制非阿里云服务器的插件安装命令后在机器上执行即可。

插件 Release Notes

1.2.11

使用本地健康检查功能，需要将插件升级至此版本。

新功能

- 新增本地及远程协议探测功能，支持Telnet、HTTP协议探测。

已知问题的修复与优化

- 修复安装脚本的临时下载目录为tmp目录可能导致提权漏洞的问题。
- 修复同一个磁盘设备被挂多次，导致提交相同设备数据的问题。
- 修复部分进程无法获得path与name的问题。
- 优化文件下载方式，解决下载可能阻塞监控进程的问题。

1.1.64

已知问题的修复与优化，建议CentOS7.2以上版本的用户升级插件至此版本。

- 调整内存使用率采集逻辑，centos7.2以上的版本使用/proc/meminfo MemAvailable字段作为可用内存估算依据，提升内存使用率计算准确性。

1.1.63

已知问题的修复与优化

- 调整默认wrapper log为info级别。
- 增加error级别日志信息，方便定位问题。
- 修复debug级别日志可能导致内存泄露风险的问题。

1.1.62

已知问题的修复与优化

- 优化HTTP Proxy选择逻辑，提升插件安装成功率。
- 添加关键日志，更容易定位问题。

1.1.61

已知问题的修复与优化

- 修复部分系统采集进程用户名时可能异常，导致topN进程采集不正确的问题。

1.1.59

已知问题的修复与优化

- 优化进程数采集方式，提升性能。
- 进程监控中进程数采集不再计算云监控插件自身的2个进程。

使用报警服务

主机监控提供报警服务，您可以在主机监控中为单个服务器设置报警规则，也可以将服务器添加到指定应用分组后，在应用分组粒度设置报警规则。查看在应用分组中设置报警规则。

创建报警规则

登录云监控的主机监控页面。

切换到主机监控页面的**报警规则** 页面。

点击页面右上角的**新建报警规则**按钮。

在新建报警规则页面填写设置报警的具体参数，相关参数说明可参考报警参数说明。

保存规则设置，完成报警规则的创建。

删除报警规则

登录云监控的主机监控页面。

切换到主机监控页面的**报警规则** 页面。

点击报警规则对应的**删除**操作，删除单条报警规则。或者勾选多个规则后，点击列表下方的**删除**按钮，删除多条规则。

修改报警规则

登录云监控的主机监控页面。

切换到主机监控页面的**报警规则** 页面。

点击报警规则对应的**修改**操作，修改单条报警规则。

查看报警规则

登录云监控的**主机监控**页面。

点击实例列表中的**报警规则**，查看单个服务器的报警规则。

切换到主机监控页面的**报警规则** 页面，可以查看全部报警规则。

站点监控

站点监控概览

应用场景

站点监控是一款定位于互联网网络探测的监控产品，主要用于通过遍布全国的互联网终端节点，发送模拟真实用户访问的探测请求，监控全国各省市运营商网络终端用户到您服务站点的访问情况。以下是站点监控的典型应用场景。

运营商网络质量分析

通过站点监控的探测点，模拟最终用户的访问行为，可以获得全国各地到目标地址的访问数据，从而知晓各地域、各运营商的网络质量，针对性进行网络优化。

性能分析

通过创建站点监控任务，可以获得访问目标地址的DNS域名解析时间、建连时间、首包时间、下载时间等，从而分析服务的性能瓶颈。

竞品分析

通过添加自己的服务站点和竞争对手的站点，选择目标探测点，针对分析探测结果，得出自己的服务和竞品服务的质量分析。

探针覆盖情况

站点监控支持从阿里云各地域的机房或全国各地终端节点发起探测请求。目前覆盖7个来自阿里巴巴机房的地域和100+个区分运营商的各省市地域。

地域	运营商
上海市 上海市	阿里巴巴
北京市 北京市	阿里巴巴
山东省 青岛	阿里巴巴
广东省 深圳	阿里巴巴
河北省 张家口	阿里巴巴
浙江省 杭州	阿里巴巴
香港 香港	阿里巴巴
浙江省 舟山市	电信
浙江省 丽水市	电信
浙江省 台州市	联通
浙江省 衢州市	联通
浙江省 舟山市	移动
天津市 天津市	电信
云南省 昆明	电信
云南省 楚雄彝族自治州	电信
云南省 楚雄彝族自治州	移动
云南省 玉溪市	移动
云南省 昭通市	移动
四川省 遂宁市	电信
四川省 绵阳市	电信
四川省 眉山市	电信
四川省 成都市	电信
四川省 雅安市	电信
四川省 广安市	联通
四川省 成都市	联通
四川省 眉山市	移动
四川省 宜宾市	移动
四川省 雅安市	移动

陕西省 西安市	电信
陕西省 汉中市	电信
陕西省 咸阳市	联通
陕西省 咸阳市	移动
山西省 吕梁市	电信
山西省 晋城市	电信
山西省 长治市	电信
山西省 吕梁市	移动
山东省 东营市	电信
山东省 淄博市	电信
山东省 济南市	电信
山东省 青岛市	联通
山东省 临沂市	联通
山东省 德州市	联通
山东省 烟台市	联通
山东省 烟台市	鹏博士
山东省 莱芜市	移动
内蒙古自治区 呼伦贝尔市	电信
内蒙古自治区 赤峰市	联通
内蒙古自治区 鄂尔多斯市	联通
内蒙古自治区 乌兰察布市	移动
辽宁省 丹东市	电信
辽宁省 盘锦市	电信
辽宁省 葫芦岛市	联通
辽宁省 大连市	鹏博士
辽宁省 大连市	移动
辽宁省 盘锦市	移动
辽宁省 抚顺市	移动
辽宁省 丹东市	移动
江西省 鹰潭市	电信
江西省 抚州市	联通
江西省 南昌市	鹏博士
江西省 萍乡市	移动

江西省 南昌市	移动
江苏省 无锡市	联通
江苏省 宿迁市	移动
江苏省 镇江市	移动
江苏省 泰州市	移动
江苏省 南通市	移动
湖南省 益阳市	电信
湖南省 长沙市	鹏博士
湖南省 湘潭市	移动
湖南省 岳阳市	移动
湖北省 黄冈市	联通
湖北省 宜昌市	联通
湖北省 武汉市	鹏博士
湖北省 咸宁市	移动
湖北省 襄樊市	移动
湖北省 荆州市	移动
湖北省 黄石市	移动
黑龙江省 哈尔滨市	电信
黑龙江省 齐齐哈尔市	电信
黑龙江省 黑河市	联通
黑龙江省 鹤岗市	联通
黑龙江省 伊春市	移动
黑龙江省 鸡西市	移动
黑龙江省 大庆市	移动
河南省 洛阳市	电信
河南省 开封市	电信
河南省 信阳市	电信
河南省 安阳市	联通
河南省 安阳市	移动
河北省 衡水市	电信
河北省 秦皇岛市	联通
海南省 三亚市	电信
贵州省 铜仁市	电信

广西壮族自治区 南宁市	移动
广西壮族自治区 百色市	移动
广东省 湛江市	电信
广东省 阳江市	电信
广东省 江门市	联通
广东省 梅州市	联通
甘肃省 兰州市	电信
甘肃省 张掖市	电信
甘肃省 天水市	电信
甘肃省 嘉峪关市	移动
福建省 宁德市	电信
福建省 泉州市	联通
福建省 宁德市	铁通
北京市 北京市	联通
安徽省 池州市	电信
安徽省 黄山市	电信
安徽省 芜湖市	移动

探测协议类型

探测类型	功能
HTTP	对指定的URL/IP进行HTTP探测，获得可用性监控以及响应时间、状态码。高级设置中支持GET/POST/HEAD 请求方式、cookie、header信息、判断页面内容是否符合匹配内容。
PING	对指定的URL/IP进行ICMP Ping探测，获得可用性监控以及响应时间、丢包率。
TCP	对指定的端口进行TCP探测，获得可用性监控以及响应时间、状态码。高级设置中支持配置TCP的请求内容及匹配响应内容。
UDP	对指定的端口进行UDP探测，获得可用性监控以及响应时间、状态码。高级设置中支持配置UDP的请求内容及匹配响应内容。
DNS	对指定的域名进行DNS探测，获得可用性监控以及响应时间、状态码。高级设置中支持查询A/MX/NS/CNAME/TXT/ANY记录。
POP3	对指定的URL/IP进行POP3探测，获得可用性监控以及响应时间、状态码。高级设置中支持端口、用户名、密码和是否使用安全链接的设置。

SMTP	对指定的URL/IP进行SMTP探测，获得可用性监控以及响应时间、状态码。高级设置中支持端口、用户名、密码和是否使用安全链接的设置。
FTP	对指定的URL/IP进行FTP探测，获得可用性监控以及响应时间、状态码。高级设置中支持端口、是否使用安全链接的设置。

管理站点监控任务

创建站点监控任务

创建站点监控任务分为设置基本信息、选择探测点、设置报警规则三步。设置报警规则为可选项，可以不设置。

操作步骤

1. 登录云监控控制台，选择页面左侧菜单中站点监控下的**站点管理**，进入站点监控任务列表页面。
2. 点击页面右上角的**新建任务**按钮，进入创建站点监控任务页面
3. 填写基础信息
   - 监控类型：监控协议，支持HTTP(S)、Ping、TCP、UDP、DNS、SMTP、POP3、FTP 8种协议。
   - 任务名称：监控任务的名称。
   - 监控地址：目标监控地址，一次可以填写多个监控地址，方便用户进行批量设置。保存时会将多个监控地址拆分成多个任务。
   - 监控频率：监控周期，例如选择1分钟频率，则各地域探测点将以1分钟/次的频率监控目标地址。
   - 高级设置：不同协议支持不同的高级设置，可根据实际情况选择使用。
4. 选择探测点
   - 快捷选择探测点：将常用探测点打包，方便您批量快速选择。
   - 探测点高级选项：按需精细化选择指定的探测点。
5. 设置报警规则
   - 可用性：分为可用探测点数量和可用探测点百分比2个选项。当探测结果中状态码大于399时即为不可用。可用探测点数量=一个周期内探测点的状态码小于400的探测结果数量，可用探测点百分比=一个周期内（探测点的状态码小于400的探测结果数量/探测结果总数量）*100。
   - 平均响应时间：指每个监控周期内所有探测点的响应时间的平均值。
   - 连续几次超过阈值后报警：实际监控值连续几次达到设置的阈值才会报警。该项用来过滤监控数据偶尔发生波动的情况。
   - 选择联系人组：发送报警通知时的接收对象。

- 报警通知方式：报警通知的发送渠道。
- 高级设置：包括通道沉默时间、生效时间、报警回调。

修改站点监控任务

1. 登录云监控控制台，选择页面左侧菜单中站点监控下的**站点管理**，进入站点监控任务列表页面。
2. 选择需要修改的任务，点击**操作**中的**修改**按钮。
3. 进入修改页面，修改相应内容。

删除站点监控任务

1. 登录云监控控制台，选择页面左侧菜单中站点监控下的**站点管理**，进入站点监控任务列表页面。
2. 选择需要修改的任务，点击**操作**中的**删除**按钮，删除相关任务。
3. 任务被删除时，相关报警规则会同步被删除。

启用或禁用站点监控任务

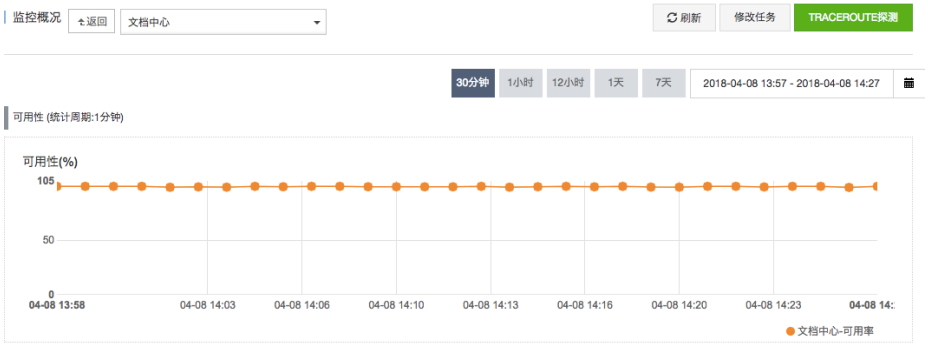
1. 登录云监控控制台，选择页面左侧菜单中站点监控下的**站点管理**，进入站点监控任务列表页面。
2. 选择需要启用或禁用的任务，点击**操作**中的**启用**或**禁用**按钮，进行任务的启用或禁用。

查看监控数据

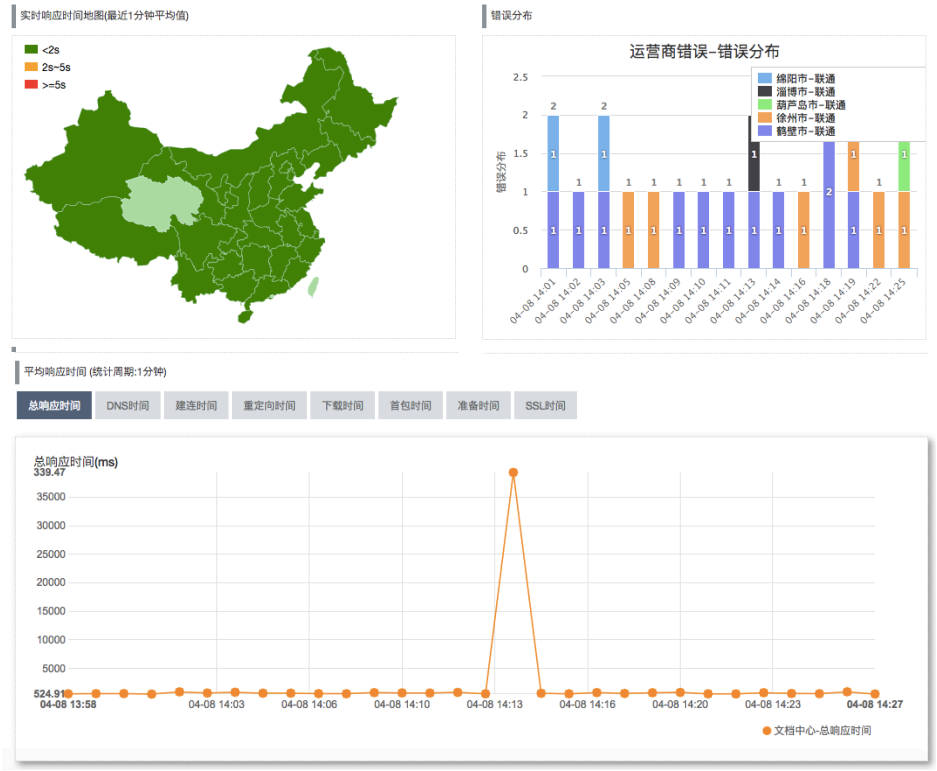
查看监控数据

概览

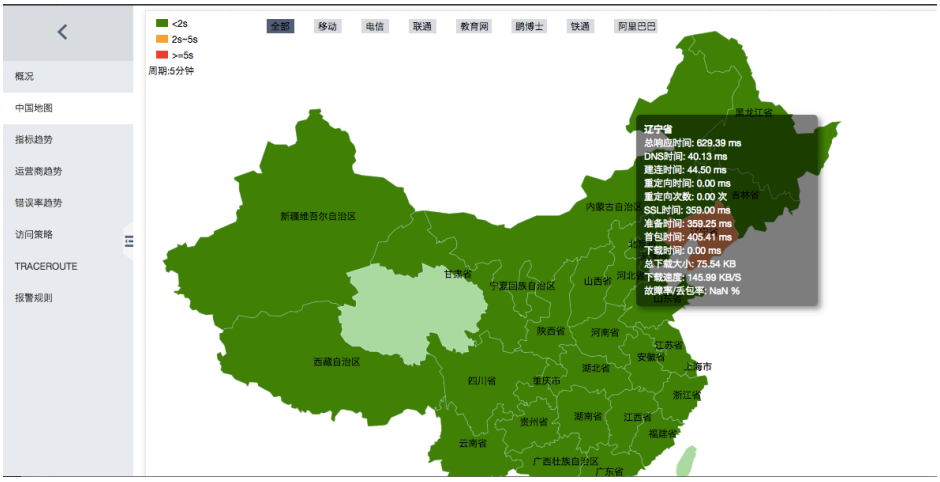
从可用性、全国各地域实时响应时间、错误分布、响应时间趋势来展现当前站点的访问情况。



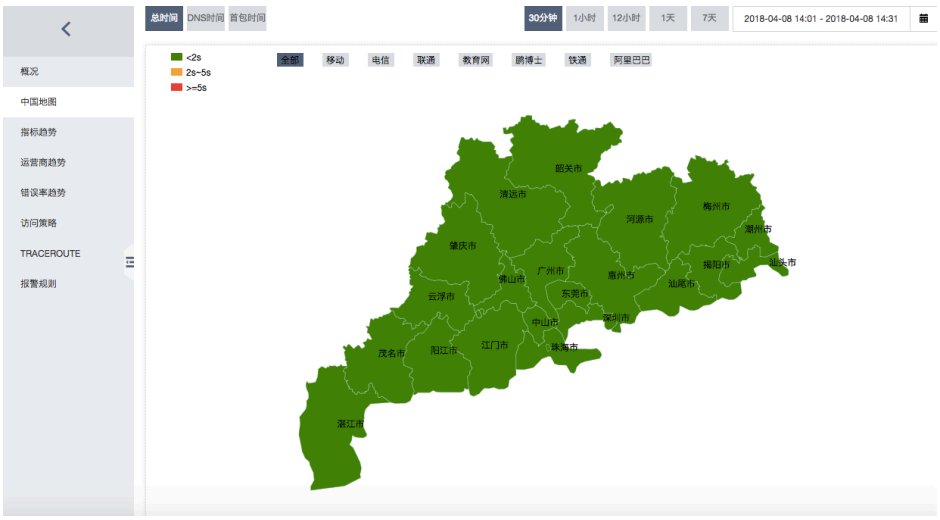
错误分布会统计一段时间内各地域运营商探测结果中状态码超过399的数量。如需查看错误详情，可点击图表下钻查看相关数据。



中国地图



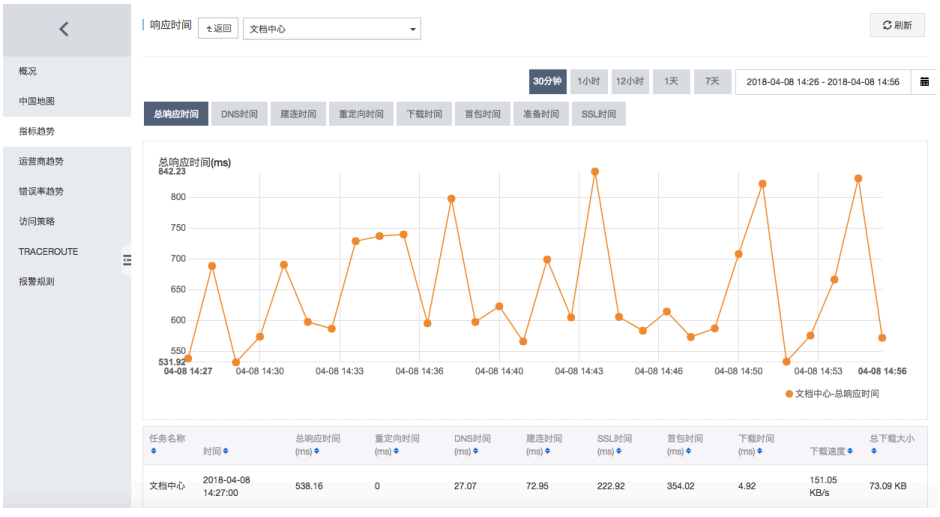
鼠标左键单击相应省份会下钻到二级地域：



地图下方提供相关地域的监控数据详情：

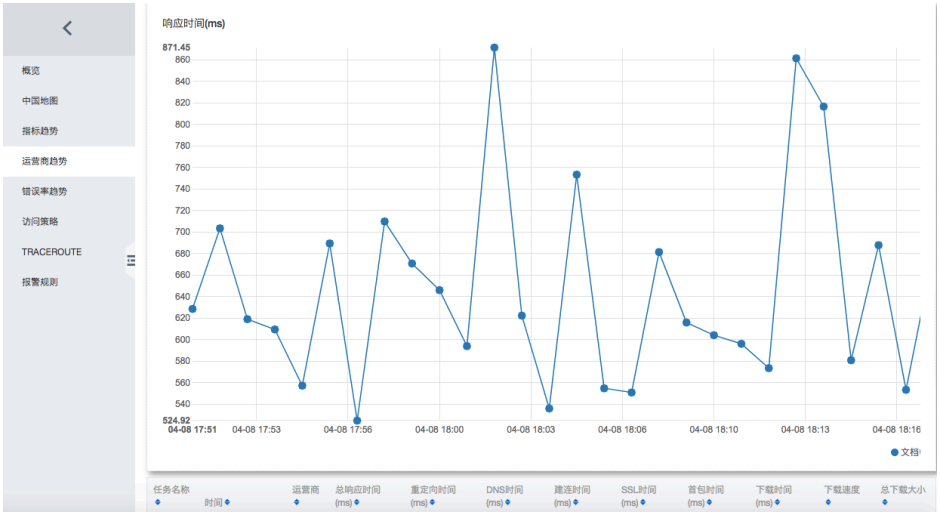
任务名称	时间	省份	城市	总响应时间(ms)	重定向时间(ms)	DNS时间(ms)	建连时间(ms)	SSL时间(ms)	首包时间(ms)	下载时间(ms)	下载速度	总下载大小
文档中心	2018-04-08 14:02:00	广东省	潮州市	553	0	57	94	234	362	0	136.47 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	佛山市	590	0	16	49	297	421	0	128.00 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	江门市	501	0	22	57	211	356	0	150.59 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	揭阳市	500	0	9	47	187	307	0	150.80 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	茂名市	475	0	12	49	185	318	0	158.94 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	汕头市	493	0	10	51	195	325	0	152.93 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	韶关市	677	0	174	215	356	480	0	111.44 KB/s	75.54 KB
文档中心	2018-04-08 14:02:00	广东省	深圳市	565	0	27	61	197	348	0	133.59 KB/s	75.54 KB

指标趋势

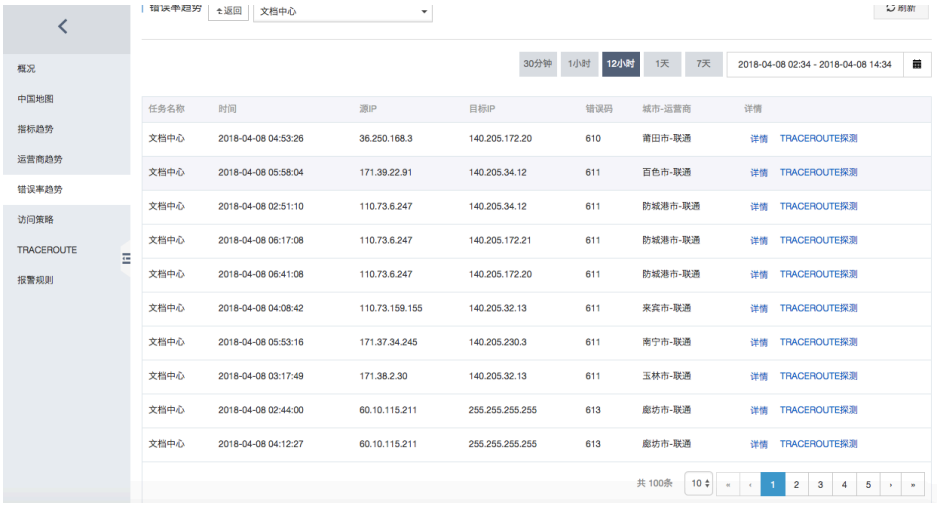


任务名称	时间	总响应时间(ms)	重定向时间(ms)	DNS时间(ms)	建连时间(ms)	SSL时间(ms)	首包时间(ms)	下载时间(ms)	下载速度	总下载大小
文档中心	2018-04-08 14:27:00	538.16	0	27.07	72.95	222.92	354.02	4.92	151.05 KB/s	73.09 KB

