阿里云
云监控

用户指南

文档版本：20190523

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **禁止:** 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 **警告:** 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 **说明:** 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
粗体	表示按键、菜单、页面名称等UI元素。	单击 确定。
`courier` 字体	命令。	执行 `cd /d C:/windows` 命令，进入Windows系统文件夹。
*## *	表示参数、变量。	`bae log list --instanceid` *`Instance_ID`*
[]或者[a|b]	表示可选项，至多选择一个。	`ipconfig` *`[-all|-t]`*
{}或者{a|b}	表示必选项，至多选择一个。	`swich` *`{stand | slave}`*

目录

1 可视化报表

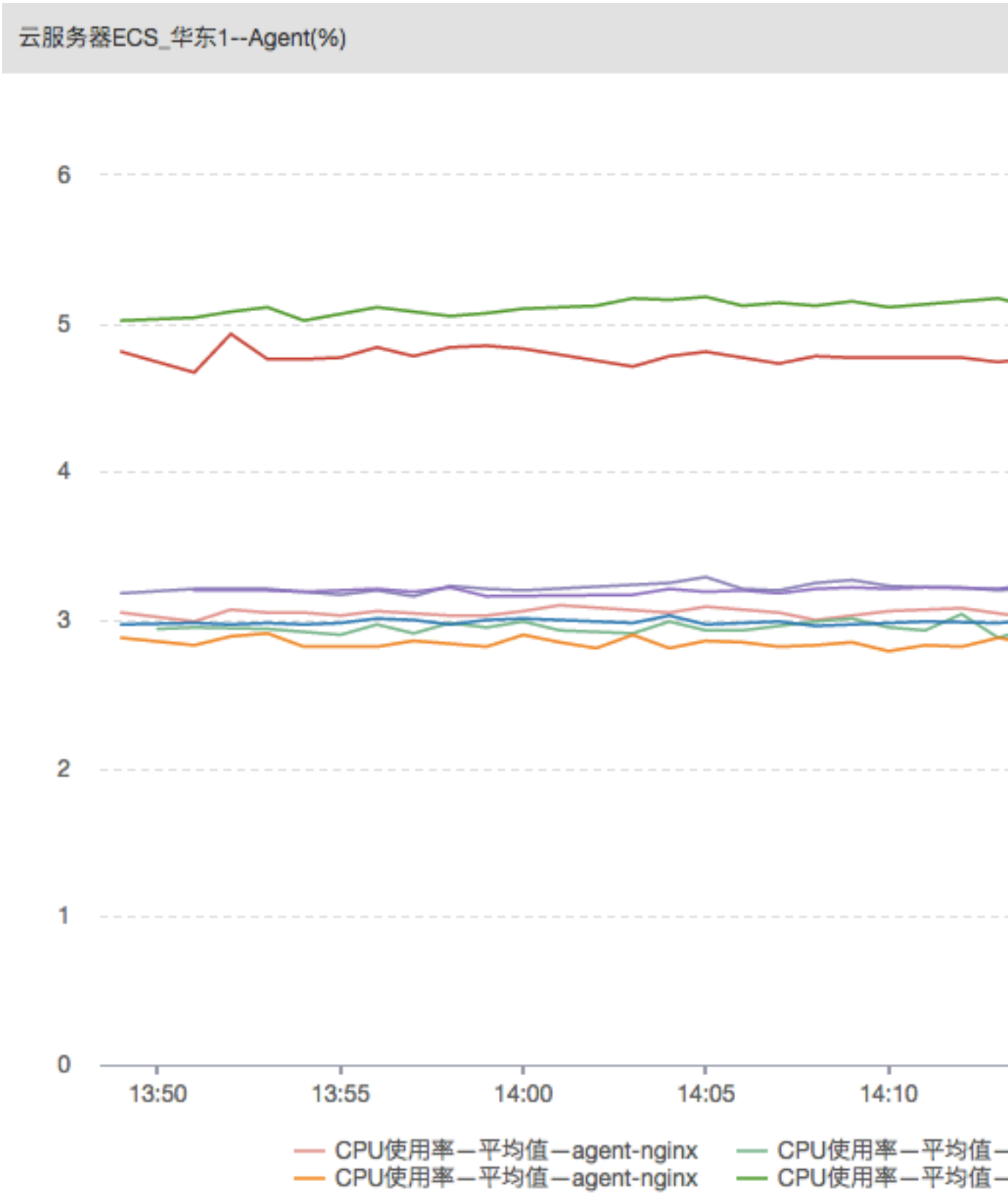
1.1 使用Dashboard

1.1.1 Dashboard概览

使用云监控的Dashboard，您不仅能够查看服务概貌，还可以查看监控细节，并排查故障。

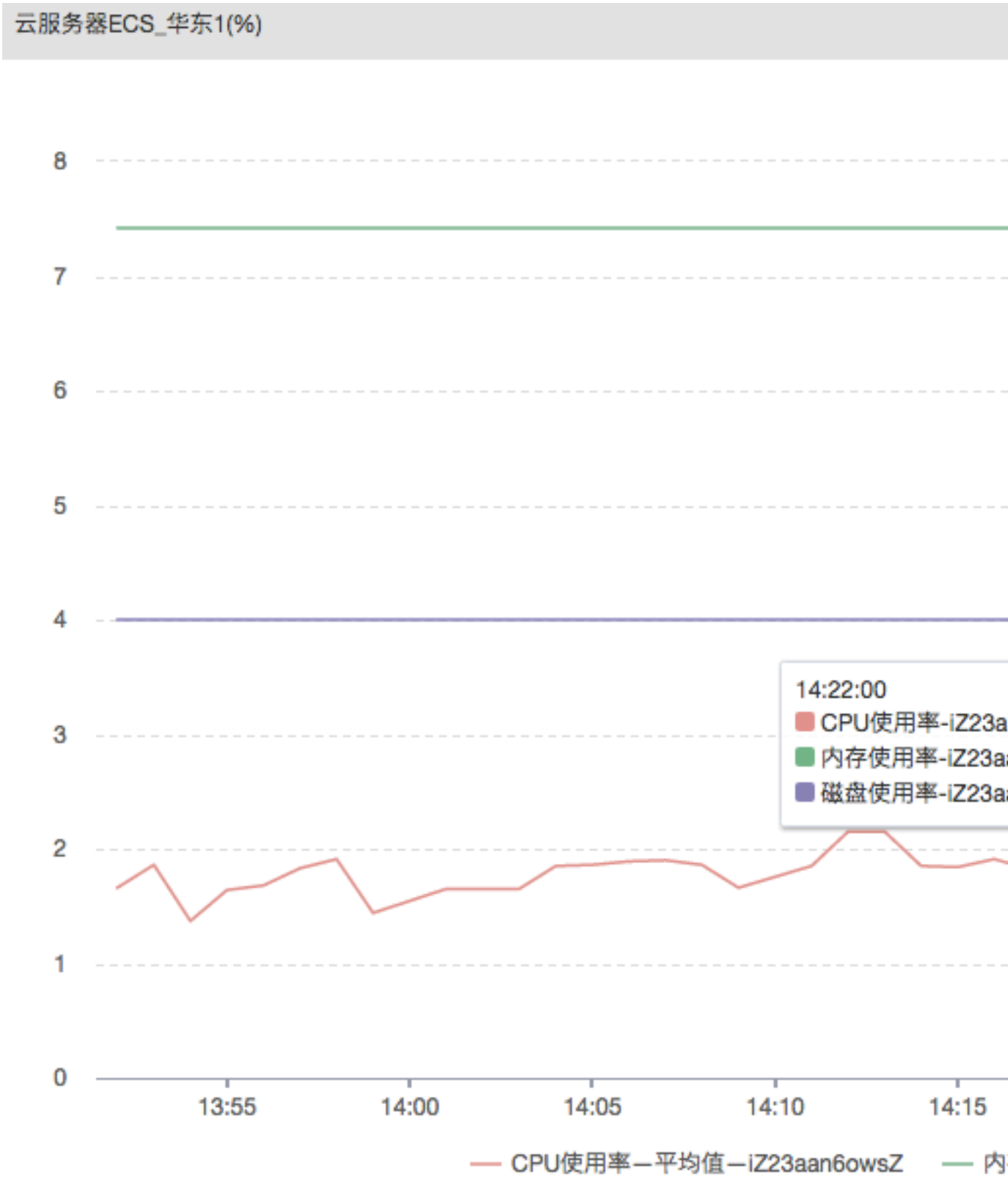
展示多个实例的监控数据走势

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

云监控可在一张图表中展示 一个ECS 实例的 CPU 使用率、内存使用率、磁盘使用率等多个指标。



展示实例的资源消耗排序

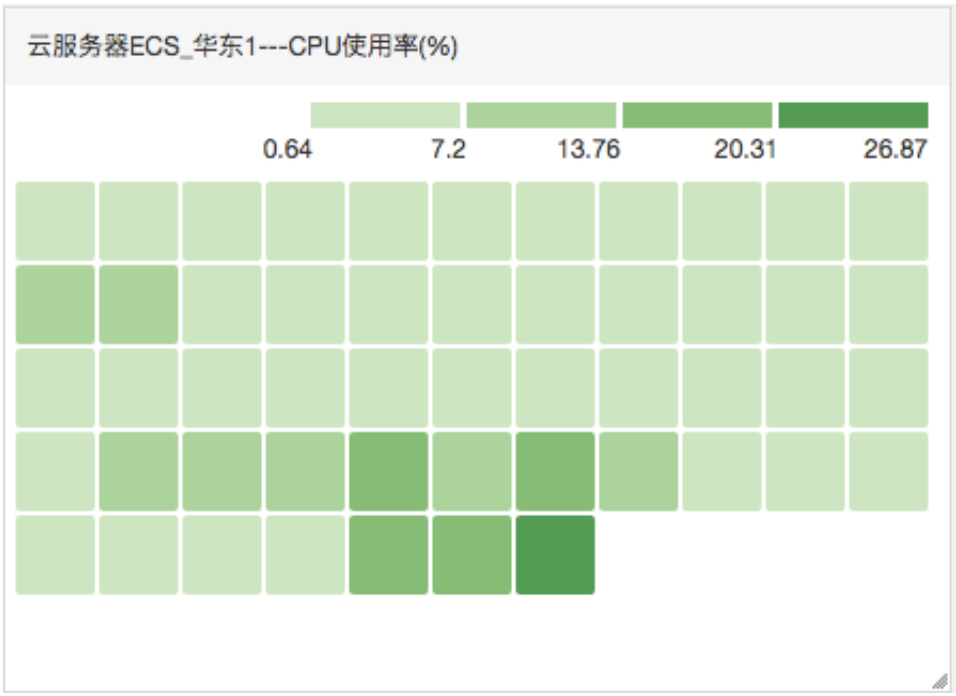
例如您有 20 台机器，通过表格展示可以查看 20 台机器的 CPU 使用率从大到小的排序。快速了解资源消耗情况，更合理的使用资源，减少不必要的花费。

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	AY1406121616449758d2Z	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，您可以将各类产品指标添加到监控大盘，在运维大屏上全屏展示。

1.1.2 管理监控大盘

您可以创建监控大盘、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

云监控的Dashboard提供用户自定义查看监控数据的功能。您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。

> **说明:**
>
> - 云监控会为您初始化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。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中Dashboard下的自定义大盘，进入当前监控大盘页面。
3. 默认展示ECS全局监控大盘，可在下拉列表中选择其他监控大盘。

4. 单击页面右上角的全屏，可全屏查看监控大屏。
5. 选择时间范围：单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。

6. 自动刷新：开启自动刷新后，当您选择查询1小时、3小时等的查询时间跨度时，可每分钟自动刷新一次。
7. 监控项的单位展示在图表名称的括号内。
8. 鼠标悬停在一个图表某个时间点时，其他图表也会跟随显示该时间点的监控值。

创建监控大盘

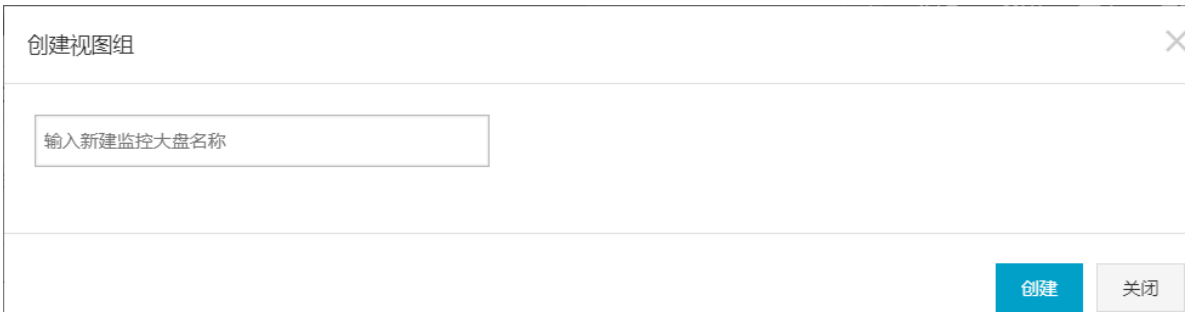
当您的业务比较复杂，默认的ECS监控大盘无法满足您的监控可视化需求时，您可以创建新的监控大盘，自定义需要展示的图表。

> **说明:**
> 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. 单击左侧导航栏中Dashboard下的自定义大盘，进入当前监控大盘页面。

3. 单击页面右上角的创建监控大盘，进入创建视图组页面。



4. 输入监控大盘名称，点击创建按钮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，您可以根据自身业务需要添加各种监控图表。
5. 鼠标悬停在监控大盘名称上，右侧会出现修改名称，单击可修改大盘名称。

删除监控大盘

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:**
> 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. 单击左侧导航栏中Dashboard下的自定义大盘，进入当前监控大盘页面。
3. 在下拉列表中选择要删除监控大盘，切换到当前大盘页面，单击页面右上角的删除当前大盘按钮，即可删除当前监控大盘。

1.1.3 添加监控图表

本文为您介绍如何为监控大盘添加监控图表，实现查看更多监控数据的目的。

背景信息

云监控已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，可以通过添加监控图表来实现。

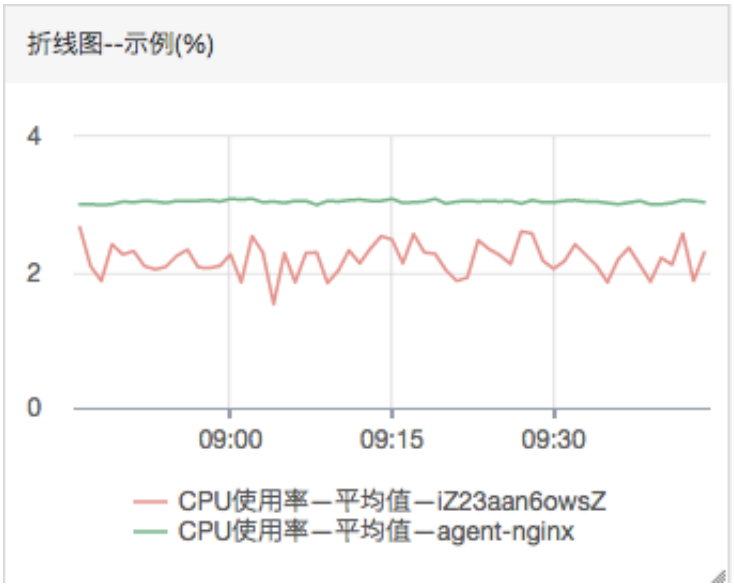
当您的业务比较复杂，默认的ECS监控大盘无法满足您的监控可视化需求时，您需要创建新的监控大盘，并添加监控图表到新的大盘展示自定义监控数据。

添加监控图表的准备工作

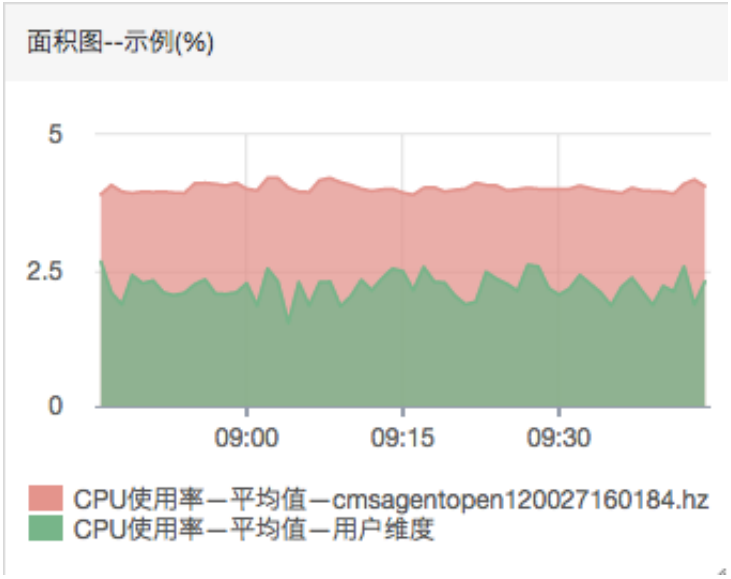
为自定义大盘添加监控图表，需要先创建好自定义大盘。

在添加监控图表之前，我们先了解一下有哪些图表类型，以便您可以准确使用图表展示监控数据。

- 折线图：按时间序列展示监控数据，可以添加多个监控项。



- **面积图：按时间序列显示监控数据，可以添加多个监控项。**

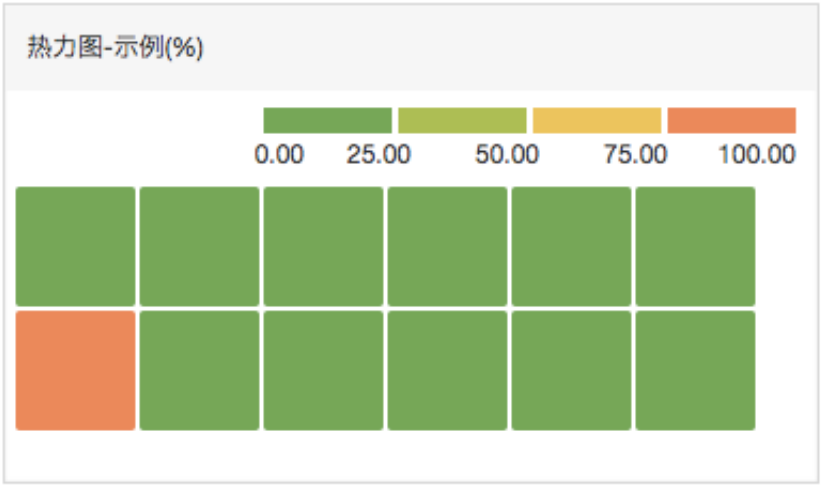


- **TopN表格：显示最近三小时内最后时刻监控数据的排序，最多显示正序的1000条或倒序的1000条数据。例如ECS分组中所有机器CPU使用率从大到小的排序。只能添加一个监控项。**

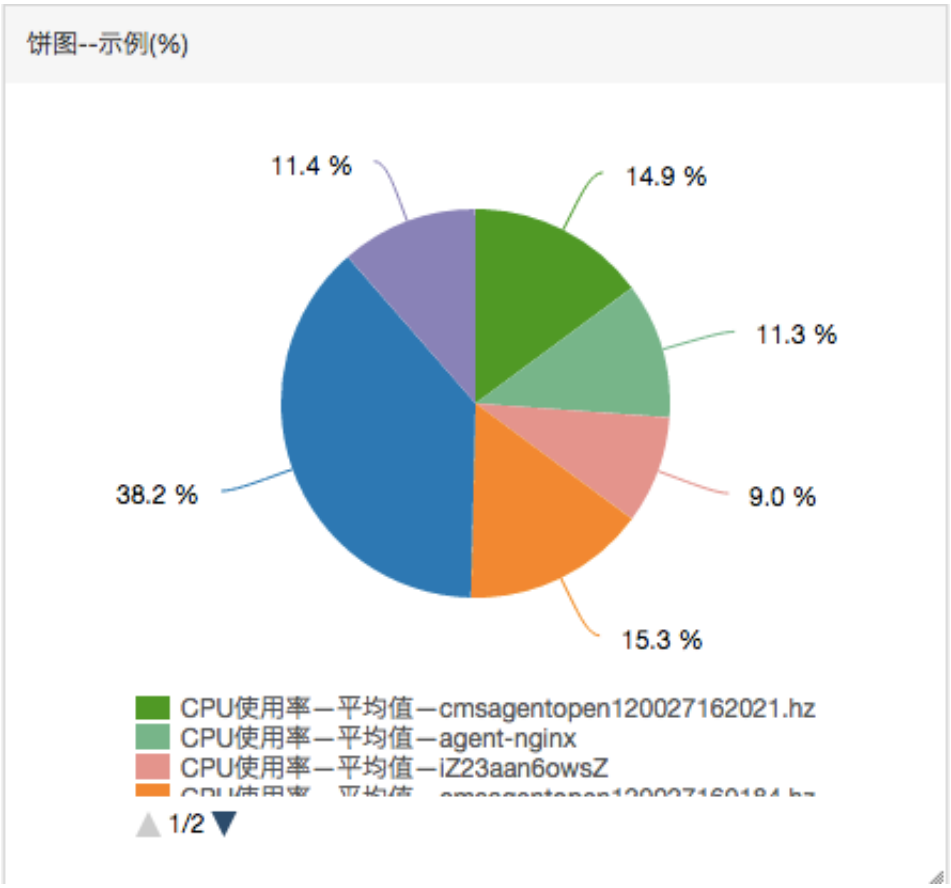
表格--示例(%)

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

- 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。



- 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。



添加监控图表的实施步骤

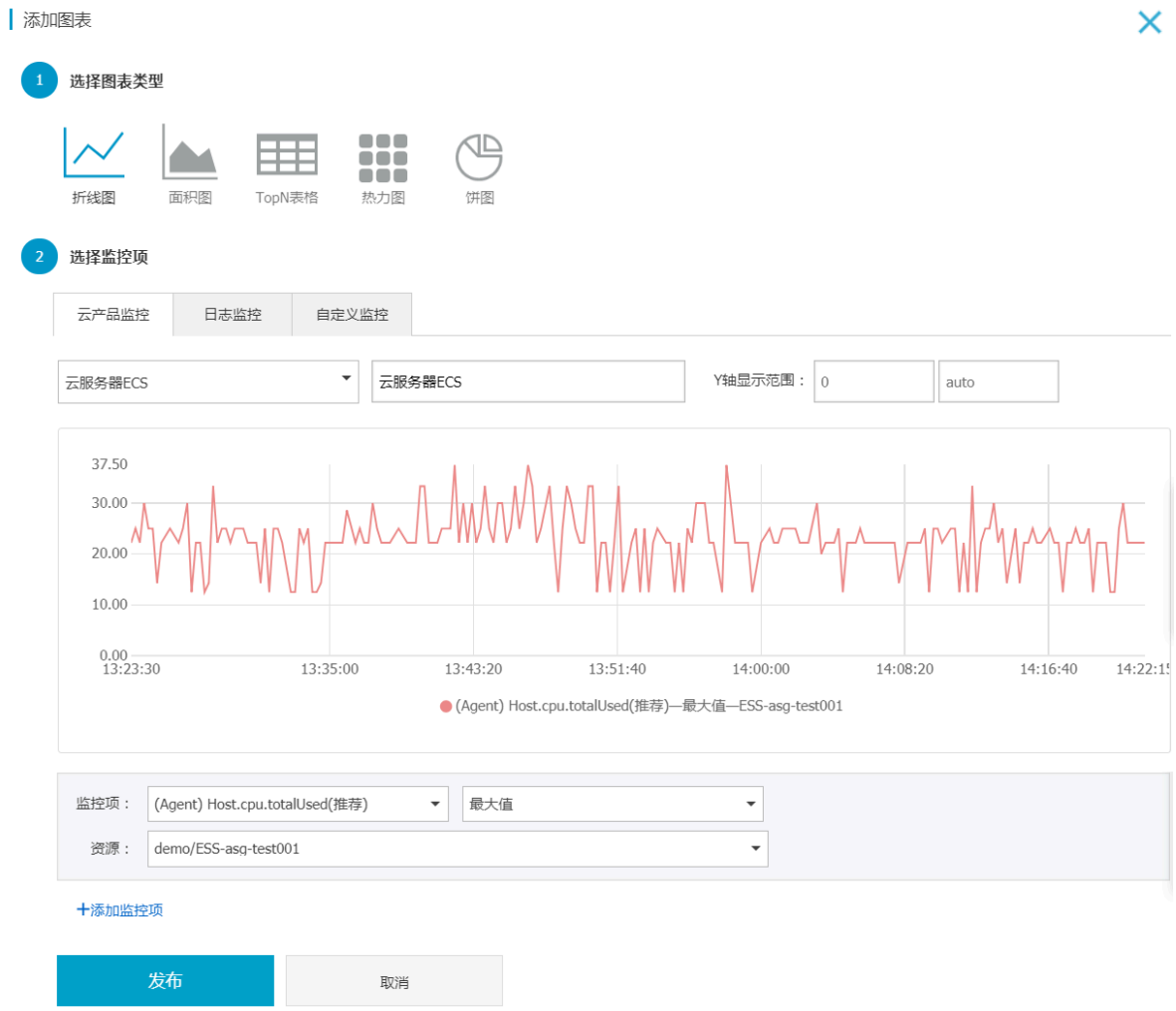
注意事项

说明:

- 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、网络出流量等7张监控图表。
- 每张监控大盘最多创建20个图表。
- 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。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中Dashboard下的自定义大盘，进入当前监控大盘页面。
3. 在当前监控大盘右侧下拉列表中选择要添加图表的大盘，单击右上角的添加图表，进入添加图表页面。



4. 选择图表类型：从折线图、面积图、TopN表格、热力图和饼图中选择一种图表类型。

5. 选择监控项：分为云产品监控、日志监控、自定义监控。以云产品监控为例，选需要查看的云产品并为图表命名，然后选择需要查看的监控指标和统计方式。

   · 选择需要查看的监控项。
   · 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，请单击添加监控项，重复上述操作即可。

6. 单击发布，即可在监控大盘中看到您所添加的图表。
7. （可选）拖拽图表右侧、下侧、右下侧，可调整图表的高度和宽度。

监控项说明

· 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。
· 自定义监控：用户通过自定义监控自行添加的监控。
· 监控项：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。

1.2 对接Grafana

本文为您介绍如何将云监控的数据添加到Grafana中进行展示。

背景信息

云监控为云上用户提供常用云产品的监控数据和用户自定义上报的监控数据。在可视化展示层面，除了在云监控控制台查看监控图表外，您还可以将云监控的数据添加到Grafana中进行展示。

对接Grafana的准备工作

1. 下载安装Grafana

   本文以CentOS为例，介绍Grafana的两种安装方式：

   安装方式一：

   ```
   yum install https://s3-us-west-2.amazonaws.com/grafana-releases/release/grafana-5.3.0-1.x86_64.rpm
   ```

   安装方式二：

   ```
   wget https://s3-us-west-2.amazonaws.com/grafana-releases/release/grafana-5.3.0-1.x86_64.rpm
   ```

```
sudo yum localinstall grafana-5.3.0-1.x86_64.rpm
```