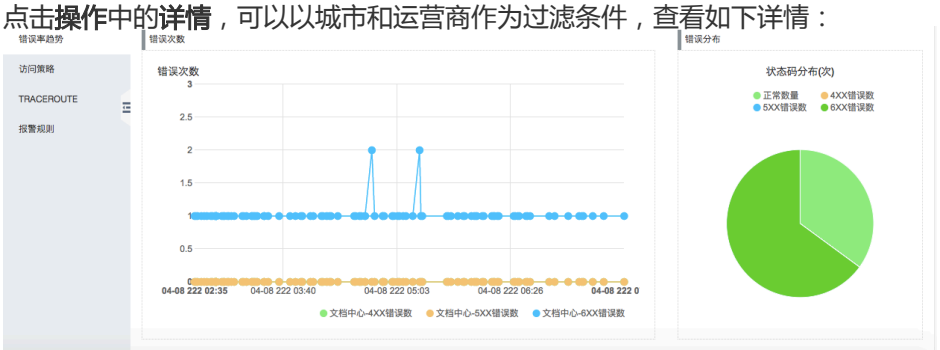
运营商趋势

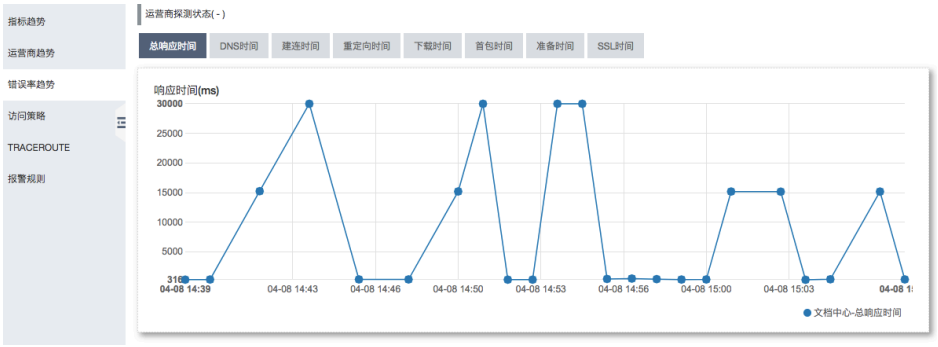


错误率趋势



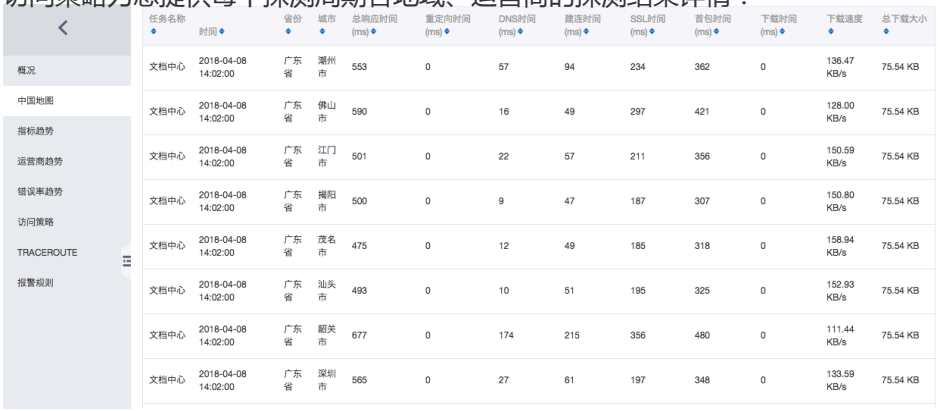
点击**操作**中的**详情**，可以以城市和运营商作为过滤条件，查看如下详情：





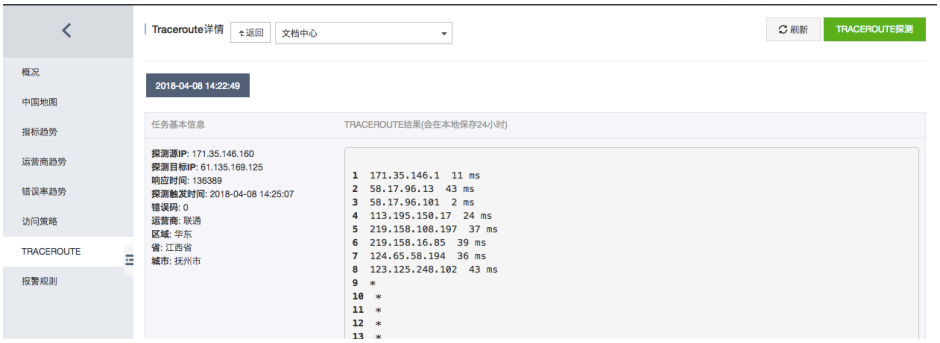
访问策略

访问策略为您提供每个探测周期各地域、运营商的探测结果详情：



TRACEROUTE

该列表为您提供24小时内各探测点发起的TRACEROUTE结果。TRACEROUTE请求需要您主动配置，点击页面右上角的**TRACEROUTE按钮**会根据配置发起一次TRACEROUTE探测。



名词解释

名词	解释
可用率	探测周期内探测点的状态码小于400的探测结果数量/探测结果总数量*100
总响应时间	从发起探测，到收到HTTP响应的第一个字节的时间。如果探测过程中有重定向，则该值包含重定向

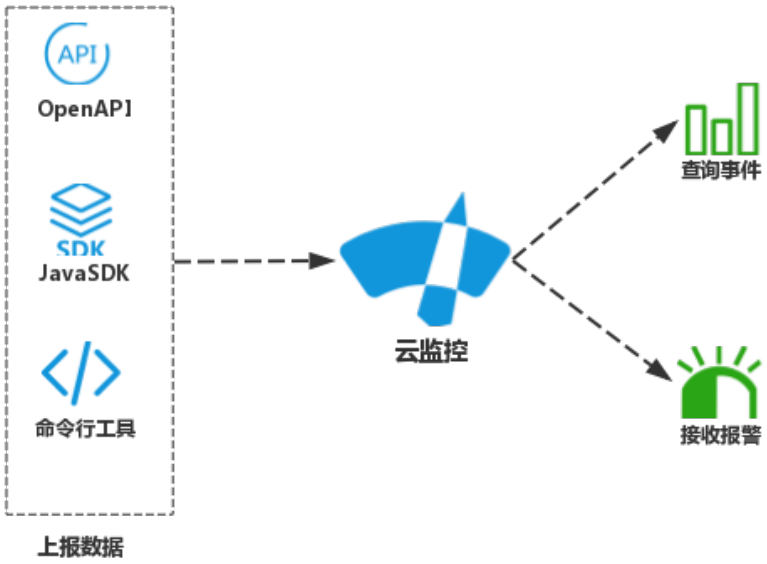
	时间。
DNS时间	即DNS域名解析时间，解析域名所耗费的毫秒数。
建连时间	从发起探测，到HTTP请求写入完成所耗费的时间，减去DNS域名解析的时间。
重定向时间	从发起探测，到发起第一个非重定向请求所花的时间。
首包时间	从发起探测，到收到HTTP回应包第一个字节所耗费的时间。
准备时间	从发起探测，到HTTP请求写入完成所耗费的时间。
SSL时间	从发起探测到完成SSL认证所耗费的时间。
下载速度	读取HTTP回应时的网络速度。
总下载大小	HTTP回应的大小, 如果回应中有Content-Length，则为该值，如果没有，则为实际读取的字节数。
TCP连接时间	从发起探测到TCP连接完成所耗费的时间（含DNS域名解析时间）。

事件监控

使用事件监控

事件监控概览

事件监控提供事件类型数据的上报、查询、报警功能。方便您将业务中的各类异常事件或重要变更事件收集上报到云监控，并在异常发生时接收报警。



事件监控与自定义监控有何区别？

事件监控用于解决非连续的事件类型数据监控数据上报、查询与报警的场景。自定义监控用于解决周期性持续采集的时间序列监控数据上报、查询与报警的场景。

使用流程

上报事件数据

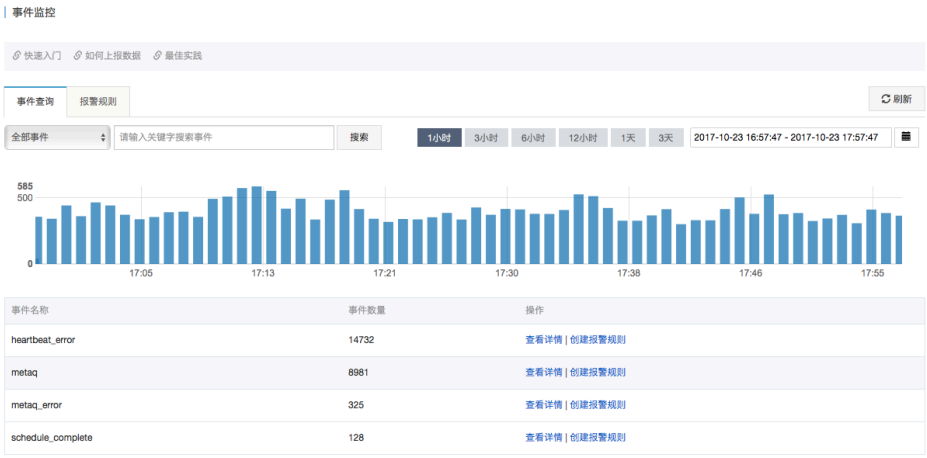
上报事件数据部分请参考**上报事件数据**。

查询事件数据

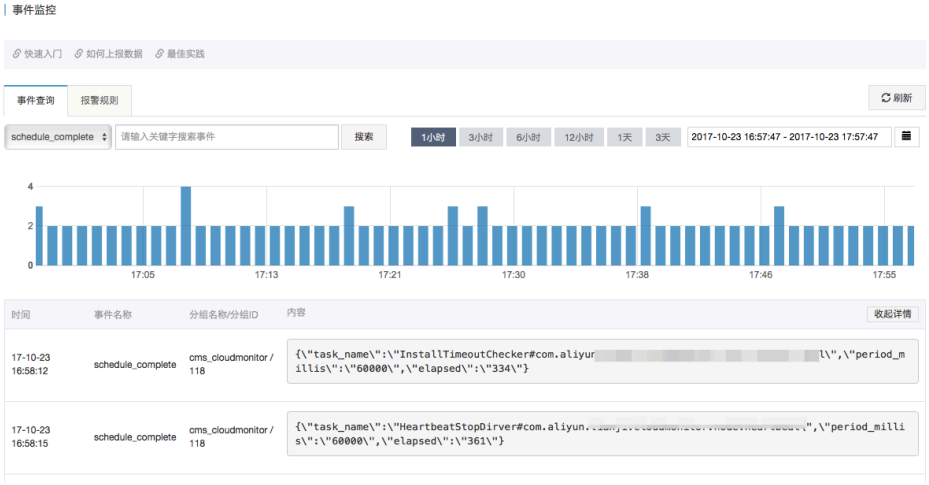
完成事件的上报后，您就可以在控制台中查看到已经上报的数据。您可以在**事件监控**中查看全部事件，也可以进入某个指定的应用分组，查看这个分组的相关事件。

查看所有上报的事件：

1. 登录云监控控制台，进入**事件监控**。
2. 查看全部事件如下：



3. 点击 **操作** 中的**查看详情**，查看具体事件的Content内容。



如果您只想查询某个指定分组的事件，进入应用分组内的事件监控页面即可。

设置报警

事件监控为您提供报警功能，设置报警时需要选择相应的应用分组，报警被触发后会发送通知给应用分组的联系人。如果您上报的事件需要报警，可以按照如下方式配置报警规则。

方式一：

1. 登录云监控控制台，进入**事件监控**。
2. 在事件列表页面，点击相应事件的**创建报警规则**。
3. 进入创建报警规则页面，填写报警规则名称、选择应用分组、设置相应的报警策略及通知方式。

方式二：

1. 登录云监控控制台，进入**应用分组**。
2. 选择相应的应用分组，进入应用分组内的**事件监控**页面。
3. 在事件列表页面，点击相应事件的**创建报警规则**。
4. 进入创建报警规则页面，填写报警规则名称、相应的报警策略及通知方式。

上报事件数据

事件监控功能为您提供上报事件的接口，方便您将业务产生的异常事件采集上报到云监控，通过对上报的事件配置报警规则来接收报警通知。

云监控为您提供 OpenAPI、Java SDK 和阿里云命令行工具（CLI）三种方式上报数据。

使用限制

- 单云账号QPS限制为20
- 单次最多上报100个事件
- 单次最多上报500KB数据

OpenAPI上报数据

服务地址

https://metrichub-cms-cn-hangzhou.aliyuncs.com

请求语法

```
POST /event/custom/upload HTTP/1.1
Authorization:<AuthorizationString>
Content-Length:<Content Length>
Content-MD5:<Content MD5>
Content-Type:application/json
Date:<GMT Date>
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-signature:hmac-sha1
x-cms-api-version:1.0
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
[{"content":"EventContent","groupId":GroupId,"name":"EventName","time":"20171023T144439.948+0800"}]
```

请求参数

名称	类型	必选	描述
name	字符串	是	事件名称
groupId	数值	是	事件所属的应用分组Id
time	字符串	是	事件发生时间
content	字符串	是	事件详情

关于API的请求头，请参考**请求头定义**。

关于API的签名算法，请参考**签名算法**。

响应元素

HTTP 状态码返回 200。

示例

请求示例

```
POST /event/custom/upload HTTP/1.1
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version:1.0
Authorization:YourAccKey:YourAccSecret
Host:metrichub-cms-cn-hangzhou.aliyuncs.com"
Date:Mon, 23 Oct 2017 06:51:11 GMT
Content-Length:180
x-cms-signature:hmac-sha1
Content-MD5:E9EF574D1AEAAA370860FE37856995CD
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
Content-Type:application/json

[{"content":"123,abc","groupId":100,"name":"Event_0","time":"20171023T144439.948+0800"}]
```

返回示例

```
{
"code":"200",
"msg":""//正常上报时返回msg为空
}
```

Java SDK上报数据

maven依赖

```
<dependency>
<groupId>com.aliyun.openservices</groupId>
<artifactId>aliyun-cms</artifactId>
<version>0.1.2</version>
</dependency>
```

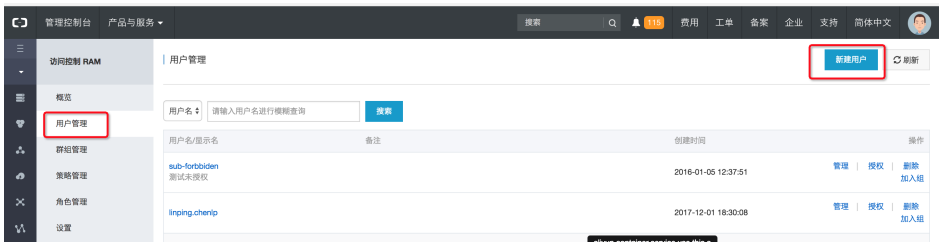
示例代码

```
public void uploadEvent() throws CMSException, InterruptedException {
//初始化客户端
CMSClient cmsClient = new CMSClient(endpoint, accKey, secret);
//构建2个事件上报
CustomEventUploadRequest request = CustomEventUploadRequest.builder()
.append(CustomEvent.builder()
.setContent("abc,123")
.setGroupId(101l)
.setName("Event001").build())
.append(CustomEvent.builder()
.setContent("abc,123")
.setGroupId(101l)
.setName("Event002").build())
.build();
CustomEventUploadResponse response = cmsClient.putCustomEvent(request);

List<CustomEvent> eventList = new ArrayList<CustomEvent>();
eventList.add(CustomEvent.builder()
.setContent("abcd,1234")
.setGroupId(101l)
.setName("Event001").build());
eventList.add(CustomEvent.builder()
.setContent("abcd,1234")
.setGroupId(101l)
.setName("Event002").build());
request = CustomEventUploadRequest.builder()
.setEventList(eventList).build();
response = cmsClient.putCustomEvent(request);
}
```

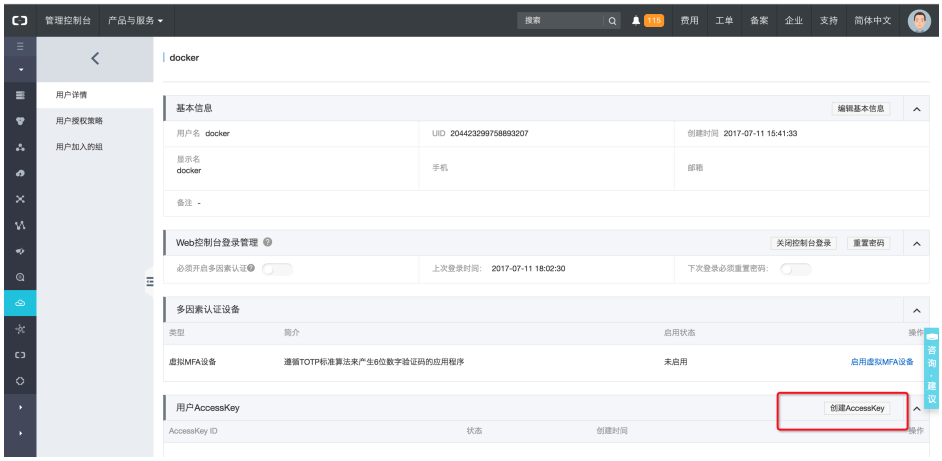
阿里云命令行（CLI）方式上报数据

前置条件：拥有阿里云账号，并生成具有云监控权限的子账号AK（使用子账号安全性更好）

创建子账号



- 为子账号生成accesskeyid， accesskeysecrret



- 为子账号授权云监控权限

第一步：安装aliyuncli工具

前置条件

- 系统要求：Linux、UNIX 或 Mac OS。
- 环境要求：已安装 Python 2.7.x。

安装 Python

- 若您的设备已安装 Python 2.7.x 版本，请跳过此步骤。
- 若您的设备没有安装 Python 2.7.x 版本，请在命令行窗口中执行下列命令，安装 Python。注意，请确保您的设备中已安装了 wget。

```
wget https://www.python.org/ftp/python/2.7.8/Python-2.7.8.tgz (或者通过其他方式下载后放在某个路径下)
tar -zxvf Python-2.7.8.tgz
cd Python-2.7.8
./configure
make
sudo make install
```

安装 pip

- 若您的设备已安装 pip，请跳过此步骤。
- 若您的设备没有安装 pip，在命令行窗口中执行如下命令，安装 pip。

```
curl "https://bootstrap.pypa.io/get-pip.py" -o "pip-install.py"
sudo python pip-install.py
```

系统显示如下类似信息，则表明安装成功。

```
Successfully installed pip-7.1.2 setuptools-18.7 wheel-0.26.0
```

安装命令行工具

如果系统内的 pip 版本过低，会造成 CLI 安装出错。用户可以使用如下指令先对 pip 软件进行升级后再进行相关操作。请使用 pip 7.x 或更高版本。若已是最新版本的 pip，请跳过此步骤。

1. 在命令行窗口中执行如下命令，升级 pip。

```
sudo pip install -U pip
```

系统显示如下类似信息，则表明升级成功。

```
Successfully uninstalled pip-7.1.2
Successfully installed pip-8.1.2
```

1. 执行如下命令，安装阿里云命令行工具。

```
sudo pip install aliyuncli
```

系统显示如下类似信息，则表明安装成功。

```
Successfully installed aliyuncli-2.1.2 colorama-0.3.3 jmespath-0.7.1
```

配置命令行工具

```
~ sudo aliyuncli configure
Aliyun Access Key ID [********************a]: youraccesskeyid
Aliyun Access Key Secret [********************b]: youraccesskeysecret
Default Region Id [cn-hangzhou]: cn-hangzhou
Default output format [json]: json
```

第二步：安装CmsSDK

Windows安装方式：在命令行窗口输入如下命令

```
cd C:\Python27\Scripts
pip install aliyun-python-sdk-cms
```

如果需要更新SDK，则使用如下命令：

```
pip install --upgrade aliyun-python-sdk-cms
```

Linux 安装方式：

```
sudo pip install aliyun-python-sdk-cms
```

如果需要升级SDK，则使用如下命令：

```
sudo pip install —upgrade aliyun-python-sdk-cms
```

第三步：上报监控数据

使用PutEvent接口。

Windows上报示例：

```
aliyuncli.exe cms PutEvent --EventInfo
"[{'content':'helloworld','time':'20171013T170923.456+0800','name':'ErrorEvent','groupId':'27147'}]"
```

Linux 上报示例：

```
aliyuncli cms PutEvent --EventInfo
"[{'content':'helloworld','time':'20171023T180923.456+0800','name':'ErrorEvent','groupId':'27147'}]"
```

上报成功后，返回200状态码

```
{
"Code":"200"
}
```

错误编码

错误代码	含义
200	正常

400	客户端请求中的语法错误
403	校验失败、限速、没有授权
500	服务器内部错误

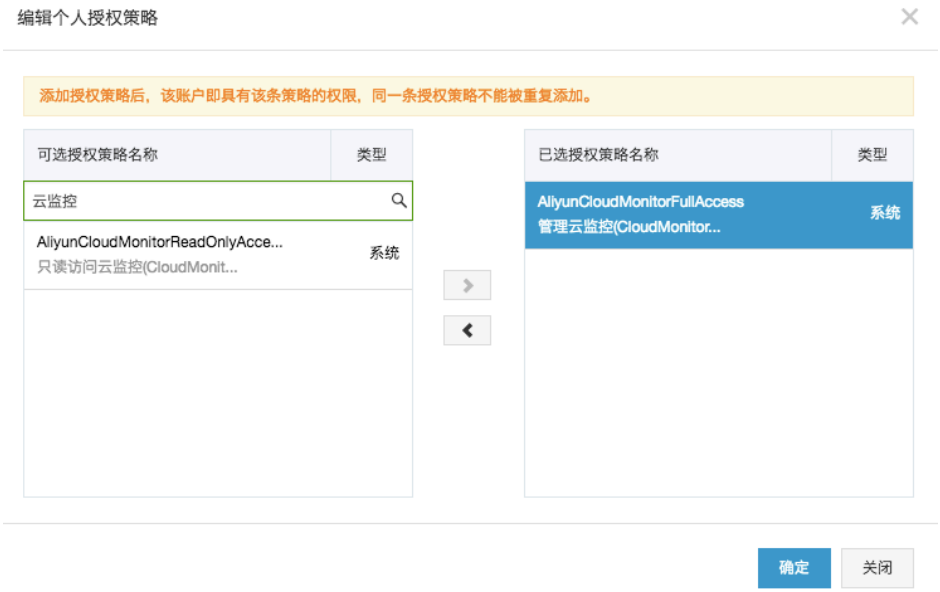
子账号授权说明

使用子账号的AK上报事件数据时，需要对相应子账号授权云监控管理权限。如果子账号未授权云监控管理权限，上报数据时会提示“cannot upload event, please use ram to auth”。

授权步骤如下：

1. 登录访问控制RAM控制台。
2. 进入**用户管理** 菜单。
3. 选择需要上报数据的子账号，在操作中点击**授权** 。

4. 在授权页面中选择**管理云监控**的权限，并点击**确定**保存授权。



签名算法

签名API请求

第一步：准备可用的阿里云访问秘钥

给 API 请求生成签名，需使用一对访问秘钥（AccessKeyId/AccessKeySecret)。您可以使用已经存在的访问秘钥对，也可以创建新的访问秘钥对，但需要保证使用的秘钥对处在“启用”状态。

第二步： 生成请求的签名字符串

API 签名字符串由 HTTP 请求中的 Method，Header 和 Body 信息一同生成，具体方式如下：

```
SignString = VERB + "\n"
+ CONTENT-MD5 + "\n"
+ CONTENT-TYPE + "\n"
+ DATE + "\n"
+ CanonicalizedHeaders + "\n"
+ CanonicalizedResource
```

上面公式中的\n 表示换行转义字符，+（加号）表示字符串连接操作，其他各个部分定义如下：

名称	定义	示例
VERB	HTTP 请求的方法名称	PUT、GET、POST 等
CONTENT-MD5	HTTP 请求中 Body 部分的 MD5 值（必须为大写字母串）	875264590688CA6171F6228AF5BBB3D2
CONTENT-TYPE	HTTP	请求中 Body 部分的类型 application/json
DATE	HTTP请求中的标准时间戳头（遵循 RFC 1123 格式，使用 GMT 标准时间）	Mon, 3 Jan 2010 08:33:47 GMT
CanonicalizedHeaders	由 HTTP 请求中以 x-cms 和 x-acs为前缀的自定义头构造的字符串	x-cms-api-version:0.1.0\nx-cms-signature
CanonicalizedResource	由 HTTP 请求资源构造的字符串（具体构造方法见下面详述）	/event/custom/upload

CanonicalizedHeaders 的构造方式如下：

1. 将所有以x-cms和 x-acs 为前缀的 HTTP 请求头的名字转换成小写字母；
2. 将上一步得到的所有 CMS自定义请求头按照字典序进行升序排序；
3. 删除请求头和内容之间分隔符两端出现的任何空格；
4. 将所有的头和内容用 \n 分隔符组合成最后的 CanonicalizedHeaders。

CanonicalizedResource 的构造方式如下：

1. 将 CanonicalizedResource 设置为空字符串（” ”）；
2. 放入要访问的URI,如/event/custom/upload
3. 如请求包含查询字符串（QUERY_STRING），则在 CanonicalizedResource 字符串尾部添加？ 和查询字符串。

其中QUERY_STRING 是 URL 中请求参数按字典序排序后的字符串，其中参数名和值之间用= 相隔组成字符串，并对参数名-值对按照字典序升序排序，然后以 & 符号连接构成字符串。其公式化描述如下：

```
QUERY_STRING = "KEY1=VALUE1" + "&" + "KEY2=VALUE2"
```

第三步 生成请求的数字签名

目前，事件上报只支持一种数字签名算法，即默认签名算法 hmac-sha1。其整个签名公式如下：

```
Signature = base16(hmac-sha1(UTF8-Encoding-Of(SignString)，AccessKeySecret))
```

请求头定义

事件监控接口的请求头定义如下：

Header	类型	说明
Authorization	字符串	内容：acckeyid:signString
User-Agent	字符串	客户端说明
Content-MD5	字符串	请求 Body 经过 MD5 计算后的字符串，计算结果为大写。如果没有 Body 部分，则不需要提供该请求头。
Content-Length	数值	RFC 2616 中定义的 HTTP 请求 Body 长度。如果请求无 Body 部分，则不需要提供该请求头。
Content-Type	字符串	只支持application/json
Date	字符串	HTTP 请求中的标准时间戳头（遵循 RFC 1123 格式，使用 GMT 标准时间）Mon, 3 Jan 2010 08:33:47 GMT
Host	string	HTTP 请求的完整 HOST 名字（不包括如 https:// 这样的协议头）。例如，metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version	string	api版本 ，当前: 1.0
x-cms-signature	string	签名算法，当前：hmac-sha1
x-cms-ip	string	上报事件的机器ip，10.1.1.1

事件监控最佳实践

应用场景

服务在运行过程中，难免出现异常情况，有些异常通过重试等手段可以自动恢复，有些则不能，严重异常甚至会中断客户业务。所以我们需要一个系统来记录这些异常，并且在满足特定的条件时触发报警。传统方法是打印文件日志，通过收集日志到特定的系统，例如开源的ELK(ElasticSearch, Logstash, Kibana)中。 这些开源的系统往往是由多个复杂的分布式系统组成，自行维护面临着技术门槛高、成本高的问题。 云监控提供了一个事件监控功能，能很好解决这些问题。

下面通过几个例子简单说明下如何使用事件监控功能。

实战案例

第一步：上报异常

事件监控提供了JAVA SDK和Open API两种上报数据的方式，这里介绍通过JAVA SDK 上报数据。

Step1 添加 Maven 依赖

```
<dependency>
<groupId>com.aliyun.openservices</groupId>
<artifactId>aliyun-cms</artifactId>
<version>0.1.2</version>
</dependency>
```

Step2 初始化SDK

```
// 这里的118代表云监控的应用分组ID，可以以应用的角度来对事件归类, 可以到云监控应用分组列表中查看分组的ID。
CMSClientInit.groupId = 118L;

// 这里的地址是事件系统上报的入口，目前是公网地址。accesskey和secretkey用于身份识别。
CMSClient c = new CMSClient("https://metrichub-cms-cn-hangzhou.aliyuncs.com", accesskey, secretkey);
```

Step3 考虑是否异步上报数据

云监控事件默认提供了同步的上报策略。 好处是编写代码简单、 保证每次上报事件的可靠，不丢失数据。

但是同步策略也带来一些问题。因为要在业务代码中嵌入事件上报代码，如果网络出现波动，可能会出现阻塞代码执行，影响正常的业务。有很多业务场景并不需要100%要求事件可靠不丢，所以我们需要一个简单的异步上报封装。将事件写到一个LinkedBlockingQueue中，然后通过ScheduledExecutorService异步在后台批量

上报。

```
//初始化queue与Executors：
private LinkedBlockingQueue<EventEntry> eventQueue = new LinkedBlockingQueue<EventEntry>(10000);
private ScheduledExecutorService schedule = Executors.newSingleThreadScheduledExecutor();

//上报事件：
//每一个事件都包含事件的名称与事件的内容，名称用于识别事件，内容是事件的详细信息，支持全文搜索。
public void put(String name, String content) {
EventEntry event = new EventEntry(name, content);

// 这里事件队列满后将直接丢弃，可以根据自己的情况调整这个策略。
boolean b = eventQueue.offer(event);
if (!b) {
logger.warn("事件队列已满，丢弃事件：{}", event);
}
}

//异步提交事件，初始化定时任务，每秒执行run方法批量上报事件。可以根据自己的情况调整上报间隔。
schedule.scheduleAtFixedRate(this, 1, 1, TimeUnit.SECONDS);

public void run() {
do {
batchPut();
} while (this.eventQueue.size() > 500);
}

private void batchPut() {
// 从队列中取出99条事件，用于批量上报
List<CustomEvent> events = new ArrayList<CustomEvent>();
for (int i = 0; i < 99; i++) {
EventEntry e = this.eventQueue.poll();
if (e == null) {
break;
}
events.add(CustomEvent.builder().setContent(e.getContent()).setName(e.getName()).build());
}
if (events.isEmpty()) {
return;
}


// 批量上报事件到云监控， 这里并未重试， SDK也没有重试， 如果对事件可靠度要求高需要自己加重试策略。
try {
CustomEventUploadRequestBuilder builder = CustomEventUploadRequest.builder();
builder.setEventList(events);
CustomEventUploadResponse response = cmsClient.putCustomEvent(builder.build());
if (!"200".equals(response.getErrorCode())) {
logger.warn("上报事件错误：msg: {}, rid: {}", response.getErrorMsg(), response.getRequestId());
}
} catch (Exception e1) {
logger.error("上报事件异常", e1);
}
}
```

Step4 事件上报Demo

Demo1：http controller的异常监控

主要目的是监控http请求是否有大量异常，如果每分钟异常次数超过一定数量就报警。实现原理是通过spring的拦截器或者servlet filter等技术对HTTP请求拦截，如果出现异常就记录日志，最后通过配置报警规则来达到报警的目的。

上报事件的demo如下：

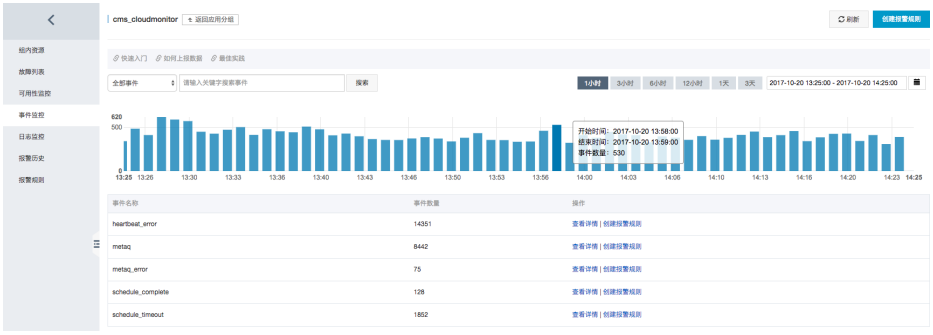
```
// 每个事件应该有丰富的信息来帮助我们搜索和定位问题，这里使用的map来组织事件， 最后转成Json格式作为事件的content。
Map<String, String> eventContent = new HashMap<String, String>();
eventContent.put("method", "GET"); // http 请求方法
eventContent.put("path", "/users"); // http path
eventContent.put("exception", e.getClass().getName()); //异常类名，方便搜索
eventContent.put("error", e.getMessage()); // 异常报错信息
eventContent.put("stack_trace", ExceptionUtils.getStackTrace(e)); // 异常堆栈，方便定位问题

// 最后使用前面封装好的异步上报方法提交事件，这里是异步上报，并且没有重试，可能会小概率丢事件，但是已经能很好的满足http未知异常报警这个场景了。
put("http_error", JsonUtils.toJson(eventContent));

![image.png](http://ata2-img.cn-hangzhou.img-pub.aliyun-inc.com/864cf095977cf61bd340dd1461a0247c.png)
```

Demo2：后台定时任务执行情况的监控与消息消费情况的监控

同上面的http事件，有很多类似的业务场景需要报警，例如后台任务与消息队列消费等，都可以通过类似的方式上报事件达到监控的目的。当异常发生时，第一时间收到报警。

```
//消息队列的事件组织：

Map<String, String> eventContent = new HashMap<String, String>();
eventContent.put("cid", consumerId); // 代表消费者的身份
eventContent.put("mid", msg.getMsgId()); // 消息的id
eventContent.put("topic", msg.getTopic()); // 消息的主题，
eventContent.put("body", body); // 消息的主体
eventContent.put("reconsume_times", String.valueOf(msg.getReconsumeTimes())); // 消息失败重试的次数
eventContent.put("exception", e.getClass().getName()); // 发生异常时的异常类名
eventContent.put("error", e.getMessage()); // 异常信息
eventContent.put("stack_trace", ExceptionUtils.getStackTrace(e)); // 异常堆栈

// 最后上报事件
put("metaq_error", JsonUtils.toJson(eventContent));
```

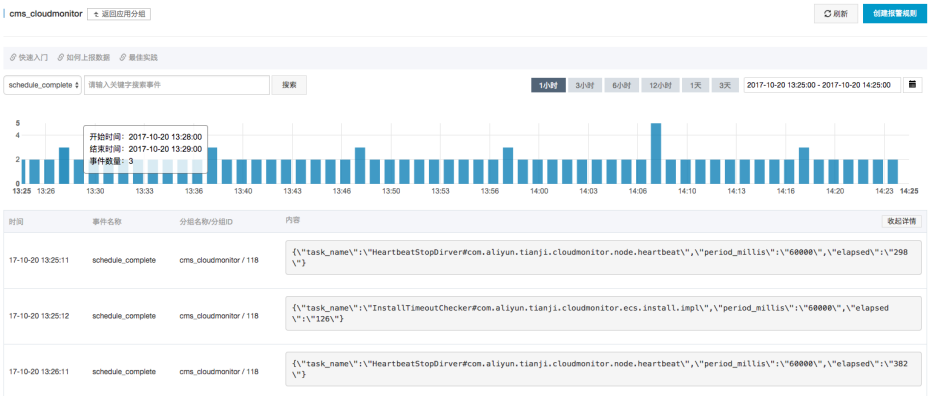
上报后查看事件：



对队列消息消费异常设置报警：

Demo 3：记录重要事件

事件还有一种使用场景是用来记录一些重要的业务发生，但是不需要报警，方便日后翻看。 例如重要业务的操作日志，改密码，修改订单，异地登录等。



云产品系统事件监控

概览

系统事件监控为用户提供各类云产品产生的系统事件的统一统计和查询入口，使得用户明确知晓云产品的使用

状态，让云更透明。

通过应用分组进行资源分类后，产品产生的系统事件会自动与组中资源关联，帮助您做各类监控信息的信息集成，方便您的业务出现问题时，快速分析、定位问题。

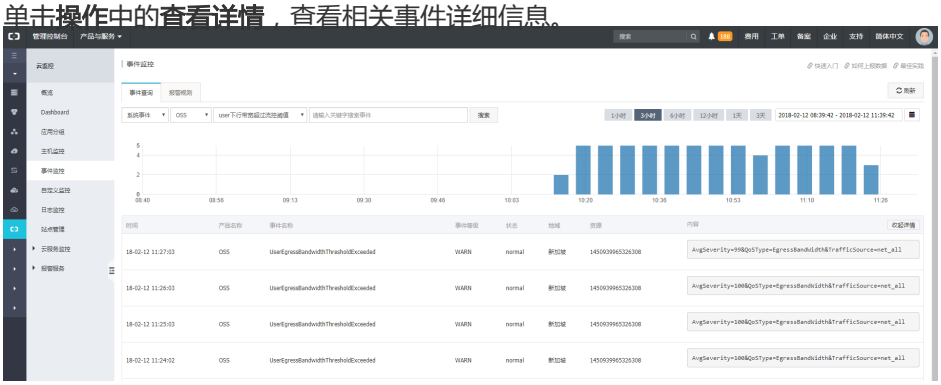
同时提供事件的报警功能，用户可以根据事件等级配置报警，通过短信、邮件、钉钉等接收通知或设置报警回调。使得用户第一时间知晓严重事件并及时处理，形成线上自动化运维闭环。

查看系统事件

方式一

1. 登录云监控控制台，进入**事件监控**页面。
2. 过滤框选择**系统事件**，查看指定时间内发生的事件。

3. 单击**操作**中的**查看详情**，查看相关事件详细信息。



方式二

如果您的实例通过应用分组进行归类管理，您还可以进入具体的应用分组查看分组内相关实例的系统事件。

1. 登录云监控控制台，进入**应用分组**页面。
2. 选择进入分组的详情页面，选择菜单中的**事件监控**。
3. 页面中展示的系统事件即为该分组中实例相关的系统事件。

设置报警

所有系统事件均可以配置报警规则，当事件发生时及时通知您。设置方法如下：

1. 进入系统事件页面，单击相应事件的**创建报警规则**操作，进入创建报警规则页面。

2. 选择需要接收的事件信息和联系人。选择联系人时，对应联系人会收到云账号下所有实例产生的事件。选择应用分组时，应用分组关联的联系人会收到组内实例产生的事件。

支持的云产品系统事件

SLB系统事件

事件名称	事件含义	事件等级
CertKeyExpired_1	证书将在1天后到期	WARN
CertKeyExpired_3	证书将在1天后到期	WARN
CertKeyExpired_7	证书将在1天后到期	WARN
CertKeyExpired_15	证书将在1天后到期	WARN
CertKeyExpired_30	证书将在1天后到期	WARN
CertKeyExpired_60	证书将在1天后到期	WARN

OSS系统事件

事件名称	事件含义	事件等级
BucketEgressBandwidth	bucket下行带宽超过汇报阈值	INFO
BucketEgressBandwidthThresholdExceeded	bucket下行带宽超过流控阈值	WARN

BucketIngressBandwidth	bucket上行带宽超过汇报阈值	INFO
BucketIngressBandwidthThresholdExceeded	bucket上行带宽超过流控阈值	WARN
UserEgressBandwidth	user下行带宽超过汇报阈值	INFO
UserEgressBandwidthThresholdExceeded	user下行带宽超过流控阈值	WARN
UserIngressBandwidth	user上行带宽超过汇报阈值	INFO
UserIngressBandwidthThresholdExceeded	user上行带宽超过流控阈值	WARN

可用性监控

管理可用性监控

应用场景

可用性监控为您定期探测本地或远程指定路径或端口是否正常响应，当出现响应超时或状态码错误时，发送报警通知。帮您快速发现本地或依赖的远程服务无响应的情况。

注意事项

- 使用可用性监控功能依赖云监控插件，使用该功能需要确保机器已安装云监控插件。
- 监控频率为每分钟1次。

创建可用性监控

- 登录云监控**控制台**，选择页面左侧菜单的**应用分组**，进入应用分组页面。
- 选择需要创建可用性监控的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的**可用性监控**，进入可用性监控管理页面。
- 点击页面右上角的新建配置按钮，进入编辑页面。
- 选择探测源，可以为分组内的所有机器配置相同的探测规则，也可以只为部分机器配置相同的探测规则。
- 选择探测类型和探测目标：支持URL/IP、RDS、OSS、Redis。选择RDS、Redis时会显示您分组中的

相关实例和访问地址。

- 选择HTTP协议探测时，支持配置HEAD、GET、POST请求方法和返回值的匹配内容。

- 选择报警配置，报警支持状态码和响应时间两种配置，任何一种配置达到阈值后都会触发报警。报警会发送给应用分组的联系人组。
  - 状态码报警：探测的状态码满足报警设置时就触发报警。
  - 通知方式：报警通知的发送渠道。
  - 高级配置：支持通道沉默时间和生效时间两种配置。通道沉默时间是指报警发生后如果未恢复正常，间隔多久重复发送一次报警通知。生效时间是指报警规则的生效时间，只会在生效时间内检查监控数据是否需要报警。

查看可用性监控任务

- 登录云监控**控制台**，选择页面左侧菜单的**应用分组**，进入应用分组页面。
- 选择需要查看可用性监控的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的**可用性监控**，进入可用性监控的页面。
- 列表中显示了应用分组中所有可用性监控的任务。

查看监控结果

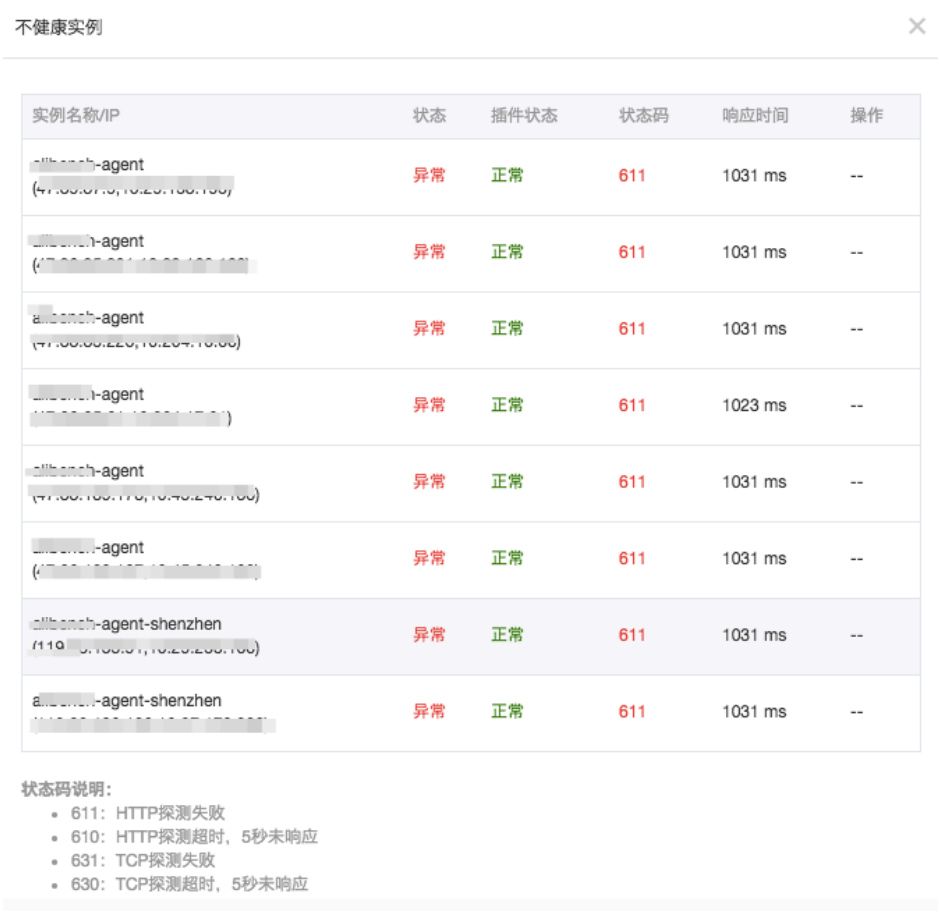
- 登录云监控**控制台**，选择页面左侧菜单的**应用分组**，进入应用分组页面。
- 选择需要查看可用性监控的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的**可用性监控**，进入可用性监控的页面。

列表中可以查看监控结果。

当任务探测未发生报警时，列表中异常机器数为0。

当探测异常发生报警时，列表中会显示发生报警的机器数量，点击异常数量可以查看异常机器详情。

- 异常详情：



修改可用性监控任务

- 登录云监控**控制台**，选择页面左侧菜单的**应用分组**，进入应用分组页面。
- 选择需要修改可用性监控的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的**可用性监控**，进入可用性监控的管理页面。
- 选择需要修改的任务，在操作中点击修改，进入修改页面。
- 在修改页面编辑内容并保存配置。

查看报警历史

- 登录云监控**控制台**，选择页面左侧菜单的**应用分组**，进入应用分组页面。
- 选择需要查看报警历史的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的**报警历史**，进入报警历史页面查看报警历史详情。

启用或禁用监控任务

本地健康检查支持对探测任务进行启用或禁用，禁用后任务不再进行健康检查和报警，启用后任务重新开始探测并在符合报警规则设置时触发报警。

- 登录云监控控制台，选择页面左侧菜单的**应用分组**，进入应用分组页面。
- 选择需要启用或禁用可用性监控的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的**可用性监控**，进入可用性监控的任务管理页面。
- 选择需要启用或禁用的任务，在操作中点击启用或禁用来修改任务状态。

本地服务可用性监控

目的

当您的业务上线对外提供服务后，如何监控服务进程是否存活，有无正常响应？本教程的目的就是举例说明如何监控本地服务进程可用性，当出现响应超时或状态码错误时，发送报警通知。