Grafana的其他详细安装步骤请参见Grafana官方文档。

2. 启动Grafana

下载载安装完成后，输入命令 `service grafana-server start` 启动服务。

对接Grafana的实施步骤

1. 安装云监控数据源服务插件

请确认Grafana的插件目录位置。例如：在CentOS的插件目录为`/var/lib/grafana/plugins/`，安装插件，重启grafana-server。

CentOS安装命令如下：

```
cd /var/lib/grafana/plugins/
git clone https://github.com/aliyun/aliyun-cms-grafana.git
service grafana-server restart
```

您也可以下载aliyun-cms-grafana.zip插件解压后，上传服务器的Grafana的plugins目录下，重启grafana-server即可。

说明:

此插件版本目前不支持对监控数据设置报警。

2. 配置云监控数据源插件

Grafana成功部署后，默认访问端口3000，用户名：admin、密码：admin。

a. 成功登录后，进入Grafana的主页面，单击左上方的Configuration，在弹出的列表中选Data Sources。

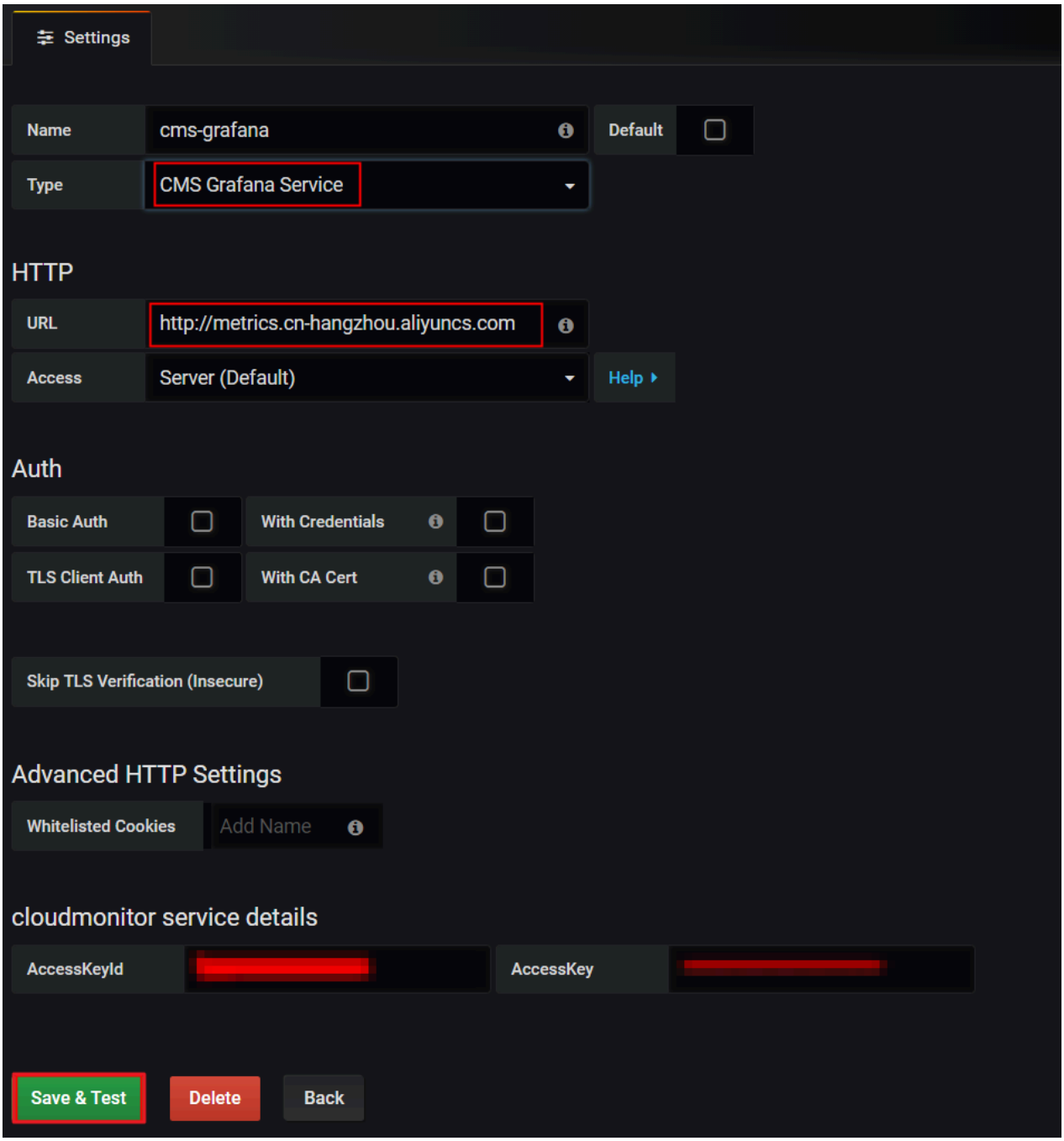
b. 成功进入Data Sources页面后，单击右上方的Add data source，添加新的数据源。

c. 填写云监控数据源的配置项。

配置项	配置内容
datasource	Name表示名称，请自定义一个新数据源的名称。Type请选择CMS Grafana Service。
Http	URL样例：`http://metrics.cn-shanghai.aliyuncs.com`，不同域选择请参考云监控接入地址。 Access默认即可。

配置项	配置内容
Auth	采用默认配置即可。
cloudmonitor service details	分别填写具备读取权限的AK信息。建议AK使用子帐号的AK。

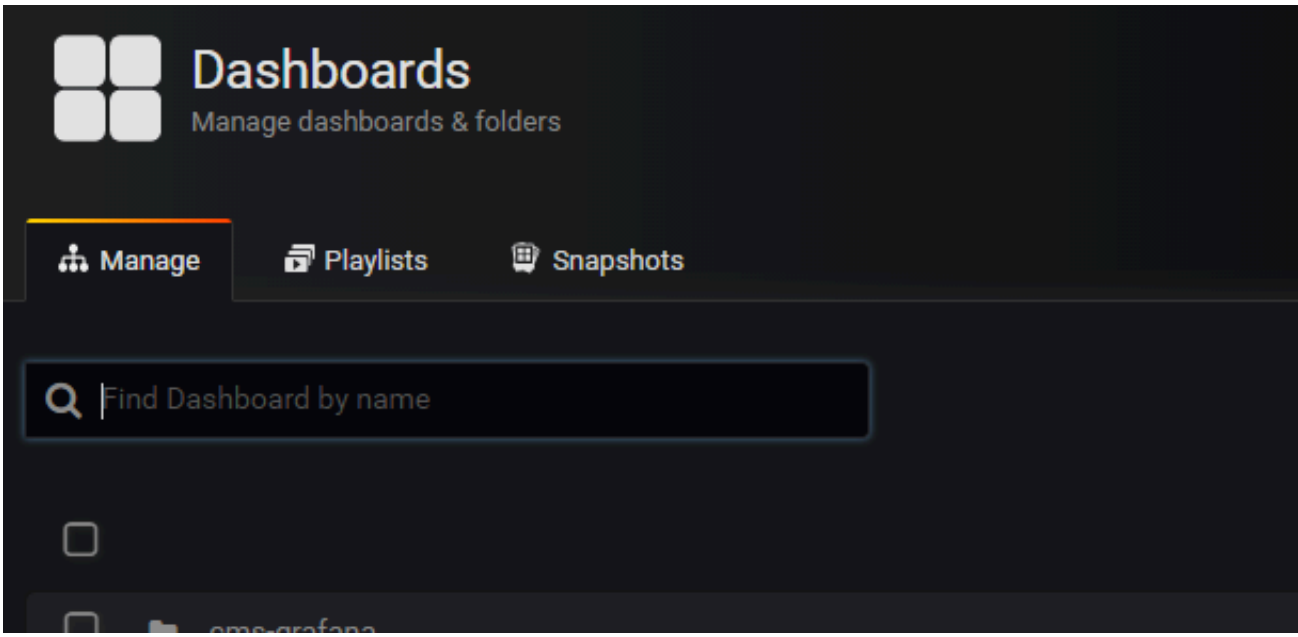
配置示例如下图：



d. 配置完成后，单击Save &Test即可完成添加DataSource。

3. 创建Dashboard

a. 单击左上方的Dashboards，在弹出的列表中选Manage，进入Manage页面。



b. 单击+Dashboard创建Dashboard。您可以选择创建一个Folder后，再创建Dashboard，您也可以导入其他Dashboard。

4. 配置Graph图表

a. 创建Dashboard后，在New Panel的Add下选择Graph图表，单击Pannel Title，在弹出的窗口中单击Edit。

b. 在Metrics配置中，选择datasource为cms-grafana，输入Project、Metric、period、Y轴和X轴等。如下图所示：

c. Project、Metric、Period等参数详情，请参见*QueryMetricList*；

Group：云账户所在云监控的应用分组；

Dimensions：Project与Metric所在监控项最新监控数据的实例集合，若选Group，则为该Group下的实例；

Y轴：可支持多选；

X轴：timestamp；

Y-column describe：对Y-column的区分描述。

如需了解更多Graph信息，请单击此处。

说明:

- 所有参数均可按*QueryMetricList*要求手动输入;
- 所有已选择(已输入)参数均可输入null取消;
- 若对应场景下Dimensions提示的实例信息不全，可刷新或按样例手动输入InstanceId的值即可。

自定义监控:

自定义监控的部分参数信息需手动输入，参数说明:

- Project：acs_customMetric_+ 云账号ID;
- Metric：上报监控数据的metricName;
- Period：上报监控数据时的Period;
- Group：上报监控数据时的Metric对应的分组ID;
- Dimensions：上报监控数据时的Dimension，暂不支持下拉选择，只支持输入单个Dimension，若输入多个，默认选第一个;

说明:

若在云监控控制台的dimensions格式为env: public, step: 5-ReadFromAlertOnline样例，请用'&'替换示例中的','后拼接输入。

- Y-column：上报监控数据时的Average、Maximum、Minimum、Sum、SampleCount、P10、P20、P99等；
- X-column：Timestamp。

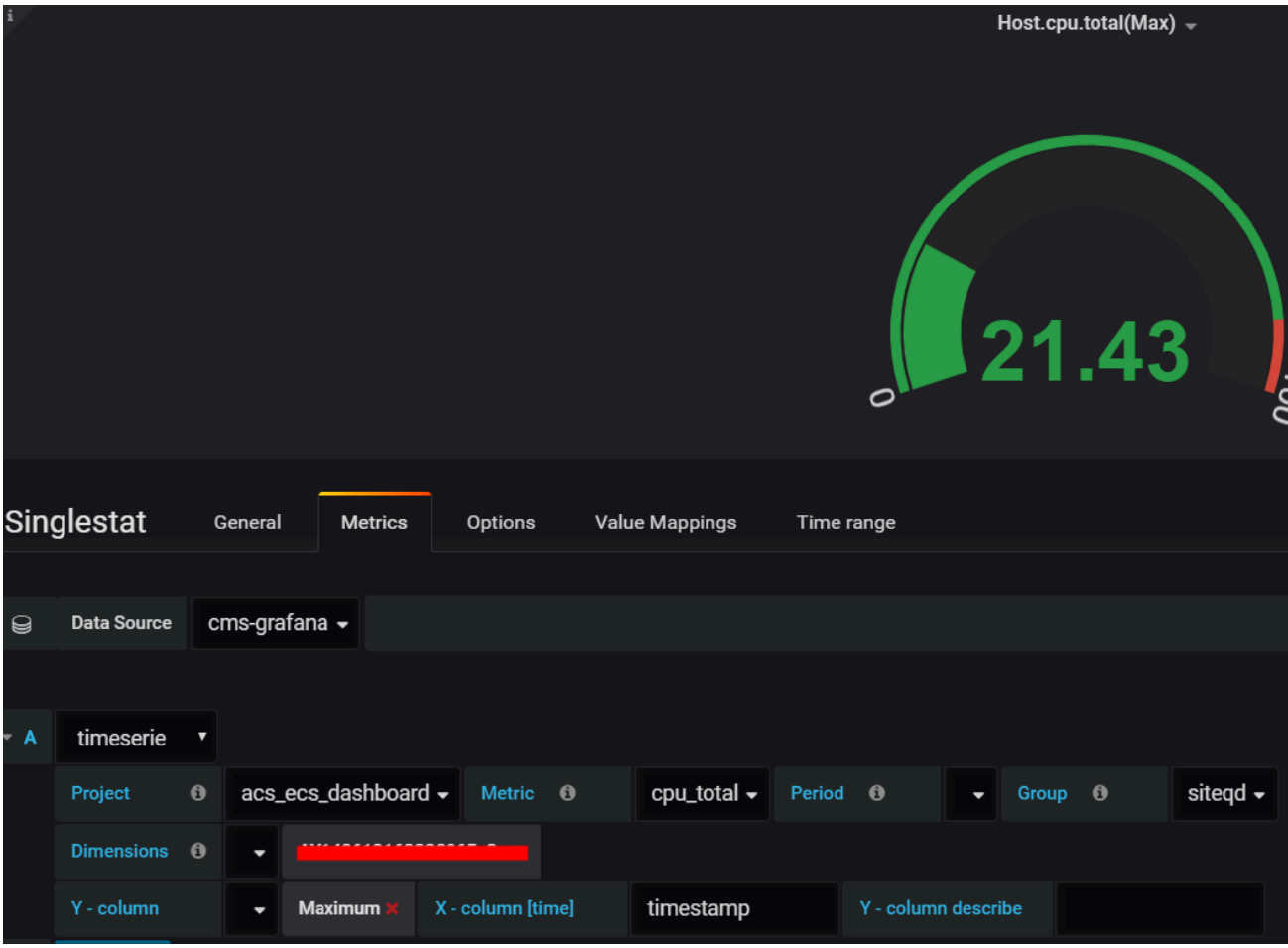
示例如下图所示：

5. 配置Singlestat面板

   a. 在New Panel的Add下选择Singlestat，单击Pannel Title，在弹出的窗口中单击Edit；

   b. Metric配置可参考前面的配置Graph图表。

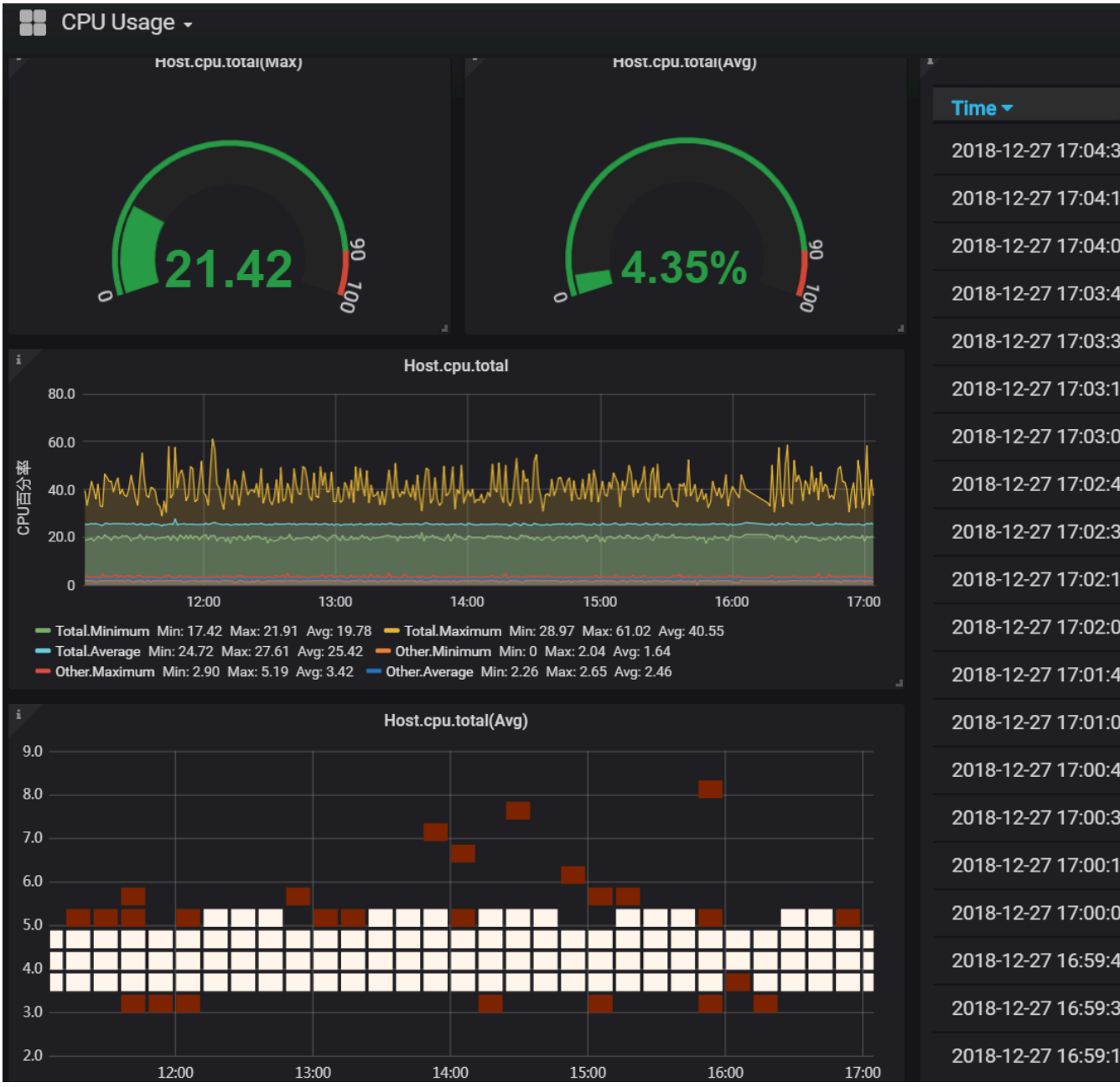
   示例如下图所示：

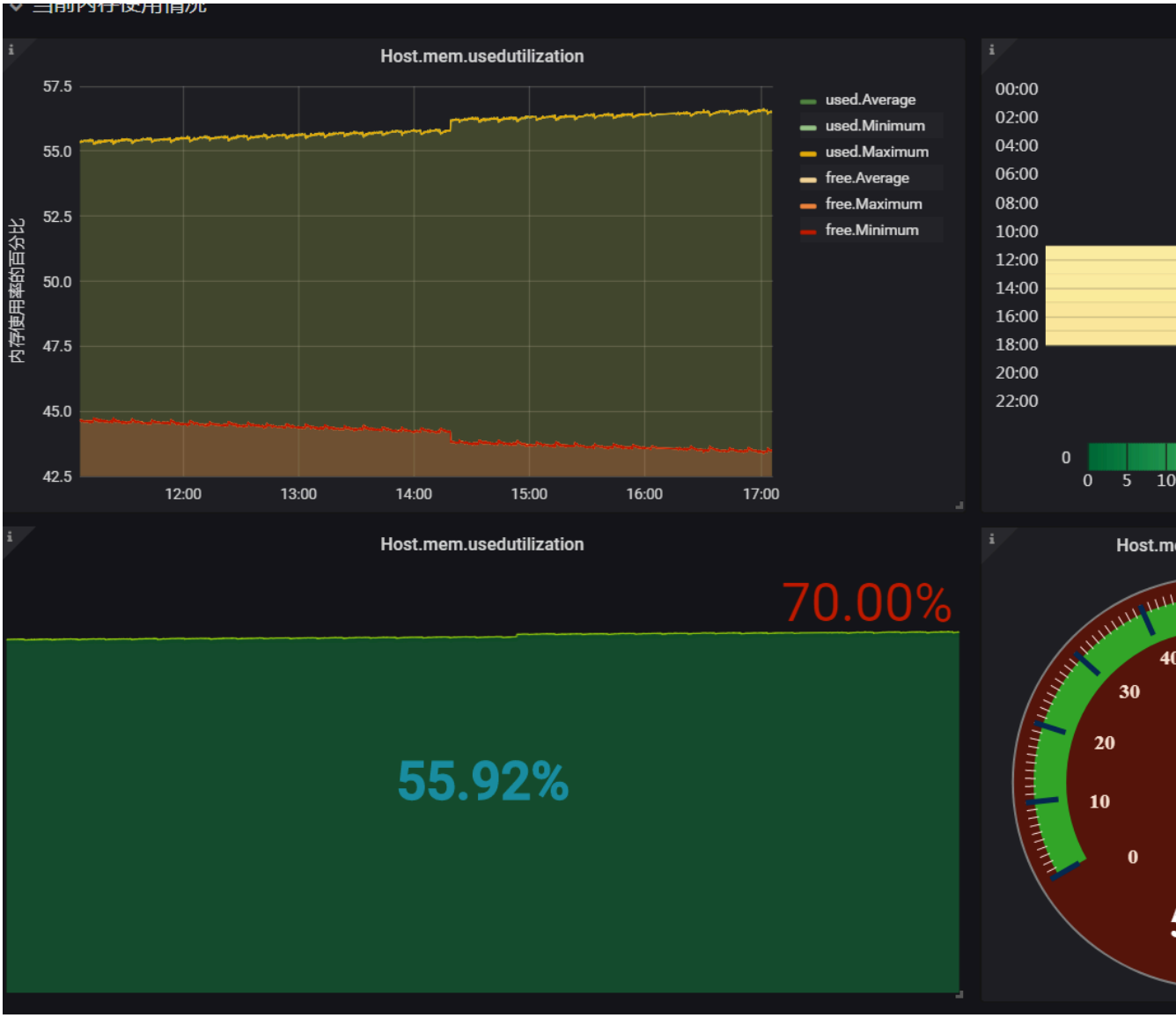


如您需了解更多*Singlestat*信息，请单击此处。

6. 查看结果

完成以上步骤的配置后，即可通过Grafana创建阿里云监控Dashboard并查看监控结果。




Host.mem.usedutilization
57.5
55.0
52.5
50.0
47.5
45.0
42.5
内存使用率的百分比
12:00
13:00
14:00
15:00
16:00
17:00
used.Average
used.Minimum
used.Maximum
free.Average
free.Maximum
free.Minimum
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
20:00
22:00
0
0 5 10
Host.mem.usedutilization
70.00%
55.92%
Host.m
40
30
20
10
0

2 主机监控

2.1 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，为您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。

主机监控服务通过安装在主机中的插件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查询以及排查故障时的监控数据查询。

混合云监控解决方案

主机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。

说明:

- 支持Linux操作系统和Windows操作系统，不支持UNIX操作系统。
- Linux操作系统安装插件需要Root权限；Windows操作系统安装插件需要管理员权限。
- 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

主机监控为您提供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。

报警能力

主机监控对以上所有监控项提供报警功能，您可以选择在实例、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。

2.2 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的CPU使用率、内存使用率以及进程打开文件数。如果您添加了进程关键字，还可以采集包含关键字的进程个数。

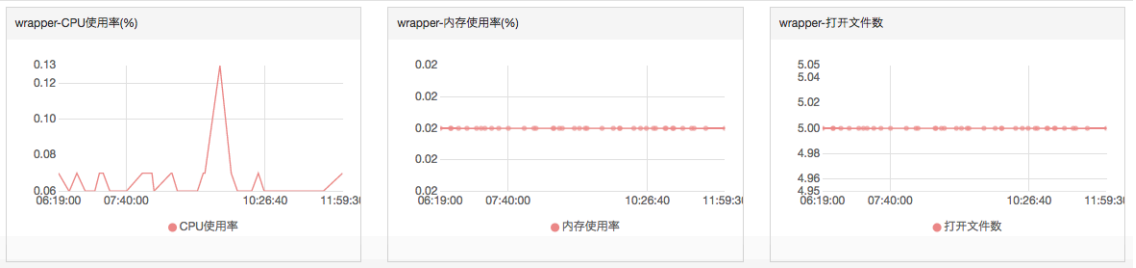
查看活跃进程消耗

- 云监控插件会每分钟统计一次CPU消耗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，请参考Linux的`top`命令。
- 当前进程打开文件数，请参考Linux的`lsof`命令。

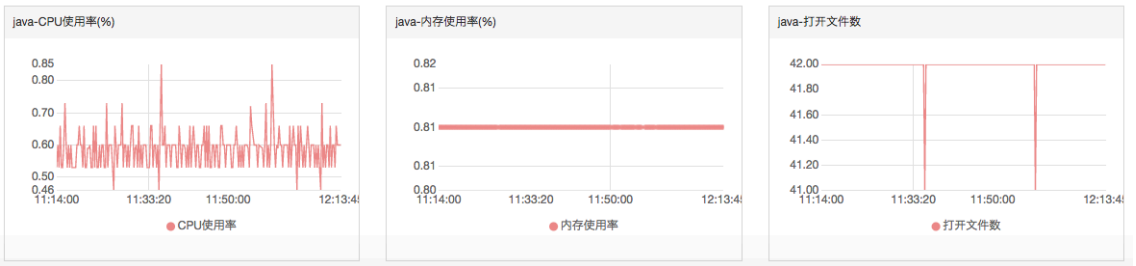
说明:

- 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，是因为这里的采集结果为多核CPU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。
  - 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。



  - 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

  假设您的主机当前运行了如下几个进程：

  - `/usr/bin/java -Xmx2300m -Xms2300m org.apache.catalina.startup.Bootstrap`
  - `/usr/bin/ruby`
  - `nginx -c /ect/nginx/nginx.conf`

  您添加了6个进程关键字，采集结果分别如下：

  - 添加进程关键字为：`ruby`，采集进程数：1，命中进程名称。
  - 添加进程关键字为：`nginx`，采集进程数：1，命中进程名称与参数。
  - 添加进程关键字为：`/usr/bin`，采集进程数：2，命中路径(两个进程包含这个路径)。
  - 添加进程关键字为：`apache.catalina`，采集进程数：1，命中部分参数。
  - 添加进程关键字为：`nginx.conf`，采集进程数：1，命中部分参数。
  - 添加进程关键字为：`-c`，采集进程数：1， 命中部分参数。

  操作步骤

  1. 登录云监控控制台。
  2. 单击左侧导航栏中的主机监控，进入主机监控页面。
  3. 单击需要添加进程监控的主机名称，或单击操作中的监控图表，进入主机的监控详情页。
  4. 单击进程监控页签，切换到进程监控页面。
  5. 在进程数监控图表，您可以添加进程关键字，统计对应进程数量。单击添加进程监控 按钮，进入添加进程监控页面。
  6. 输入进程名称或进程关键字，单击增加即可。

- 删除指定进程监控

  1. 登录云监控控制台。
  2. 单击左侧导航栏中的主机监控，进入主机监控页面。
  3. 单击需要添加进程监控的主机名称，或单击操作中的监控图表，进入主机的监控详情页。
  4. 单击进程监控页签，切换到进程监控页面。
  5. 在进程数监控图表上，单击添加进程监控 按钮，进入添加进程监控页面。
  6. 在列表中，单击操作栏中的删除，可删除对应的进程监控。

- 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. 单击左侧导航栏中的主机监控，进入主机监控页面。
  3. 选择需要添加进程监控报警的主机，单击操作栏中的报警规则，进入报警规则页面。
  4. 单击右上角的新建报警规则按钮，进入创建报警规则页面。
  5. 在设置报警规则的规则描述下拉列表中，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，可以单击添加报警规则一次为多个进程配置报警规则。

2.3 GPU监控

GPU监控数据可以通过云监控控制台和API查询。

监控指标说明

GPU相关监控指标提供如下三个维度的数据：GPU、实例、分组。

- GPU维度监控指标

  GPU维度的监控指标采集每个GPU层面的监控数据，GPU维度的监控指标如下表所示：

MetricName	单位	名称	dimensions
gpu_memory_freespace	Byte	GPU维度显存空闲量	instanceId,gpuId
gpu_memory_totalspace	Byte	GPU维度显存总量	instanceId,gpuId
gpu_memory_usedspace	Byte	GPU维度显存使用量	instanceId,gpuId

MetricName	单位	名称	dimensions
gpu_gpu_usedutilization	%	GPU维度GPU使用率	instanceId,gpuId
gpu_encoder_utilization	%	GPU维度编码器使用率	instanceId,gpuId
gpu_decoder_utilization	%	GPU维度解码器使用率	instanceId,gpuId
gpu_gpu_temperature	℃	GPU维度GPU温度	instanceId,gpuId
gpu_power_readings_power_draw	W	GPU维度GPU功率	instanceId,gpuId
gpu_memory_freeutilization	%	GPU维度显存空闲率	instanceId,gpuId
gpu_memory_useutilization	%	GPU维度显存使用率	instanceId,gpuId

- 实例维度监控指标

  实例维度监控指标对单个ECS实例上的多个GPU监控数据做最大值、最小值、平均值的聚合，便于查询实例层面的整体使用情况。

MetricName	单位	名称	dimensions
instance_gpu_decoder_utilization	%	实例维度GPU解码器使用率	instanceId
instance_gpu_encoder_utilization	%	实例维度GPU编码器使用率	instanceId
instance_gpu_gpu_temperature	℃	实例维度GPU温度	instanceId
instance_gpu_gpu_usedutilization	%	实例维度GPU使用率	instanceId
instance_gpu_memory_freespace	Byte	实例维度GPU显存空闲量	instanceId

MetricName	单位	名称	dimensions
instance_gpu_memory_freeutilization	%	实例维度GPU显存空闲率	instanceId
instance_gpu_memory_totalspace	Byte	实例维度GPU显存总量	instanceId
instance_gpu_memory_usedspace	Byte	实例维度GPU显存使用量	instanceId
instance_gpu_memory_usedutilization	%	实例维度GPU显存使用率	instanceId
instance_gpu_power_readings_power_draw	W	实例维度GPU功率	instanceId

- 分组维度监控指标

  分组维度监控指标对单个应用分组里的多个ECS 实例的监控数据做最大值、最小值、平均值的聚合，便于查询集群层面的整体使用情况。

MetricName	单位	名称	dimensions
group_gpu_decoder_utilization	%	分组维度GPU解码器使用率	groupId
group_gpu_encoder_utilization	%	分组维度GPU编码器使用率	groupId
group_gpu_gpu_temperature	℃	分组维度GPU温度	groupId
group_gpu_gpu_usedutilization	%	分组维度GPU使用率	groupId
group_gpu_memory_freespace	Byte	分组维度GPU显存空闲量	groupId
group_gpu_memory_freeutilization	%	分组维度GPU显存空闲率	groupId

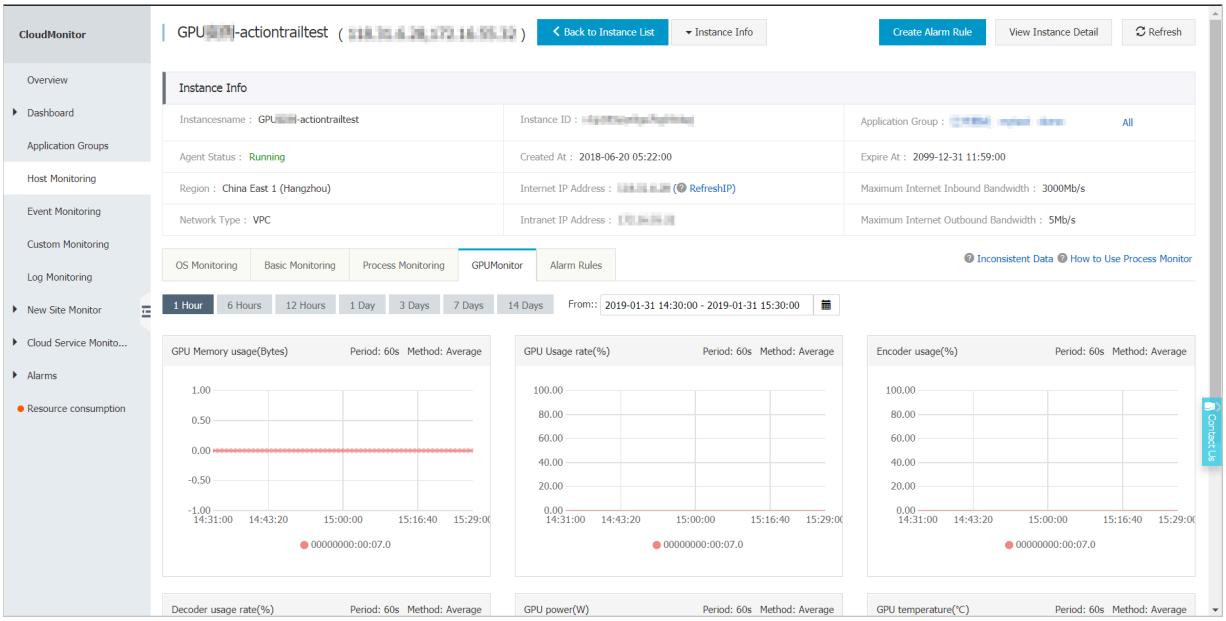
MetricName	单位	名称	dimensions
group_gpu_memory_totalspace	Byte	分组维度GPU显存总量	groupId
group_gpu_memory_usedspace	Byte	分组维度GPU显存使用量	groupId
group_gpu_memory_usedutilization	%	分组维度GPU显存使用率	groupId
group_gpu_power_readings_power_draw	W	分组维度GPU功率	groupId

通过云监控控制台查询GPU监控数据

您在购买ECS的GPU计算型实例后，只需安装GPU驱动和云监控插件，即可查看GPU相关监控图表、配置监控图表或设置报警规则。

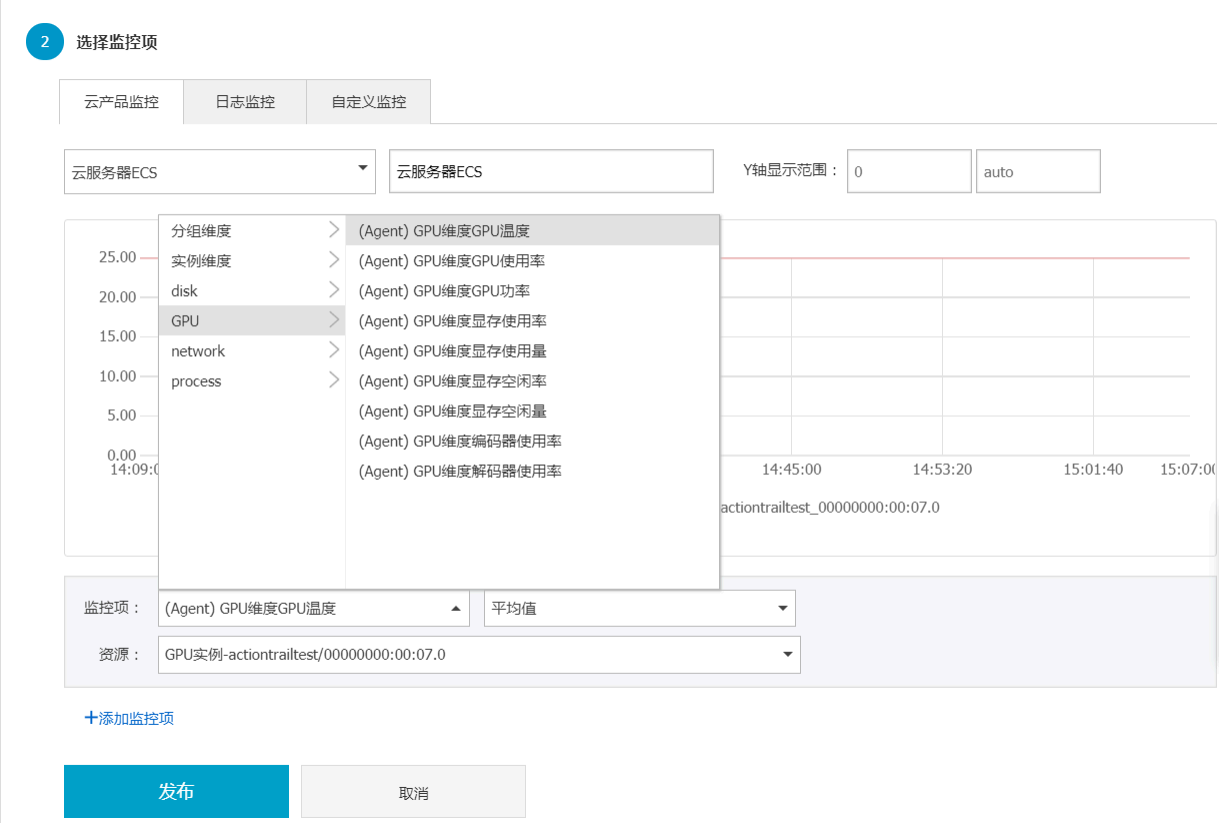
查看监控图表

1. 登录云监控控制台。
2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 在实例列表中，单击实例名称，进入实例详情页面，单击GPU监控页签，切换至GPU监控页签，可查看GPU相关监控图表。



配置监控图表

1. 登录云监控控制台。
2. 单击左侧导航栏中Dashboard下的自定义大盘，进入当前监控大盘页面。
3. 单击创建监控大盘，弹出创建视图组对话框，输入监控大盘名称后，单击创建按钮即可。
4. 单击右上角的添加图表，进入添加图表页面。
5. 选择图表类型：从折线图、面积图、TopN表格、热力图和饼图中选择您需要的图表类型。
6. 选择监控项：在监控项下拉列表中，选择您需要的监控指标，配置完成后，点击发布即可。



设置报警规则

为新增GPU监控指标添加报警规则，建议您通过创建模板后将模板应用于分组的方式批量添加GPU报警规则，详情请参见最佳实践报警模板。

通过API查询GPU监控数据

- **通过API查询GPU监控数据，请参考*QueryMetricList*。**
- **参数说明：Project参数的取值为acs_ecs_dashboard，Metric及Dimensions的取值，请参考上述表格中的GPU指标。**

2.4 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。

说明:

您在查看ECS基础监控和操作系统监控数据（来源于插件采集数据）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

  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CPU百分比。	%	该项数值比较高说明有很频繁的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

  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。	byte	服务器的内存总量。

监控项名称	监控项含义	单位	说明
Host.mem.used	已用内存量。	byte	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。	byte	- 计算方法1.（used - buffers - cached） - 计算方法2. (total - available) Centos 7.2与Ubuntu 16.04以上(包含)的系统使用了新的Linux内核，在内存的估算上更准确, available这一列的具体含义可以参见内核的这个 *commit*.
Host.mem.free	剩余内存量。	byte	计算方法:（total-used）
Host.mem.freeutilization	剩余内存百分比。	%	计算方法:（available/total*100%）
Host.mem.usedutilization	内存使用率。	%	计算方法:（actualused/total*100%）

- 系统平均负载监控项

  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

监控项名称	监控项含义	单位
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。	byte
Host.disk.utilization	磁盘使用率。	%
Host.diskusage.free	磁盘的剩余存储空间。	byte
Host.diskussage.total	磁盘存储总量。	byte
Host.disk.readbytes	磁盘每秒读取的字节数。	byte/s
Host.disk.writebytes	磁盘每秒写入的字节数。	byte/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。	%	Windows操作系统没有此指标。UNIX/Linux系统内部不使用文件名，而使用inode号码来识别文件。当磁盘还未存满，但inode已经分配完时会出现无法在磁盘新建文件的情况，因此要监控inode使用率。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

      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

      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。	bit/s
Host.netout.rate	网卡每秒发送的比特数，即网卡的下行带宽。	bit/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

监控项名称	监控项含义	单位
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。	

- 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	备注
Host.process.cpu	某个进程消耗的CPU百分比。	%	不支持设置报警。
Host.process.memory	某个进程消耗的内存百分比。	%	不支持设置报警。
Host.process.openfile	当前进程打开文件数。	个	不支持设置报警。
Host.process.number	指定关键字的进程数。	个	不支持设置报警。

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。	bit/s
ECS.IntranetInRate	私网入流量平均速率。	bit/s
ECS.InternetOutRate	公网出流量平均速率。	bit/s

监控项名称	监控项含义	单位
ECS.IntranetOutRate	私网出流量平均速率。	bit/s
ECS.SystemDiskReadbps	系统磁盘每秒读取字节总数。	byte/s
ECS.SystemDiskWritebps	系统磁盘每秒写入字节总数。	byte/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。	byte
ECS.InternetOut	公网流出流量。	byte
ECS.IntranetIn	内网流入流量。	byte
ECS.IntranetOut	内网流出流量。	byte

2.5 使用报警服务

主机监控提供报警服务功能，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。在应用分组中设置报警规则，请参见管理报警规则。

创建报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 单击报警规则页签。
4. 单击右上角的新建报警规则，进入创建报警规则页面。
5. 设置关联资源、设置报警规则和通知方式，相关参数说明可参考管理报警规则。
6. 单击确认按钮，完成报警规则的创建。

删除报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 单击报警规则页签。
4. 在报警规则列表操作栏中，单击删除，可删除单条报警规则。勾选多个报警规则后，单击列表下方的删除按钮，可删除多条报警规则。

修改报警规则

1. 登录云监控控制台。

2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 单击报警规则页签。
4. 在报警规则列表操作栏中，单击修改，可对该报警规则进行修改。

查看报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 在实例列表操作栏中，单击报警规则，可以查看单个服务器的报警规则。
4. 单击报警规则页签，可以查看全部报警规则。

2.6 云监控Java版本插件介绍

云监控主机监控服务是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的。

安装位置

- Linux：*/usr/local/cloudmonitor*
- Windows：*C:\Program Files\Alibaba\cloudmonitor*

进程信息

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

- 通过TCP协议监听、访问本地主机的32000端口， 用于守护进程。
- 通过TCP协议访问远程服务器的3128、8080、443端口， 用于心跳联网与监控数据上报，非阿里云主机使用443端口，阿里云主机使用3128或8080端口。
- 通过HTTP协议访问远程服务器的80端口，用于云监控插件升级。

插件日志

- 监控数据日志位于*/usr/local/cloudmonitor/logs* 。
- 启动、关闭、守护进程等日志位于 */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1~2%的单核CPU。
- 安装包大小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Java版本插件，使用Java语言编写，内置JRE 1.8。
- Java service wrapper 用于守护进程、开机启动、Windows服务注册等。
- `ss -s`命令用于采集TCP连接数，如果当前系统没有此命令，需要您自己安装iproute。

安装说明

请参见云监控Java版本插件安装。

非阿里云主机安装方法

1. 登录云监控控制台。
2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 单击页面上方的 非阿里云主机安装 按钮，进入监控安装指引页面，选择监控类型、操作系统后，可查看与其对应的安装方法。

2.7 云监控Java版本插件安装

Linux插件安装说明

常用命令

```
# 运行状态
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh status

# 启动
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh start

# 停止
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh stop

# 重启
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh restart

# 卸载
/usr/local/cloudmonitor/wrapper/bin/cloudmonitor.sh remove && \
```

```
rm -rf /usr/local/cloudmonitor
```

安装命令

直接复制以下命令后在服务器上使用Root权限运行即可。

华北1 青岛 cn-qingdao

```
REGION_ID=cn-qingdao VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-qingdao.oss-cn-qingdao-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

华北2 北京 cn-beijing

```
REGION_ID=cn-beijing VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-beijing.oss-cn-beijing-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

华北3 张家口 cn-zhangjiakou

```
REGION_ID=cn-zhangjiakou VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-zhangjiakou.oss-cn-zhangjiakou-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

华北5 呼和浩特 cn-huhehaote

```
REGION_ID=cn-huhehaote VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-huhehaote.oss-cn-huhehaote-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

华东1 杭州 cn-hangzhou

```
REGION_ID=cn-hangzhou VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

华东2 上海 cn-shanghai

```
REGION_ID=cn-shanghai VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-shanghai.oss-cn-shanghai-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

华南1 深圳 cn-shenzhen

```
REGION_ID=cn-shenzhen VERSION=1.3.7 \
```

```
bash -c "$(curl https://cms-agent-cn-shenzhen.oss-cn-shenzhen-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

香港 香港 cn-hongkong

```
REGION_ID=cn-hongkong VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-hongkong.oss-cn-hongkong-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

美国西部1 硅谷 us-west-1

```
REGION_ID=us-west-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-us-west-1.oss-us-west-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

美国东部1 弗吉尼亚 us-east-1

```
REGION_ID=us-east-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-us-east-1.oss-us-east-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

亚太东南1 新加坡 ap-southeast-1

```
REGION_ID=ap-southeast-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-1.oss-ap-southeast-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

亚太东南2 悉尼 ap-southeast-2

```
REGION_ID=ap-southeast-2 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-2.oss-ap-southeast-2-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

亚太东南3 吉隆坡 ap-southeast-3

```
REGION_ID=ap-southeast-3 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-3.oss-ap-southeast-3-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

亚太东南5 雅加达 ap-southeast-5

```
REGION_ID=ap-southeast-5 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-southeast-5.oss-ap-southeast-5-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

亚太东北1 东京 ap-northeast-1

```
REGION_ID=ap-northeast-1 VERSION=1.3.7 \
```

```
bash -c "$(curl https://cms-agent-ap-northeast-1.oss-ap-northeast-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

亚太南部1 孟买 ap-south-1

```
REGION_ID=ap-south-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-ap-south-1.oss-ap-south-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

欧洲中部1 法兰克福 eu-central-1

```
REGION_ID=eu-central-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-eu-central-1.oss-eu-central-1-
internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

欧洲西部 英国伦敦 eu-west-1

```
REGION_ID=eu-west-1 VERSION=1.3.7 \ bash -c "$(curl https://cms-agent
-eu-west-1.oss-eu-west-1-internal.aliyuncs.com/release/cms_instal
l_for_linux.sh)"
```

中东东部 迪拜 me-east-1

```
REGION_ID=me-east-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-me-east-1.oss-me-east-1-internal.
aliyuncs.com/release/cms_install_for_linux.sh)"
```

华东1金融云 杭州 cn-hangzhou

```
REGION_ID=cn-hangzhou VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/release/cms_install_for_linux.sh)"
```

华东2金融云 上海 cn-shanghai-finance-1

```
REGION_ID=cn-shanghai-finance-1 VERSION=1.3.7 \
bash -c "$(curl https://cms-agent-cn-shanghai-finance-1.oss-cn-
shanghai-finance-1-pub-internal.aliyuncs.com/release/cms_instal
l_for_linux.sh)"
```

华南1金融云 深圳 cn-shenzen-finance-1

```
REGION_ID=cn-shenzhen-finance-1 VERSION=1.3.7 \
```

```
bash -c "$(curl http://cms-agent-cn-shenzhen-finance-1.oss-cn-shenzhen
-finance-1-internal.aliyuncs.com/release/cms_install_for_linux.sh)"
```

Windows插件安装说明

安装步骤

1. 根据系统情况，下载云监控插件64位版本插件或32位版本插件。
2. 在*C:/Program Files/Alibaba*路径下新建文件夹*cloudmonitor*。
3. 解压到*C:/Program Files/Alibaba/cloudmonitor*目录。
4. 使用管理员权限双击运行安装云监控*C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/InstallApp-NT.bat*。
5. 使用管理员权限双击运行启动云监控*C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/StartApp-NT.bat*。
6. 安装完成后，可以通过Windows服务面板来查看、启动、停止云监控服务（Cloud Monitor Application）。

卸载步骤

1. 使用Windows服务面板停止云监控服务。
2. 通过管理员权限运行*C:/Program Files/Alibaba/cloudmonitor/wrapper/bin/UninstallApp-NT.bat*来删除云监控服务。
3. 到安装目录删除整个目录*C:/Program Files/Alibaba/cloudmonitor*。

无公网下载

如果没有公网可以通过内网地址下载，例如青岛64位安装包下载地址为：*http://cms-agent-cn-qingdao.oss-cn-qingdao.aliyuncs.com/release/1.3.7/windows64/agent-windows64-1.3.7-package.zip*

- 可以通过修改两处cn-qingdao切换到其他region下载地址
- 可以通过将两处windows64修改为windows32来切换到32位版本
- 可以通过修改两处1.3.7切换到其他版本

安全配置说明

以下是云监控插件与服务端交互用到的端口，这些端口被安全软件禁用后，会导致监控数据采集异常，如果您的ECS服务器对安全要求较高，需要针对具体IP地址放行，可以将下列IP加入白名单。

说明:

未来随着云监控版本的更新维护，可能会加入更多的IP地址或变更IP地址，为简化防火墙规则的配置，可以直接配置允许100.100网段的出方向，这个网段是阿里云内网保留网段，用于提供阿里云官方服务。

Region	IP	方向	描述
cn-hangzhou 华东 1 杭州	100.100.19.43:3128	出方向	监控配置管理等管控类操作
	100.100.45.73:80	出方向	收集监控数据到云监控服务端
cn-beijing 华北 2 北京	100.100.18.22:3128	出方向	监控配置管理等管控类操作
	100.100.18.50:80	出方向	收集监控数据到云监控服务端
cn-qingdao 华北 1 青岛	100.100.36.102:3128	出方向	监控配置管理等管控类操作
	100.100.15.23:80	出方向	收集监控数据到云监控服务端
cn-shenzhen 华南 1 深圳	100.100.0.13:3128	出方向	监控配置管理等管控类操作
	100.100.0.31:80	出方向	收集监控数据到云监控服务端
cn-hongkong 香港	100.103.0.47:3128	出方向	监控配置管理等管控类操作
	100.103.0.45:80	出方向	收集监控数据到云监控服务端
cn-huhehaote 华北 5 呼和浩特	100.100.80.135:8080	出方向	监控配置管理等管控类操作
	100.100.80.12:80	出方向	收集监控数据到云监控服务端
cn-zhangjiakou 华北 3 张家口	100.100.80.92:8080	出方向	监控配置管理等管控类操作
	100.100.0.19:80	出方向	收集监控数据到云监控服务端
cn-shanghai 华东 2 上海	100.100.36.11:3128	出方向	监控配置管理等管控类操作
	100.100.36.6:80	出方向	收集监控数据到云监控服务端

Region	IP	方向	描述
cn-chengdu 西南 1 成都	100.100.80.229:8080	出方向	监控配置管理等管控类操作
	100.100.80.14:80	出方向	收集监控数据到云监控服务端
us-east-1 美国东部 1 弗吉尼亚	100.103.0.95:3128	出方向	监控配置管理等管控类操作
	100.103.0.94:80	出方向	收集监控数据到云监控服务端
us-west-1 美国西部 1 硅谷	100.103.0.95:3128	出方向	监控配置管理等管控类操作
	100.100.29.7:80	出方向	收集监控数据到云监控服务端
eu-central-1 欧洲中部 1 德国 法兰克福	100.100.80.241:8080	出方向	监控配置管理等管控类操作
	100.100.80.72:80	出方向	收集监控数据到云监控服务端
eu-west-1 英国 伦敦	100.100.0.3:8080	出方向	监控配置管理等管控类操作
	100.100.0.2:80	出方向	收集监控数据到云监控服务端
ap-southeast-1 亚太东南 1 新加坡	100.100.30.20:3128	出方向	监控配置管理等管控类操作
	100.100.103.7:80	出方向	收集监控数据到云监控服务端
ap-southeast-2 亚太东南 2 澳大利亚 悉尼	100.100.80.92:8080	出方向	监控配置管理等管控类操作
	100.100.80.13:80 [47.91.39.6:443]	出方向	收集监控数据到云监控服务端
ap-southeast-3 亚太东南 3 吉隆坡	100.100.80.153:8080	出方向	监控配置管理等管控类操作
	100.100.80.140:80	出方向	收集监控数据到云监控服务端
ap-southeast-5亚太东南 5 雅加达	100.100.80.160:8080	出方向	监控配置管理等管控类操作

Region	IP	方向	描述
	100.100.80.180:80	出方向	收集监控数据到云监控服务端
me-east-1 中东东部 1 迪拜	100.100.80.142:8080	出方向	监控配置管理等管控类操作
	100.100.80.151:80 [47.91.99.5:443]	出方向	收集监控数据到云监控服务端
ap-northeast-1 亚太东北 1 日本 东京	100.100.80.184:8080	出方向	监控配置管理等管控类操作
	100.100.80.137:80 [47.91.8.7:443]	出方向	收集监控数据到云监控服务端
ap-south-1 亚太南部 1 孟买	100.100.80.152:8080	出方向	监控配置管理等管控类操作
	100.100.80.66:80	出方向	收集监控数据到云监控服务端

资源消耗

- 插件安装包大小：75M。
- 安装后大小：200M。
- 内存：64M。
- CPU：1%以下。
- 网络：使用内网网络，不消耗公网流量。

常见问题

- 云监控日志位置：
  - Linux：*/usr/local/cloudmonitor/logs*
  - Windows：*C:/Program Files/Alibaba/cloudmonitor/logs*
- 插件占用的端口和我的业务端口冲突怎么办?
  1. 修改云监控配置来更换端口范围，文件位置：*/usr/local/cloudmonitor/wrapper/conf/wrapper.conf*
  2. 重启云监控