实战案例

注意事项

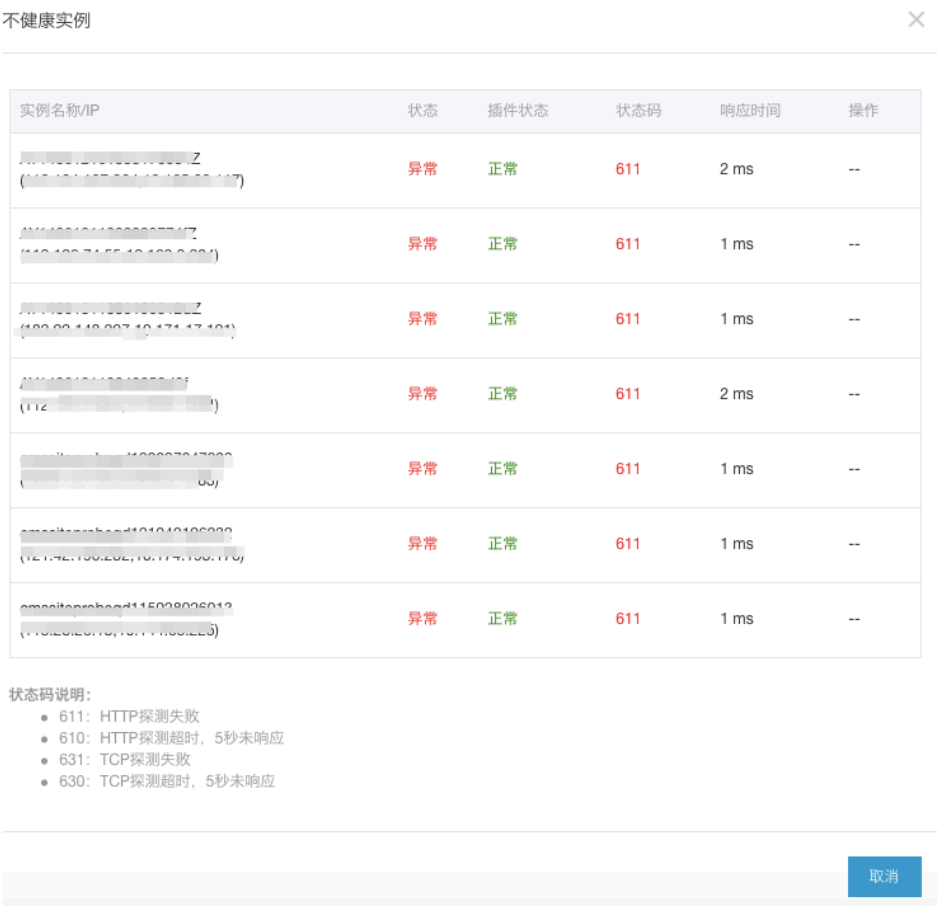
- 使用该功能依赖云监控插件，使用该功能需要确保机器已安装云监控插件。
- 可用性探测频率为每分钟1次。
- 使用该功能前请先创建应用分组。

使用步骤

- 登录云监控控制台，选择页面左侧菜单的应用分组，进入应用分组页面
- 选择需要创建本地服务可用性监控的应用分组，点击应用分组名称，进入应用分组详情页面。
- 选择页面左侧菜单的可用性监控，进入可用性监控页面。
- 点击页面右上角的新建配置按钮，进入编辑页面。
- 选择探测源：即探测的发起方，本地服务可用性探测源和探测目标都是机器本身。
- 选择探测类型：选择URL或IP
- 探测目标：HTTP协议填写格式为“localhost:port/path”，Telnet协议填写格式为“127.0.0.1:port”。比如要探测mysql的连通性，选择Telnet后填写“127.0.0.1:3306”，探测的tomcat是否响应正常，选择HTTP后填写“localhost:8080/monitor”
- 选择报警配置，报警支持状态码和响应时间两种配置，任何一种配置达到阈值后都会触发报警。报警会发送给应用分组的联系人组。本地可用性监控配置状态码大于400即可。
    - 状态码报警：探测的状态码满足报警设置时就触发报警。
    - 通知方式：报警通知的发送渠道。
    - 高级配置：支持通道沉默时间和生效时间两种配置。通道沉默时间是指报警发生后如果未恢复正常，间隔多久重复发送一次报警通知。生效时间是指报警规则的生效时间，只会在生效时间内检查监控数据是否需要报警。可根据实际情况自行配置。

完成以上配置并保存，就完成一个本地服务可用性监控的创建。当您的服务无响应时会发出短信、邮件等报警通知，列表中会显示发生报警的机器数量，点击异常数量可以查看异常机器详情。

点击探测异常机器数，显示异常机器详情。



探测状态码说明

可用性探测在探测异常时会返回自定义状态码，状态码说明如下

协议类型	状态码	含义
HTTP	610	超时。发出HTTP请求后5秒内没有响应，视为超时
HTTP	611	探测失败
Telnet	630	超时，5秒内没有响应，视为超时
Telnet	631	探测失败

日志监控

日志监控概览

在企业级的业务运维和运营场景中， 日志正扮演着越来越重要的角色。业务日志的简单本地化存储，很难挖掘日志背后真正的数据价值。将日志存储到集中的服务端后，将其处理成指导运维、指导运营的指标，成为企业日益迫切的需求。

面临的困难

虽然日志处理、可视化和报警是很多业务都迫切需要的，但是将日志处理成真正有价值的数据，却决非易事。比如以下问题：

- 日志格式的多样性，数据采集处理的逻辑复杂
- 海量日志数据的分析能力
- 处理结果的存储
- 数据的可视化
- 与报警服务的打通、自动化运维的实现
- 与服务器等基础监控数据的整合

一般来说，基于日志的监控分析服务，需要解决以上所有问题，才能形成业务闭环，完美解决企业的监控运维与运营诉求。

传统架构

日志监控的经典方案是ELK，相信大家都不陌生。ELK是成熟的日志监控方案，有着配置简单，前端展示绚丽，开源等诸多特点。 但ELK对一般企业来讲投入成本依然比较大：

- 架构、技术栈复杂，开发运维成本高。
- 只能解决日志监控中的一部分问题。无法解决报警、数据整合等其他重要需求。

日志监控解决方案

鉴于ELK投入成本大，但企业日常的日志处理场景大都比较简单，比如

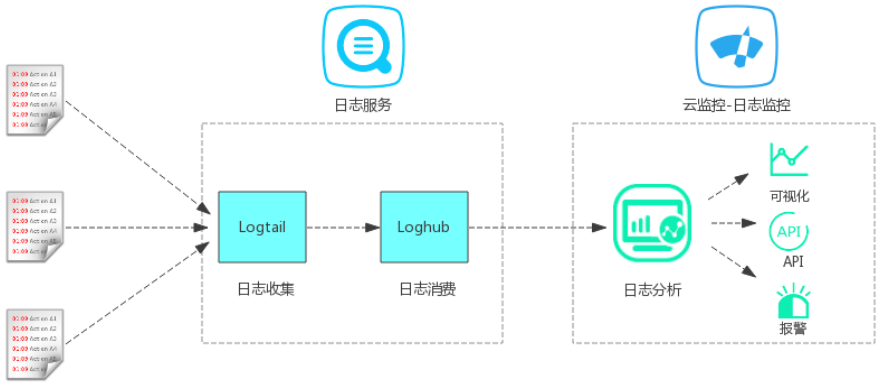
- 对日志中的关键字报警
- 统计单位时间内的QPS、RT
- 统计单位时间内的PV、 UV

传统的企业用户如果使用传统架构去解决这些常用的简单需求，投入大量时间和人力搭建庞大的攻城武器、付出沉重的运维成本，确实有些得不偿失。

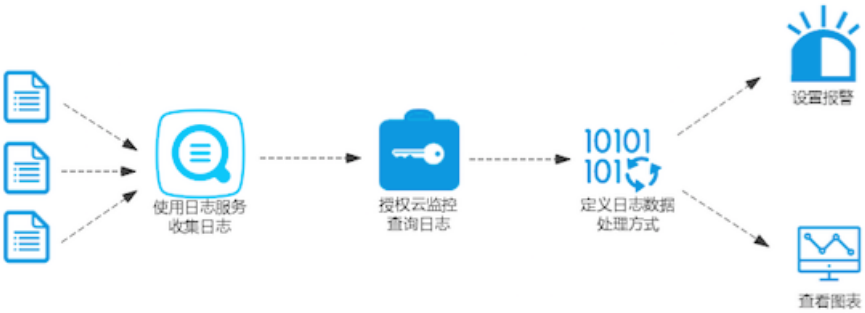
针对上述问题，阿里云监控和日志服务结合， 推出了非常轻量级，但全面、易用的解决方案-日志监控。

云监控-日志监控的目标，是将复杂的传统日志监控功能实现，转化为鼠标的几次轻轻点击。

日志监控闭环



使用流程概览



1. 通过日志服务收集日志，日志服务介绍。
2. 授权日志给云监控可读权限，查询您的日志。
3. 使用日志监控定义监控指标的日志数据处理方式。
4. 为监控指标设置报警规则、定义图表展示(可选)。

我们的优势

- 简单易用、好上手。
- 免开通，随时用（只需要开通日志服务，将本地log收集日志服务），复杂的底层技术细节对您全透明。
- 完美结合云监控的主机监控、云服务监控、站点监控、应用分组、Dashboard、报警服务，形成完整的监控闭环。提供您一个完整统一的视角，洞悉关于监控的一切。
- 基于阿里云Apsara Monitor服务，给您稳定可靠的体验。
- 全SaaS服务，几乎无运维成本。
- 成本优势：几乎无时间和人力成本，帮您更快速的完成日志监控需求。

管理日志监控

您可以在日志监控中对监控项进行创建、查看、修改、删除操作。

创建日志监控

创建日志监控用于定义日志数据如何处理，监控项是否归属于应用分组。

参数说明

以下为新建日志监控页面的参数说明：

分组名称：应用分组的名称。可以将监控项添加到具体的应用分组中。

关联资源：选择处理的日志服务数据源。

地域：日志服务的地域。

日志 Project：日志服务的 Project。

日志 Logstore：日志服务的 Logstore。

分析日志：定义日志服务如何分析日志数据。

监控项名称：定义一个监控指标的名称。

统计方法：指在统计周期内如何计算日志数据的函数方法。包括求和、求最大值、求最小值、求平均值、sumps、countps、求P50、求P75、求P90、求P95、求P98、求P99。

- 求和：计算1分钟内指定字段数值之和。
- 求最大值：计算统计周期内指定字段数值的最大值。
- 求最小值：计算统计周期内指定字段数值的最小值。
- 求平均值：计算统计周期内指定字段数值的平均值。
- countps：计算统计周期内指定字段求count后的每秒平均值。
- sumps：计算统计周期内指定字段求sum后的每秒平均值。
- distinct：去重后计算统计周期内指定字段出现的次数。
- 求P75：计算1分钟内指定字段的第75百分位数。以统计 rt的Percentile75结果为30ms为例，表示75% 的请求rt小于30ms。
- 分布：计算一个周期内指定范围的日志条数，比如统计1分钟内HTTP请求为5XX的状态码个数，则定义为 (499,599]。统计方式为左开右闭。

扩展字段：扩展字段为统计方法中的结果提供四则运算的功能。例如在统计方法中配置了HTTP状态码请求总数TotalNumber、HTTP状态码大于499的请求书5XXNumber，则可以通过扩展字段计算出服务端错误率：5XXNumber/TotalNumber*100。

日志筛选：相当于 SQL 中的 where 条件。不填写则表示对全部数据进行处理。假设日志中有 **level：Error** 字段，需要统计每分钟 **Error** 出现的次数，则统计方法可以定义为对level求和，并且level=Error。

Group-by：对数据进行空间维度聚合，相当于 SQL 中的 Group By，根据指定的维度，对监控数据进行分组。如果 Group By 不选择任何维度。则根据聚合方法对全部监控数据进行聚合。

Select SQL：将上述分析方式转化成类 SQL 语句，方便您理解数据的处理方式。

操作步骤

登录云监控，进入**日志监控页面**。

点击页面右上角的**新建日志监控**，进入新建日志监控页面。

选择关联资源。

定义日志数据的分析方式。点击预览可以查看最近的统计结果做参考。

（可选）快速创建报警规则，默认发送邮件。

（可选）将监控项添加到某个应用分组中管理。

查看日志监控

这里指查看日志的监控项，如需查看处理后的监控数据，可参考查看监控数据

登录云监控，进入日志监控页面。

可以在列表中查看监控项的日志数据源、筛选和统计方法定义等信息。

修改日志监控

修改监控项定义时，可以查看以下步骤：

登录云监控，进入日志监控页面。

选择需要修改的监控项名称，点击 **编辑** 按钮，进入编辑页面。

参考创建日志监控步骤，对需要修改的参数进行修改。

删除日志监控

删除监控项定义时，可以查看以下步骤。监控项删除后，仍然可以通过 API 查询到删除时间点之前的监控数据。

登录云监控，进入日志监控页面。

选择需要修改的监控项名称，点击**删除**按钮，将指定监控项删除。

查看监控数据

定义好日志监控的监控项后，云监控提供3种方式查看监控数据：

在日志监控的监控项图表页直接查看。

在应用分组中添加日志监控的图表。

在 Dashboard 中添加日志监控的图表(敬请期待)。

直接查看监控数据

登录云监控，进入**日志监控**页面。

选择需要查看数据的监控项，单击监控项名称或操作中的**监控图表**。即可进入监控详情页面查看监控数据。

添加日志监控数据到应用分组

在应用分组中添加日志监控图表前，请先将对应监控项添加到日志分组中。以下是对一个应用分组添加日志监控图表的步骤：

登录云监控，进入**应用分组**，选择需要添加监控图表的分组后，进入分组详情页面。

单击页面中**监控图表**部分的**添加监控图表**按钮，进入添加监控图表页面。

在页面中选择日志监控的相关信息后单击**保存**，即完成监控图表的添加。

授权日志监控

主账号授权日志监控授权

使用日志监控功能时，需要授权云监控查询您日志服务的权限，授权方法请参考以下步骤。

1. 登录云监控控制台, 进入日志监控页面。如果主账号没有授权过云监控访问您日志服务的权限，会提示“您尚未授权云监控读取您的日志，请点击进行授权”。
2. 点击授权后进入授权页面，点击“**同意授权**”后，完成授权。

子账号使用日志监控

子账号授权日志监控

子账号如需授权云监控读取日志服务数据，需要具备以下权限：

- 云监控只读（AliyunCloudMonitorReadOnlyAccess）或读写（AliyunCloudMonitorFullAccess）权限。
- 管理访问管理服务(RAM)的（AliyunRAMFullAccess ）权限。

拥有以上条件后，子账号便可向主账号一样对日志监控进行授权，授权过程同主账号一致。

子账号使用日志监控功能

- 管理日志监控(查看、新建、修改等操作)：需要授权云监控读写（AliyunCloudMonitorFullAccess）权限和日志服务的只读（AliyunRAMFullAccess）权限。
- 查询日志监控数据：只需要授权云监控只读权限（AliyunCloudMonitorReadOnlyAccess）即可。

日志监控常见问题排查

1. 创建监控成功，但是监控图表没有数据

- 请检查AccessKey是否已经激活。可参考业务日志的统计监控与报警文档的“使用前提”相关介绍。
- 请点击日志监控列表对应监控项的“编辑”按钮，在“SQL”中，查看生成的SQL是否包含中文，SQL中不能包含中文。
- 请确保设置的统计方法、日志筛选条件能匹配上日志数据，可以点击日志监控列表对应监控项的“编辑”按钮，在日志预览中查看是否有匹配的日志数据（展示最近1小时内的最近100条数据），或者登陆“日志服务”控制台，查询更长时间内是否有匹配的日志数据。

2. 报警数据不足

- 请依照问题1检查监控图是否有数据，如果图表没有数据，报警规则会出现“数据不足”现象。

3. 监控数据达到阈值，但是没有收到报警

- 检查报警通知是否进入通道沉默。一条报警发出后，如果这个异常在24小时之内未被处理，则24小时

内不会再次触发报警。

4. 创建日志监控时页面报错

创建日志监控时页面弹出如下错误，是因为没有激活AccessKey，可参考业务日志的统计监控与报警文档的“使用前提”相关介绍激活AccessKey。

云服务监控

云数据库RDS监控

关系型数据库RDS监控

概览

云监控通过监控 RDS 的磁盘使用率、IOPS 使用率、连接数使用率、CPU 使用率等监控指标，让您一目了然的了解 RDS 的运行状态。用户购买 RDS 产品后，云监控会自动对上述四个监控项收集数据，无需其他操作。

注意事项

RDS 只有主实例和只读实例提供监控和报警服务。

云监控会默认为每个主实例和只读实例创建报警规则。内容分别是 CPU 使用率>80%，连接数使用率>80%，IOPS 使用率>80%，磁盘使用率 >80%。超过阈值时会短信和邮件通知云账号联系人。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
磁盘使用率	数据库实例中磁盘空间的使用百分率	实例	百分比	5分钟
IOPS使用率	数据库实例的每秒IO请求次数	实例	百分比	5分钟
连接数使用率	连接数是指应用程序可以连接到RDS实例的数量。连接数使用率即已经使用的连接数百分率	实例	百分比	5分钟
CPU使用率	实例对CPU的使用率，数据库内存的大小决定CPU的性能	实例	百分比	5分钟
内存使用率	数据库实例中内存的已用占比，目前只有MySQL类型数据库支持内存实例率	实例	百分比	5分钟
只读实例延迟	Mysql只读实例延迟时间	实例	秒	5分钟
网络入流量	实例每秒钟的输入流量	实例	bits/s	5分钟
网络出流量	实例每秒钟的输出流量	实例	bits	5分钟
实例故障	事件类型指标，可设置报警规则	-	-	-
实例主备切换	事件类型指标，可设置报警规则	-	-	-

备注：网络入流量和网络出流量仅支持 MySQL 和 SQLServer 数据库类型。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**云数据库 RDS**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：RDS 提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为 1 分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

a. 平均值：统计周期内监控数据的平均值。统计结果是 15 分钟内采集的所有监控数据的平均值，当这个平均值大于 80% 时，才算超过阈值。

b. 最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过 80%，即为超过阈值。

c. 最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过 80%，即为超过阈值。

d. 求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过 80% 即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 RDS** 实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

负载均衡监控

负载均衡 Sever Load Balancer 监控

云监控通过监控 Sever Load Balancer 的流入流量、流出流量等 7 个监控项，为用户展示 Sever Load Balancer 的运行状态，帮助用户监测实例的运行状态，并支持用户对监控项设置报警规则。用户创建 Sever Load Balancer 实例后云监控会自动对上述监控项收集数据。

监控服务

监控项说明

4层协议监控项：

监控项	含义	维度	单位	最小监控粒度
端口流入流量	从外部访问 Sever Load Balancer 指定端口所需要消耗的流量	端口	bit/s	1分钟
端口流出流量	Sever Load Balancer 指定端口访问外部所需要消耗的流量	端口	bit/s	1分钟
端口流入数据包数	Sever Load Balancer 指定端口每秒接到的请求数据包数量	端口	Count/Second	1分钟
端口流出数据包数	Sever Load Balancer 指定端口每秒发出的数据包数量	端口	Count/Second	1分钟
端口新建连接数	统计周期内平均每秒 TCP 三次握手的第一次 SYN_SENT 状态	端口	Count	1分钟

	的数量			
端口活跃连接数	当时所有ESTABLISHED状态的连接	端口	Count	1分钟
端口非活跃连接数	指除ESTABLISHED状态的其他所有状态的当时tcp连接数	端口	Count	1分钟
端口并发连接数	端口当时连接数总量(活跃连接数和非活跃连接数之和)	端口	Count	1分钟
后端健康ECS实例个数	健康检查正常实例数	端口	Count	1分钟
后端异常ECS实例个数	健康检查异常实例数	端口	Count	1分钟
端口丢弃连接数	端口平均每秒丢弃的连接数	端口	Count/Second	1分钟
端口丢弃流入数据包数	端口平均每秒丢失的流入包数	端口	Count/Second	1分钟
端口丢弃流出数据包数	端口平均每秒丢失的流出包数	端口	Count/Second	1分钟
端口丢弃流入流量	端口平均每秒丢失的入流量	端口	bit/s	1分钟
端口丢失流出流量	端口平均每秒丢失的出流量	端口	bit/s	1分钟
实例活跃连接数	实例当时所有ESTABLISHED状态的连接	实例	Count/Second	1分钟
实例非活跃连接数	实例当时除ESTABLISHED状态的其他所有状态tcp连接数	实例	Count/Second	1分钟
实例丢弃连接数	实例每秒丢弃的连接数	实例	Count/Second	1分钟
实例丢弃流入数据包数	实例每秒丢弃的流入数据包数量	实例	Count/Second	1分钟
实例丢弃流出数据包数	实例每秒丢弃的流出数据包数量	实例	Count/Second	1分钟
实例丢弃流入流量	实例每秒丢弃的流入流量	实例	bit/s	1分钟
实例丢弃流出流量	实例每秒丢弃的流出流量	实例	bit/s	1分钟

实例最大并发连接数	实例当时连接数总量(活跃连接数和非活跃连接数之和)	实例	Count/Second	1分钟
实例新建连接数	实例统计周期内平均每秒TCP三次握手的第一次SYN_SENT状态的数量	实例	Count/Second	1分钟
实例流入数据包数	实例每秒接到的请求数据包数量	实例	Count/Second	1分钟
实例流出数据包数	实例平均每秒发出的数据包数量	实例	Count/Second	1分钟
实例流入流量	从外部访问Sever Load Balancer 实例所需要消耗的流量	实例	bit/s	1分钟
实例流出流量	Sever Load Balancer 实例访问外部所需要消耗的流量	实例	bit/s	1分钟

七层协议监控项：

监控项	含义	维度	单位	最小监控粒度
端口QPS	监听维度的QPS	端口	Count/Second	1分钟
端口RT	端口维度的请求平均延时	端口	ms	1分钟
端口2xx 状态码个数	端口维度的slb返回给client的2xx状态码统计	端口	Count/Second	1分钟
端口3xx 状态码个数	端口维度的slb返回给client的3xx状态码统计	端口	Count/Second	1分钟
端口4xx 状态码个数	端口维度的slb返回给client的4xx状态码统计	端口	Count/Second	1分钟
端口5xx 状态码个数	端口维度的slb返回给client的5xx状态码统计	端口	Count/Second	1分钟
端口其他状态码个数	端口维度的slb返回给client的other状态码统计	端口	Count/Second	1分钟
端口Upstream 4xx 状态码个数	端口维度的rs返回给slb的4xx状态码统计	端口	Count/Second	1分钟
端口Upstream	端口维度的rs返	端口	Count/Second	1分钟

5xx 状态码个数	回给client的5xx状态码统计			
端口UpstreamRT	端口维度的rs发给proxy的平均请求延迟	端口	ms	1分钟
实例QPS	实例维度的QPS	实例	Count/Second	1分钟
实例Rt	实例维度的请求平均延时	实例	Count/Second	1分钟
实例2xx 状态码个数	实例维度的slb返回给client的2xx状态码统计	实例	Count/Second	1分钟
实例3xx 状态码个数	实例维度的slb返回给client的3xx状态码统计	实例	Count/Second	1分钟
实例4xx 状态码个数	实例维度的slb返回给client4xx状态码统计	实例	Count/Second	1分钟
实例5xx 状态码个数	实例维度的slb返回给client的5xx状态码统计	实例	Count/Second	1分钟
实例其他 状态码个数	实例维度的slb返回给client的Other状态码统计	实例	Count/Second	1分钟
实例Upstream 4XX状态码个数	实例维度的rs返回给slb的4xx状态码统计	实例	Count/Second	1分钟
实例Upstream 5XX状态码个数	实例维度的rs返回给slb的5xx状态码统计	实例	Count/Second	1分钟
实例Upstream RT	实例维度的rs发给proxy的平均请求延迟	实例	ms	1分钟

注意事项

- 新建连接数、活跃连接数、非活跃连接数统计的均是客户端到 Sever Load Balancer 的 TCP 连接请求。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**负载均衡**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：负载均衡提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是15分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使 用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**负载均衡**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

对象存储OSS监控

OSS 监控服务为用户提供系统基本运行状态、性能以及计量等方面的监控数据指标，并且提供自定义报警服务，帮助用户跟踪请求、分析使用情况、统计业务趋势，及时发现以及诊断系统的相关问题。