```
wrapper.port.min=40000
wrapper.port.max=41000
wrapper.jvm.port.min=41001
wrapper.jvm.port.max=42000
```

2.8 云监控Go语言版本插件介绍

云监控主机监控服务是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的。

安装位置

- Linux：*/usr/local/cloudmonitor*
- Windows：*C:\Program Files\Alibaba\cloudmonitor*

进程信息

插件安装后，会在您的服务器上运行以下进程：

- Linux 32位：CmsGoAgent.linux-386
- Linux 64位：CmsGoAgent.linux-amd64
- Windows 32位：CmsGoAgent.windows-386.exe
- Windows 64位：CmsGoAgent.windows-amd64.exe

端口说明

- 通过TCP协议访问远程服务器的3128、8080或443端口， 用于心跳联网与监控数据上报。阿里云主机使用3128或8080端口，非阿里云主机使用443端口。
- 通过HTTP协议访问远程服务器的80端口，用于云监控插件升级。

插件日志

- 监控数据日志位于logs目录
- 可以通过修改config/conf.properties的cms.log.level配置来调整日志级别。如果文件里没有该key，您可以手动创建。Go语言版插件支持的日志级别：DEBUG、INFO、WARNING、ERROR、FATAL。

资源占用情况

- 插件进程占用10~20M左右内存和1~2%的单核CPU。
- 安装包大小在10~15M。
- 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。

安装说明

请参见云监控Go语言版本插件安装。

非阿里云主机安装方法

1. 登录云监控控制台。
2. 单击左侧导航栏中的主机监控，进入主机监控页面。
3. 单击页面上方的 非阿里云主机安装 按钮，进入监控安装指引页面，选择监控类型、操作系统后，可查看与其对应的安装方法。

2.9 云监控Go语言版本插件安装

系统要求

操作系统	硬件架构	备注
Windows 7, Windows Server 2008 R2 or later	amd64, 386	
Linux 2.6.23 or later with glibc	amd64, 386	CentOS/RHEL 5.x not supported.

资源消耗

- 插件安装包大小： 10~15MB。
- 内存：10~15MB，加上共享空间约为20MB（视您的系统内存的大小而有所不同）。
- CPU：1~2%。
- 网络： 使用内网网络，不消耗公网流量。

Linux插件安装说明

说明:

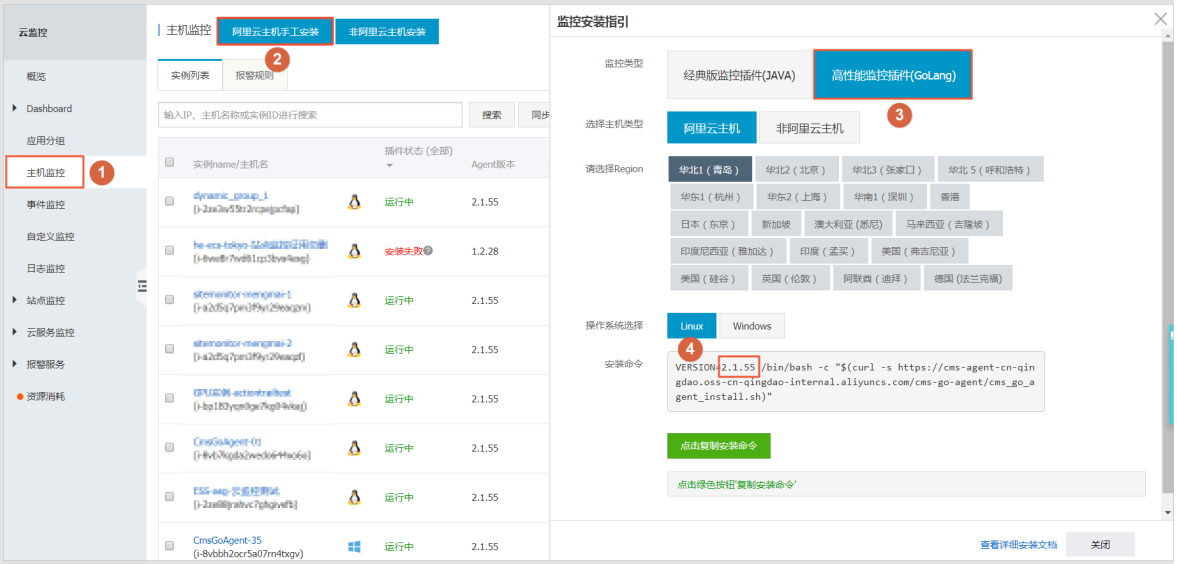
1. Go语言版本插件二进制文件命名

   `CmsGoAgent.linux-${ARCH}`

   其中ARCH根据Linux架构的不同，分为：amd64和386。

2. 版本号

本文使用的插件版本为：2.1.55，建议您使用最新版本。最新版本号可在云监控的主机监控页面查到。



常用命令

```
# 注册为系统服务
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH}install
# 从系统服务中移除
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH} uninstall
# 启动
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH} start
# 停止
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH} stop
# 重启
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH} restart
# 卸载
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH} stop && \
/usr/local/cloudmonitor/CmsGoAgent.linux-${ARCH} uninstall && \
rm -rf /usr/local/cloudmonitor
```

安装命令

直接复制以下命令后在服务器上使用Root权限运行即可。

说明:

以下安装命令已在监控安装指引页面自动生成，您也可以去该页面直接复制使用。

华北1 青岛 cn-qingdao

```
REGION_ID=cn-qingdao VERSION=2.1.55 \
```

```
bash -c "$(curl https://cms-agent-cn-qingdao.oss-cn-qingdao-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华北2 北京 cn-beijing

```
REGION_ID=cn-beijing VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-beijing.oss-cn-beijing-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华北3 张家口 cn-zhangjiakou

```
REGION_ID=cn-zhangjiakou VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-zhangjiakou.oss-cn-zhangjiakou-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华北5 呼和浩特 cn-huhehaote

```
REGION_ID=cn-huhehaote VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-huhehaote.oss-cn-huhehaote-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华东1 杭州 cn-hangzhou

```
REGION_ID=cn-hangzhou VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华东2 上海 cn-shanghai

```
REGION_ID=cn-shanghai VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-shanghai.oss-cn-shanghai-internal
.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华南1 深圳 cn-shenzhen

```
REGION_ID=cn-shenzhen VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-shenzhen.oss-cn-shenzhen-internal
.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

香港 香港 cn-hongkong

```
REGION_ID=cn-hongkong VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-hongkong.oss-cn-hongkong-internal
.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

美国西部1 硅谷 us-west-1

```
REGION_ID=us-west-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-us-west-1.oss-us-west-1-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

美国东部1 弗吉尼亚 us-east-1

```
REGION_ID=us-east-1 VERSION=2.1.55 \
```

```
bash -c "$(curl https://cms-agent-us-east-1.oss-us-east-1-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

亚太东南1 新加坡 ap-southeast-1

```
REGION_ID=ap-southeast-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-ap-southeast-1.oss-ap-southeast-1-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

亚太东南2 悉尼 ap-southeast-2

```
REGION_ID=ap-southeast-2 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-ap-southeast-2.oss-ap-southeast-2-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

亚太东南3 吉隆坡 ap-southeast-3

```
REGION_ID=ap-southeast-3 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-ap-southeast-3.oss-ap-southeast-3-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

亚太东南5 雅加达 ap-southeast-5

```
REGION_ID=ap-southeast-5 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-ap-southeast-5.oss-ap-southeast-5-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

亚太东北1 东京 ap-northeast-1

```
REGION_ID=ap-northeast-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-ap-northeast-1.oss-ap-northeast-1-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

亚太南部1 孟买 ap-south-1

```
REGION_ID=ap-south-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-ap-south-1.oss-ap-south-1-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

欧洲中部1 法兰克福 eu-central-1

```
REGION_ID=eu-central-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-eu-central-1.oss-eu-central-1-
internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

欧洲西部 英国伦敦 eu-west-1

```
REGION_ID=eu-west-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-eu-west-1.oss-eu-west-1-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

中东东部 迪拜 me-east-1

```
REGION_ID=me-east-1 VERSION=2.1.55 \
```

```
bash -c "$(curl https://cms-agent-me-east-1.oss-me-east-1-internal.
aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华东1金融云 杭州 cn-hangzhou

```
REGION_ID=cn-hangzhou VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-hangzhou.oss-cn-hangzhou-internal
.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh)"
```

华东2金融云 上海 cn-shanghai-finance-1

```
REGION_ID=cn-shanghai-finance-1 VERSION=2.1.55 \
bash -c "$(curl https://cms-agent-cn-shanghai-finance-1.oss-cn-
shanghai-finance-1-pub-internal.aliyuncs.com/cms-go-agent/cms_go_age
nt_install.sh)"
```

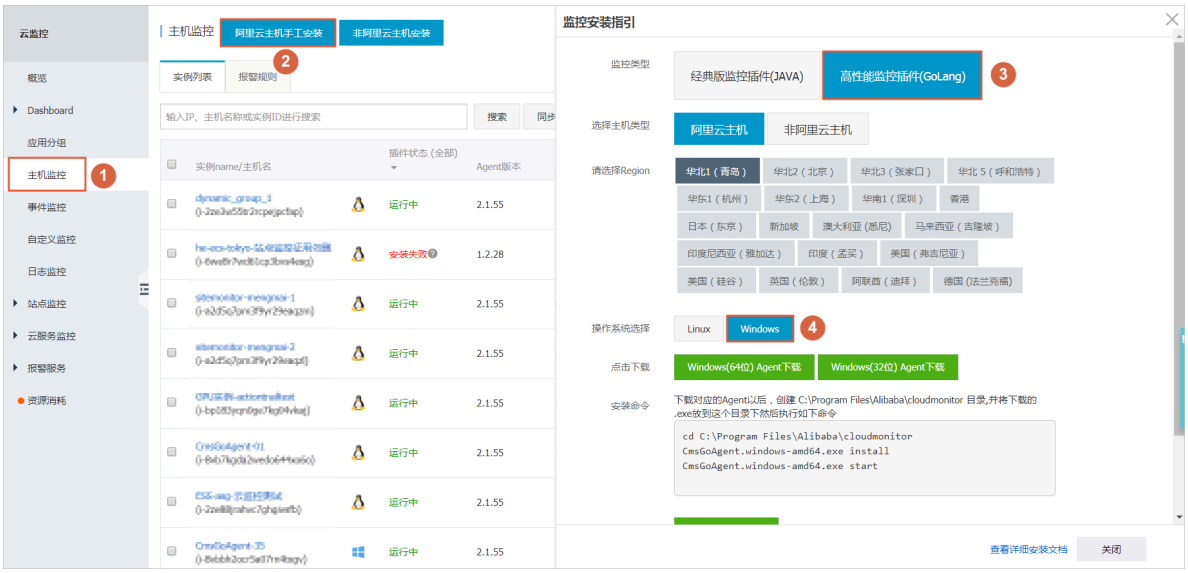
华南1金融云 深圳 cn-shenzen-finance-1

```
REGION_ID=cn-shenzhen-finance-1 VERSION=2.1.55 \
bash -c "$(curl http://cms-agent-cn-shenzhen-finance-1.oss-cn-shenzhen
-finance-1-internal.aliyuncs.com/cms-go-agent/cms_go_agent_install.sh
)"
```

Windows插件安装说明

安装步骤

1. 根据系统情况（所在Region，主机类型），下载云监控插件64位版本插件或32位版本插件 到C:\Program Files\Alibaba\cloudmonitor目录下。

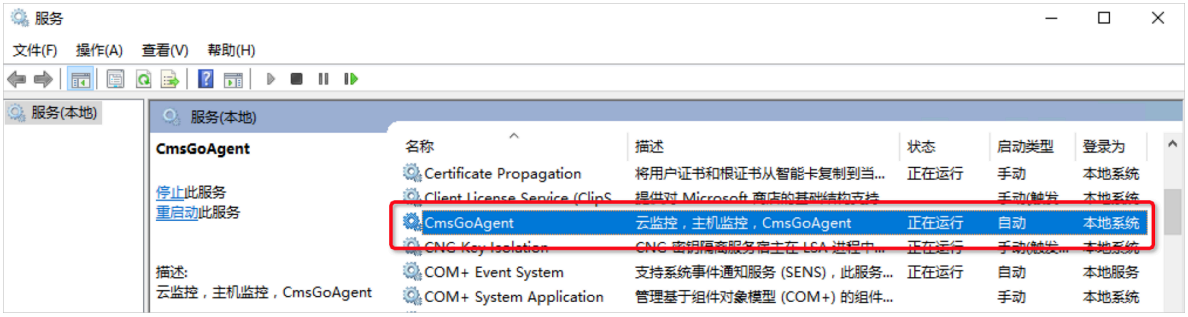


2. 使用管理员权限启动命令提示符。
3. 输入并执行以下命令：

```
cd"C:\Program Files\Alibaba\cloudmonitor"
CmsGoAgent.windows-amd64.exe install
```

```
CmsGoAgent.windows-amd64.exe start
```

4. 安装完成后，可以通过Windows系统的服务来查看、启动、停止云监控服务。



卸载步骤

1. 使用管理员权限启动命令提示符。
2. 输入并执行以下命令：

```
cd"C:\Program Files\Alibaba\cloudmonitor"
CmsGoAgent.windows-amd64.exe stop
CmsGoAgent.windows-amd64.exe uninstall
```

3. 关闭命令提示符，将`C:\Program Files\Alibaba\cloudmonitor`整个目录删除。

无公网下载

如果没有公网可以通过内网地址下载，例如青岛64位安装包下载地址为：*http://cms-agent-cn-qingdao.oss-cn-qingdao.aliyuncs.com/cms-go-agent/2.1.55/CmsGoAgent.windows-amd64.exe*

- 可以通过修改两处cn-qingdao切换到其他region下载地址
- 可以通过将amd64修改为386来切换到32位版本
- 可以通过修改2.1.55切换到其他版本

安全配置说明

以下是云监控插件与服务端交互用到的端口，这些端口被安全软件禁用后，会导致监控数据采集异常，如果您的ECS服务器对安全要求较高，需要针对具体IP地址放行，可以将下列IP加入白名单。

说明:

1. 未来随着云监控版本的更新维护，可能会加入更多的IP或变更IP地址，为简化防火墙规则的配置，可以直接配置允许100.0.0.0/8网段的出方向，这个网段是阿里云内网保留网段，用于提供阿里云官方服务。
2. 下表中被中括号括起来的IP地址，属可选部分，主要是作为网络不好情况下的备用地址。

Region	IP	方向	描述
cn-hangzhou 华东 1 杭州	100.100.19.43:3128	出方向	监控配置管理等管控类操作
	100.100.45.73:80	出方向	收集监控数据到云监控服务端
cn-beijing 华北 2 北京	100.100.18.22:3128	出方向	监控配置管理等管控类操作
	100.100.18.50:80	出方向	收集监控数据到云监控服务端
cn-qingdao 华北 1 青岛	100.100.36.102:3128	出方向	监控配置管理等管控类操作
	100.100.15.23:80	出方向	收集监控数据到云监控服务端
cn-shenzhen 华南 1 深圳	100.100.0.13:3128	出方向	监控配置管理等管控类操作
	100.100.0.31:80	出方向	收集监控数据到云监控服务端
cn-hongkong 香港	100.103.0.47:3128	出方向	监控配置管理等管控类操作
	100.103.0.45:80	出方向	收集监控数据到云监控服务端
cn-huhehaote 华北 5 呼和浩特	100.100.80.135:8080	出方向	监控配置管理等管控类操作
	100.100.80.12:80	出方向	收集监控数据到云监控服务端
cn-zhangjiakou 华北 3 张家口	100.100.80.92:8080	出方向	监控配置管理等管控类操作
	100.100.0.19:80	出方向	收集监控数据到云监控服务端
cn-shanghai 华东 2 上海	100.100.36.11:3128	出方向	监控配置管理等管控类操作
	100.100.36.6:80	出方向	收集监控数据到云监控服务端
cn-chengdu 西南 1 成都	100.100.80.229:8080	出方向	监控配置管理等管控类操作

Region	IP	方向	描述
	100.100.80.14:80	出方向	收集监控数据到云监控服务端
us-east-1 美国东部 1 弗吉尼亚	100.103.0.95:3128	出方向	监控配置管理等管控类操作
	100.103.0.94:80	出方向	收集监控数据到云监控服务端
us-west-1 美国西部 1 硅谷	100.103.0.95:3128	出方向	监控配置管理等管控类操作
	100.100.29.7:80	出方向	收集监控数据到云监控服务端
eu-central-1 欧洲中部 1 德国 法兰克福	100.100.80.241:8080	出方向	监控配置管理等管控类操作
	100.100.80.72:80	出方向	收集监控数据到云监控服务端
eu-west-1 英国 伦郭	100.100.0.3:8080	出方向	监控配置管理等管控类操作
	100.100.0.2:80	出方向	收集监控数据到云监控服务端
ap-southeast-1 亚太东南 1 新加坡	100.100.30.20:3128	出方向	监控配置管理等管控类操作
	100.100.103.7:80	出方向	收集监控数据到云监控服务端
ap-southeast-2 亚太东南 2 澳大利亚 悉尼	100.100.80.92:8080	出方向	监控配置管理等管控类操作
	100.100.80.13:80 [47.91.39.6:443]	出方向	收集监控数据到云监控服务端
ap-southeast-3 亚太东南 3 吉隆坡	100.100.80.153:8080	出方向	监控配置管理等管控类操作
	100.100.80.140:80	出方向	收集监控数据到云监控服务端
ap-southeast-5亚太东南 5 雅加达	100.100.80.160:8080	出方向	监控配置管理等管控类操作
	100.100.80.180:80	出方向	收集监控数据到云监控服务端

Region	IP	方向	描述
me-east-1 中东东部 1 迪拜	100.100.80.142:8080	出方向	监控配置管理等管控类操作
	100.100.80.151:80 [47.91.99.5:443]	出方向	收集监控数据到云监控服务端
ap-northeast-1 亚太东北 1 日本 东京	100.100.80.184:8080	出方向	监控配置管理等管控类操作
	100.100.80.137:80 [47.91.8.7:443]	出方向	收集监控数据到云监控服务端
ap-south-1 亚太南部 1 孟买	100.100.80.152:8080	出方向	监控配置管理等管控类操作
	100.100.80.66:80	出方向	收集监控数据到云监控服务端

常见问题

云监控日志位置：

- Linux：/usr/local/cloudmonitor/logs
- Windows：C:\Program Files\Alibaba\cloudmonitor\logs

2.10 插件 Release Notes

本文档为您介绍主机监控插件的版本发布信息。

2.1.55

发布时间：2019-01-24

已知问题的修复与优化：

修复重启ECS实例后，插件无法采集监控数据的问题。

升级建议：

建议使用Go语言版本插件（版本号低于2.1.55）的主机升级至此版本。

2.1.54

发布时间：2019-01-03

已知问题的修复与优化：

修复无法采集Windows操作系统的GPU计算型主机监控数据的问题。

升级建议：

建议使用Go语言版本插件（版本号低于2.1.54）且操作系统为Windows的GPU类型主机升级至此版本。

2.1.53

发布时间：2018-12-25

已知问题的修复与优化：

修复无法采集经典网络ECS监控数据的问题。

升级建议：

建议使用Go语言版本插件（版本号低于2.1.53）且网络类型为经典网络的主机进行升级。

2.1.51

发布时间：2018-12-04

已知问题的修复与优化：

- 修复磁盘监控挂载点显示为16进制字符串乱码的问题。
- 新增插件安装前置检查：执行安装插件动作前，检查操作系统版本、系统内存、磁盘剩余容量以及与Cloudmonitor服务器的连通性，以便判断是否可以成功安装插件。

升级建议：

建议使用Go语言版本插件（版本号低于2.1.50）的主机进行升级。

2.1.50

发布时间：2018-11-29

新功能：

Go语言版本正式发布，较Java版本大幅降低对主机的性能消耗并提供更稳定的监控服务。插件详情请参见云监控Go语言版本插件介绍。

升级建议：

建议使用Java版插件（版本号为1.X.X）的主机升级至此版本。您可在主机监控页面实例列表中勾选主机，单击列表下方的批量安装插件按钮进行升级。

1.2.11

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。

升级建议

使用本地健康检查功能，需要将插件升级至此版本。

1.1.64

已知问题的修复与优化：

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。

升级建议：

建议CentOS7.2以上版本的主机升级插件至此版本。

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。**

3 站点监控

3.1 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20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。

探测协议类型

探测类型	功能
HTTP/HTTPS	对指定的URL/IP进行HTTP/HTTPS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。

探测类型	功能
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。

3.2 创建站点监控

本文为您介绍如何通过创建站点监控，对互联网进行网络探测，进而实现网络质量分析、性能分析、竞品分析等目的。

背景信息

站点监控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。

- 通过站点监控的探测点，模拟最终用户的访问行为，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，可针对性的进行网络优化。
- 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。
- 通过添加自己和竞争对手的服务站点，选择目标探测点，针对分析探测结果，得出自己与竞品服务的质量分析。
- 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。

创建站点监控的准备工作

- 如果您需要在创建站点监控的同时设置报警规则，建议您先创建报警联系人和报警联系组，以便在设置报警规则时选择相应的报警联系组，用于接收报警通知，如何创建报警联系人和报警联系组，请参见创建报警联系人/报警联系组。
- 如果您需要在设置报警规则时使用报警回调功能，那么请准备能通过公网访问的回调URL，并在已有的运维系统或消息通知系统的告警方式中开启URL回调。

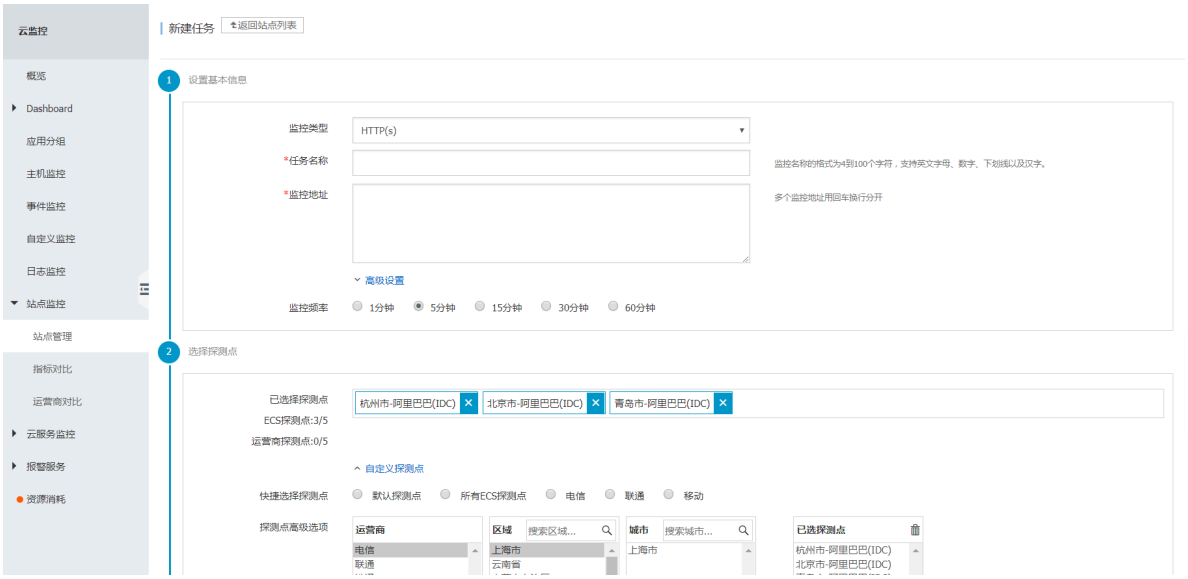
创建站点监控的实施步骤

注意事项

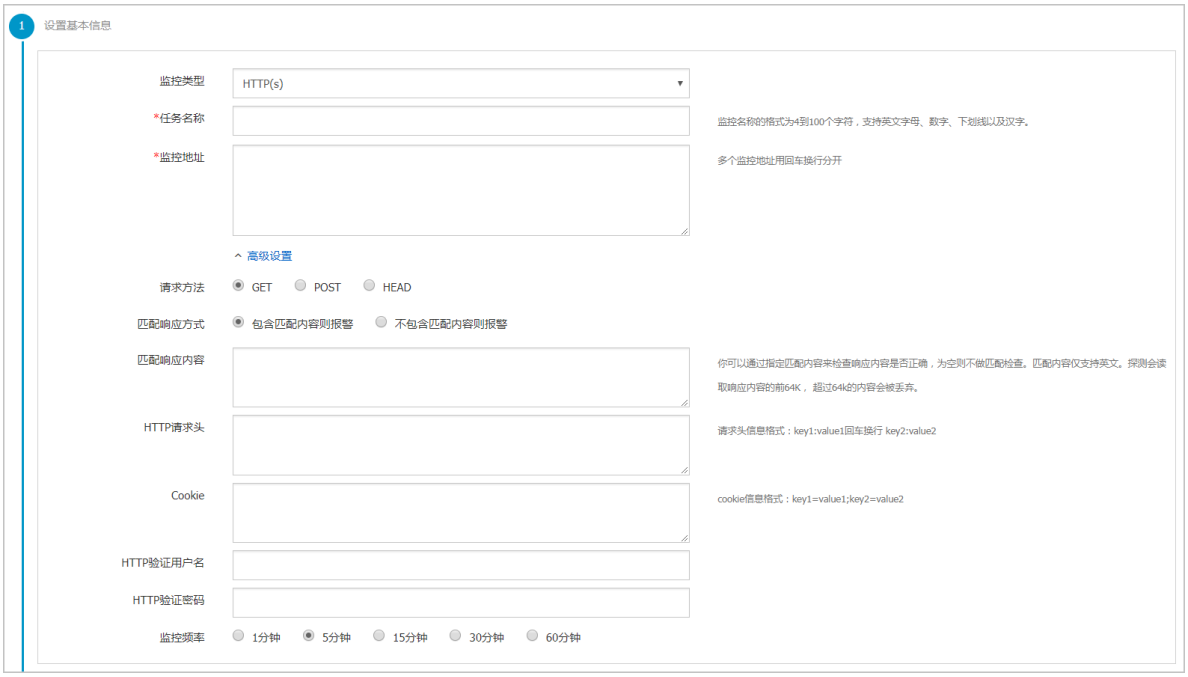
> **说明:**
> 创建站点监控任务时，设置报警规则为可选项，可以不设置。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中站点监控下的站点管理，进入站点管理页面。
3. 单击右上角的新建监控任务按钮，进入新建任务页面。



4. 设置基本信息：

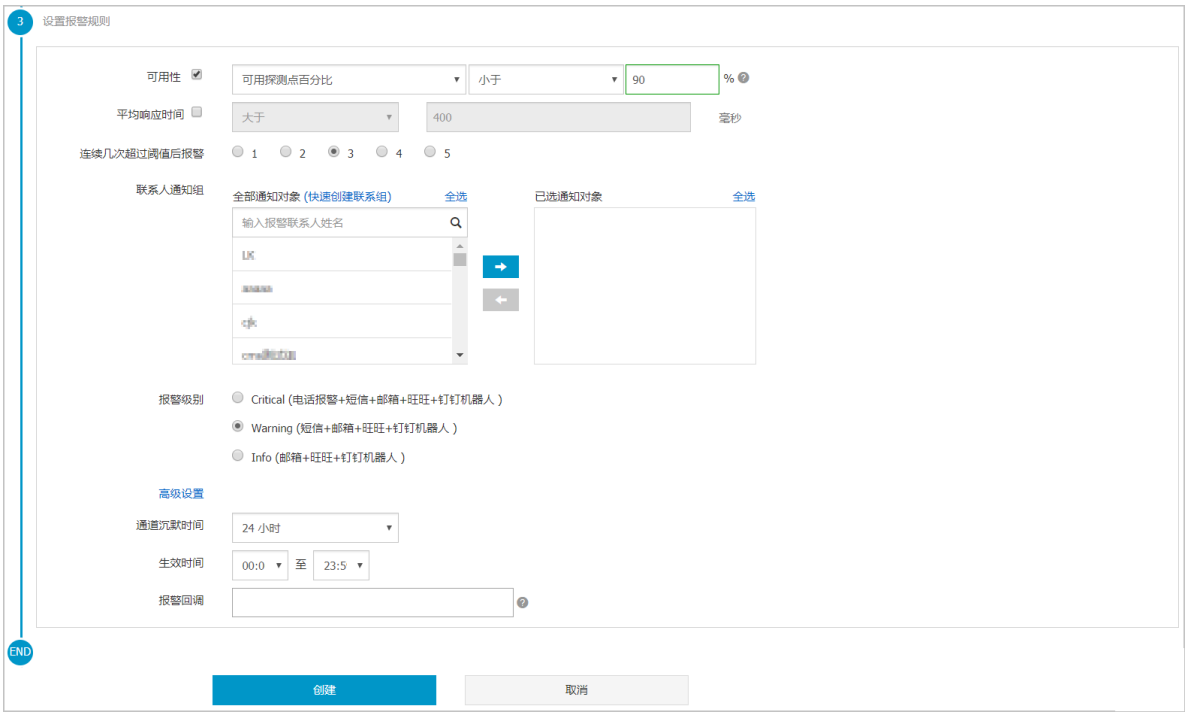


- 监控类型：支持HTTP(S)、PING、TCP、UDP、DNS、SMTP、POP3、FTP、TRACEROUTE 等监控协议。
- 任务名称：监控任务的名称，格式为4到100个字符，支持英文字母、数字、下划线以及汉字。
- 监控地址：目标监控地址，一次可以填写多个监控地址，多个监控地址用回车换行分开，方便您进行批量设置。保存时会将多个监控地址拆分成多个任务。
- 监控频率：监控周期，分为1分钟、5分钟、15分钟、30分钟和60分钟。例如选择1分钟频率，则各地域探测点将以1分钟/次的频率监控目标地址。
- 高级设置：不同协议支持不同的高级设置，请根据实际情况选择使用。请参见本文监控类型高级设置说明部分。

5. 选择探测点，也可以自定义探测点。

- 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。

6. （可选）设置报警规则。



- 可用性：分为可用探测点数量、可用探测点百分比、任意状态码（独立报警）和所以状态码（组合报警）等4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。
- 联系人通知组：选择发送报警通知时的接收对象。
- 报警级别：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。
  - 通道沉默时间：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：报警规则的生效时间，报警规则只在生效时间内发送报警通知，非生效时间内产生的报警只记录报警历史。
  - 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7. 完成上述设置后，单击创建按钮，即可完成创建站点监控任务。

监控类型高级设置说明

- HTTP(S)高级设置

选项	输入方式	必填	说明
监控地址	url	是	url中最好含有schema部分，例如：https://www.baidu.com。 如果没有schema部分，则缺省认为是：http。
请求内容	表单数据 或JSON对象	否	如果是JSON格式，则仅支持JSON对象，即以大括号({})括起来的数据，否则系统将会当作表单数据处理。

选项	输入方式	必填	说明
请求方法	单选	是	支持三种HTTP方法：GET、POST、HEAD。 缺省为GET。
匹配响应方式	单选	是	当匹配响应内容非空时，站点监控读取HTTP服务器回应Body的前64K字节，从中查找匹配响应内容，有两种结果： 1. 包含匹配相应内容。 2. 不包含匹配相应内容。 站点监控会根据匹配响应方式来决定是否报警。 阿里巴巴探测点支持中/英文，运营商探测点仅支持英文。如果您的任务同时选择了2种探测点，为避免探测结果不支持，强烈建议在匹配响应内容中仅使用英文。
匹配响应内容	文本	否	

选项	输入方式	必填	说明
HTTP请求头	多行文本	否	每行的格式与HTTP Header的格式相同，都是以英文冒号分隔的KV结构。站点监控会在请求头中预置以下Header: Host: ${监控地址中的域名} Pragma: no-cache Cache-Control: no-cache User-Agent: Chrome/57 Accept: */* 当请求内容是表单时，还会有以下Header: Content-Type: application/x-www-form-urlencoded; charset=UTF-8 如果您的header中出现了以上内容的某一项或某几项，则这几项将被您的设置所覆盖。 注：根据Http协议，您提供的请求头中的key会被站点监控转换为canonical format of MIME Header形式: 1. 首字母以及连字符"-"后面的字母

选项	输入方式	必填	说明
Cookie		否	HTTP规则的cookie文本
HTTP验证用户名	用户名	否	注：此处的验证，是指通过http协议的basic auth进行的验证。
HTTP验证密码	密码	否	

- PING高级设置

选项	输入方式	必填	说明
监控地址	域名或IP地址	是	
ping包数目	正整数	是	发起ping的次数，缺省为20， 有效取值：(0, 40]。

- TCP/UDP高级设置

选项	输入方式	必填	说明
监控地址	域名或IP地址	是	
请求内容的格式	单选	是	请求内容非空时有效。有两种选项：16进制格式或文本.

选项	输入方式	必填	说明
请求内容	[普通]文本 或十六进制[文本]	否	［普通］文本 就是我们通常说的String，即由可见字符组成的字符串。注：普通文本不支持转义，即不会将\n转为回车符，只是当做两个字符：\和n。 16进制格式是指：当请求的内容是byte串，无法用可见字符表达时，我们可以将byte串转换为16进制表示的可见字符串形式。具体转换规则为：一个byte转换成2字节的16进制字符，如(byte)1转换成十六进制为01，byte(17)转换成十六进制为1B，等等。 则二进制数组(java形式)：{(byte)1, (byte)26}转换为16进制为：011b或011B。站点监控对16进制不区分大小写。将字符串"011B"填入请求内容中，同时请求内容的格式选择16进制格式。

选项	输入方式	必填	说明
响应内容的格式	单选	是	响应内容非空时有效。有两种选项：16进制格式或文本。
响应内容	[普通]文本 或十六进制[文本]	否	参见请求内容。

- DNS高级设置

高级选项	输入方式	必填	说明
监控域名	域名	是	
DNS查询类型	单选	是	支持以下六种，默认为A查询： A、MX、NS、CNAME、TXT、ANY。
DNS服务器	服务器IP地址	否	如果为空，则使用探针默认dns服务器地址。可以是域名或IP地址。
期望解析IP	多行文本	否	实际应为：期望解析列表。每行代表一个IP地址或者一个域名。 当期望列表是DNS列表的子集时，才认为探测成功。

- POP3(S)高级设置

高级选项	输入方式	必填	说明
监控地址	url	是	如果是pop3s，则url中必须含有schema，例如pop3s://pop3.aliyun.com。 如果不含schema，则认为是pop3。 pop3s使用tls进行加密传输
用户名	文本	是	使用USER和PASS命令进行认证。 请谨慎输入用户名密码，站点监控会按您设置的频率进行探测，如果用户名密码错误，过于频繁的探测可能会导致对方服务屏蔽您的账号。
密码	文本	是	

- SMTP(S)高级设置

高级选项	输入方式	必填	说明
监控地址	url	是	如果是smtps，则url中必须含有schema，如smtps://smtp.aliyun.com。 如果不含schema，则认为是smtp。 smtps: 通过STARTTLS命令与服务器进行协商加密，使用安全连接时，认证也是通过加密进行的。
用户名	文本	是	使用PLAIN进行进行认证。 请谨慎输入用户名密码，站点监控会按您设置的频率进行探测，如果用户名密码错误，过于频繁的探测可能会导致对方服务屏蔽您的账号。
密码	文本	是	

- FTP高级设置

高级选项	输入方式	必填	说明
监控地址	url	是	例如: ftp://smtp.aliyun.com
是否匿名登录	单选	是	缺省：匿名登录。 当选择：需要身份证时，用户名和密码为必填。

高级选项	输入方式	必填	说明
用户名	文本		进行FTP认证时的用户名和密码。 当选择匿名登录时，用户名/密码为：anonymous/ftp@example.com。
密码	文本		

- TRACEROUTE高级设置

高级选项	输入方式	必填	说明
监控地址	域名	是	
最大跳转次数	正整数	是	缺省：为30次。有效取值为：(0, 40]

3.3 管理站点监控任务

本文为您介绍如何修改、删除、启用和禁用站点监控任务。

修改站点监控任务

1. 登录云监控控制台。
2. 单击左侧导航栏中站点监控下的站点管理，进入站点管理页面。
3. 选择需要修改的站点监控任务，单击操作中的修改，进入修改页面。
4. 修改相应内容后，点击修改按钮即可。

删除站点监控任务

1. 登录云监控控制台。
2. 单击左侧导航栏中站点监控下的站点管理，进入站点管理页面。
3. 选择需要删除的任务，单击操作中的删除即可。

> 说明:
> 站点监控任务被删除后，与之相关报警规则也会同步被删除。

启用或禁用站点监控任务

1. 登录云监控控制台。
2. 单击左侧导航栏中站点监控下的站点管理，进入站点管理页面。

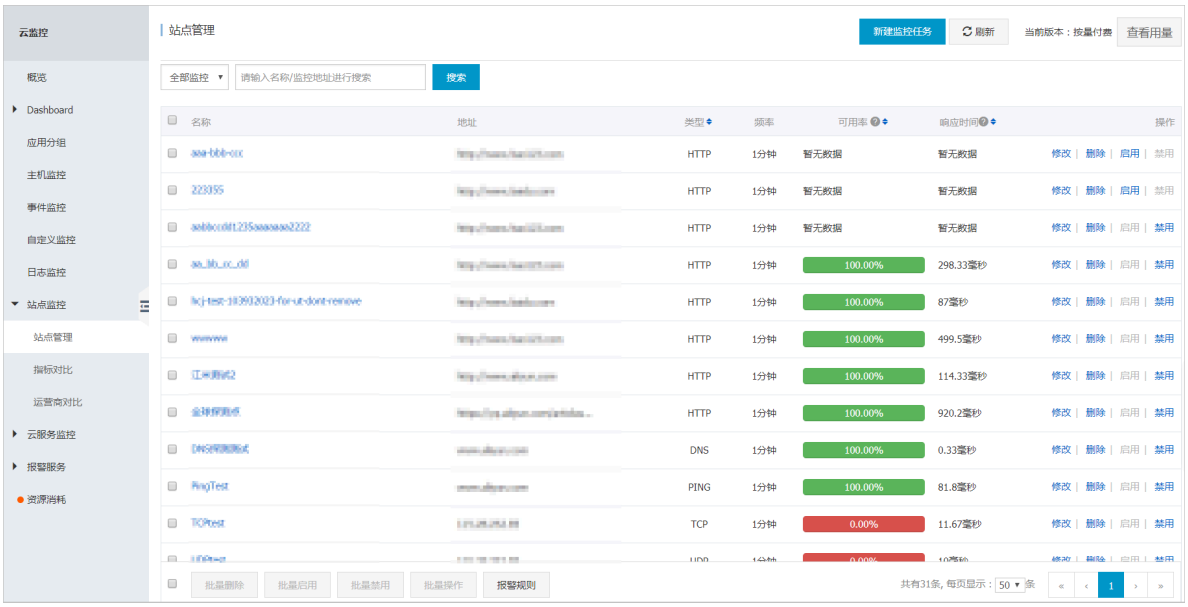
3. 选择需要启用或禁用的任务，点击操作中的启用或禁用，可对该站点监控任务进行启用或禁用。

3.4 查看监控数据

本文为您介绍如何查看站点监控的监控数据。

查看监控数据的操作步骤

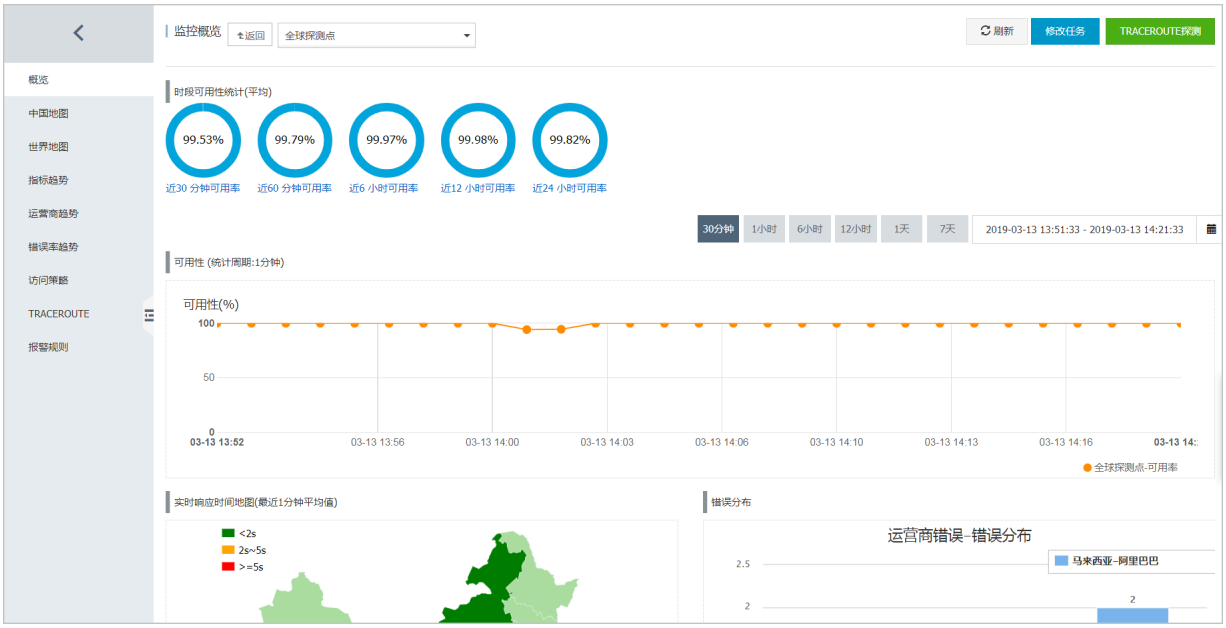
1. 登录云监控控制台。
2. 单击左侧导航栏中站点监控下的站点管理，进入站点管理页面。



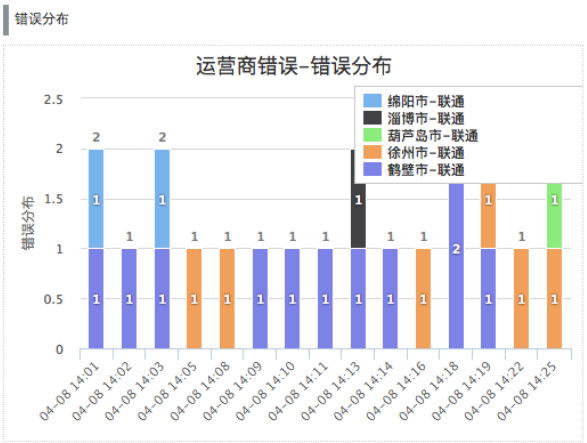
3. 单击列表中的站点名称，进入监控概览页面，默认展示概览页。您可单击左侧导航菜单查看其它监控数据。

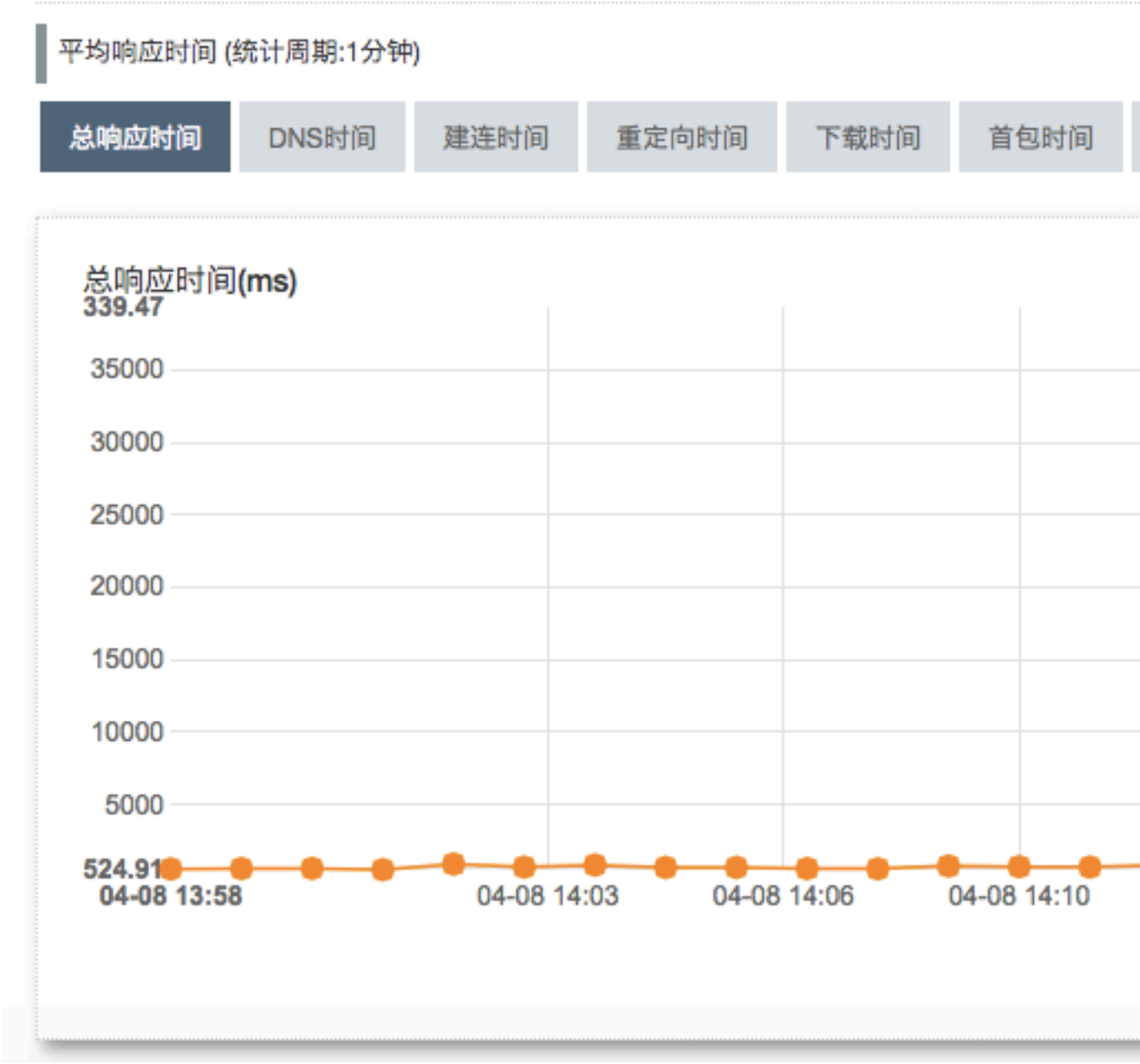
概览

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。



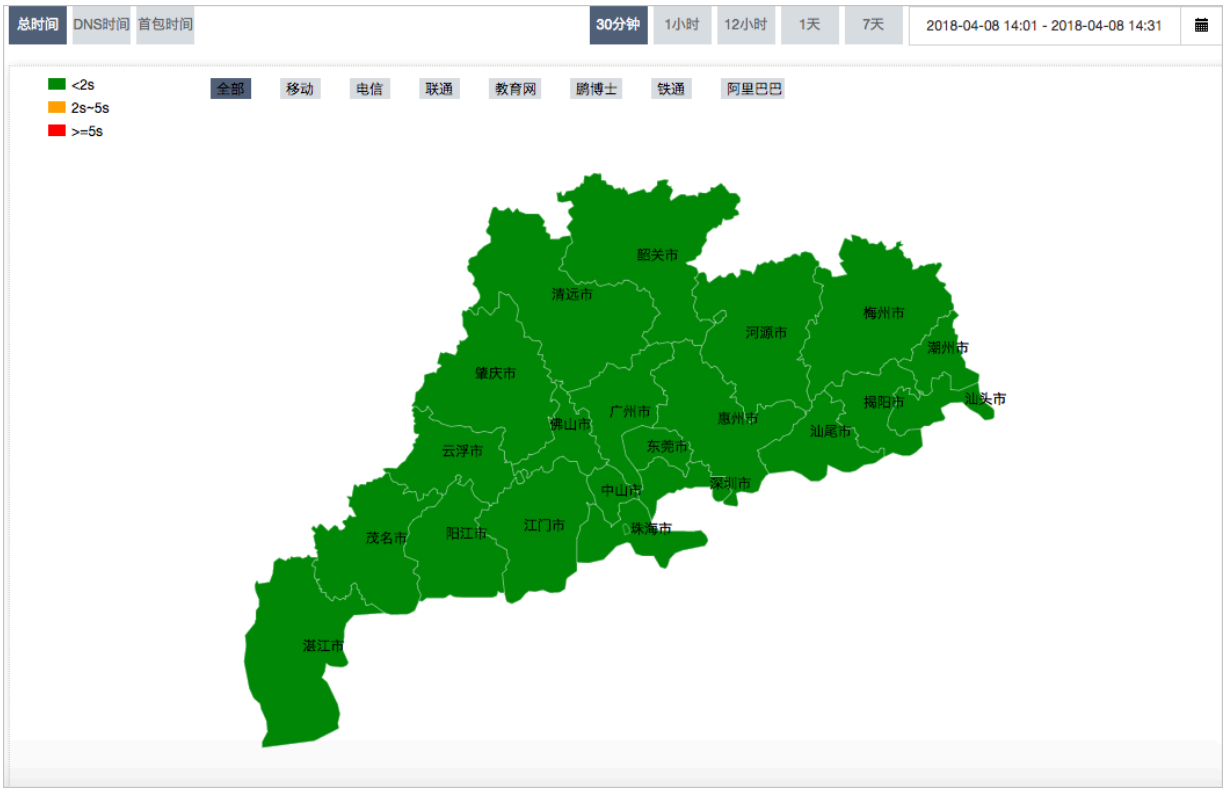
错误分布会统计一段时间内各地域运营商探测结果中状态码超过399的数量。如需查看错误详情，可单击图表下钻查看相关数据。




平均响应时间 (统计周期:1分钟)
总响应时间
DNS时间
建连时间
重定向时间
下载时间
首包时间
总响应时间(ms)
339.47
35000
30000
25000
20000
15000
10000
5000
524.91
04-08 13:58
04-08 14:03
04-08 14:06
04-08 14:10

中国地图

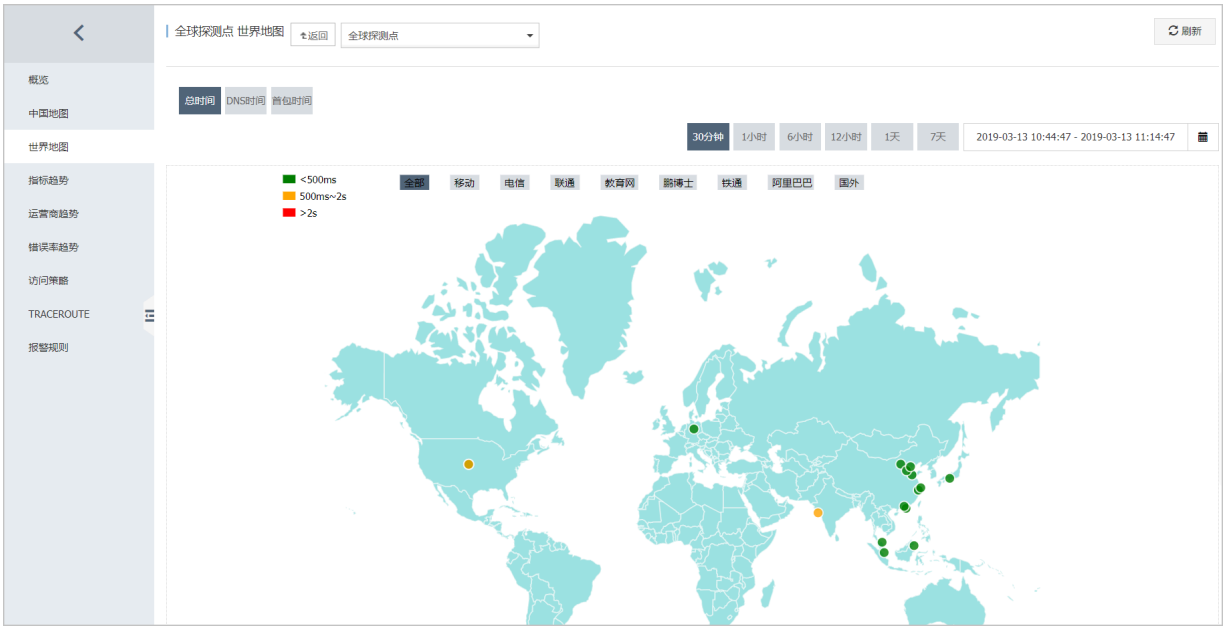
鼠标左键单击相应省份会显示二级地域



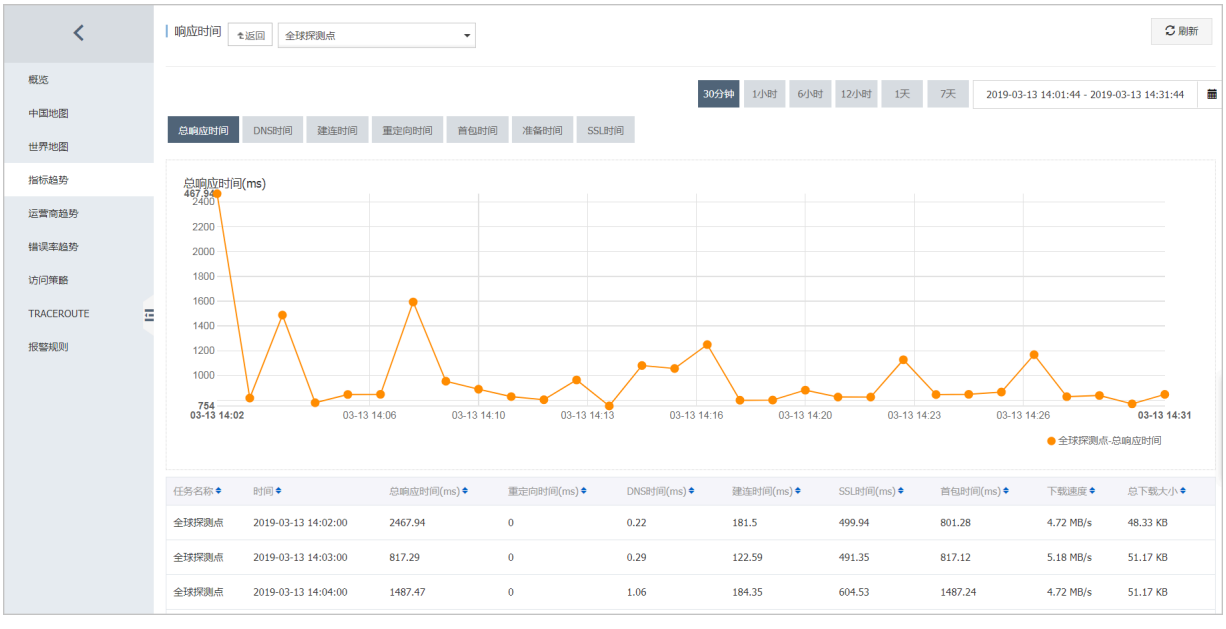
地图下方提供相关地域的监控数据详情

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)	下载速度	总下载大小
全球探测点	2019-03-13 13:57:00	广东省	深圳市	389	0	0	28	114	389	254.20 KB/s	51.18 KB
全球探测点	2019-03-13 13:58:00	广东省	深圳市	378	0	0	28	112	378	1.81 MB/s	51.18 KB
全球探测点	2019-03-13 13:59:00	广东省	深圳市	377	0	0	29	118	377	1.71 MB/s	51.16 KB
全球探测点	2019-03-13 14:00:00	广东省	深圳市	286	0	0	30	119	286	1.69 MB/s	51.18 KB
全球探测点	2019-03-13 14:01:00	广东省	深圳市	394	0	0	28	112	394	1.77 MB/s	51.18 KB
全球探测点	2019-03-13 14:02:00	广东省	深圳市	293	0	0	30	120	293	251.70 KB/s	51.18 KB
全球探测点	2019-03-13 14:03:00	广东省	深圳市	304	0	0	31	125	304	1.47 MB/s	51.16 KB
全球探测点	2019-03-13 14:04:00	广东省	深圳市	300	0	0	31	124	300	1.60 MB/s	51.18 KB
全球探测点	2019-03-13 14:05:00	广东省	深圳市	397	0	0	27	111	397	1.82 MB/s	51.18 KB
全球探测点	2019-03-13 14:06:00	广东省	深圳市	280	0	0	29	117	280	1.74 MB/s	51.16 KB