监控服务

监控项说明

OSS监控指标分类详细，主要可以归类为基础服务指标、性能指标和计量指标，详细参考OSS监控指标参考手册。

注意事项

为了保持和计费策略的统一，计量指标的收集和展现存在一定的特殊性，如下说明：

计量指标数据是按照小时粒度输出的，即每个小时内的资源计量信息都会聚合成一个值，代表这个小时总的计量情况；

计量指标数据会有近半个小时的延时输出；

计量指标数据的数据时间是指该数据所统计时间区间的开始时间；

计量采集截止时间是当月最后一条计量数据所统计时间区间的结束时间，如果当月没有产生任何一条计量监控数据，那么计量数据采集截止时间为当月1号0点；

计量指标数据的展示都是尽最大可能推送的，准确计量请参考费用中心—使用记录。

举个例子，假设用户只使用PutObject这个请求上传数据，每分钟平均10次。那么在2016-05-10 08:00:00到2016-05-10 09:00:00这一个小时时间区间内，用户的PUT类请求数的计量数据值为600次(10*60分钟)，并且数据时间为2016-05-10 08:00:00，并且这条数据将会在2016-05-10 09:30:00左右被输出。如果这条数据是从2016-05-01 00:00:00开始到现在的最后一条计量监控数据，那么当月的计量数据采集截止时间就是2016-05-10 09:00:00。如果2016年5月该用户没有产生任何的计量数据，那么计量采集截止时间为2016-05-01 00:00:00。

报警服务

注意事项

OSS bucket 全局唯一，如果删掉 bucket 之后再创建同名的bucket，那么被删掉的 bucket 的监控以及报警规则会作用在新的同名 bucket 上。

除计量指标和统计指标，其他的监控指标均可配置为报警规则加入报警监控，并且一个监控指标可以配置为多个不同的报警规则。

使用指南

报警服务相关概念参考报警服务概览。

OSS报警服务使用指南详见OSS报警服务使用指南。

CDN监控

概览

云监控通过监控 CDN 的 QPS、BPS、字节命中率等 9 个监控项，帮助用户获取域名的使用情况。用户添加一个加速域名后，云监控自动开始对其监控，您登录云监控的 CDN 页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警息。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
每秒访问次数	时间粒度内的总	域名	次	1分钟

	访问次数/时间粒度			
网络带宽BPS	单位时间内网络流量的最大值	域名	bps	1分钟
命中率	时间粒度内请求的字节数命中缓存的概率，注“字节=请求数 x traffic”，字节命中率更直接反馈了回源流量	域名	百分比	1分钟
公网网络出流量	即CDN的公网下行流量	域名	字节	5分钟
返回码4xx占比	时间粒度内http返回码4XX占全部返回码的百分比	域名	百分比	1分钟
返回码5xx占比	时间粒度内http返回码5XX占全部返回码的百分比	域名	百分比	1分钟

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**CDN**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：CDN 提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是15分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为5分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期*(连续探测次数-1)=5*(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**CDN**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

弹性公网IP监控

概览

云监控通过监控弹性公网 IP 的流出流量、流入流量、流出数据包数、流入数据包数 4 个监控项，帮助用户监测服务的运行状态，并支持用户对监控项设置报警规则。用户购买弹性公网 IP 服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
网络流入带宽	平均每秒通过EIP流入ECS的流量	实例	bits/s	1分钟
网络流出带宽	平均每秒ECS通过EIP向外流出的流量	实例	bits/s	1分钟
流入数据包数	平均每秒通过EIP流入ECS的数据包数量	实例	packages/s	1分钟
流出数据包数	平均每秒ECS通过EIP向外流出的数据包数量	实例	packages/s	1分钟

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**弹性公网 IP**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：弹性公网 IP 提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用

率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是 15 分钟内采集的所有监控数据的平均值，当这个平均值大于 80% 时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过 80% 即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过80%报警，统计周期为5分钟，连续3次超过阈值后报警，则第一次探测CPU 使用率超过80%时，不会发出报警通知。5分钟后第二次探测CPU使用率超过80%，也不会发出报警。第三次探测仍然超过80%时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期*(连续探测次数-1)=5*(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**弹性公网 IP**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

云数据库Memcache版监控

概览

云监控通过监控云数据库 Memcache 版服务实例的已用缓存、读取命中率等 7 个监控项，帮助用户监测实例的运行状态，并支持用户对监控项设置报警规则。用户购买 Memcache 服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
已用缓存	已经使用的缓存量	实例	字节	1分钟
读取命中率	读取kv成功的概率	实例	百分比	1分钟
QPS	每秒读取kv的总次数	实例	个数	1分钟
记录数	当前kv的总个数	实例	个数	1分钟
缓存输入带宽	访问缓存所产生的流量	实例	Bps	1分钟
缓存输出带宽	读取缓存所产生的流量	实例	Bps	1分钟
逐出	每秒逐出的kv数	实例	个数每秒	1分钟

注意事项

监控数据最多保存31天。

用户最多可连续查看14天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**云数据库 Memcache 版监控**实例列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

单击页面上方的**时间范围**快速选择按钮或精确选择功能。

单击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

云监控为Memcache 的所有监控项提供报警服务，用户对重要监控项设置报警规则后，可以在监控数据超过阈值后及时收到报警通知，从而迅速进行处理，减少故障发生的可能性。

参数说明

- 监控项：云服务器 Redis 版提供的监控指标。
- 统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是15分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 Memcache 版监控**实例列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

单击监控图右上角的**铃铛**按钮，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 Memcache 版监控**实例列表。

实例列表页面选中所需实例后，在页面下方单击**设置报警规则**，即可批量添加报警规则。

云数据库Redis版监控

概览

云监控通过监控 Redis 的已用容量百分比、已用连接数百分比等监控项，帮助用户获取 Redis 的运行状态和使用情况。用户创建 Redis 实例后，云监控自动开始对其监控，您登录云监控的 Redis 页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警息。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
已用容量	当前已使用Redis容量	实例	字节	1分钟
已用连接数	当前客户端连接总数量	实例	个数	1分钟
写入网速	当前每秒写入网络流量	实例	bps	1分钟

读取网速	当前每秒读取网络流量	实例	bps	1分钟
操作失败数	当前操作KVSTORE失败次数	实例	个数	1分钟
已用容量百分比	当前已使用容量占总容量的比例	实例	百分比	1分钟
已使用连接百分比	当前已建立的连接数占总连接的比例	实例	百分比	1分钟
写入带宽使用率	当前写入带宽占总带宽的百分比	实例	百分比	1分钟
读取带宽使用率	当前读取带宽占总带宽的百分比	实例	百分比	1分钟
实例故障	事件类型指标，可设置报警规则	-	-	-
实例主备切换	事件类型指标，可设置报警规则	-	-	-

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**云服务器 Redis 版**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：云服务器 Redis 版提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔 1 分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是 15 分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为5分钟，连续3次超过阈值后报警，则第一次探测 CPU 使用率超过80%时，不会发出报警通知。5分钟后第二次探测 CPU 使用率超过80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**云服务器 Redis 版**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

云数据库 MongoDB 版

概览

云监控通过监控云数据库 MongoDB 版服务实例的 CPU 使用率、内存使用率等多个监控项，帮助用户监测实例的运行状态，并支持用户对监控项设置报警规则。用户购买 MongoDB 服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

监控项	含义	维度	单位	最小监控粒度
CPU使用率	实例的CPU使用率	用户维度、实例维度、主备维度	百分比	5分钟
内存使用率	实例的内存使用率	用户维度、实例维度、主备维度	百分比	5分钟
磁盘使用率	实例的磁盘使用率	用户维度、实例维度、主备维度	百分比	5分钟
IOPS使用率	实例的IOPS使用率	用户维度、实例维度、主备维度	百分比	5分钟
连接数使用率	连接数是指应用程序可以连接到MongoDB实例的数量。连接数使用率即已经使用的连接数百分率	用户维度、实例维度、主备维度	百分比	5分钟
平均每秒SQL查询数	MongoDB实例的平均每秒SQL查询数	用户维度、实例维度、主备维度	个数	5分钟
连接数使用量	当前应用程序连接到MongoDB实例的数量	用户维度、实例维度、主备维度	个数	5分钟
实例占用磁盘空间量	实例实际使用的磁盘空间总量	用户维度、实例维度、主备维度	字节	5分钟
数据占用磁盘空间量	数据占用的磁盘空间容量	用户维度、实例维度、主备维度	字节	5分钟
日志占用磁盘空间量	日志占用的磁盘空间容量	用户维度、实例维度、主备维度	字节	5分钟
内网入流量	实例的网络流入流量	用户维度、实例维度、主备维度	字节	5分钟
内网出流量	实例的网络流出流量	用户维度、实例维度、主备维度	字节	5分钟
请求数	发送到服务端的请求总量	用户维度、实例维度、主备维度	个数	5分钟
Insert操作次数	从MongoDB实	用户维度、实例	个数	5分钟

	例最近一次启动到现在累计接收到的insert命令的次数	维度、主备维度		
Query操作次数	从MongoDB实例最近一次启动到现在累计接收到的query命令的次数	用户维度、实例维度、主备维度	字节	5分钟
Update操作次数	从MongoDB实例最近一次启动到现在累计接收到的update命令的次数	用户维度、实例维度、主备维度	次数	5分钟
Delete操作次数	从MongoDB实例最近一次启动到现在累计执行delete的操作次数	用户维度、实例维度、主备维度	次数	5分钟
Getmore操作次数	从MongoDB实例最近一次启动到现在累计执行getmore的操作次数	用户维度、实例维度、主备维度	次数	5分钟
Command操作次数	从MongoDB实例最近一次启动到现在向数据库发出的command的累计次数	用户维度、实例维度、主备维度	次数	5分钟
实例故障	事件类型指标，可设置报警规则	-	-	-

注意事项

监控数据最多保存31天。

用户最多可连续查看14天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**云数据库 MongoDB 版**实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续 14 天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：云数据库 MongoDB 版提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

a. 平均值：统计周期内监控数据的平均值。统计结果是15分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

b. 最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

c. 最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

d. 求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置CPU使用率超过80%报警，统计周期为5分钟，连续3次超过阈值后报警，则第一次探测CPU使用率超过80%时，不会发出报警通知。5分钟后第二次探测CPU使用率超过80%，也不会发出报警。第三次探测仍然超过80%时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期*(连续探测次数-1)=5*(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 MongoDB 版**实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 MongoDB 版**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

消息服务监控

消息通知服务Message Service监控

概览

云监控通过监控 Message Service 的延迟消息、无效消息、活跃消息3个监控项，帮助用户获取 Message Service 队列的 使用情况。用户创建 Message Service 的消息队列后，云监控自动开始对其监控，您登陆云监控的 Message Service 页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警信息。

监控项说明

监控项	含义	维度	单位	最小监控粒度
ActiveMessages	在该Queue中处于Active状态的消息总数	userId,region,bid,queue	个数	5分钟
InactiveMessages	在该Queue中处于Inactive状态	userId,region,bid,queue	个数	5分钟

	的消息总数			
DelayMessage	在该Queue中处于Delayed状态的消息总数	userId,region,bid,queue	个数	5分钟
SendMessageCount	发送消息请求量	userId,region,queue	个	3600
BatchSendMessageCount	批量发送消息请求量	userId,region,queue	个	3600
ReceiveMessageCount	接收消息请求量	userId,region,queue	个	3600
BatchReceiveMessageCount	批量接收消息请求量	userId,region,queue	个	3600
BatchDeleteMessageCount	批量删除消息请求量	userId,region,queue	个	3600
ChangeMessageVisibilityCount	更改消息可见性计数	userId,region,queue	个	3600

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**消息服务**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：消息服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

a. 平均值：统计周期内监控数据的平均值。统计结果是 15 分钟内采集的所有监控数据的平均值，当这个平均值大于 80% 时，才算超过阈值。

b. 最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

c. 最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

d. 求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80% 即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过80%，也不会发出报警。第三次探测仍然超过80%时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期*(连续探测次数-1)=5*(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**消息服务**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

分析型数据库监控

分析型数据库 Analytic DB监控

概览

云监控通过提供 Analytic DB 的磁盘额定容量、磁盘已用容量、磁盘使用率 3 项信息，帮助用户获取 Analytic

DB 服务的使用情况。用户开通使用 Analytic DB 服务后，云监控自动开始对其监控，您登录云监控的 Analytic DB 页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警息。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
diskSize	磁盘额定容量	instanceId,tableSchema,workerId	兆字节	1分钟
diskUsed	磁盘已用容量	instanceId,tableSchema,workerId	兆字节	1分钟
diskUsedPercent	磁盘使用率	instanceId,tableSchema,workerId	百分比	1分钟

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**分析型数据库**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：分析型数据库提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和

值。

平均值：统计周期内监控数据的平均值。统计结果是15分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**分析型数据库**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

日志服务监控

概览

云监控通过监控日志服务的出入流量、总体 QPS、日志统计方法等 11 个监控项，帮助用户获取日志服务的使

用情况。用户创建日志服务后，云监控自动开始对其监控，您登录云监控的日志服务页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警息。

监控项说明

监控项	含义	维度	单位	最小监控粒度
Inflow	logStore每分钟的流入流量和流出流量	userId、Project、Logstore	字节	1分钟
Outflow	logStore每分钟的流出流量	userId、Project、Logstore	字节	1分钟
SumQPS	logStore每分钟的写入总次数	userId、Project、Logstore	个数	1分钟
LogMethodQPS	logStore中各method下每分钟的写入次数	userId、Project、Logstore、Method	个数	1分钟
LogCodeQPS	logStore中各状态码每分钟的写入次数	userId、Project、Logstore、Status	个数	1分钟
SuccessdByte	logStore中解析成功的字节数	userId、Project、Logstore	字节	10分钟
SuccessdLines	logStore中解析日志成功行数	userId、Project、Logstore	个数	10分钟
FailedLines	logStore中解析日志失败行数	userId、Project、Logstore	个数	10分钟
AlarmPV	logStore中ECS发生配置错误数的总和	userId、Project、Logstore	个数	5分钟
AlarmUv	logStore中发生配置错误数的ECS数量总和	userId、Project、Logstore	个数	5分钟
AlarmIPCount	logStore中各IP发生的错误数量	userId、Project、Logstore、alarm_type、source_ip	个数	5分钟

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**日志服务**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：日志服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是15分钟内采集的所有监控数据的平均值，当这个平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过80%即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置CPU使用率超过80%报警，统计周期为5分钟，连续3次超过阈值后报警，则第一次探测CPU使用率超过80%时，不会发出报警通知。5分钟后第二次探测CPU使用率超过80%，也不会发出报警。第三次探测仍然超过80%时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

注意事项

- 设置报警规则时，日志方法QPS监控项可选择具体的method对应的值，各状态码下QPS可选择具体的status对应的值，如果不选择，会默认作用全部字段。

  method字段包括：PostLogStoreLogs 、 GetLogtailConfig 、 PutData、 GetCursorOrData、GetData 、GetLogStoreHistogram 、GetLogStoreLogs、 ListLogStores、ListLogStoreTopics。

  status字段包括：200 、400 、401 、403 、405 、500 、502。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**日志服务**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

容器服务监控

概览

云监控通过监控容器服务的 CPU 使用率、内存使用率等 7 个监控项，帮助用户获取容器服务的使用情况。用户创建容器服务后，云监控自动开始对其监控，您登录云监控的容器服务页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警通知。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
containerCpuUtilization	容器CPU使用率	用户维度、容器维度	百分比	30秒

containerMemoryUtilization	容器内存使用率	用户维度、容器维度	百分比	30秒
containerMemoryAmount	容器内存使用量	用户维度、容器维度	字节	30秒
containerInternetIn	容器入网流量	用户维度、容器维度	字节	30秒
containerInternetOut	容器出网流量	用户维度、容器维度	字节	30秒
containerIORead	容器IO读	用户维度、容器维度	字节	30秒
containerIOWrite	容器IO写	用户维度、容器维度	字节	30秒

注意事项

监控数据最多保存31天。

用户最多可连续查看14天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**容器服务**实例列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

单击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续 14 天的监控数据。

单击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

设置单条报警规则：点击监控图右上角的**铃铛**按钮，可对该实例对应的监控项设置报警规则。

设置批量报警规则：实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报

警规则。

共享带宽

共享带宽

概览

云监控通过监控共享带宽的网络出入带宽等监控项，帮助用户监测共享带宽的网络使用情况，并支持用户对监控项设置报警规则。用户购买共享带宽服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
带宽包网络流入带宽	用户维度、实例维度	bits/s	1分钟
带宽包网络流出带宽	用户维度、实例维度	bits/s	1分钟
带宽包网络流入数据包	用户维度、实例维度	packages/s	1分钟
带宽包网络流出数据包	用户维度、实例维度	packages/s	1分钟
带宽包网络流出带宽使用率	用户维度、实例维度	%	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 7 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**共享带宽**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续7天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即共享带宽的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**共享带宽**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**共享带宽**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

全球加速

概览

云监控通过监控全球加速的网络出入带宽等监控项，帮助用户监测全球加速的网络使用情况，并支持用户对监控项设置报警规则。用户购买全球加速服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
网络流入带宽	用户维度、实例维度	bits/s	1分钟
网络流出带宽	用户维度、实例维度	bits/s	1分钟
网络流入数据包	用户维度、实例维度	pps	1分钟
网络流出数据包	用户维度、实例维度	pps	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 7 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**全球加速**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续7天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即全球加速的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**全球加速**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**全球加速**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

高性能时间序列数据库HiTSDB

概览

云监控通过监控HiTSDB的磁盘使用率、时间线数量、时间点增量等监控项，帮助用户监测HiTSDB使用情况，并支持用户对监控项设置报警规则。您购买HiTSDB后，云监控会自动对HiTSDB的监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
磁盘使用率	用户维度、实例维度	%	20秒
时间线数量	用户维度、实例维度	Count	20秒
时间点数量增长率	用户维度、实例维度	Count/Second	20秒

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**HiTSDB**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即HiTSDB的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**HiTSDB**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**HiTSDB**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

VPN网关

概览

云监控通过监控VPN网关的网络出入带宽等监控项，帮助用户监测VPN网关的网络使用情况，并支持用户对监控项设置报警规则。用户购买VPN网关服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
带宽包网络流入带宽	用户维度、实例维度	bits/s	1分钟
带宽包网络流出带宽	用户维度、实例维度	bits/s	1分钟
带宽包网络流入数据包	用户维度、实例维度	pps	1分钟
带宽包网络流出数据包	用户维度、实例维度	pps	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 7 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**VPN网关**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续7天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即VPN网关的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**VPN网关**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**VPN网关**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

API网关监控

概览

云监控通过提供 API 网关的 API 的流入流量、流出流量、响应时间等监控数据，帮助用户获取API网关服务的使用情况。用户开通使用 API 网关服务后，云监控自动开始对其监控，您登录云监控的 API 网关页面即可查看监控详情。您还可以对监控项设置报警规则，以便数据异常时收到报警息。

监控服务

监控项说明

监控项	含义	维度	单位	最小监控粒度
错误分布	监控周期内某API响应 2XX、4XX、5XX状态码的次数	用户维度、API维度	个	1分钟
流入流量	监控周期内某APIrequest 流量之和	用户维度、API维度	Bytes	1分钟
流出流量	监控周期内某API response 流量之和	用户维度、API维度	Bytes	1分钟
响应时间	监控周期内某API经网关发起调用后端服务到收到后端返回结果的时间差	用户维度、API维度	秒	1分钟
总体请求次数	监控周期内某API收到的请求量之和	用户维度、API维度	次	1分钟

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**API 网关**实例列表。

单击实例名称或**操作**中的**监控图表**，进入监控详情页面。

单击大小图切换按钮，切换大图显示(可选)。

报警服务

参数说明

监控项：API 网关提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为 1 分钟，则每间隔 1 分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。统计结果是 15 分钟内采集的所有监控数据的平均值，当这个平均值大于 80% 时，才算超过阈值。

最大值：统计周期内监控数据的最大值。统计周期内采集的监控数据中，最大值超过 80%，即为超过阈值。

最小值：统计周期内监控数据的最小值。统计周期内采集的监控数据中，最小值超过 80%，即为超过阈值。

求和值：统计周期内监控数据的总和。对统计周期内采集的监控数据进行求和，求和后的结果超过 80% 即为超过阈值。流量类指标需要用到此类统计方法。

连续几次超过阈值后报警：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置报警规则

登录云监控控制台。

进入**云服务监控**下的**API网关**实例列表。

单击实例列表**操作**中的**报警规则**，进入实例的报警规则页面。

单击报警规则页面右上角的**新建报警规则**，根据参数创建一条报警规则。

DDoS高防IP

概览

云监控通过提供DDoS高防IP的流出带宽监控项，帮助用户监测DDoS高防IP的使用情况，并支持用户对监控项设置报警规则。用户购买DDoS高防IP后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
网络带宽	实例维度、IP维度	bits/s	30s

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**DDoS高防IP**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即DDoS高防IP服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**DDoS高防IP**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**DDoS高防IP**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

邮件推送监控

概览

云监控为您提供邮件推送服务的WEB/API发信方式、SMTP发信方式和账号异常类相关监控指标。帮助用户实时监控邮件推送服务的服务状态，并支持用户对监控项设置报警规则。用户购买并使用邮件推送服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	单位	最小监控粒度
WEB/API错误-长度超限QPS	Count/Min	1分钟
WEB/API错误-额度超限QPS	Count/Min	1分钟
WEB/API错误-垃圾邮件QPS	Count/Min	1分钟
WEB/API发信成功QPS	Count/Min	1分钟
SMTP认证失败QPS	Count/Min	1分钟
SMTP认证成功QPS	Count/Min	1分钟
SMTP错误-长度超限QPS	Count/Min	1分钟
SMTP错误-额度超限QPS	Count/Min	1分钟
SMTP错误-垃圾邮件QPS	Count/Min	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**邮件推送**监控页面，可以查看邮件推送服务的监控信息。

报警服务

云监控为用户提供邮件推送服务相关监控指标的报警功能，方便用户在服务指标发生异常时快速知晓异常信息。

设置报警规则

设置报警规则有以下两种方法：

方法一

登录云监控控制台。

进入**云服务监控**下的**邮件推送**监控页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

方法二

登录云监控控制台。

进入**云服务监控**下的**邮件推送**监控页面。

点击**报警规则**tab，进入报警规则列表页后，点击页面右上角的**创建报警规则**按钮创建报警规则。

Elasticsearch监控

概览

云监控通过监控Elasticsearch的集群状态、集群查询QPS、集群写入QPS等监控项，帮助用户监测Elasticsearch服务的使用情况，并支持用户对监控项设置报警规则。用户购买Elasticsearch后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
集群状态	集群维度		1分钟
集群查询QPS	集群维度	Count/Second	1分钟
集群写入QPS	集群维度	Count/Second	1分钟
节点CPU使用率	节点维度	%	1分钟
节点磁盘使用率	节点维度	%	1分钟
节点HeapMemory使用率	节点维度	%	1分钟
节点load_1m	节点维度		1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**Elasticsearch**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即Elasticsearch服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**Elasticsearch**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**Elasticsearch**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

E-MapReduce监控

E-MapReduce

概览

云监控通过监控 E-MapReduce 集群的 CPU 空闲率、内存容量、磁盘容量等多个监控项，帮助用户监测集群的运行状态，并支持用户对监控项设置报警规则。用户购买 E-MapReduce 服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表，hadoop 指标含义可参考官网文档。