世界地图

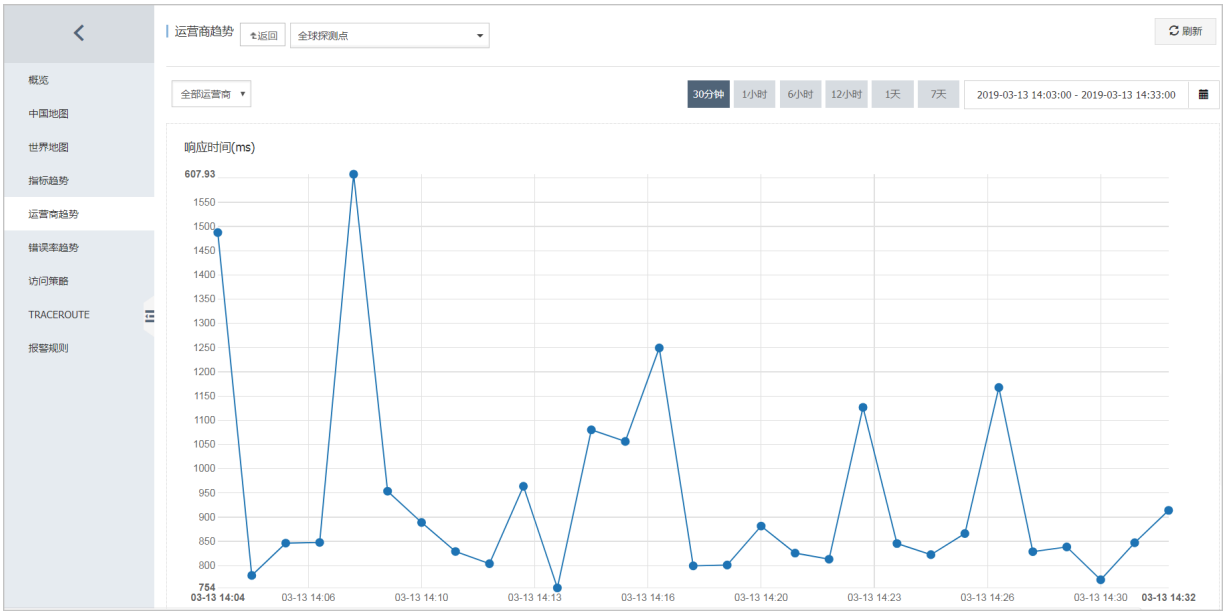


指标趋势

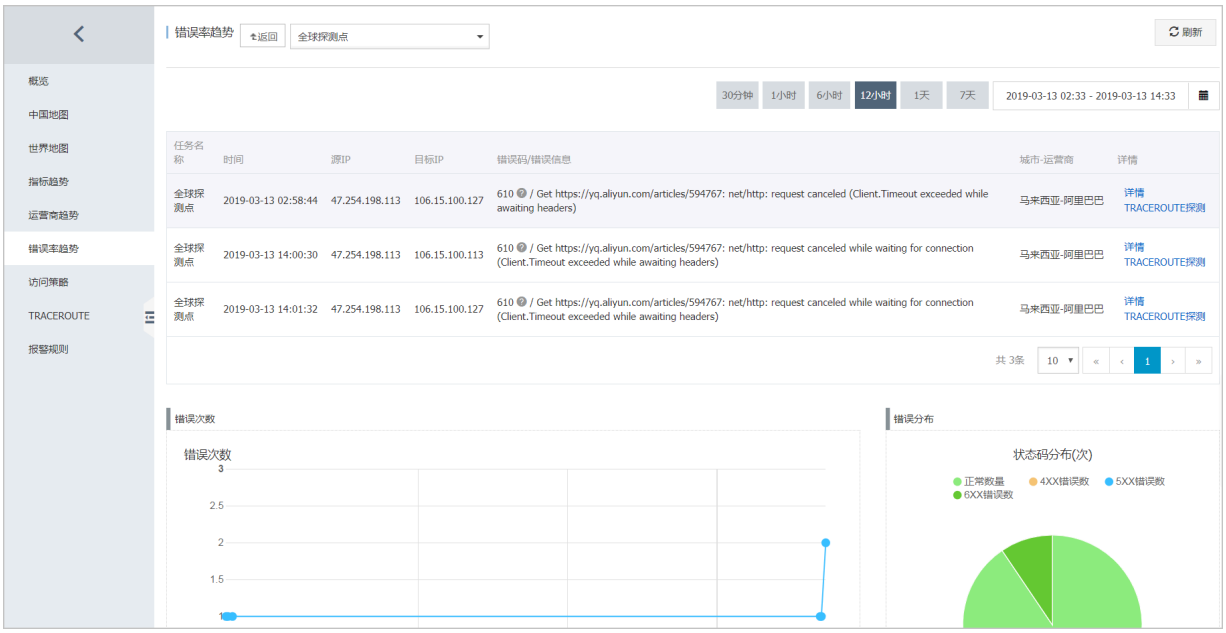


任务名称	时间	总响应时间(ms)	重定向时间(ms)	DNS时间(ms)	建连时间(ms)	SSL时间(ms)	首包时间(ms)	下载速度	总下载大小
全球探测点	2019-03-13 14:02:00	2467.94	0	0.22	181.5	499.94	801.28	4.72 MB/s	48.33 KB
全球探测点	2019-03-13 14:03:00	817.29	0	0.29	122.59	491.35	817.12	5.18 MB/s	51.17 KB
全球探测点	2019-03-13 14:04:00	1487.47	0	1.06	184.35	604.53	1487.24	4.72 MB/s	51.17 KB

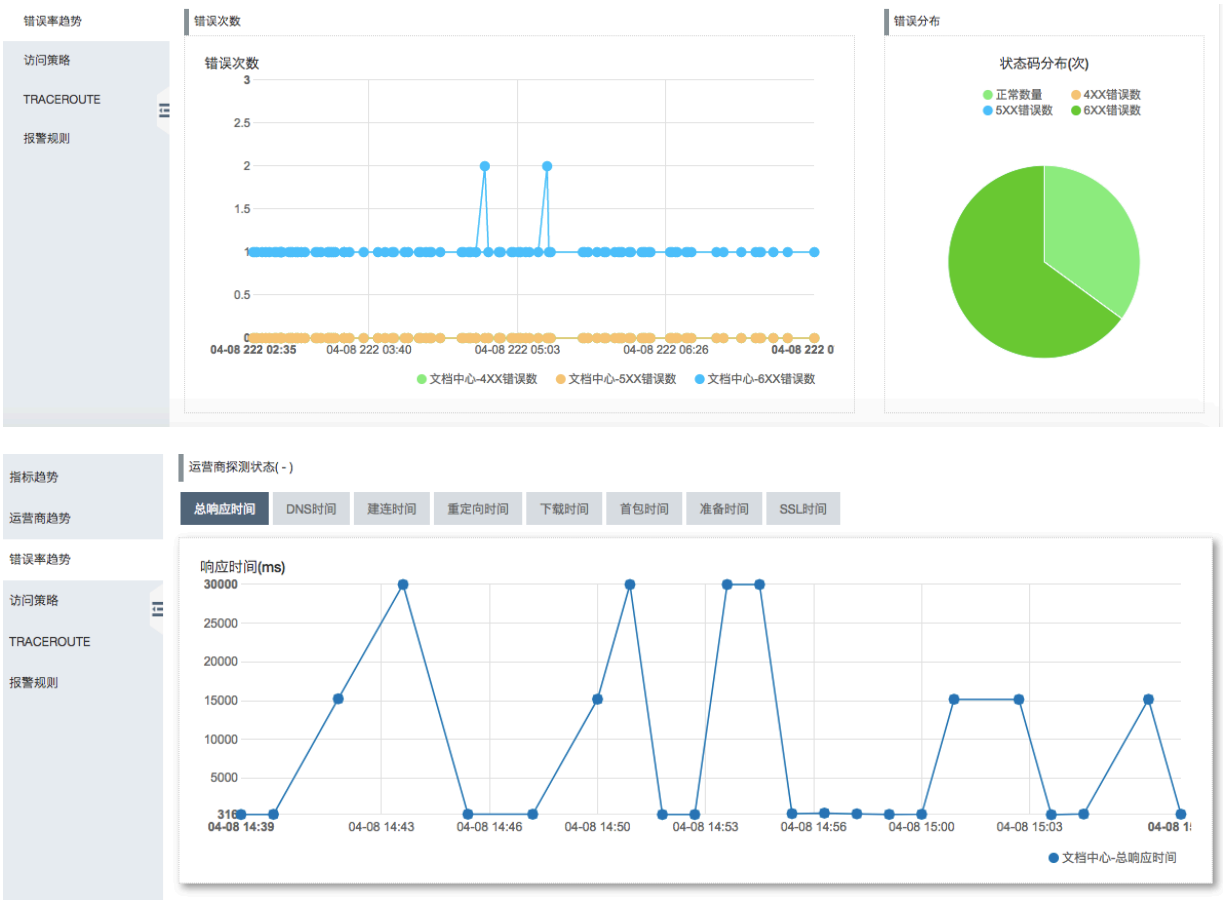
运营商趋势



错误率趋势

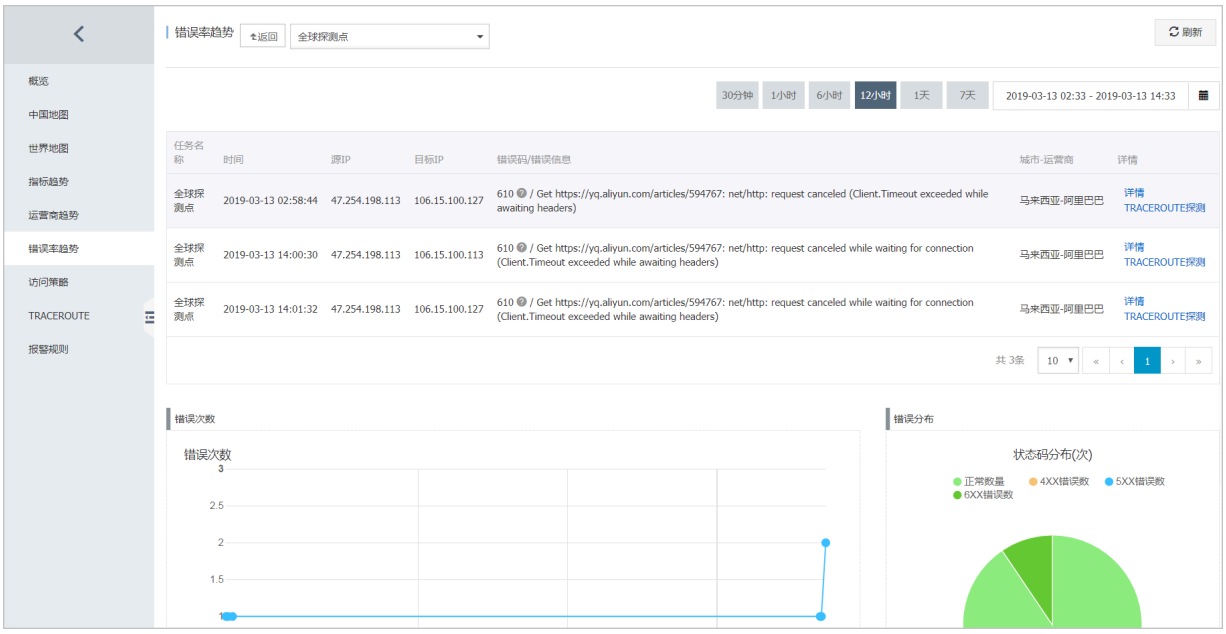


单击操作中的详情，可以以城市和运营商作为过滤条件，查看如下详情。



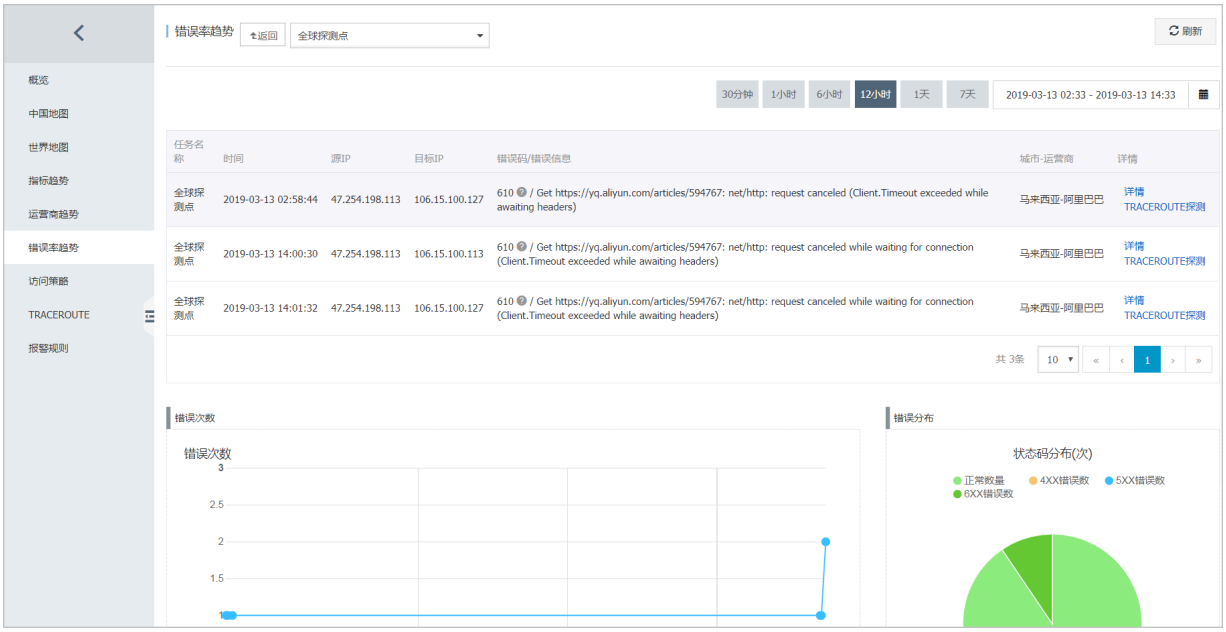
访问策略

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，单击页面右上角的TRACEROUTE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。

名词	解释
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）。

3.5 状态码说明

站点监控的每种协议在进行探测时，都会返回状态码，以下为常见状态码说明。

云监控自定义状态码含义

协议	状态码	含义
HTTP	610	超时(连接超时、SSL证书交换超时，超时时间为30s)
HTTP	613	DNS解析错误
HTTP	615	内容不匹配
HTTP	616	认证失败
HTTP	611	其他原因导致的探测失败
HTTP	617	超过最大跳转次数 ECS探测点允许的3XX重定向最大跳转次数为5次 运营商探测点允许的3XX重定向最大跳转次数为2次
HTTP	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。
Ping	550	网络不通
Ping	610	网络稳定，但发出的所有包在2秒内均无响应
Ping	613	无法通过host解析出IP地址
Ping	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。

协议	状态码	含义
TCP	550	无法打开socket(通常是因为系统资源耗尽)
TCP	610	接收回应失败(超时或无回应)
TCP	611	连接失败(超时或对端拒绝)
TCP	615	内容不匹配
TCP	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。
UDP	550	无法打开socket(通常是因为系统资源耗尽)
UDP	611	连接失败(host无法解析)
UDP	610	发送或接收失败
UDP	615	内容不匹配
UDP	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。
DNS	610	DNS解析失败
DNS	613	DNS query通信出现异常
DNS	615	内容不匹配
DNS	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。
SMTP	610	连接超时
SMTP	611	无法成功访问您的站点，失败原因包含但不限于DNS解析失败、Email格式不正确、初始化SMTP客户端失败等
SMTP	616	登录被拒绝
SMTP	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。
POP3	611	无法成功访问您的站点

协议	状态码	含义
POP3	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。
FTP	610	FTP传输失败
FTP	611	其它原因导致的失败，如DNS解析失败，TCP连接失败等
FTP	616	登录失败
FTP	703	禁止对服务器进行内网探测。内网探测可以使用可用性监控功能。

HTTP协议常用标准状态码含义

状态码	含义	备注
200	请求已完成	2XX状态码均为正常状态码返回。
300	多种选择	服务器根据请求可执行多种操作。服务器可根据请求者 (User agent) 来选择一项操作，或提供操作列表供请求者选择。
301	永久移动	请求的网页已被永久移动到新位置。服务器返回此响应（作为对 GET 或 HEAD 请求的响应）时，会自动将请求者转到新位置。您应使用此代码通知 Googlebot 某个网页或网站已被永久移动到新位置。
302	临时移动	服务器目前正从不同位置的网页响应请求，但请求者应继续使用原有位置来进行以后的请求。此代码与响应 GET 和 HEAD 请求的 301 代码类似，会自动将请求者转到不同的位置。

状态码	含义	备注
303	查看其他位置	当请求者应对不同的位置进行单独的 GET 请求以检索响应时，服务器会返回此代码。对于除 HEAD 请求之外的所有请求，服务器会自动转到其他位置。
304	未修改	自从上次请求后，请求的网页未被修改过。服务器返回此响应时，不会返回网页内容。
305	使用代理	请求者只能使用代理访问请求的网页。如果服务器返回此响应，那么，服务器还会指明请求者应当使用的代理。
400	错误请求	服务器不理解请求的语法。
401	未授权	请求要求进行身份验证。登录后，服务器可能会对页面返回此响应。
403	已禁止	服务器拒绝请求。
404	未找到	服务器找不到请求的网页。例如，如果请求是针对服务器上不存在的网页进行的，那么，服务器通常会返回此代码。
405	方法禁用	禁用请求中所指定的方法。
406	不接受	无法使用请求的内容特性来响应请求的网页。
407	需要代理授权	此状态代码与401（未授权）类似，但却指定了请求者应当使用代理进行授权。如果服务器返回此响应，那么，服务器还会指明请求者应当使用的代理。
408	请求超时	服务器等候请求时超时。

状态码	含义	备注
409	冲突	服务器在完成请求时发生冲突。服务器的响应必须包含有关响应中所发生的冲突的信息。服务器在响应与前一个请求相冲突的PUT请求时可能会返回此代码，同时会提供两个请求的差异列表。
411	需要有效长度	服务器不会接受包含无效内容长度标头字段的请求。
412	未满足前提条件	服务器未满足请求者在请求中设置的其中一个前提条件。
413	请求实体过大	服务器无法处理请求，因为请求实体过大，已超出服务器的处理能力。
414	请求的URI过长	请求的URI（通常为网址）过长，服务器无法进行处理。
415	不支持的媒体类型	请求的格式不受请求页面的支持。
416	请求范围不符合要求	如果请求是针对网页的无效范围进行的，那么，服务器会返回此状态代码。
417	未满足期望值	服务器未满足期望请求标头字段的要求。
499	客户端断开连接	因服务端处理时间过长，客户端关闭了连接。
500	服务器内部错误	服务器遇到错误，无法完成请求。
501	尚未实施	服务器不具备完成请求的功能。例如，当服务器无法识别请求方法时，服务器可能会返回此代码。
502	错误网关	服务器作为网关或代理，从上游服务器收到了无效的响应。
503	服务不可用	目前无法使用服务器（由于超载或进行停机维护）。通常，这只是一种暂时的状态。

状态码	含义	备注
504	网关超时	服务器作为网关或代理，未及时从上游服务器接收请求。
505	HTTP版本不受支持	服务器不支持请求中所使用的HTTP协议版本。

4 报警服务

4.1 报警服务概览

您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。您可以在全部资源、应用分组和单实例维度设置报警规则。

报警服务支持电话、短信、邮件、旺旺、钉钉机器人等多种方式。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。

主机监控报警规则

您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

您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

您可以对各类云产品中的资源设置性能消耗类指标的阈值报警，也可以对实例或服务的状态设置事件类的报警。

自定义监控报警规则

您通过自定义监控接口上报监控数据后，可对对应监控信息设置报警规则，当监控数据阈值达到报警条件时，触发相应报警通知方式。

自定义事件报警规则

您通过自定义事件接口上报异常事件后，可对对应事件设置报警规则，当上报的事件符合报警条件时，触发相应报警通知方式。

4.2 创建报警模板

本文为您介绍如何通过创建和使用报警模板，达到简化报警规则的创建和维护过程的目的。

背景信息

当您拥有大量云资源（ECS、RDS、SLB、OSS等），各云资源逐一的去设置报警规则是一件很繁琐的事。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，当您创建报警

规则时可以直接使用模板，无需每次重复定义报警规则描述的过程。您可以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，可极大简化报警的创建和维护过程。

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。

创建报警模板的准备工作

报警模板需要与应用分组配合使用，您可以先创建创应用分组，然后再创建报警模板，并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。如何创建应用分组，请参见创建应用分组。

创建报警模板的实施步骤

注意事项

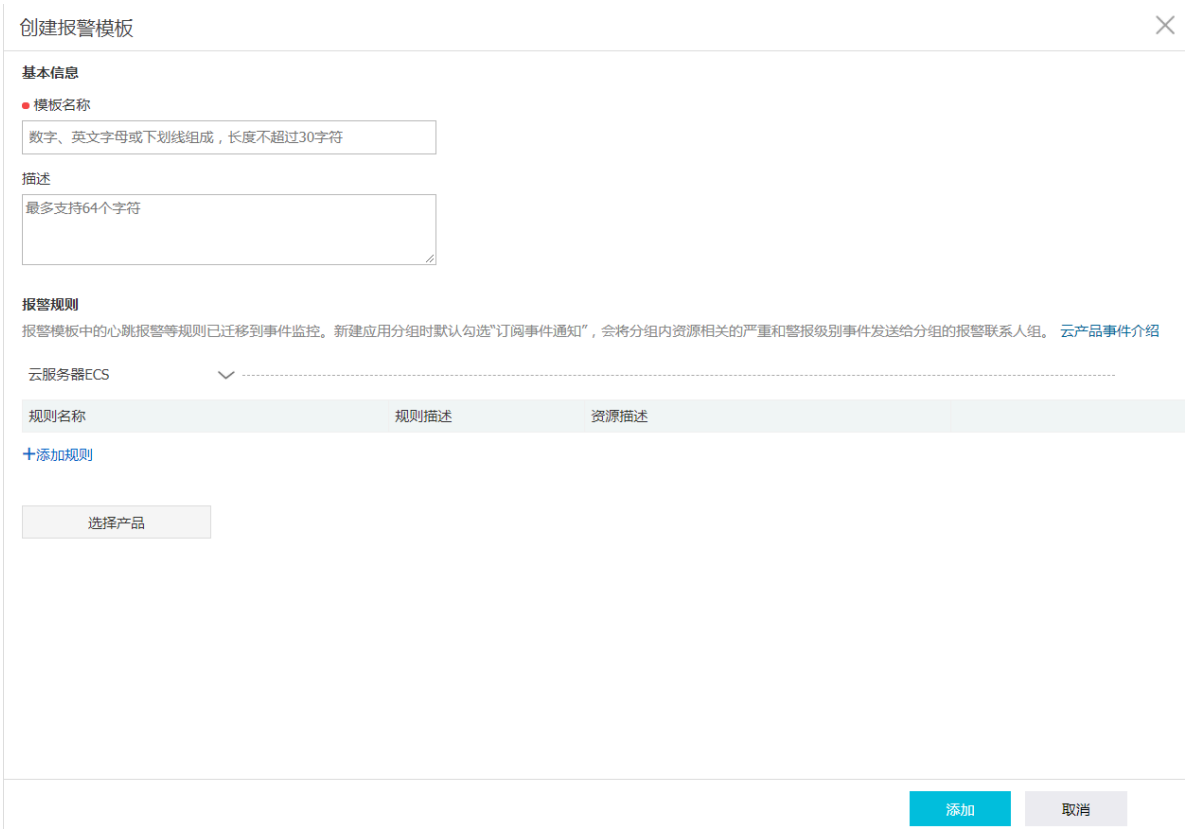
说明:

- 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。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警模板，进入报警模板页面。

3. 单击页面右上角的创建报警模板按钮，进入创建报警模板页面。



4. 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。
5. 配置报警规则，单击添加规则，增加规则配置。
6. 配置完报警规则后，单击添加即可。

如何使用报警模板

- 创建应用分组时使用报警模板

  您为资源创建应用分组时，可以在监控报警的配置部分直接选择已有的报警模板。应用分组创建成功后，云监控会按照报警模板为您生成报警规则。

- 将报警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。

更多信息

- 将报警模板应用到分组
- 创建阈值报警规则

4.3 报警规则

4.3.1 创建阈值报警规则

本文为您介绍如何创建阈值报警规则，通过对监控项报警阈值进行监控，帮您第一时间得知监控数据异常，以便及时处理问题。

背景信息

当您需要管理和监控各云产品资源的使用和运行情况时，您以通过创建阈值报警规则，实现监控项超过设定阈值后自动发送报警通知，帮您及时得知监控数据异常并快速进行处理。

创建阈值报警规则准备工作

在创建阈值报警规则之前，建议您先创建报警联系人和报警联系组，以便在创建报警规则时选择相应的报警联系组，接收报警通知，如何创建报警联系人和报警联系组，请参见创建报警联系人/报警联系组。