监控项	维度	单位	最小监控粒度
网络流入速率	用户维度、集群维度、角色维度	bits/s	30s
网络流出速率	用户维度、集群维度、角色维度	bits/s	30s
CPU空闲率	用户维度、集群维度、角色维度	%	1分钟
用户态CPU使用率	用户维度、集群维度、角色维度	%	30s
系统态CPU使用率	用户维度、集群维度、角色维度	%	30s
空闲磁盘容量	用户维度、集群维度、角色维度	Bytes	30s
磁盘总容量	用户维度、集群维度、角色维度	Bytes	30s
15分钟平均负载	用户维度、集群维度、角色维度	-	30s
5分钟平均负载	用户维度、集群维度、角色维度	-	30s
1分钟平均负载	用户维度、集群维度、角色维度	-	30s
空闲内存容量	用户维度、集群维度、角色维度	Bytes	30s
总内存容量	用户维度、集群维度、角色维度	Bytes	30s
数据包流入速率	用户维度、集群维度、角色维度	个/秒	30s
数据包流出速率	用户维度、集群维度、角色维度	个/秒	30s
运行中的进程数目	用户维度、集群维度、	个	30s

	角色维度		
总进程数目	用户维度、集群维度、角色维度	个	30s
阻塞的进程数目	用户维度、集群维度、角色维度	个	30s
创建的进程/线程数目	用户维度、集群维度、角色维度	个	30s
MemNonHeapUsedM	用户维度、集群维度、角色维度	Bytes	30s
MemNonHeapCommittedM	用户维度、集群维度、角色维度	Bytes	30s
MemNonHeapMaxM	用户维度、集群维度、角色维度	Bytes	30s
MemHeapUsedM	用户维度、集群维度、角色维度	Bytes	30s
MemHeapCommittedM	用户维度、集群维度、角色维度	Bytes	30s
MemHeapMaxM	用户维度、集群维度、角色维度	Bytes	30s
MemMaxM	用户维度、集群维度、角色维度	Bytes	30s
ThreadsNew	用户维度、集群维度、角色维度	-	30s
ThreadsRunnable	用户维度、集群维度、角色维度	-	30s
ThreadsBlocked	用户维度、集群维度、角色维度	-	30s
ThreadsWaiting	用户维度、集群维度、角色维度	-	30s
ThreadsTimedWaiting	用户维度、集群维度、角色维度	-	30s
ThreadsTerminated	用户维度、集群维度、角色维度	-	30s
GcCount	用户维度、集群维度、角色维度	-	30s
GcTimeMillis	用户维度、集群维度、角色维度	-	30s
CallQueueLength	用户维度、集群维度、角色维度	-	30s
NumOpenConnections	用户维度、集群维度、角色维度	-	30s
ReceivedBytes	用户维度、集群维度、	-	30s

	角色维度		
SentBytes	用户维度、集群维度、角色维度	-	30s
BlockCapacity	用户维度、集群维度、角色维度	-	30s
BlocksTotal	用户维度、集群维度、角色维度	-	30s
CapacityRemaining	用户维度、集群维度、角色维度	-	30s
CapacityTotal	用户维度、集群维度、角色维度	-	30s
CapacityUsed	用户维度、集群维度、角色维度	-	30s
CapacityUsedNonDFS	用户维度、集群维度、角色维度	-	30s
CorruptBlocks	用户维度、集群维度、角色维度	-	30s
ExcessBlocks	用户维度、集群维度、角色维度	-	30s
ExpiredHeartbeats	用户维度、集群维度、角色维度	-	30s
MissingBlocks	用户维度、集群维度、角色维度	-	30s
PendingDataNodeMessageCount	用户维度、集群维度、角色维度	-	30s
PendingDeletionBlocks	用户维度、集群维度、角色维度	-	30s
PendingReplicationBlocks	用户维度、集群维度、角色维度	-	30s
PostponedMisreplicatedBlocks	用户维度、集群维度、角色维度	-	30s
ScheduledReplicationBlocks	用户维度、集群维度、角色维度	-	30s
TotalFiles	用户维度、集群维度、角色维度	-	30s
TotalLoad	用户维度、集群维度、角色维度	-	30s
UnderReplicatedBlocks	用户维度、集群维度、角色维度	-	30s
BlocksRead	用户维度、集群维度、角色维度	-	30s
BlocksRemoved	用户维度、集群维度、	-	30s

	角色维度		
BlocksReplicated	用户维度、集群维度、角色维度	-	30s
BlocksUncached	用户维度、集群维度、角色维度	-	30s
BlocksVerified	用户维度、集群维度、角色维度	-	30s
BlockVerificationFailures	用户维度、集群维度、角色维度	-	30s
BlocksWritten	用户维度、集群维度、角色维度	-	30s
BytesRead	用户维度、集群维度、角色维度	-	30s
BytesWritten	用户维度、集群维度、角色维度	-	30s
FlushNanosAvgTime	用户维度、集群维度、角色维度	-	30s
FlushNanosNumOps	用户维度、集群维度、角色维度	-	30s
FsyncCount	用户维度、集群维度、角色维度	-	30s
VolumeFailures	用户维度、集群维度、角色维度	-	30s
ReadBlockOpNumOps	用户维度、集群维度、角色维度	-	30s
ReadBlockOpAvgTime	用户维度、集群维度、角色维度	ms	30s
WriteBlockOpNumOps	用户维度、集群维度、角色维度	-	30s
WriteBlockOpAvgTime	用户维度、集群维度、角色维度	ms	30s
BlockChecksumOpNumOps	用户维度、集群维度、角色维度	-	30s
BlockChecksumOpAvgTime	用户维度、集群维度、角色维度	ms	30s
CopyBlockOpNumOps	用户维度、集群维度、角色维度	-	30s
CopyBlockOpAvgTime	用户维度、集群维度、角色维度	ms	30s
ReplaceBlockOpNumOps	用户维度、集群维度、角色维度	-	30s
ReplaceBlockOpAvg	用户维度、集群维度、	ms	30s

Time	角色维度		
BlockReportsNumOps	用户维度、集群维度、角色维度	-	30s
BlockReportsAvgTime	用户维度、集群维度、角色维度	ms	30s
NodeManager_AllocatedContainers	用户维度、集群维度、角色维度	-	30s
ContainersCompleted	用户维度、集群维度、角色维度	-	30s
ContainersFailed	用户维度、集群维度、角色维度	-	30s
ContainersIniting	用户维度、集群维度、角色维度	-	30s
ContainersKilled	用户维度、集群维度、角色维度	-	30s
ContainersLaunched	用户维度、集群维度、角色维度	-	30s
ContainersRunning	用户维度、集群维度、角色维度	-	30s
ActiveApplications	用户维度、集群维度、角色维度	-	30s
ActiveUsers	用户维度、集群维度、角色维度	-	30s
AggregateContainersAllocated	用户维度、集群维度、角色维度	-	30s
AggregateContainersReleased	用户维度、集群维度、角色维度	-	30s
AllocatedContainers	用户维度、集群维度、角色维度	-	30s
AppsCompleted	用户维度、集群维度、角色维度	-	30s
AppsFailed	用户维度、集群维度、角色维度	-	30s
AppsKilled	用户维度、集群维度、角色维度	-	30s
AppsPending	用户维度、集群维度、角色维度	-	30s
AppsRunning	用户维度、集群维度、角色维度	-	30s
AppsSubmitted	用户维度、集群维度、角色维度	-	30s
AvailableMB	用户维度、集群维度、	-	30s

	角色维度		
AvailableVCores	用户维度、集群维度、角色维度	-	30s
PendingContainers	用户维度、集群维度、角色维度	-	30s
ReservedContainers	用户维度、集群维度、角色维度	-	30s

注意事项

监控数据最多保存31天。

用户最多可连续查看14天的监控数据。

查看监控数据

1. 登录云监控控制台。

   进入**云服务监控**下的**E-MapReduce**实例列表。

   点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

   点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

   点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即 E-MapReduce 服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。例如统计方法选择15分钟内采集的所有监控数据的平均值，则当平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。例如统计方法选择15分钟内采集的所有监控数据的最大值，则当最大值大于80%时，才算超过阈值。

最小值：统计周期内监控数据的最小值。例如统计方法选择15分钟内采集的所有监控数据的最小值，则当最小值大于80%时，才算超过阈值。

求和值：统计周期内监控数据的总和。例如统计方法选择15分钟内采集的所有监控数据的求和值，则当求和值大于80%时，才算超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过80%报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5分钟后第二次探测 CPU 使用率超过80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**E-MapReduce**实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**E-MapReduce监控**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

弹性伸缩

弹性伸缩

概览

云监控通过监控弹性伸缩组的最小实例数、最大实例数等多个监控项，帮助用户监测伸缩组的实例状态，并支持用户对监控项设置报警规则。用户购买弹性伸缩服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
最小实例数	用户维度、弹性伸缩组	个	5分钟
最大实例数	用户维度、弹性伸缩组	个	5分钟
总实例数	用户维度、弹性伸缩组	个	5分钟
运行实例数	用户维度、弹性伸缩组	个	5分钟
正在加入实例数	用户维度、弹性伸缩组	个	5分钟
正在移除实例数	用户维度、弹性伸缩组	个	5分钟

注意事项

监控数据最多保存31天。

用户最多可连续查看14天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**弹性伸缩**的伸缩组列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

单击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

单击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即弹性伸缩服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。例如统计方法选择 15 分钟内采集的所有监控数据的平均值，则当平均值大于 80% 时，才算超过阈值。

最大值：统计周期内监控数据的最大值。例如统计方法选择 15 分钟内采集的所有监控数据的最大值，则当最大值大于 80% 时，才算超过阈值

最小值：统计周期内监控数据的最小值。例如统计方法选择 15 分钟内采集的所有监控数据的最小值，则当最小值大于 80% 时，才算超过阈值

求和值：统计周期内监控数据的总和。例如统计方法选择 15 分钟内采集的所有监控数据的求和值，则当求和值大于 80% 时，才算超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**弹性伸缩**的伸缩组列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

单击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**弹性伸缩监控**实例列表。

实例列表页面选中所需实例后，在页面下方单击**设置报警规则**，即可批量添加报警规则。

高速通道

高速通道

概览

云监控通过监控高速通道实例的网络流入流量、网络流出流量等多个监控项，帮助用户监测高速通道服务的网络使用情况，并支持用户对监控项设置报警规则。用户购买高速通道服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
网络流入流量	用户维度、实例维度	Bytes	1分钟
网络流出流量	用户维度、实例维度	Bytes	1分钟
网络流入带宽	用户维度、实例维度	bits/s	1分钟
网络流出带宽	用户维度、实例维度	bits/s	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**高速通道**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即高速通道的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。例如统计方法选择 15 分钟内采集的所有监控数据的平均值，则当平均值大于 80% 时，才算超过阈值。

最大值：统计周期内监控数据的最大值。例如统计方法选择 15 分钟内采集的所有监控数据的最大值，则当最大值大于 80% 时，才算超过阈值

最小值：统计周期内监控数据的最小值。例如统计方法选择 15 分钟内采集的所有监控数据的最小值，则当最小值大于 80% 时，才算超过阈值

求和值：统计周期内监控数据的总和。例如统计方法选择 15 分钟内采集的所有监控数据的求和值，则当求和值大于 80% 时，才算超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**高速通道**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**高速通道**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

函数计算监控

概览

云监控通过监控函数服务Service级别和Function级别的TotalInvocations 、平均Duration、请求状态分布等监控指标。帮助用户实时监控函数计算服务的服务状态，并支持用户对监控项设置报警规则。用户购买并使用函数计算服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
BillableInvocations	用户维度、服务维度、函数维度	Count	1分钟
BillableInvocationsRate	用户维度、服务维度、函数维度	Percent	1分钟
ClientErrors	用户维度、服务维度、函数维度	Count	1分钟
ClientErrorsRate	用户维度、服务维度、函数维度	Percent	1分钟
ServerErrors	用户维度、服务维度、函数维度	Count	1分钟
ServerErrorsRate	用户维度、服务维度、函数维度	Percent	1分钟
Throttles	用户维度、服务维度、函数维度	Count	1分钟
ThrottlesRate	用户维度、服务维度、函数维度	Percent	1分钟
TotalInvocations	用户维度、服务维度、函数维度	Count	1分钟
平均Duration	用户维度、服务维度、函数维度	毫秒	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**函数计算**的监控页面，可以查看函数计算服务的整体监控概况。

点击 **Service列表**可以查看Service或Function级别的监控信息。

报警服务

云监控为用户提供函数计算相关监控指标的报警功能，方便用户在服务指标发生异常时快速知晓异常信息。

设置报警规则

设置报警规则有以下两种方法：

方法一

登录云监控控制台。

进入**云服务监控**下的**函数计算**的监控页面。

点击Service列表或Function列表**操作**中的**监控图表**即可进入相应的监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

方法二

登录云监控控制台。

进入**云服务监控**下的**函数计算**的监控页面。

点击**报警规则**tab，进入报警规则列表页后，点击页面右上角的**创建报警规则**按钮创建报警规则。

流计算

流计算

概览

云监控通过监控流计算的业务延迟监控项，帮助用户监测流计算服务的业务运行情况，并支持用户对监控项设置报警规则。用户购买流计算服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表

监控项	维度	单位	含义	最小监控粒度
业务延迟	Project维度、Job维度	秒	数据生产时间到数据被处理时间的差值	1分钟
读入RPS	Project维度、Job维度	RPS	任务平均每秒读入的数据条数	1分钟
写出RPS	Project维度、Job维度	RPS	任务平均每秒写出的数据条数	1分钟
FailoverRate	Project维度、Job维度	%	衡量当前Job发生failover的频率，越低越好	1分钟

注意事项

监控数据最多保存31天。

用户最多可连续查看14天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**流计算**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

5. 点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即流计算的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为 1 分钟，则每间隔 1 分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。例如统计方法选择 15 分钟内采集的所有监控数据的平均值，则当平均值大于 80% 时，才算超过阈值。

最大值：统计周期内监控数据的最大值。例如统计方法选择 15 分钟内采集的所有监控数据的最大值，则当最大值大于 80% 时，才算超过阈值

最小值：统计周期内监控数据的最小值。例如统计方法选择 15 分钟内采集的所有监控数据的最小值，则当最小值大于 80% 时，才算超过阈值

求和值：统计周期内监控数据的总和。例如统计方法选择 15 分钟内采集的所有监控数据的求和值，则当求和值大于 80% 时，才算超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**流计算**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**流计算**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

云数据库HybridDB版

概览

云监控通过监控 HybridDB 的 CPU 使用率、内存使用率等监控项，帮助用户监测 HybridDB 实例的使用情况，并支持用户对监控项设置报警规则。用户购买 HybridDB 后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
磁盘使用率	用户维度、实例维度	%	5分钟
连接数使用率	用户维度、实例维度	%	5分钟
CPU使用率	用户维度、实例维度	%	5分钟
内存使用率	用户维度、实例维度	%	5分钟
IO吞吐量使用率	用户维度、实例维度	%	5分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的 HybridDB 的实例列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

单击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续 14 天的监控数据。

单击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即 HybridDB 的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为 1 分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。例如统计方法选择 15 分钟内采集的所有监控数据的平均值，则当平均值大于 80% 时，才算超过阈值。

最大值：统计周期内监控数据的最大值。例如统计方法选择 15 分钟内采集的所有监控数据的最大值，则当最大值大于 80% 时，才算超过阈值。

最小值：统计周期内监控数据的最小值。例如统计方法选择 15 分钟内采集的所有监控数据的最小值，则当最小值大于 80% 时，才算超过阈值。

求和值：统计周期内监控数据的总和。例如统计方法选择 15 分钟内采集的所有监控数据的求和值，则当求和值大于 80% 时，才算超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的 **HybridDB** 的实例列表。

单击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

单击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的 **HybridDB** 实例列表。

实例列表页面选中所需实例后，在页面下方单击**设置报警规则**，即可批量添加报警规则。

NAT网关监控

NAT网关

概览

云监控通过监控NAT网关的SNAT连接数等监控项，帮助用户监测NAT网关服务的网络使用情况，并支持用户对监控项设置报警规则。用户购买NAT网关服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
SNAT连接数	用户维度、实例维度	Count/Min	1分钟
带宽包网络流入带宽	用户维度、实例维度	bits/s	1分钟
带宽包网络流出带宽	用户维度、实例维度	bits/s	1分钟
带宽包网络流入数据包	用户维度、实例维度	pps	1分钟
带宽包网络流出数据包	用户维度、实例维度	pps	1分钟
带宽包网络流出带宽使用率	用户维度、实例维度	%	1分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**NAT网关**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即NAT网关的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**NAT网关**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**NAT网关**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

营销引擎监控

概览

云监控通过监控营销引擎的 RTB 竞价 PV、RTB 竞价 QPS、广告点击 PV 等13个监控指标。帮助用户实时了解营销引擎服务的服务状态，并支持用户对监控项设置报警规则。用户购买并使用营销引擎服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
RTB 竞价 PV	用户维度	Count	1分钟
RTB 竞价 QPS	用户维度	次/秒	1分钟
广告点击 PV	用户维度	Count	1分钟
广告点击 QPS	用户维度	次/秒	1分钟
广告点击延时	用户维度	毫秒	1分钟
广告曝光 PV	用户维度	Count	1分钟
广告曝光 QPS	用户维度	次/秒	1分钟
广告曝光延时	用户维度	毫秒	1分钟
DMP 有效人群数	用户维度	个/天	1小时
DMP 有效人群请求量	用户维度	次/天	1小时
DMP 占用存储	用户维度	字节/天	1小时
友盟+ DIP 有效人群数	用户维度	个/天	1小时
友盟+ DIP 有效人群请	用户维度	次/天	1小时

求量			

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**营销引擎**的监控页面，可以查看营销引擎服务的整体监控概况。

报警服务

云监控为用户提供营销引擎服务的相关监控指标的报警功能，方便用户在服务指标发生异常时快速知晓异常信息。

设置报警规则

设置报警规则有以下两种方法：

方法一

登录云监控控制台。

进入**云服务监控**下的**营销引擎**的监控页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

方法二

登录云监控控制台。

进入**云服务监控**下的**营销引擎**的监控页面。

点击**报警规则** tab，进入报警规则列表页后，点击页面右上角的**创建报警规则**按钮创建报警规则。

阿里云OpenAPI监控

概览

云监控通过提供阿里云OpenAPI的调用次数、错误次数、错误率，帮助用户监测阿里云OpenAPI的使用情况，并支持用户对监控项设置报警规则。用户使用阿里云OpenAPI后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度	说明
调用次数	产品维度、API维度	个	60s	统计周期内调用接口的总次数
错误次数	产品维度、API维度	个	60s	统计周期内调用的返回状态码大于等于500的次数
错误率	产品维度、API维度	%	60s	统计周期内返回状态码大于等于500的次数/调用总次数*100

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**OpenAPI**的接口列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即阿里云OpenAPI提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**OpenAPI**的接口列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**OpenAPI**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

开放搜索监控

概览

云监控通过监控开放搜索的存储容量、文档总数、查询QPS等监控项，帮助用户监测开放搜索服务的使用情况，并支持用户对监控项设置报警规则。用户购买开放搜索后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表：

监控项	维度	单位	最小监控粒度
存储容量	APP维度	Bytes	10分钟
存储容量使用率	APP维度	%	10分钟
文档总数	APP维度	个	10分钟
查询QPS	APP维度	Count/Second	20秒
查询限流QPS	APP维度	Count/Second	20秒
查询耗时	APP维度	ms	20秒
计算资源	APP维度	LCU	20秒
计算资源使用率	APP维度	%	20秒
单次查询计算消耗	APP维度	LCU	20秒

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**开放搜索**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即开放搜索服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**开放搜索**的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**开放搜索**实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

云数据库PetaData

云数据库PetaData

概览

云监控通过监控云数据库 PetaData 实例的最小实例数、最大实例数等多个监控项，帮助用户监测伸缩组的实例状态，并支持用户对监控项设置报警规则。用户购买弹性伸缩服务后，云监控会自动对上述监控项收集数据。

监控服务

监控项

云监控提供的监控指标见如下列表:

监控项	维度	单位	最小监控粒度
磁盘使用量	用户维度、实例维度	Bytes	5分钟
网络流入带宽	用户维度、实例维度	Bytes/Second	5分钟
网络流出带宽	用户维度、实例维度	Bytes/Second	5分钟
QPS	用户维度、实例维度	Count/Second	5分钟

注意事项

监控数据最多保存 31 天。

用户最多可连续查看 14 天的监控数据。

查看监控数据

登录云监控控制台。

进入**云服务监控**下的**云数据库 PetaData** 的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面，查看各项指标。

点击页面上方的**时间范围**快速选择按钮或精确选择功能，监控数据最长支持查看连续14天的监控数据。

点击监控图右上角的**放大**按钮，可查看监控大图。

报警服务

参数说明

监控项：即云数据库 PetaData 的服务提供的监控指标。

统计周期：报警系统会按照这个周期检查您对应的监控数据是否超过了报警阈值。例如设置内存使用率报警规则的统计周期为1分钟，则每间隔1分钟会检查一次内存使用率是否超过了阈值。

统计方法：统计方法指对超出阈值范围的设置。统计方法中可以设置平均值、最大值、最小值、求和值。

平均值：统计周期内监控数据的平均值。例如统计方法选择15分钟内采集的所有监控数据的平均值，则当平均值大于80%时，才算超过阈值。

最大值：统计周期内监控数据的最大值。例如统计方法选择15分钟内采集的所有监控数据的最大值，则当最大值大于80%时，才算超过阈值

最小值：统计周期内监控数据的最小值。例如统计方法选择15分钟内采集的所有监控数据的最小值，则当最小值大于80%时，才算超过阈值

求和值：统计周期内监控数据的总和。例如统计方法选择15分钟内采集的所有监控数据的求和值，则当求和值大于80%时，才算超过阈值。流量类指标需要用到此类统计方法。

连续次数：指连续几个统计周期监控项的值持续超过阈值后触发报警。

例如：设置 CPU 使用率超过 80% 报警，统计周期为 5 分钟，连续 3 次超过阈值后报警，则第一次探测 CPU 使用率超过 80% 时，不会发出报警通知。5 分钟后第二次探测 CPU 使用率超过 80%，也不会发出报警。第三次探测仍然超过 80% 时，才会发出报警通知。即从实际数据第一次超过阈值到最终发出报警规则，最少需要消耗的时间为统计周期×(连续探测次数-1)=5×(3-1)=10分钟。

设置单条报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 PetaData** 的实例列表。

点击实例名称或**操作**中的**监控图表**即可进入实例监控详情页面。

点击监控图右上角的**铃铛**按钮或页面右上角的**新建报警规则**，可对该实例对应的监控项设置报警规则。

设置批量报警规则

登录云监控控制台。

进入**云服务监控**下的**云数据库 PetaData** 实例列表。

实例列表页面选中所需实例后，在页面下方点击**设置报警规则**，即可批量添加报警规则。

自定义监控

使用自定义监控

自定义监控概览

自定义监控是提供给用户自由定义监控项及报警规则的一项功能。通过此功能，用户可以针对自己关心的业务指标进行监控，将采集到监控数据上报至云监控，由云监控来进行数据的处理，并根据结果进行报警。