如果您想在报警规则中使用报警回调，还需要准备能通过公网访问的回调URL并在已有的运维系统或消息通知系统的告警方式中开启URL回调。

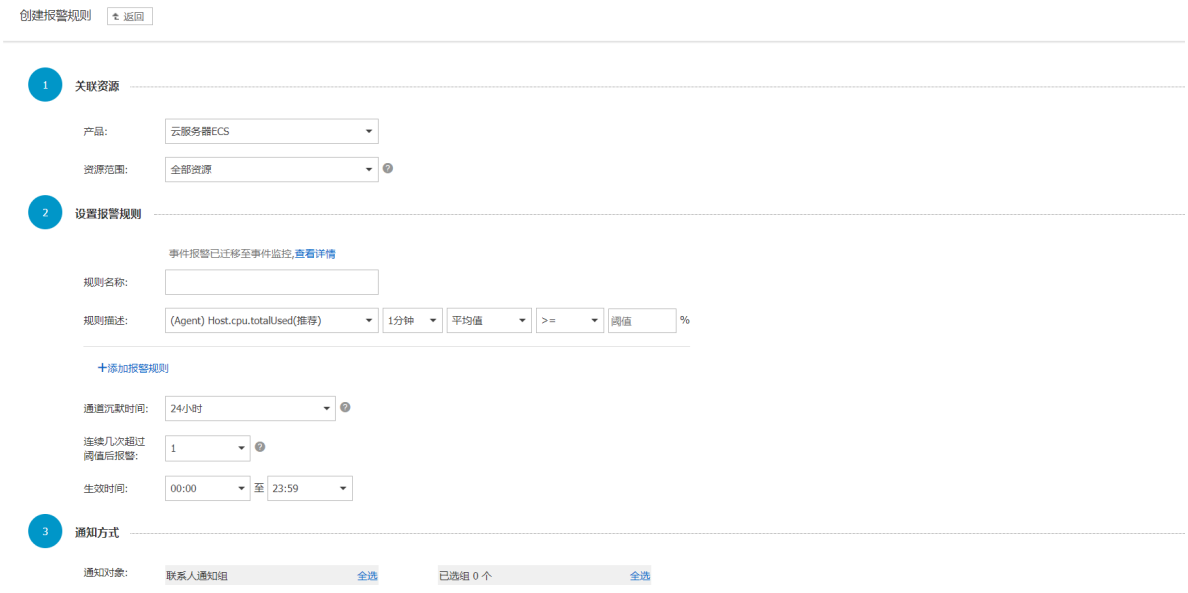
创建阈值报警规则的实施步骤

注意事项

报警服务支持电话、短信、邮件、旺旺、钉钉机器人等多种方式。如果您想通过多种方式接收报警通知，请在设置报警联系人时确保各通知方式信息准确无误。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警规则，进入报警规则列表页面，默认为阈值报警列表。
3. 单击列表上方的创建报警规则按钮，进入创建报警规则页面。



4. 选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。报警规则参数相关说明，请参见报警规则参数说明。

更多信息

- 如何使用报警回调
- 如何创建和使用报警模板
- 如何使用一键报警

4.3.2 创建事件报警规则

本文为您介绍如何创建事件报警规则，以便在阿里云产品发生系统异常时，您能及时接收报警通知并处理异常。

背景信息

当阿里云产品发生系统异常时，如何能够及时接收到异常报警通知并及时进行处理？云监控的报警服务为您提供以下两种事件报警通知能力，方便您及时知晓事件发生、自动化处理异常：

- 提供通过电话、短信、邮件、钉钉群的方式，对事件发生进行报警。
- 将事件分发到您的消息服务队列、函数计算、URL回调，以便您根据业务场景自动化处理异常事件。

创建事件报警规则的准备工作

在创建事件报警规则之前，建议您先创建报警联系人和报警联系组，以便在创建报警规则时选择相应的报警联系组，接收报警通知，如何创建报警联系人和报警联系组，请参见创建报警联系人/报警联系组。

如果您想在系统事件的报警方式中使用报警回调，还需要准备能通过公网访问的回调URL并在已有的运维系统或消息通知系统的告警方式中开启URL回调。

如果您想在系统事件的报警方式中使用消息队列、函数计算，请创建相应的消息队列、函数。

创建事件报警规则的实施步骤

注意事项

事件报警规则分为系统事件和自定义事件，不同类型事件对应的报警规则和通知方式有所不同。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警规则，进入报警规则列表页面，默认为阈值报警列表。

3. 单击事件报警页签，单击右上角的创建事件报警，弹出创建/修改事件报警对话框。

4. 在基本信息区域，填写报警规则名称。
5. 设置事件报警规则：

   a. 选择事件类型为系统事件时，

      - 产品类型、事件等级、事件名称：按照实际情况填写
      - 资源范围：选择全部资源时，任何资源发生相关事件，都会按照配置发送通知；选择应用分组时，只有指定分组内的资源发生相关事件时，才会发送通知。

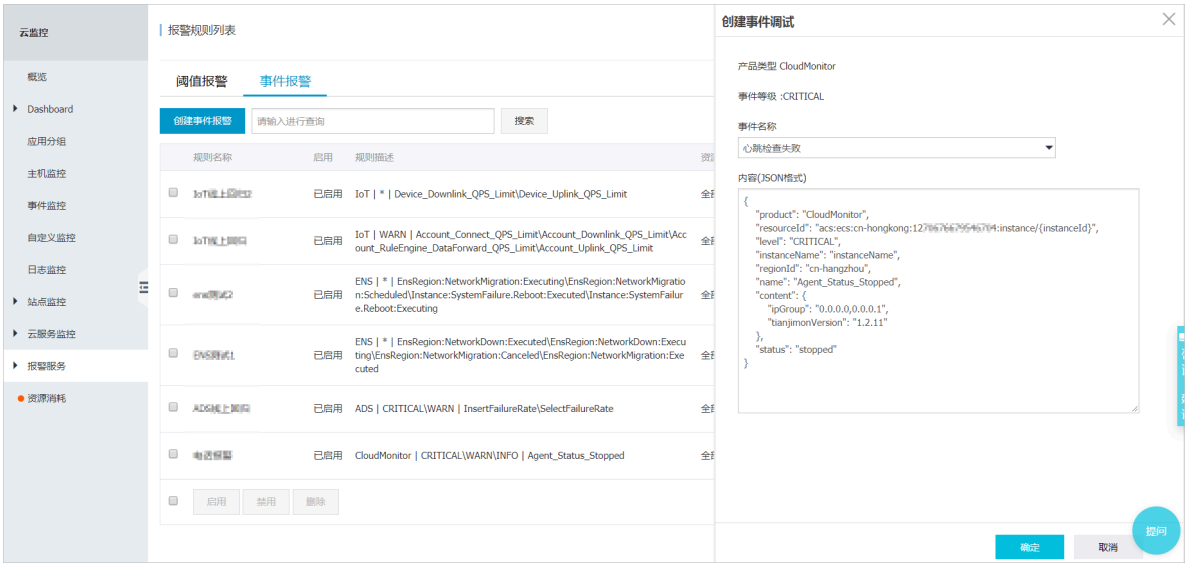
   b. 选择事件类型为自定义事件时，所属应用分组、事件名称、规则描述请按照实际情况填写。
6. 选择报警方式。目前系统事件支持报警通知、消息服务队列、函数服务、URL回调四种方式；自定义事件支持支持报警通知和报警回调两种种方式。
7. 完成以上设置后，单击确定按钮即可。

后续操作

创建事件报警规则后，您可以使用系统事件的调试功能，模拟系统事件的发生，以便验证系统事件报警规则中设置的消息服务队列是否能正常接收时间、函数计算的函数是否能正常被触发。

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警规则，进入报警规则列表页面，默认为阈值报警列表。
3. 单击事件报警页签，进入事件监控的报警规则列表页面。

4. 单击操作中的调试，进入创建事件调试页面。



5. 选择需要调试的事件，内容中会显示相应的事件内容，可以根据实际情况修改内容中的实例ID等字段。
6. 单击确定按钮，将根据内容发送一个事件，触发报警规则设置的报警通知、消息服务队列、函数计算、报警回调。

4.3.3 报警规则参数说明

本文为您介绍阈值报警规则相关参数说明。

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个可能会导致达到阈值不报警的问题，建议您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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。
  - 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。例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%，就会发送报警通知。
  - 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。
- 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50M 。
- 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发送报警通知，非生效时间内产生的报警只记录报警历史。
- 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。

4.3.4 管理报警规则

报警服务是云监控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，以便及时处理问题。

云监控为您提供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。
- 在各云服务监控中设置报警规则。
- 在站点监控中设置报警规则。
- 在自定义监控中设置报警规则。

4.3.5 使用报警回调

本文旨在介绍如何报使用警回调功能，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。

背景信息

云监控除了电话、短信、邮件、钉钉机器人等报警通知方式外，还可以使用报警回调方式。无论您是运维人员还是开发人员，您会发现报警回调可以让您更自由、更灵活的处理告警事件。

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。

使用报警回调的准备工作

- 准备能通过公网访问的回调URL。
- 在已有的运维系统或消息通知系统的告警方式中开启URL回调。

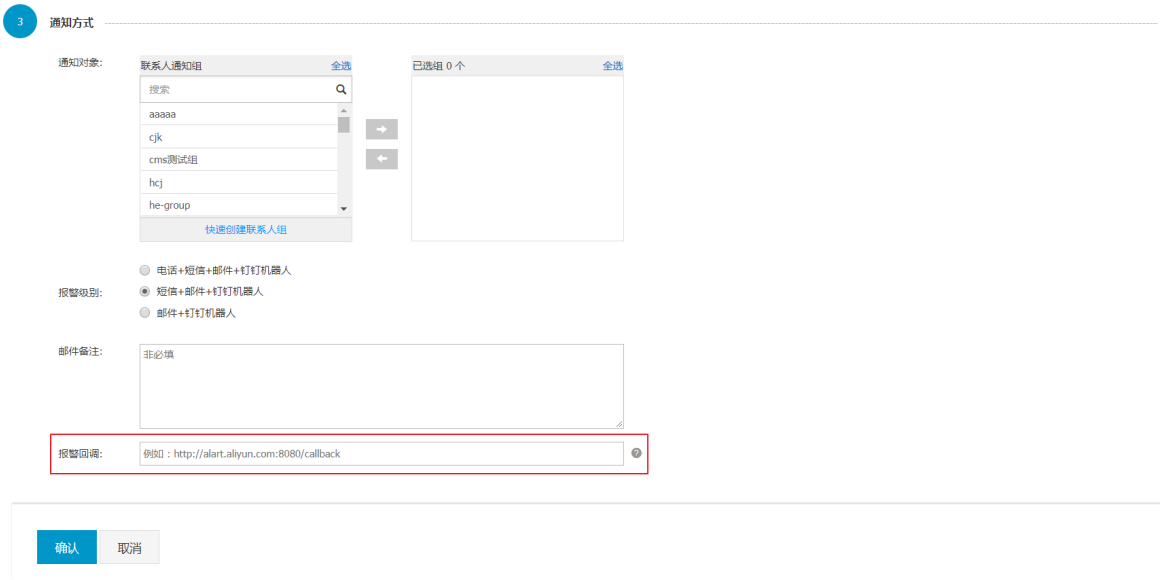
使用报警回调的实施步骤

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。
- 目前仅支持HTTP协议。

操作步骤

1. 登录云监控控制台。
2. 修改需要增加回调的报警规则，或者创建新的报警规则。



3. 在报警通知方式中，填写需要报警回调的URL地址，确认即可。当报警规则被触发时，云监控会将报警消息发送到您指定的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-de017a8327
f6",
    "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"
}
```

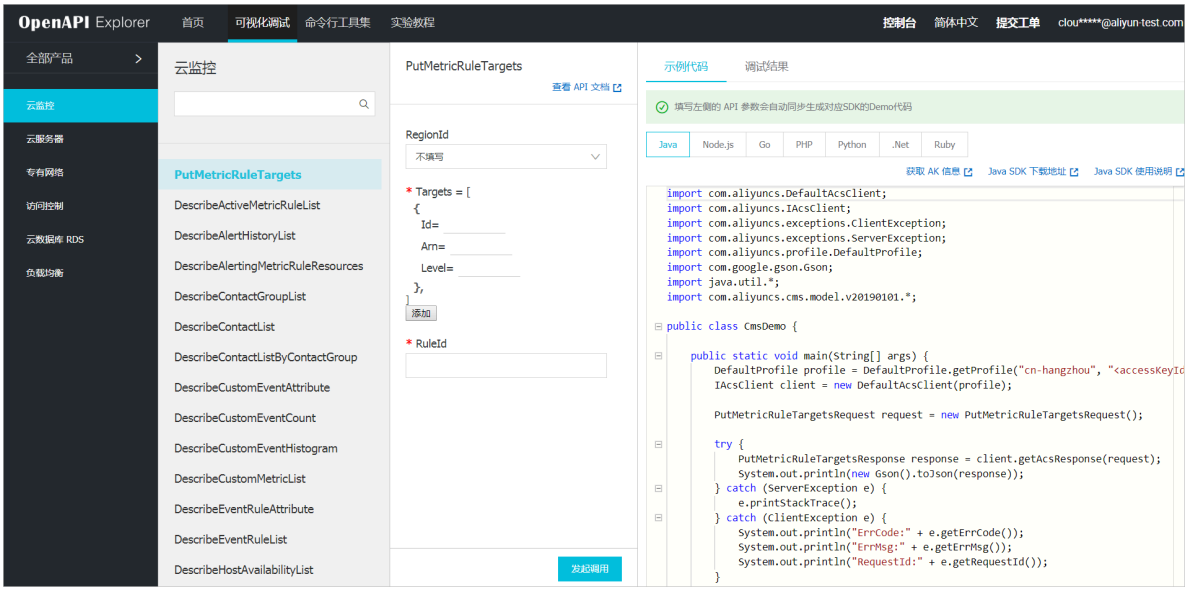
4.3.6 报警信息写入消息服务 MNS

本文为您介绍如何将阈值类指标的报警信息写入到指定的消息服务 MNS。

操作步骤

1. **授权云监控将报警信息写入消息服务 MNS的权限，单击这里进行授权。**

2. **通过阿里云 OpenAPI Explorer 调用*PutResourceMetricRule*接口，创建报警规则。**
3. **调用*PutMetricRuleTargets*接口，创建一个指定报警规则的报警信息，并写入指定MNS的配置。**



ARN：指具体写入的MNS queue或topic，写入queue的ARN格式为`"acs:mns:{$RegionId}:{$UserId}:/queues/{$queueName}/messages"`，写入topic的ARN格式为`"acs:mns:{$RegionId}:{$UserId}:/topics/{$queueName}/messages"`。

PutMetricRuleTargets接口参数示例：

```
RuleId:"db17-4afc-b11a-568512d5a1f9",
Targets:[{
    Id: 1,
    Arn:"acs:mns:{$RegionId}:{$UserId}:/queues/{$queueName}/messages",
    Level: ["INFO", "WARN", "CRITICAL"],
}]
```

写入消息服务 MNS 的消息体说明

写入MNS的MessageBody为JSON String，从MNS消费到MessageBody后，请按JSON字符串来解析，消息结构如下：

```
{
  "ruleId": "putNewAlarm_group_778af9ba-a291-46ab-ac53-3983bcee****",
  "ruleName": "test",
  //当前Level
  "curLevel": "WARN",
  //前一级别
  "preLevel": "OK",
  //触发本次报警的实例
  "resources": "{\"instanceId\": \"i-uf61rfofjd2iku7e****\"}",
  //触发本次报警的条件
  "escalation": {
    "comparisonOperator": "GreaterThanYesterday",
    "level": 3,
    "statistics": "Average",
    "tag": "WARN",
    "threshold": "0",
    "times": 1
  },
  "metricData": {
    "timestamp": 1534736160000,
    "userId": "127067667954****",
    "instanceId": "i-uf61rfofjd2iku7e****",
    "Average": 470687744,
    "Maximum": 470794240,
    "Minimum": 470556672,
    //环比同比相关参数--开始
    "AliyunCmsPrevValues": { //对比的数据
      "timestamp": 1534649760000,
      "userId": "127067667954****",
      "instanceId": "i-uf61rfofjd2iku7e****",
      "Average": 468463616,
      "Maximum": 468549632,
      "Minimum": 468258816
    },
    //对比计算的公式
    "AliyunCmsComplexExpression": "100.0 * ($Average-$$prevAverage)/$$
prevAverage",
    //对比计算的换算式
    "AliyunCmsComplexMath": "100.0 * (470687744-468463616)/468463616",
    //对比计算的结果
    "AliyunCmsComplexValue": 0.47477070236336133
    //环比同比相关参数--结束
  },
  //metric信息
  "metricName": "memory_actualusedspace#60",
  "namespace": "acs_ecs_dashboard",
  "period": "60",
```

```
  //应用分组信息
  "groupBy": "group",
  "productGroupName": "RDS实例组",
  "groupId":"44958",

  //报警时间
  "lastTime": 327362743, //持续时间
  "time": 1534736160000, //数据发生时间

  "userId": "173651113438****",
  "eventName": "AlertOk",
  "eventType": "Alert",
  //用来trace消息
  "batchId": "4272653-152082****-0",
  "version": "1.0"
}
```

4.4 报警联系人

4.4.1 创建报警联系人/报警联系组

本文为您介绍如何创建报警联系人/报警联系组，并将联系人添加到联系组，从而实现通过报警联系组接收报警通知的目的。

背景信息

报警联系人和联系组是云监控发送报警通知的基础，您需要先创建报警联系人并把联系人添加到报警联系组，然后在创建报警规则时选择相应的报警联系组，才能收到报警通知。

报警联系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，都是通过报警联系组发送报警通知的。

创建报警联系人/报警联系组的准备工作

准备报警联系人信息，确保各通知方式信息准确无误。

创建报警联系人/报警联系组的实施步骤

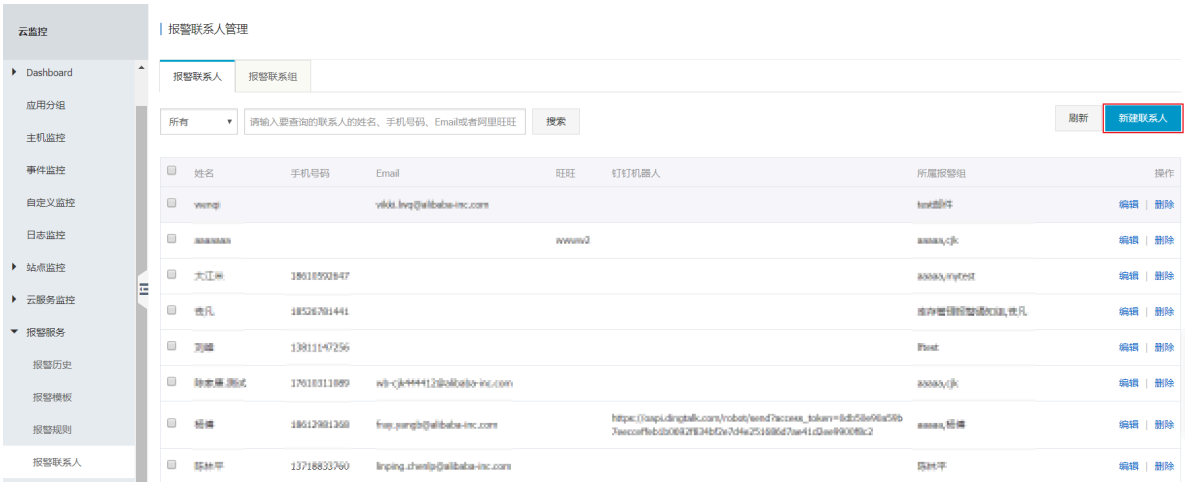
注意事项

> 说明:
>
> 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。

创建报警联系人

1. 登录云监控控制台。

2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。



3. 单击右上角的新建联系人按钮，填写姓名、手机号、邮箱等信息。

4. 信息验证无误后，单击保存按钮即可完成创建报警联系人。

创建报警联系组

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。
3. 单击上方的报警联系组页签。

4. 单击右上角的新建联系组，弹出新建联系组页面。

5. 填写组名并选择需要加入到组中的联系人，点击确定即可完成创建报警联系组。

批量添加联系人到报警联系组

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。
3. 在报警联系人列表中，勾选需要添加的联系人。
4. 单击列表最下方的添加到报警联系组。
5. 在弹窗中选择对应的联系组，点击确定即可将所选联系人批量添加到指定报警联系组中。

4.4.2 报警联系人/报警联系组管理

本文为您介绍如何对报警联系人/报警联系组进行修改、删除等操作。

报警联系人管理

- 编辑报警联系人

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。
3. 在报警联系人列表，单击操作中的编辑按钮，可对联系人信息进行编辑。

- 删除报警联系人

  1. 登录云监控控制台。
  2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。
  3. 在报警联系人列表，单击操作中的删除按钮，即可删除该联系人。

  > 说明:
  > 删除报警联系人后，该联系人将不再收到云监控报警通知。

报警联系组管理

报警联系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，都是通过报警联系组发送报警通知的。

- 编辑报警联系组

  1. 登录云监控控制台。
  2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。
  3. 单击页面上方的报警联系组页签。
  4. 在报警联系组列表，单击操作中的编辑图标，可增减联系组中的联系人。

- 删除报警联系组

  1. 登录云监控控制台。
  2. 单击左侧导航栏中报警服务下的报警联系人，进入报警联系人管理页面。
  3. 单击页面上方的报警联系组页签。
  4. 在报警联系组列表，单击操作中的删除图标，可删除对应的联系组。

4.5 查看报警历史

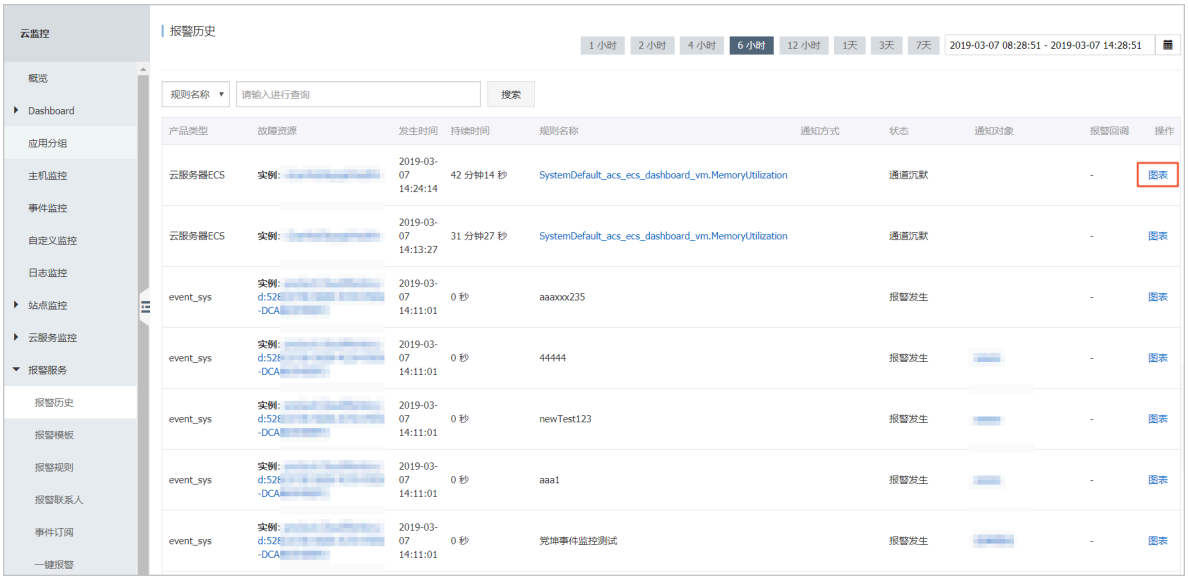
本文为您介绍报警发生后如何查看报警历史信息。

云监控报警服务为您提供了查看云监控报警历史信息功能，您可以按规则名称或分组名称进行搜索查询。

查看报警历史的操作步骤

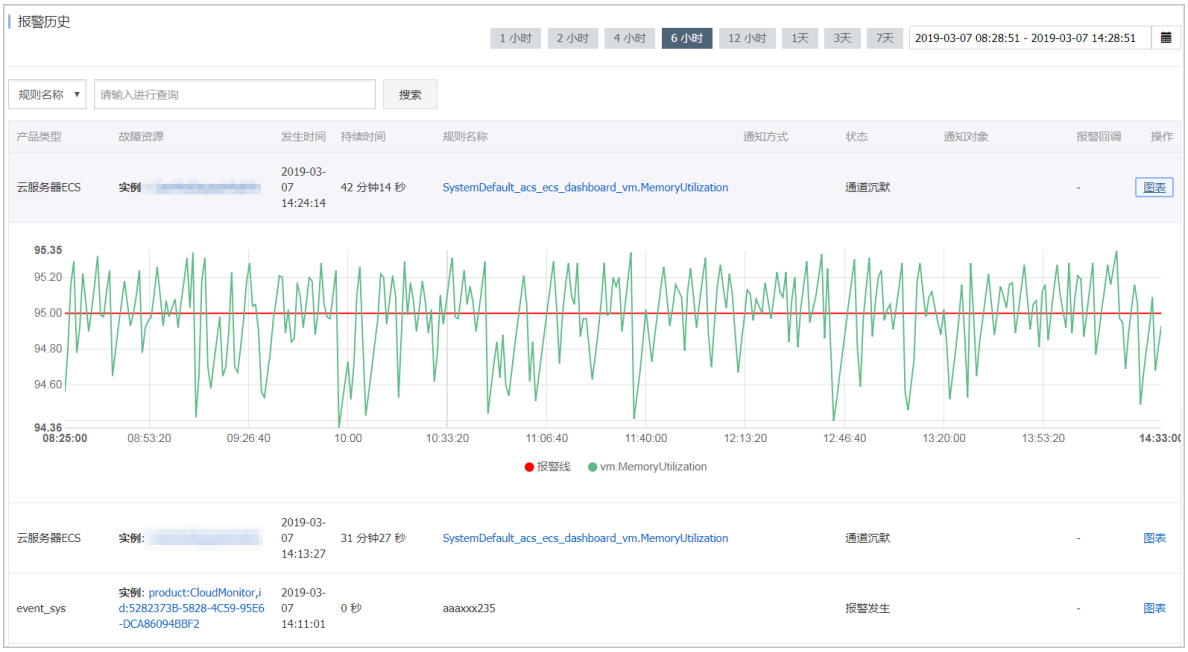
1. 登录云监控控制台。

2. 单击左侧导航栏中报警服务下的报警历史，进入报警历史页面。



3. 在搜索条件下拉框中，选择搜索条件（规则名称或分组名称），输入关键字，单击搜索按钮，即可搜索出符合条件的报警历史记录。

4. 在搜索结果列表操作栏中，单击图表，可展开查看报警图表。



5. 单击页面上方的时间范围快速选择按钮或自定义时间范围，可按所选时间查看报警历史，不支持查询31天前的数据。

4.6 使用一键报警

本文旨在介绍如何使用一键报警功能一键开启关键监控项报警的服务。

背景信息

一键报警功能为您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。

使用一键报警的准备工作

使用一键报警功能前，我们先了解一下一键报警功能目前支持哪些产品及规则详情。

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。

服务名称	指标名称	规则描述
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。

服务名称	指标名称	规则描述
	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。

服务名称	指标名称	规则描述
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。

使用一键报警的实施步骤

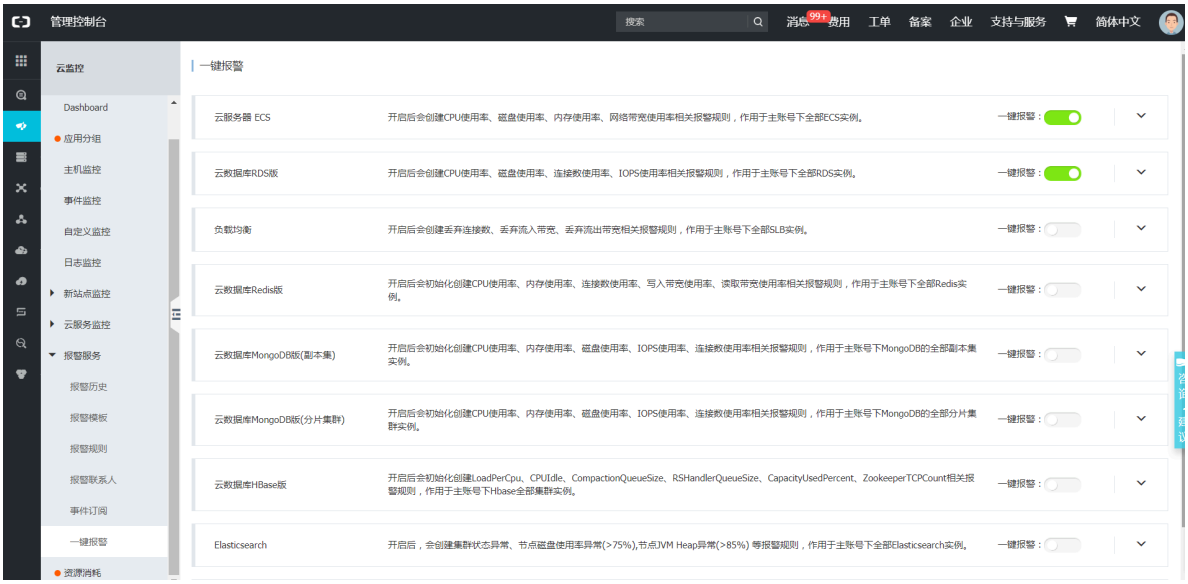
注意事项

- 一键报警功能开启后，默认开启云监控预置的报警规则，快速建立云监控报警体系监控重要指标，并未全面覆盖所有监控指标。
- 一键报警功能开启后，对应的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。
- 一键报警功能支持您对预置的报警规则进行修改、禁用和删除操作。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中报警服务下的一键报警，进入一键报警页面。

3. 对需要设置报警的云产品，单击一键报警开关，开启一键报警。



4. 单击一键报警右侧的下拉按钮，可查看云监控为您自动生成的报警规则。

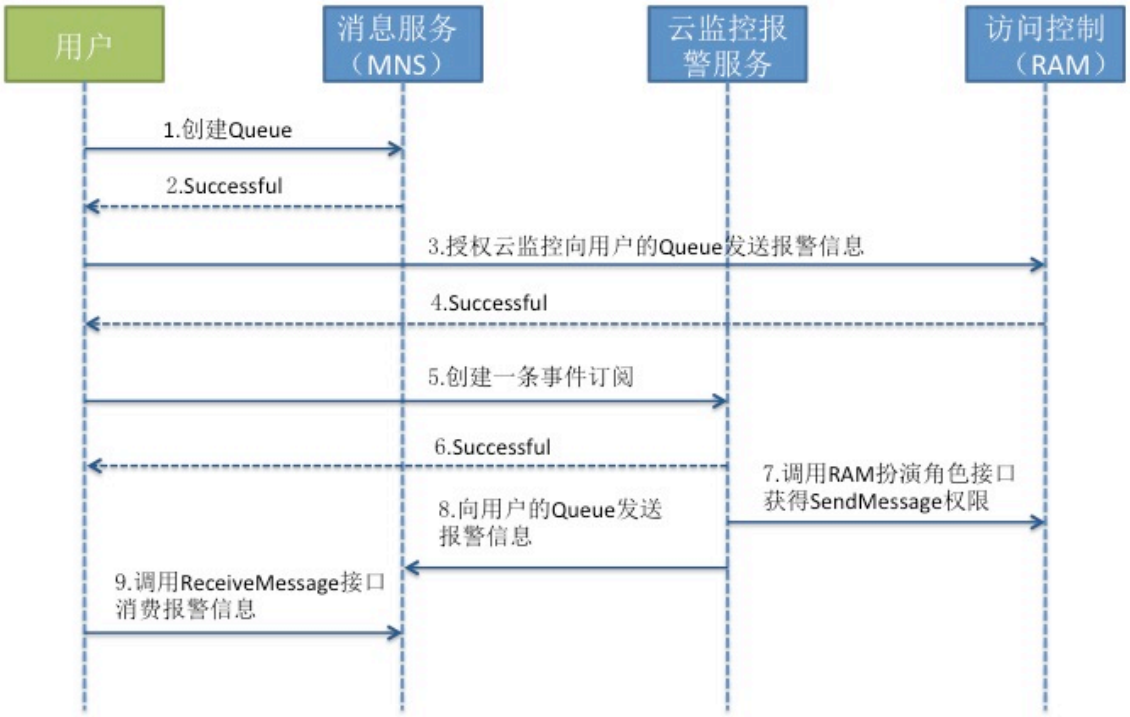
5. （可选）您可以单击操作栏中的禁用、修改、删除，禁用、修改、删除对应的报警规则。

4.7 事件订阅

4.7.1 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。



4.7.2 事件订阅最佳实践

本文为您介绍如何通过云监控创建事件订阅，将报警信息推送到您指定的消息队列中。

背景信息

事件订阅是云监控推出的一种报警信息获取方式，可将生产出的报警信息写入您的消息队列，供您自行消费，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。

使用事件订阅的前提条件

您需要先开通消息服务。

使用事件订阅的实施步骤

注意事项

> **说明:**
> 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

1. 对云监控授权。

   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。

   a. 登录云监控控制台。

   b. 单击左侧导航栏中报警服务下的事件订阅，进入事件订阅页面。

   c. 单击开通权限。

   d. 单击同意授权即可。

2. 创建事件。

   创建一个接收报警通知的事件。

   a. 在事件订阅页面，单击右上角创建事件。

   b. 选择需要接收报警通知的消息队列、消息类型以及事件所属产品，单击确定即可完成创建事件。

3. 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。

报警信息示例

ECS