事件监控与自定义监控有何区别？

事件监控用于解决非连续的事件类型数据监控数据上报、查询与报警的场景。自定义监控用于解决周期性持续采集的时间序列监控数据上报、查询与报警的场景。

使用流程

上报监控数据

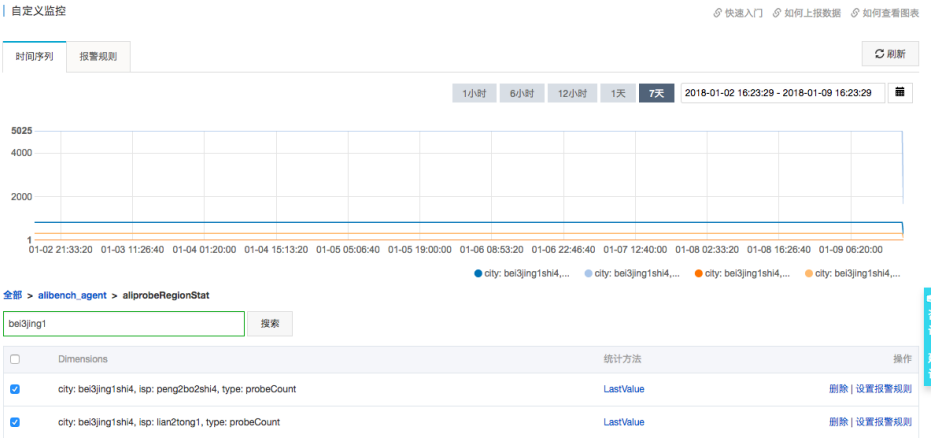
上报监控数据部分请参考**上报监控数据**

查询监控数据

完成监控数据的上报后，您就可以在控制台中查看到已经上报的数据。您可以在自定义监控中查看全部监控数据，也可以进入某个指定的应用分组，查看这个分组的相关自定义监控数据

查看所有自定义监控数据

1. 登录云监控控制台，进入**自定义监控**。
2. 选择对应的应用分组、监控项，进入时间序列详情页面。
3. 勾选需要查看的时间序列。



查看应用分组下自定义监控数据

1. 登录云监控控制台，进入**应用分组**列表页面。
2. 选择相应的应用分组，进入分组详情页。
3. 点击**自定义监控**菜单，进入自定义监控详情页。
4. 选择对应的监控项，进入时间序列详情页面。
5. 勾选需要查看的时间序列。

设置报警规则

自定义监控为您提供报警功能，设置报警时需要选择相应的应用分组，报警被触发后会发送通知给应用分组的联系人。如果您上报的监控数据需要报警，可以按照如下方式配置报警规则。

方式一：

1. 登录云监控控制台，进入**自定义监控**。
2. 选择对应的应用分组、监控项，进入时间序列详情页面。
3. 选择需要创建报警的时间序列，在**操作**中点击**设置报警规则**。
4. 进入创建报警规则页面，填写报警规则名称、设置相应的报警策略及通知方式。

方式二：

1. 登录云监控控制台，进入**应用分组**列表页面。
2. 选择相应的应用分组，进入应用分组内的**自定义监控**页面。
3. 选择需要创建报警规则的时间序列，在**操作**中点击**设置报警规则**。
4. 进入创建报警规则页面，填写报警规则名称、选择相应的监控项、维度、报警策略及通知方式。

上报监控数据

自定义监控功能为您提供上报监控数据的接口，方便您将自己采集的时序数据上报到云监控，并配置报警规则来接收报警通知。

云监控为您提供 OpenAPI、Java SDK 和阿里云命令行工具（CLI）三种方式上报数据。

使用限制

- 单云账号QPS限制为100。
- 单次最多上报100条数据，body最大为256KB。
- “metricName”字段只支持字母、数字、下划线。需要以字母开头，非字母开头会替换为大写“A”，非法字符替换为“_”。

- “dimensions”字段不支持“=”、“&”、“,” ，非法字符会被替换为“_”。
- metricName 和dimensions的Key-value 最大均为64字节，超过64字节会被截断。
- 其他限制请关注计量计费说明。

OpenAPI上报数据

服务地址

公网服务地址：https://metrichub-cms-cn-hangzhou.aliyuncs.com

内网服务地址：

地域	服务地址
华东 1 (杭州)	http://metrichub-cn-hangzhou.aliyun.com
华北 3（张家口）	http://metrichub-cn-zhangjiakou.aliyun.com
华东 2 (上海)	http://metrichub-cn-shanghai.aliyun.com
华北 2 (北京)	http://metrichub-cn-beijing.aliyun.com
华北 1 (青岛)	http://metrichub-cn-qingdao.aliyun.com
华南 1 (深圳)	http://metrichub-cn-shenzhen.aliyun.com
香港	http://metrichub-cn-hongkong.aliyun.com
华北 5 （呼和浩特）	http://metrichub-ap-southeast-5.aliyuncs.com
中东东部 1（迪拜）	http://metrichub-me-east-1.aliyun.com
美国西部 1（硅谷 ）	http://metrichub-us-east-1.aliyun.com
美国东部 1（弗吉尼亚）	http://metrichub-us-west-1.aliyun.com
亚太东北 1 （日本 ）	http://metrichub-ap-northeast-1.aliyun.com
欧洲中部 1（法兰克福）	http://metrichub-eu-central-1.aliyun.com
亚太东南 2（悉尼）	http://metrichub-ap-southeast-2.aliyun.com
亚太东南 1（新加坡）	http://metrichub-ap-southeast-1.aliyun.com
亚太东南3（吉隆坡）	http://metrichub-ap-southeast-3.aliyun.com
亚太南部 1 （孟买）	http://metrichub-ap-south-1.aliyuncs.com

请求语法

```
POST /metric/custom/upload HTTP/1.1
Authorization:<AuthorizationString>
Content-Length:<Content Length>
Content-MD5:<Content MD5>
Content-Type:application/json
```

```
Date:<GMT Date>
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-signature:hmac-sha1
x-cms-api-version:1.0
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0

[{"groupId":101,"metricName":"","dimensions":{"sampleName1":"value1","sampleName2":"value2"},"time":"","type":0,"period":60,"values":{"value":10.5,"Sum":100}}]
```

请求参数

名称	类型	必选	描述
groupId	long	是	应用分组的id
metricName	string	是	监控项名称，支持字母、数字、连接符“_-.八”，其他为非法字符，最大长度为64字节，超过64字节时截取前64字节
dimensions	object	是	维度map，key-value都为字符串, 支持字母、数字、连接符“_-.八”，键值对数量最大为10，key长度最大64字节，value长度最大64字节，超过64字节时截取前64字节
time	string	是	指标发生时间，支持“yyyyMMdd’T’HHmmss.SSSZ”和long型时间戳2种方式，例如“20171012T132456.888+0800”或“1508136760000”
type	int	是	上报数值的类型，0为原始值，1为聚合数据。当上报聚合数据时，建议60s、300s 周期的数据均上报，否则会无法正常查询跨度大于7天的监控数据。
period	string	否	聚合周期，单位为秒。如果 type=1则需要传此字段，取值为60、300
values	object	是	指标值集合，当type=0时，key只能为”value”，上报的

			是原始值，云监控会按周期将原始值聚合为多个值，比如最大、计数、求和等

通过接口上报原始数据后，云监控会按以下统计方式计算1分钟、5分钟的统计结果：

- Average：平均值
- Maximum：最大值
- Minimum：最小值
- Sum：求和
- SampleCount：计数
- SumPerSecond：求和/对应周期的秒数，也可以使用滑动平均计算
- CountPerSecond：计数/对应周期的秒数，也可以使用滑动平均计算
- LastValue：本周期最后一个采样值，类似gauge
- P10：percentile 0.1，大于10%本周期所有采样数据
- P20：percentile 0.2，大于20%本周期所有采样数据
- P30：percentile 0.3，大于30%本周期所有采样数据
- P40：percentile 0.4，大于40%本周期所有采样数据
- P50：percentile 0.5，大于50%本周期所有采样数据，中位数
- P60：percentile 0.6，大于60%本周期所有采样数据
- P70：percentile 0.7，大于70%本周期所有采样数据
- P75：percentile 0.75，大于75%本周期所有采样数据
- P80：percentile 0.8，大于80%本周期所有采样数据
- P90：percentile 0.9，大于90%本周期所有采样数据
- P95：percentile 0.95，大于95%本周期所有采样数据
- P98：percentile 0.98，大于98%本周期所有采样数据
- P99：percentile 0.99，大于99%本周期所有采样数据

关于API的请求头，请参考**请求头定义**。

关于签名算法，请参考**签名算法**。

响应元素

HTTP 状态码返回 200。

示例

请求示例

```
POST /metric/custom/upload HTTP/1.1
Host: metrichub-cms-cn-hangzhou.aliyuncs.com
x-cms-api-version:1.0
Authorization:yourAccessKeyId:yourAccessKeySecret
```

```
Host:metrichub-cms-cn-hangzhou.aliyuncs.com"
Date:Mon, 23 Oct 2017 06:51:11 GMT
Content-Length:180
x-cms-signature:hmac-sha1
Content-MD5:E9EF574D1AEAAA370860FE37856995CD
x-cms-ip:30.27.84.196
User-Agent:cms-java-sdk-v-1.0
Content-Type:application/json

[{"groupId":101,"metricName":"","dimensions":{"sampleName1":"value1","sampleName2":"value2"},"time":"","type":
0,"period":60,"values":{"value":10.5,"Sum":100}}]
```

返回示例

```
{
"code":"200",
"msg":""//正常上报时返回msg为空
}
```

Java SDK上报数据

SDK支持上报原始值和聚合值2种方式。

maven依赖

```
<dependency>
<groupId>com.aliyun.openservices</groupId>
<artifactId>aliyun-cms</artifactId>
<version> 0.2.2 </version>
</dependency>
```

示例代码

上报原始数据

```
CMSClientInit.groupId = 101L;//设置公共的应用组id
CMSClient cmsClient = new CMSClient(endpoint, accKey, secret);//初始化client
CustomMetricUploadRequest request = CustomMetricUploadRequest.builder()
.append(CustomMetric.builder()
.setMetricName("testMetric")//指标名
.setGroupId(102L)//设置定制的分组id
.setTime(new Date())
.setType(CustomMetric.TYPE_VALUE)//类型为原始值,
.appendValue(MetricAttribute.VALUE, 1f)//原始值，key只能为这个
.appendDimension("key", "value")//添加维度
.appendDimension("ip", "127.0.0.1")//添加维度
.build())
```

```
.build();
CustomMetricUploadResponse response = cmsClient.putCustomMetric(request);//上报
System.out.println(JSONObject.toJSONString(response));
```

自动完成多周期聚合上报

SDK支持在本地做聚合后再上报数据的功能，聚合周期为1分钟、5分钟。

数据类型	描述	聚合的值	内存消耗不含名称、维度,单时间序列，单聚合周期）
value	一般值类型	除了LastValue外的所有属性	约4K
gauge	采样值	LastValue	4字节
meter	求和及速率	Sum，SumPerSecond	50字节
counter	计数	SampleCount	10字节
timer	计算时间	SampleCount、CountPerSecond、Average、Maximum、Minimum、PXX(P10-P99)	约4K
histogram	分布	SampleCount、Average、Maximum、Minimum、PXX(P10-P99)	约4K

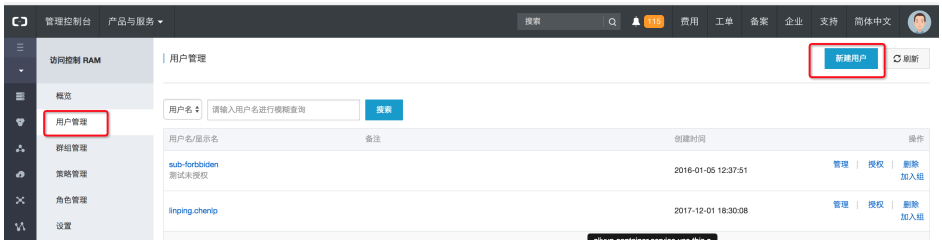
```
//初始化
CMSClientInit.groupId = 0L;
CMSClient cmsClient = new CMSClient(accKey, secret, endpoint);//创建client
CMSMetricRegistryBuilder builder = new CMSMetricRegistryBuilder();
builder.setCmsClient(cmsClient);
final MetricRegistry registry = builder.build();//创建registry 包含2个聚合周期
//或者 final MetricRegistry registry = builder.build(RecordLevel._60S);//只创建1分钟聚合周期的

//使用value
ValueWrapper value = registry.value(MetricName.build("value"));
value.update(6.5);

//使用meter
MeterWrapper meter = registry.meter(MetricName.build("meter"));
meter.update(7.2);

//使用counter
CounterWrapper counter = registry.counter(MetricName.build("counter"));
counter.inc(20);
counter.dec(5);
```

```
//使用timer
TimerWrapper timer = registry.timer(MetricName.build("timer"));
timer.update(30, TimeUnit.MILLISECONDS);

//使用histogram
HistogramWrapper histogram = registry.histogram(MetricName.build("histogram"));
histogram.update(20);

//使用gauge
final List list = new ArrayList();
registry.gauge(MetricName.build("gauge"), new Gauge() {
@Override
public Number getValue() {
return list.size();
}
});
```

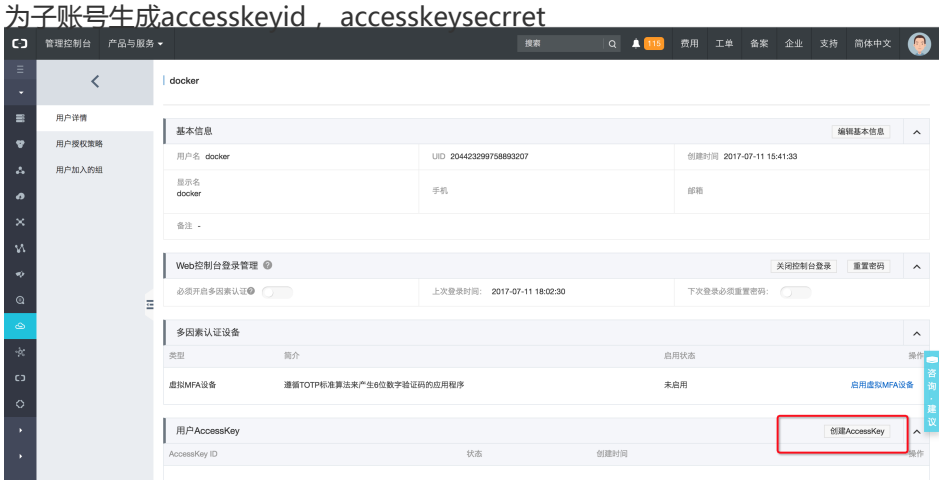
阿里云命令行（CLI）方式上报数据

前置条件：拥有阿里云账号，并生成具有云监控权限的子账号AK（使用子账号安全性更好）

创建子账号



- 为子账号生成accesskeyid， accesskeysecrret



- 为子账号授权云监控权限

第一步：安装aliyuncli工具

前置条件

- 系统要求：Linux、UNIX 或 Mac OS。
- 环境要求：已安装 Python 2.7.x。

安装 Python

- 若您的设备已安装 Python 2.7.x 版本，请跳过此步骤。
- 若您的设备没有安装 Python 2.7.x 版本，请在命令行窗口中执行下列命令，安装 Python。注意，请确保您的设备中已安装了 wget。

```
wget https://www.python.org/ftp/python/2.7.8/Python-2.7.8.tgz (或者通过其他方式下载后放在某个路径下)
tar -zxvf Python-2.7.8.tgz
cd Python-2.7.8
./configure
make
sudo make install
```

安装 pip

- 若您的设备已安装 pip，请跳过此步骤。
- 若您的设备没有安装 pip，在命令行窗口中执行如下命令，安装 pip。

```
curl "https://bootstrap.pypa.io/get-pip.py" -o "pip-install.py"
sudo python pip-install.py
```

系统显示如下类似信息，则表明安装成功。

```
Successfully installed pip-7.1.2 setuptools-18.7 wheel-0.26.0
```

安装命令行工具

如果系统内的 pip 版本过低，会造成 CLI 安装出错。用户可以使用如下指令先对 pip 软件进行升级后再进行相关操作。请使用 pip 7.x 或更高版本。若已是最新版本的 pip，请跳过此步骤。

1. 在命令行窗口中执行如下命令，升级 pip。

```
sudo pip install -U pip
```

系统显示如下类似信息，则表明升级成功。

```
Successfully uninstalled pip-7.1.2
Successfully installed pip-8.1.2
```

1. 执行如下命令，安装阿里云命令行工具。

```
sudo pip install aliyuncli
```

系统显示如下类似信息，则表明安装成功。

```
Successfully installed aliyuncli-2.1.2 colorama-0.3.3 jmespath-0.7.1
```

配置命令行工具

```
~ sudo aliyuncli configure
Aliyun Access Key ID [********************a]: youraccesskeyid
Aliyun Access Key Secret [********************b]: youraccesskeysecret
Default Region Id [cn-hangzhou]: cn-hangzhou
Default output format [json]: json
```

第二步：安装CmsSDK。

Windows安装方式

在命令行窗口输入如下命令：

```
cd C:\Python27\Scripts
pip install aliyun-python-sdk-cms
```

如果需要更新SDK，则使用如下命令：

```
pip install --upgrade aliyun-python-sdk-cms
```

Linux 安装方式

在命令行窗口输入如下命令：

```
sudo pip install aliyun-python-sdk-cms
```

如果需要升级SDK，则使用如下命令：

```
sudo pip install —upgrade aliyun-python-sdk-cms
```

第三步：上报监控数据。

使用PutCustomMetric接口

Linux 上报示例：

```
aliyuncli cms PutCustomMetric --MetricList "[{'groupId': 101,'metricName': 'hearteate','dimensions': {'name':
'127.0.0.1','sex': 'hosta'},'type': 0,'values': {'value': 10.5}}]"
```

上报成功后，返回200状态码：

```
{
"Code":"200"
}
```

错误编码

错误代码	含义
200	正常
400	客户端请求中的语法错误
403	校验失败、限速、没有授权
500	服务器内部错误

子账号授权说明

使用子账号的AK上报事件数据时，需要对相应子账号授权云监控管理权限。如果子账号未授权云监控管理权限，上报数据时会提示“cannot upload, please use ram to auth”。

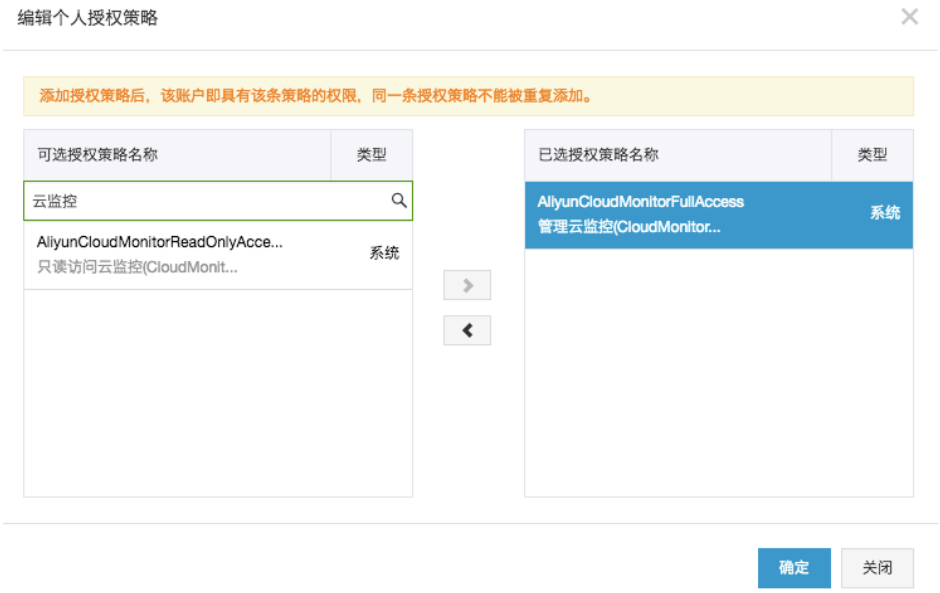
授权步骤如下：

1. 登录访问控制RAM控制台。

2. 进入**用户管理** 菜单。

选择需要上报数据的子账号，在操作中点击**授权** 。

在授权页面中选择**管理云监控**的权限，并点击**确定**保存授权。



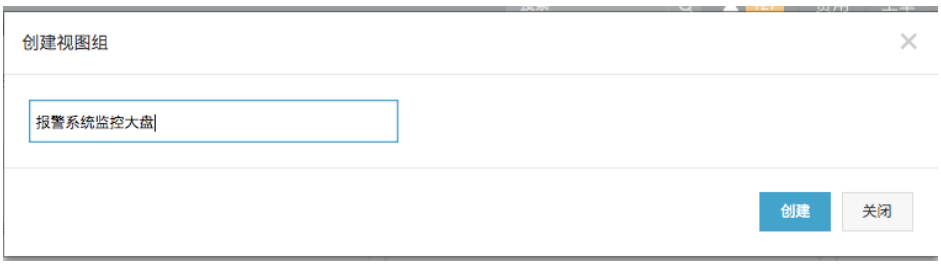
配置Dashboard监控大盘

您的监控数据上报到自定义监控后，可以在Dashboard中添加监控大盘，方便随时查看监控报表。

操作步骤

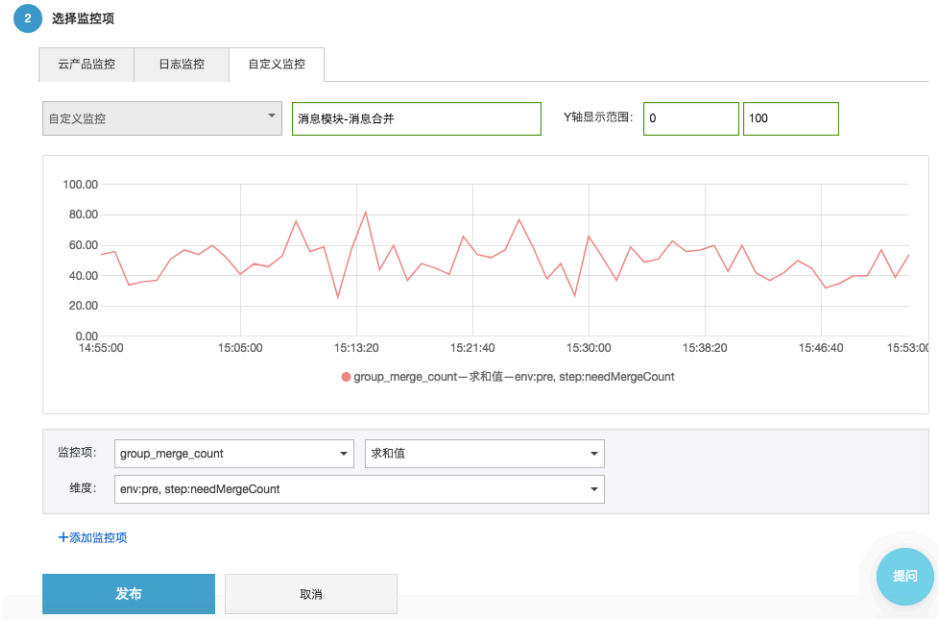
创建监控大盘

1. 登录云监控，进入Dashboard页面。
2. 点击页面右上角的**创建监控大盘**按钮，填写监控大盘名称后点击**创建** 即可创建新的监控大盘。

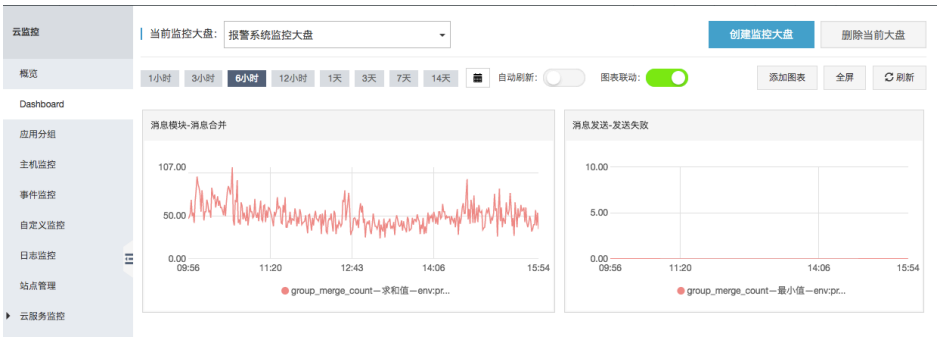


添加监控图表

1. 点击监控大盘右上角的**添加图表**按钮，进入监控图表配置页面。
2. 选择**自定义监控**模块，并定义图表名称。
3. 选择需要展示的监控项、统计方式、维度。
4. 点击**发布**按钮，保存配置。



发布后即可看到如下大盘：



报警服务

报警服务概览

概览

用户可以对主机监控中的监控项、站点监控中的探测点、云服务监控中的实例和自定义监控中的监控项设置报警规则。

用户可以在全部资源、应用分组和单实例维度设置报警规则。

主机监控报警规则

用户可以对主机监控中的全部监控项设置报警规则，云监控提供的报警探测频率最小为每分钟1次。

站点监控报警规则

用户可对站点监控中的探测点创建报警规则。站点监控中报警规则的统计周期和探点的探测周期是一致的。即您创建了1个探测周期为5分钟的探测点，则报警规则的统计周期也为5分钟，会5分钟监测一次探测点返回的数据，对比实际值是否超过了阈值。

云服务报警规则

用户可对云服务监控中各产品的实例设置报警规则。各个产品的监控项均可设置报警规则。

自定义监控报警规则

用户创建监控项后，可对探测点的响应时间、状态码、丢包率等监控项设置报警规则。报警规则的统计周期和创建监控项时的统计周期一致。

报警服务支持短信、邮件、旺旺、事件订阅四种方式。旺旺仅支持PC端报警消息推送。如果您安装了阿里云APP，也可以通过阿里云APP接收报警通知。

管理报警规则

报警服务是为云上用户提供监控报警能力，帮您第一时间得知监控数据异常，及时处理问题。

参数说明

- 产品：例如主机监控、RDS、OSS 等。
- 资源范围：报警规则的作用范围。分为**全部资源**、**应用分组**、**实例**三种范围。

资源范围选择**全部资源**时，报警的资源最多1000个，超过1000个可能会出现达到阈值不报警的问题，建议使用应用分组按业务划分资源后再设置报警。

全部资源：表示该规则作用在用户名下对应产品的全部实例上。比如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户下有MongoDB CPU使用率大于80%，就会命中这条规则。

应用分组：表示该规则作用在某个应用分组下的全部实例上。比如设置了应用分组粒度的主机 CPU使用率大于80%报警，则只要这个分组下有主机 CPU使用率大于80%，就会命中这条规则。

实例：表示该规则只作用在某个具体实例上。比如设置了实例粒度的主机 CPU 使用率大于80%报警，则只有这个实例 CPU使用率大于80% ，才会命中这条规则。

规则名称：报警规则的名称。

规则描述：报警规则的主体，定义在监控数据满足何种条件时，触发报警规则。例如规则描述为**CPU使用率1分钟平均值>=90%**，则报警服务会1分钟检查一次1分钟内的数据是否满足平均值>=90%

报警规则举例说明：以主机监控为例，单个服务器监控指标15秒上报一个数据点，5分钟有20个数据点。

- CPU使用率 5分钟 平均值>90%， 含义是 CPU使用率 5分钟的20个数据点平均值大于90%。

  CPU使用率 5分钟 总是>90%， 含义是CPU使用率 5分钟的20个数据点全部大于90%。

  CPU使用率 5分钟 只要有一次>90%，含义是CPU使用率 5分钟的20个数据点至少有1个大于90%。

  公网流出流量 5分钟 总计>50M ，含义是公网流出流量5分钟的20个数据点求和结果大于5M。

连续几次超过阈值后报警：指连续探测几次后，结果都符合报警规则的描述，才发送报警通知。

生效时间：报警规则的生效时间，报警规则只在生效时间内才会检查监控数据是否需要报警。

通知对象：发送报警的联系人组。

报警等级：分为Critical 、Warning、Info三个等级，不同等级对应不同的通知方式。

- Critical：电话语音+手机短信+邮件+钉钉机器人
- Warning：手机短信+邮件+钉钉机器人
- Info：邮件+钉钉机器人

邮件备注：自定义报警邮件补充信息。填写邮件备注后，发送报警的邮件通知中会附带您的备注。

管理报警规则

云监控为用户提供3个入口管理报警规则，分别是应用分组页面、各类监控的监控列表页面和报警服务的报警规则列表页面。

在应用分组中管理报警规则。

在主机监控中管理报警规则。

在各云服务监控中管理报警规则。

在站点监控中使用报警规则。

在自定义监控中管理报警规则

报警联系人和报警联系组

联系人和联系组信息是发送报警通知的基础，用户需要先创建联系人和联系组信息，然后在创建报警规则时选择相应的联系组，才能收到报警通知。

报警联系人管理

报警联系人的管理包括对联系人手机、邮箱等通知方式进行创建、删除、修改操作。

创建联系人

登录云监控控制台。

进入报警联系人页面。

单击页面右上角的**新建联系人**按钮，填写手机、邮箱等信息。

添加手机和邮箱时需要对手机和邮件进行验证，防止您填写了错误的信息，无法及时收到报警通知。

编辑联系人

登录云监控控制台。

进入报警联系人页面。

单击联系人列表**操作**中的**编辑**按钮，对联系人信息进行编辑。

删除联系人

登录云监控控制台。

进入报警联系人页面。

单击联系人列表**操作**中的**删除**按钮，对联系人信息进行。

删除联系人后，联系人将不再收到云监控告警通知。

报警联系组管理

报警组是一组报警联系人，可以包含一个或多个**报警联系人**。同一个报警联系人，可以加入多个报警联系组。在报警规则设置中，均通过**报警联系组**发送报警通知。

创建联系组

登录云监控控制台。

进入报警联系人页面。

单击页面上方的**报警联系组**菜单，切换到报警联系组列表。

单击页面右上角的**新建联系组**，弹出新建联系组页面。

填写组名并选择需要加入组中的联系人。

编辑联系组

登录云监控控制台。

进入报警联系人页面。

单击页面上方的**报警联系组**菜单，切换到报警联系组列表。

单击联系组列表**操作**中的**编辑**按钮，可修改联系组中包含的联系人。

删除联系组

登录云监控控制台。

进入报警联系人页面。

单击页面上方的**报警联系组**菜单，切换到报警联系组列表。

单击联系组列表**操作**中的**删除**按钮，删除对应的联系组。

批量添加联系人到联系组

登录云监控控制台。

进入报警联系人页面。

在报警联系人列表中勾选需要添加的联系人。

单击页面最下方的**添加到报警联系组**。

在弹出的页面中选择对应的联系组并确认。

使用报警回调

功能描述

报警回调功能可以让您将云监控发送的报警通知集成到已有运维体系或消息通知体系中。云监控通过HTTP协议的POST请求推送报警通知到您指定的公网URL，您在接收到报警通知后，可以根据通知内容做进一步处理。

注意事项

报警回调的重试策略为重试3次，超时时间为5秒。

创建报警回调

1. 登录云监控控制台。
2. 选择您需要增加回调的报警规则。
3. 在通知方式中填写需要回调的URL地址。

回调参数

报警规则回调URL时，推送的POST请求内容如下：

参数	数据类型	说明
userId	string	用户ID
alertName	string	报警名称
timestamp	string	发生报警的时间戳
alertState	string	报警状态，会根据实际情况返回OK 、ALERT、INSUFFICIENT_DATA 三种状态中的一种
dimensions	string	发生报警的对象，示例：[{“userId”:”12345”,”instanceId”:”i-12345”}]
expression	string	报警条件，示例

		：[{“expression”:”$value>12”,”level”:4,”times”:2}]表示阈值连续2次大于12后触发报警。level=4时表示还通过邮件为您推送报警，level=3表示还通过短信、邮件为您推送报警。times字段表示设置报警规则时选择的连续几次达到报警阈值的次数。
curValue	string	报警发生或恢复时监控项的当前值
metricName	string	监控项名称
metricProject	string	产品名称，监控项和产品名称可参考文档预设监控项参考

POST请求示例如下：

```
{
"userId":"12345",
"alertName":"putNewAlarm_group_a37cd898-ea6b-4b7b-a8a8-de017a8327f6",
"timestamp":"1508136760",
"alertState":"ALARM",
"dimensions":[
{
"userId":"12345",
"instanceId":"i-12345"
}
],
"expression":"[{\"expression\":\"$Average>90\",\"level\":4,\"times\":2}]",
"curValue":"95",
"metricName":"CPUUtilization",
"metricProject":"acs_ecs_dashboard"
}
```

使用报警模板

功能描述

报警模板功能支持将各类云产品监控项的报警规则描述设置保存在模板中，创建报警时直接使用模板，无需每次重复定义报警规则描述的过程。当您有大量云资源（ECS、RDS、SLB、OSS等）时，建议您按照业务应用对资源创建应用分组，然后创建报警模板，创建好报警模板后将模板直接应用在分组即可，可极大简化报警的创建和维护过程。

报警模板需要与应用分组配合使用，您可以创建好报警模板后，将模板应用在各个应用分组上，为各业务模块快速创建好报警规则。

云监控默认为您提供一个初始化报警模板，模板中包含ECS、RDS、SLB、CDN、Redis、Mongodb、OSS产品的常用于报警的监控项，方便您快速开始使用模板。

注意事项

- 报警模板只能和应用分组配合使用，即报警模板只能使用在资源范围为“应用分组”的报警规则上。
- 每个云账号最多能创建100个模板。
- 每个模板最多包含30个监控项。
- 报警模板只是创建报警规则的快捷方式，报警模板和报警规则不是一一绑定的关系，即修改报警模板后通过报警模板生成的规则不会被修改。如果需要批量修改分组的规则，需要将修改后的模板重新应用到分组上。

创建或编辑模板

1. 登录云监控控制台，单击左侧导航的**报警服务>报警模板**进入报警模板页面。
2. 点击页面右上角的**创建报警模板**按钮，进入创建模板页面。
3. 填写基本信息中的模板名称和描述，方便您管理模板和备注模板用途。
4. 配置报警策略，在模板中添加报警规则的定义。
5. 单击**确认**后保存模板。

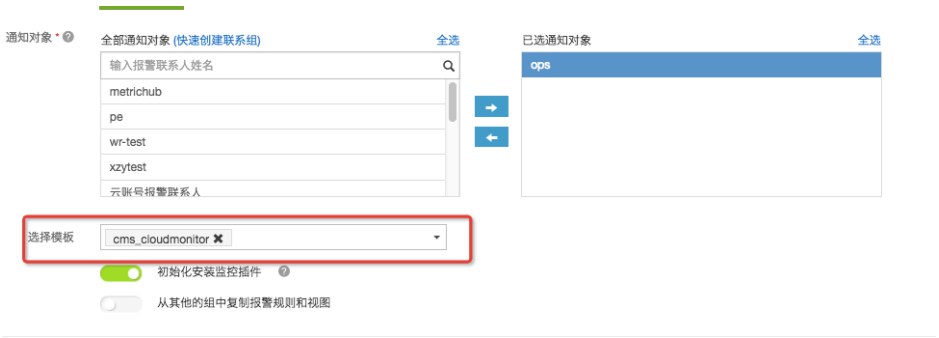
使用报警模板

使用报警模板有3种方式：

- 创建应用分组时，可以在创建分组的页面直接选择该分组需要使用的报警模板。为应用分组初始化报警规则。
- 在报警模板列表页面，将指定模板应用于选中的应用分组上。此方式为对应用分组重新生成报警规则，会在模板应用到分组时，删除分组原有的报警规则。
- 创建报警规则时，可以在资源范围选择**应用分组**后，选择需要使用的报警模板。此方式为对应用分组添加更多报警规则，不会删除原有报警规则。

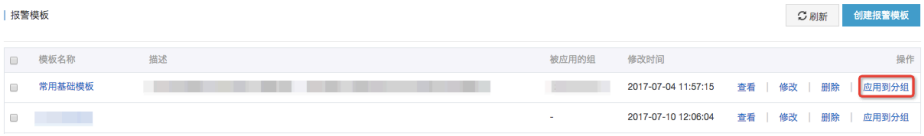
方法1. 创建应用分组时使用报警模板

您在为资源创建应用分组时，可以在创建分组的最后一步直接选择应用分组需要使用的报警模板，应用分组创建成功后云监控会按照报警模板为您生成应用分组维度的报警规则。



方法2. 将模板直接应用于应用分组

如果您已经创建好应用分组，但还未对应用分组创建报警规则，您可以在创建好模板后，直接将模板快速应用于分组上。



方法3. 创建报警规则时使用报警模板

如果您的应用分组需要添加更多报警规则，可以在创建报警规则页面的资源范围选择应用分组后，在设置报警规则时选择使用模板并选择相应的模板，快速创建报警规则。

使用一键报警

功能描述

一键报警功能为用户提供一键开启关键监控项报警的服务，旨在解决刚刚接触云服务的开发、运维人员，面对种类繁多的云产品和监控项时，无法快速建立起基本的云上监控报警体系，导致重要指标异常无法快速知晓的问题。

操作步骤

1. 登录云监控，进入报警服务菜单的**一键报警**功能页面。
2. 对需要设置报警的云产品开启一键报警按钮，完成设置。

3. 点击**一键报警**右侧的下拉按钮，可能快速查看为您自动生成的报警规则。该报警规则作用于您选中产品的当前实例及后续新生成的实例。

目前支持的产品及规则详情

服务名称	指标名称	规则描述
ECS	CPUUtilization （CPU使用率）	一分钟内最大值>90%，连续五次，沉默时间1小时，邮件通知
	vm.DiskUtilization （磁盘使用率）	一分钟内最大值>90%，连续五次，沉默时间1小时，短信、邮件通知
	vm.MemoryUtilization （内存使用率）	一分钟内最大值>90%，连续五次，沉默时间1小时，邮件通知
	InternetOutRate_Percent （公网流出带宽使用率）	一分钟内最大值>90%，连续五次，沉默时间1小时，邮件通知

RDS	CpuUsage （CPU使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	DiskUsage （磁盘使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，短信、邮件通知
	IOPSUsage （IOPS使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	ConnectionUsage （连接数使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时， 邮件通知
	DataDelay （只读实例延迟）	五分钟内最大值>5，连续五次，沉默时间1小时，邮件通知
SLB	DropConnection （监听每秒丢失连接数）	一分钟内最大值>0，连续五次，沉默时间1小时，邮件通知
	DropTrafficRX （监听每秒丢失入bit数）	一分钟内最大值>0，连续五次，沉默时间1小时，邮件通知
	DropTrafficTX （监听每秒丢失出bit数 ）	一分钟内最大值>0，连续五次，沉默时间1小时，邮件通知
Redis	CpuUsage （CPU使用率 ）	一分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	ConnectionUsage （连接数使用率）	一分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	MemoryUsage （内存使用率）	一分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	IntranetInRatio （写入带宽使用率）	一分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	IntranetOutRatio （读取带宽使用率）	一分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
MongoDB（副本集）	CPUUtilization （CPU使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	MemoryUtilization （内存使用百分比）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	DiskUtilization （磁盘使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	IOPSUtilization （IOPS使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	ConnectionUtilization （连接数使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
MongoDB （分片集群）	ShardingCPUUtilization （CPU使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	ShardingMemoryUtilization （内存使用百分比）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	ShardingDiskUtilization （磁盘使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知

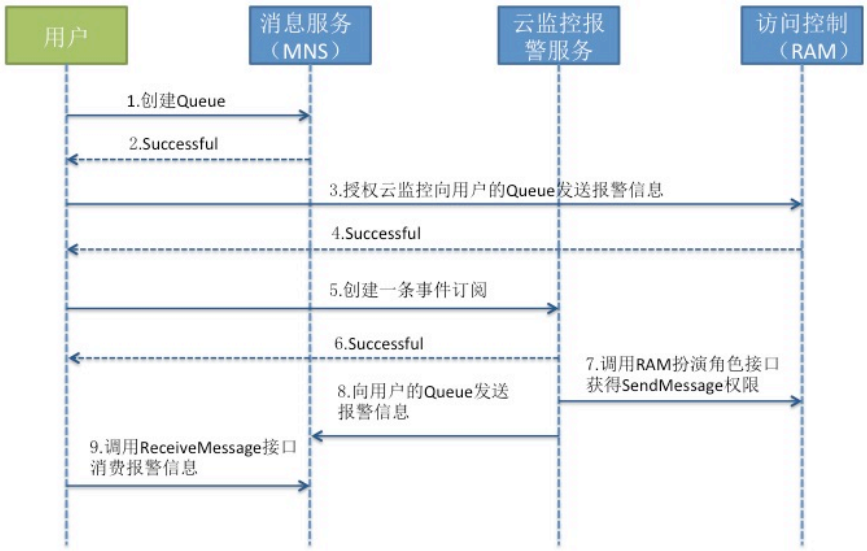
	ShardingIOPSUtilization（IOPS使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
	ShardingConnectionUtilization（连接数使用率）	五分钟内最大值>80%，连续五次，沉默时间1小时，邮件通知
HBase	LoadPerCpu	五分钟内最大值>3，连续三次，沉默时间1小时，邮件通知
	cpu_idle	五分钟内最大值<10，连续三次，沉默时间1小时，邮件通知
	compactionQueueSize	五分钟内最大值>2000，连续三次，沉默时间1小时，邮件通知
	rs_handlerQueueSize	五分钟内最大值>1000，连续三次，沉默时间1小时，邮件通知
	CapacityUsedPercent	五分钟内最大值>0.8，连续三次，沉默时间1小时，邮件通知
	zookeeper_tcp_count	五分钟内最大值>2000，连续三次，沉默时间1小时，邮件通知
ElasticSearch	ClusterStatus（集群状态）	一分钟内最大值>2，连续十次，沉默时间1小时，邮件通知
	NodeDiskUtilization（节点磁盘使用率 ）	一分钟内最大值>75%，连续十次，沉默时间1小时，邮件通知
	NodeHeapMemoryUtilization（节点HeapMemory使用率）	一分钟内最大值>85%，连续十次，沉默时间1小时，邮件通知
Opensearch 开放搜索	DocSizeRatiobyApp（存储容量使用率）	十分钟内最大值>85%，连续一次，沉默时间1小时，邮件通知
	ComputeResourceRatiobyApp（计算资源使用率）	十分钟内最大值>85%，连续一次，沉默时间1小时，邮件通知

事件订阅

事件订阅服务概览

事件订阅是云监控推出的一种报警信息获取方式，将生产出的报警信息写入用户的消息队列，供用户自行消费，对接自己的报警通知系统。

您可以在开通消息服务后，在云监控控制台订阅报警信息，服务流程图如下所示：



使用方法

使用方法

通过创建事件订阅，云监控会将报警信息推送到用户指定的消息队列中，用户可以通过消费队列中的报警信息对接自己的业务系统。

注意事项

向消息服务的队列推送报警信息的频率，也受通道沉默限制，同一报警规则告警后，24小时内状态不变时，不会再发送报警通知。

操作步骤

开通消息服务服务。

a. 消息服务产品介绍及开通链接查看。

b. 消息服务购买指导请查看消息服务购买文档

对云监控授权。

a. 在控制台选择“事件订阅”后，如果您是第一次使用事件订阅，需要向云监控授权Message Service 消息队列写入权限。

创建事件订阅。

a. 点击右上角“创建事件”，创建一个接收报警规则的事件。

b. 选取需要接收报警规则的队列信息和需要接收的报警类别。

消费报警信息。

您可以通过消息服务的API来消费报警数据，也可以通过Message Service的控制台查看接收情况。

a. 消息服务API文档

b. 消息服务Java SDK文档

报警信息格式

您在Message Service中收到的报警格式如下：

ECS报警内容：

```
{
"message":{
"expression":"平均值>80%",// 报警规则描述
"curValue":"85.65",
"unit":"%",//单位
"levelDescription":"发生告警",//报警状态,包含“发生告警”和“恢复告警”
"time":1464257700000,//报警发生时间
"metricProject":"acs_ecs",//产品名称
"userId":"1078500464551219",
"dimensions":"云服务器名称=yapot_server_1,云服务器实例
ID=AY14051913564762762e,IP=182.92.79.214,mountpoint=/mnt",//监控维度
"evaluationCount":"1",//重试次数
"period":"5分钟",//统计周期
"metricName":"磁盘使用率",// 监控指标名称
"alertName":"AY14051913564762762e_98591490-9eb4-42a1-ba2a-3bdbe04196df"
},
"type":0
}
```

SLB报警内容：

```
{
"message":{
"expression":"最大值>2.0Kb/s",// 报警规则描述
"curValue":"5",
"unit":"Kb/s", //单位
"levelDescription":"发生告警", //报警状态,包含“发生告警”和“恢复告警”
"time":1451767500000, //报警发生时间
"metricProject":"acs_slb", //产品名称
"userId":"UserName", //
"dimensions":"instanceId=InstanceId,端口=3306,vip=10.157.161.2",//监控维度
"evaluationCount":"3",//重试次数
"period":"15分钟", //统计周期
"metricName":"每秒流入数据量", // 监控指标名称
"alertName":"14a850c9d49-cn-beijing-btc-a01_3306_3da5a7df-0821-4cce-93bf-dafe8ce56a68"
},
"type":0 //保留字段，0表示报警通知，有发生有恢复，1故障通知，触发一次报警一次，不记录状态。
}
```

访问控制

概述

云监控支持通过**访问控制**实现子账号对云服务监控的监控数据、管理报警规则、管理联系人和联系人组的权限控制。

访问控制的详细使用可查看**产品文档**。

注意事项

目前支持以下云产品的监控数据查询：

- 云服务器 ECS
- 云数据库 RDS
- 负载均衡
- 对象存储 OSS
- CDN
- 云数据库 Memcache 版
- 弹性公网 IP
- 云数据库 Redis 版
- 消息服务
- 日志服务

权限说明

访问控制系统权限中的“只读访问云监控(CloudMonitor)的权限”包含查询监控数据、报警服务相关数据。

鉴权类型

除基本的子账号权限控制外，目前支持时间、MFA、IP三种鉴权类型。

资源描述

目前不支持细粒度资源描述，资源授权用“*”通配。

操作描述

监控数据

查询数据的action分为两部分，各产品的实例列表展示和云监控的查询监控数据。授权子账号登录云监控portal查看监控数据时，需要同时授权对应的产品实例列表权限和监控数据查询权限。

对应的接口Action如下表所示：

产品名称	action
CMS	QuerMetricList
CMS	QueryMetricLast
ECS	DescribeInstances
RDS	DescribeDBInstances
SLB	DescribeLoadBalancer*
OSS	ListBuckets
OCS	DescribeInstances
EIP	DescribeEipAddresses
Aliyun Cloud for Redis	DescribeInstances
Message Service	ListQueue
CDN	DescribeUserDomains

报警服务

报警服务包括报警规则管理、联系人和联系人组管理、事件订阅相关功能，具体Action见下表。

查询操作对应的Action如下：

Action	含义

QueryAlarm	查询报警规则
QueryAlarmHistory	查询报警历史
QueryContactGroup	查询联系人组
QueryContact	查询联系人
QuerySms	查询短信使用条数
QueryMns	查询事件订阅配置

管理操作对应的Action如下：

Action	含义
UpdateAlarm	修改报警规则
CreateAlarm	创建报警规则
DeleteAlarm	删除报警规则
DisableAlarm	禁用报警规则
EnableAlarm	启用报警规则
CreateContact	创建联系人
DeleteContact	删除联系人
UpdateContact	修改联系人
SendEmail	发送邮件验证码
SendSms	发送短信验证码
CheckEmail	检查邮件验证码
CheckSms	检查短信验证码
CreateGroup	创建联系人组
DeleteGroup	删除联系人组
UpdateGroup	修改联系人组
CreateMns	创建事件订阅
DeleteMns	删除事件订阅
UpdateMns	修改事件订阅