```
{
    "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":"UserName",
        "dimensions":"云服务器名称=yapot_serv****,云服务器实例ID=AY14051913564762****,IP=182.92.XX.XXX,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-
3bdbe041****"
    },
    "type":0
}
```

SLB

```
{
    "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.XXX.X
",//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-dafe8ce5****"
    },
    "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。
}
```

5 可用性监控

5.1 创建可用性监控

本文为您介绍如何通过创建可用性监控，快速发现本地或依赖的远程服务无响应的情况。

背景信息

为了满足广大云用户探测本地、远程指定路径或端口是否正常响应的需要，云监控的可用性监控功能可以帮助云用户快速发现本地或远程服务无响应的情况，并能够在出现响应超时或状态码错误时发送报警通知。

创建可用性监控的准备工作

- 为您要进行可用性监控的资源创建分组，详情请参见创建应用分组。
- 为被监控主机安装云监控插件，详情请参见云监控Go语言版本插件介绍。

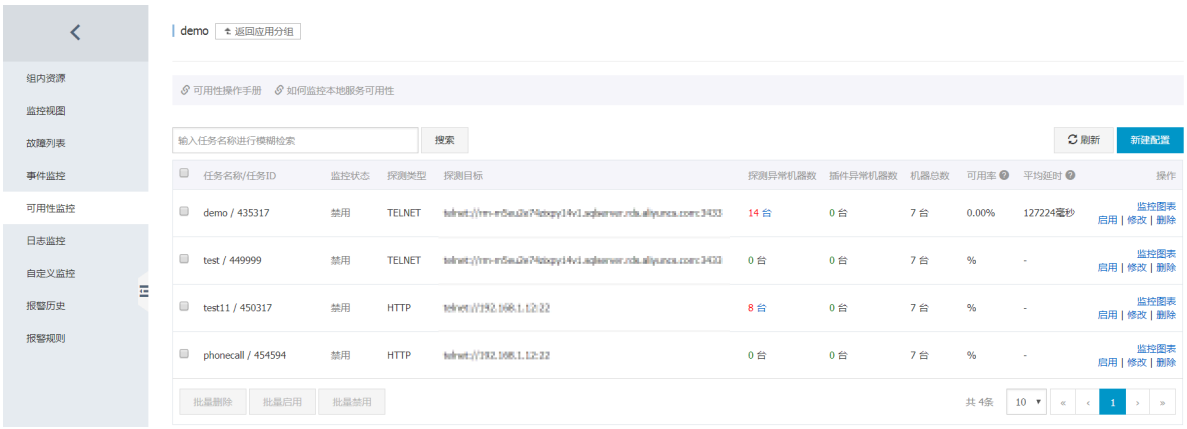
创建可用性监控的实施步骤

注意事项

> **说明:**
>
> - 使用可用性监控功能依赖云监控插件，请确保被监控主机已安装云监控插件。
> - 监控频率为每分钟1次。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要创建可用性监控的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 单击左侧导航栏中的可用性监控，进入可用性监控页面。



5. 单击右上角的新建配置按钮，进入创建可用性监控页面。

6. 输入任务名称，选择探测源（可以是分组内的所有机器配置相同的探测规则，也可以只是部分机器配置相同的探测规则）。
7. 选择探测类型和探测目标：支持URL或者IP、云数据库RDS版、云数据库Redis版三种探测类型。
   - 探测类型为URL或者IP时，支持HTTP(S)、TELNET、PING三种探测目标。当探测目标为HTTP(S)协议时，支持配置HEAD、GET、POST请求方法和返回值的匹配内容。
   - 探测类型为云数据库RDS版、云数据库Redis版时，会显示您分组中的相关实例和访问地址。

8. 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：探测的状态码满足报警设置时就触发报警。
   - 响应时间：探测的响应时间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，报警规则只在生效时间内发送报警通知，非生效时间内产生的报警只记录报警历史。
9. 完成以上配置后，单击确定按钮即可。

5.2 管理可用性监控

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。

查看可用性监控任务

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要查看可用性监控的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 单击左侧导航栏中的可用性监控，进入可用性监控页面，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

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要查看可用性监控的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 选择页面左侧菜单的可用性监控，进入可用性监控页面。

5. 在任务列表中，您可以查看监控结果。

- 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，单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

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要修改可用性监控的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 单击左侧导航栏中的可用性监控，进入可用性监控的管理页面。
5. 选择需要修改的任务，在操作中单击修改，进入修改可用性监控页面。
6. 修改完成后，单击确定即可。

查看报警历史

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要查看报警历史的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 单击左侧导航栏中的报警历史，进入报警历史页面，您可以查看报警历史详情。

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。

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要启用或禁用可用性监控的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 单击左侧导航栏中的可用性监控，进入可用性监控页面。
5. 选择需要启用或禁用的任务，在操作中单击启用或禁用，可以修改任务工作状态。

5.3 本地服务可用性监控

本文为您介绍如何监控本地服务进程的可用性，当本地服务出现响应超时或状态码错误时，发送报警通知。

背景信息

本地服务可用性监控可以帮助云用户快速发现本地服务无响应的情况，并能够在出现响应超时或状态码错误时发送报警通知。

创建本地服务可用性监控的准备工作

- 本地服务可用性监控依赖云监控插件，被监控主机需要安装云监控插件，详情请参见云监控Go语言版本插件介绍。
- 使用本地服务可用性监控前，请先创建应用分组。

创建本地服务可用性监控的实施步骤

注意事项

说明:

- 本地服务可用性监控依赖云监控插件，请确保主机已安装云监控插件。
- 可用性探测频率为每分钟1次。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要创建本地服务可用性监控的应用分组，单击应用分组名称，进入应用分组详情页面。
4. 单击左侧导航栏中的可用性监控，进入可用性监控页面。

5. 单击页面右上角的新建配置按钮，进入创建可用性监控页面。

6. 输入任务名称，选择探测源（可以是分组内的所有机器配置相同的探测规则，也可以只是部分机器配置相同的探测规则）。
7. 选择探测类型和探测目标：支持URL或者IP、云数据库RDS版、云数据库Redis版三种探测类型。
8. 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。
9. 完成以上配置后，单击确定按钮，即可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。

10.（可选）在可用性监控列表中会显示发生报警的异常机器数，单击探测异常机器数，可查看异常机器详情。

参数说明

- 监控配置区域：
  - 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。
  - 探测类型：选择URL或者IP。
  - 探测目标：HTTP(S)填写格式为localhost:port/path；TELNET填写格式为127.0.0.1:port。比如要探测tomcat是否响应正常，选择HTTP(S)后填写localhost:8080/monitor；要探测mysql的连通性，选择TELNET后填写127.0.0.1:3306。
- 报警配置区域：

  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：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：
    - 通道沉默时间：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：报警规则的生效时间，报警规则只在生效时间内发送报警通知，非生效时间内产生的报警只记录报警历史。

5.4 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。

6 日志监控

6.1 日志监控概览

应用场景

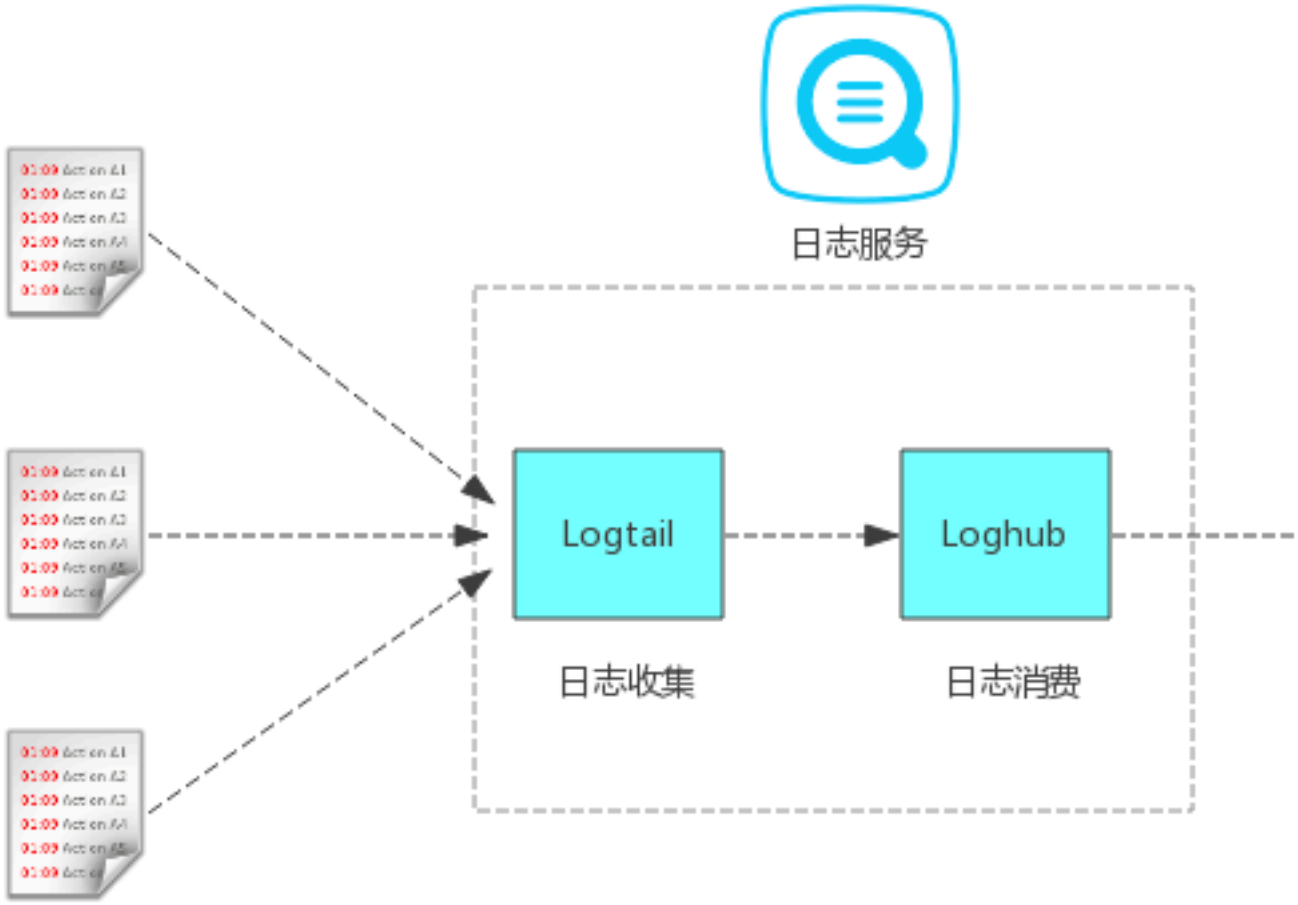
在企业级的业务运维和运营场景中， 日志正扮演着越来越重要的角色。业务日志的简单本地化存储，很难挖掘日志背后真正的数据价值。将日志存储到集中的服务端后，将其处理成指导运维、指导运营的指标，成为企业日益迫切的需求。

日志监控提供对日志数据实时分析，监控图表可视化展示和报警服务。您只需要开通日志服务，将本地日志通过日志服务进行收集，即可解决企业的监控运维与运营诉求。此外，还可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。

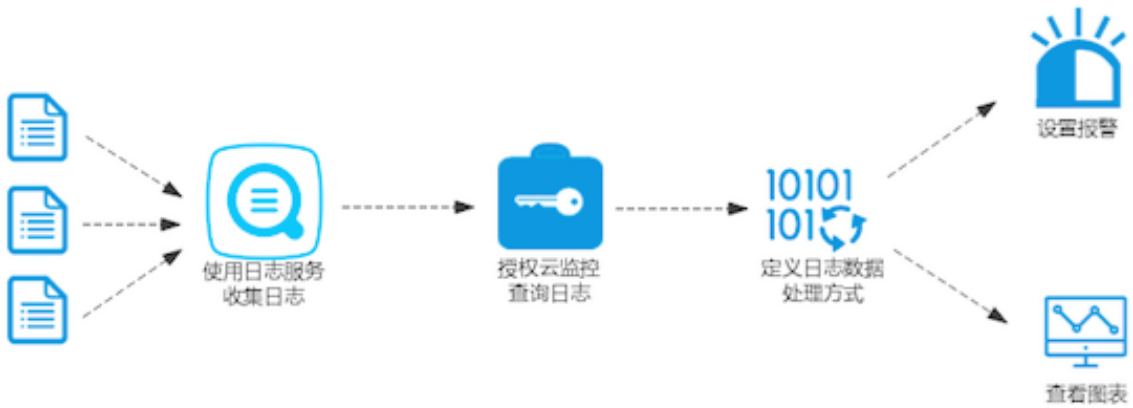
日志监控解决方案

通过将云监控与日志服务结合， 推出了非常轻量级，但全面、易用的解决方案——日志监控。

- 简单、易用，相比传统ELK方案，零编码即可享有完整监控解决方案。
- 提供日志数据实时分析、监控图表展示、报警服务的全套解决方案。
- 基于阿里云Apsara Monitor服务，提供稳定可靠的日志监控体验。
- 全SaaS服务，几乎无时间成本、人力成本和运维成本，让您快速拥有企业级业务日志实时监控能力。



业务流程概览



1. **通过日志服务收集日志。**
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）。**

6.2 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。

说明:

本功能为收费功能，需要付费后才能使用。

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的请求数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

1. 登录云监控控制台。
2. 点击左侧导航栏中的日志监控，进入日志监控页面。
3. 点击页面右上角的新建日志监控，进入新建日志监控页面。
4. 选择关联资源。
5. 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。
6. （可选）快速创建报警规则，默认发送邮件。
7. （可选）将监控项添加到某个应用分组中管理。

查看日志监控项

1. 登录云监控控制台。
2. 点击左侧导航栏中的日志监控，进入日志监控页面。
3. 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。

修改日志监控项

1. 登录云监控控制台。
2. 点击左侧导航栏中的日志监控，进入日志监控页面。
3. 选择需要修改的监控项名称，点击 编辑 按钮，进入编辑页面。
4. 参考创建日志监控步骤，对需要修改的参数进行修改。

删除日志监控项

说明:

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。

1. 登录云监控控制台。

2. 点击左侧导航栏中的日志监控，进入日志监控页面。
3. 选择需要删除的监控项名称，点击删除按钮，将指定监控项删除。

6.3 查看监控数据

定义好日志监控的监控项后，云监控提供2种查看监控数据方式：

- 在日志监控的监控项图表页直接查看。
- 在 Dashboard 中添加日志监控的图表。

在日志监控的监控项图表页直接查看

1. 登录云监控控制台。
2. 单击左侧导航栏中的日志监控，进入日志监控页面。
3. 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。

在 Dashboard 中添加日志监控的图表

1. 登录云监控控制台。
2. 单击左侧导航栏中的Dashboard，进入当前监控大盘页面。
3. 在页面右上角，单击添加图表按钮，进入添加图表页面。
4. 选择图表类型，选择监控项为日志监控，然后选择日志监控的相关信息后，单击发布，即可完成监控图表的添加。

6.4 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。
2. 点击左侧导航栏中的日志监控，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”。
3. 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权限** `AliyunCloudMonitorFullAccess` **和日志服务的只读权限** `AliyunRAMFullAccess`**。**
  - **查询日志监控数据：只需要授权云监控只读权限** `AliyunCloudMonitorReadOnlyAccess` **即可。**

7 云服务监控

7.1 云数据库RDS监控

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。在您购买RDS产品后，云监控会自动对上述监控项收集数据，无需其他操作。

说明:

- 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	数据库实例中IOPS的使用百分率	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

监控项	含义	维度	单位	最小监控粒度
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	bit/s	5分钟
网络出流量	实例每秒钟的输出流量	实例	bit/s	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	-	-	-

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

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的云数据库 RDS，进入云数据库RDS监控列表页面。
3. 单击实例名称或操作中的监控图表，进入监控图表页面。
4. (可选)单击大小图切换按钮，切换大图显示。

报警服务

- 设置报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的云数据库 RDS，进入云数据库RDS监控列表页面。
3. 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。
4. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明
  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的RDS CPU使用率大于80%报警，则只要用户名下有RDS CPU使用率大于80%，就会发

送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.2 负载均衡监控

云监控通过监控Sever Load Balancer的流入流量、流出流量等多个监控项，为您展示Sever Load Balancer的运行状态，帮助您监测实例的运行状态，并支持对监控项设置报警规则。当您创建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

- 四层协议监控项

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 状态的数量	端口	Count	1分钟
端口活跃连接数	当时所有 ESTABLISHED 状态的连接	端口	Count	1分钟

监控项	含义	维度	单位	最小监控粒度
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

监控项	含义	维度	单位	最小监控粒度
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	监听端口维度的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

监控项	含义	维度	单位	最小监控粒度
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 5xx 状态码个数	端口维度的rs返回给client的5xx状态码统计	端口	Count/Second	1分钟
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

监控项	含义	维度	单位	最小监控粒度
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

说明:

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

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的负载均衡，进入负载均衡监控列表页面。
3. 在列表上方，选择地域，列表中会显示您在该地域下所有的实例。
4. 单击实例名称或操作中的监控图表，进入监控图表页面，查看相关监控数据。
5. 单击大小图切换按钮，切换大图显示(可选)。

报警服务

- 设置报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的负载均衡，进入负载均衡监控列表页面。
3. 在列表上方，选择地域，列表中会显示您在该地域下所有的实例。
4. 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。
5. 单击右上角的新建报警规则，按照上述参数说明进行报警规则配置后，点击确认按钮即可。报警规则参数相关说明，请参见报警规则参数说明。

7.3 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，请参见OSS监控指标参考手册。

> 说明:
> 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，说明如下：
> - 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。
>
> 例如，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

说明:

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。

7.4 CDN监控

云监控通过监控CDN的QPS、BPS、字节命中率等监控项，帮助您获取域名的使用情况。当您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，以便在数据异常时收到报警信息。

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	时间粒度内的总访问次数/时间粒度	域名	次	1分钟
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

监控项	含义	维度	单位	最小监控粒度
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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的CDN，进入CDN域名监控列表页面。
  3. 单击页面上方的域名列表页签。
  4. 单击实例名称或操作中的监控图表，进入监控图表页面。
  5. (可选)单击放大图标，切换大图显示。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的CDN，进入CDN域名监控列表页面。
  3. 单击页面上方的域名列表页签。
  4. 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。
  5. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明
  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、域名。
    - 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。资源范围选择全部资源时，报警的资源最多1000个，超过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。
    - 域名：表示该规则只作用在某个具体域名上。
  - 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QPS1分钟平均值>=90个，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个。

    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50M。
  - 通道沉默时间：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。
  - 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%，连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
  - 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。
  - 报警级别：
    - 电话+短信+邮件+钉钉机器人
    - 短信+邮件+钉钉机器人
    - 邮件+钉钉机器人
  - 邮件主题：默认为产品名称+监控项名称+实例ID。

- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.5 弹性公网IP监控

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、流入数据包数等监控项，帮助您监测服务的运行状态，并支持您对监控项设置报警规则。在您购买弹性公网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	bit/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	bit/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
限速丢包速率	由于实际业务带宽使用超过设置的带宽峰值导致的数据包被丢弃的速率。	实例	pps	1分钟

· 查看监控数据

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的弹性公网IP，进入弹性公网IP监控列表页面。
3. 单击实例名称或操作中的监控图表，进入监控图表页面。
4. (可选)单击大小图切换图标，切换大图显示。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的弹性公网IP，进入弹性公网IP监控列表页面。
  3. 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。
  4. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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。例如规则描述为网络入流量5分钟平均值>=100Mbytes，则报警服务会5分钟检查一次5分钟内的数据是否满足平均值>=100Mbytes。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.6 云数据库Memcache版监控

云监控通过监控云数据库Memcache版服务实例的已用缓存、读取命中率等监控项，帮助您监测实例的运行状态，并支持您对监控项设置报警规则。在您购买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

说明:

- 监控数据最多保存31天。
- 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。
  2. 单击左侧导航栏中云服务监控下的新版云数据库 Memcache版，进入新版Memcache列表页面。
  3. 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。
  4. 单击页面上方的时间范围快速选择按钮或精确选择功能。
  5. （可选）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，您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。

- 设置单条报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的新版云数据库 Memcache 版，进入新版Memcache列表页面。
  3. 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。
  4. 单击监控图右上角的铃铛图标，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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的新版云数据库 Memcache 版，进入新版Memcache列表页面。
  3. 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。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.7 云数据库Redis版监控

云监控通过监控云数据库Redis版的已用容量百分比、已用连接数百分比等监控项，帮助您获取Redis的运行状态和使用情况。在您创建Redis实例后，云监控自动开始对其进行监控，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	-	-	-

监控项	含义	维度	单位	最小监控粒度
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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的云数据库Redis版，进入云数据库Redis版监控列表页面。
  3. 单击实例名称或操作中的监控图表，进入监控图表页面。
  4. (可选)单击大小图切换按钮，切换大图显示。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的云数据库Redis版，进入云数据库Redis版监控列表页面。
  3. 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。
  4. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.8 云数据库MongoDB版监控

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，帮助您监测实例的运行状态，并支持您对监控项设置报警规则。在您购买MongoDB服务后，云监控会自动对上述监控项收集数据。

监控服务

· 监控项说明

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

监控项	含义	维度	单位	最小监控粒度
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实例最近一次启动到现在累计接收到的insert命令的次数	用户维度、实例维度、主备维度	个数	5分钟
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

监控项	含义	维度	单位	最小监控粒度
实例故障	事件类型指标，可设置报警规则	-	-	-

说明:

- 监控数据最多保存31天。
- 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。
2. 单击左侧导航栏中云服务监控下的云数据库MongoDB版，进入MongoDB监控列表页面。
3. 单击实例名称或操作中的监控图表即可进入实例监控图表页面，查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围图标，监控数据最长支持查看连续14 天的监控数据。
5. （可选）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

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的云数据库MongoDB版，进入MongoDB监控列表页面。
3. 单击实例名称或操作中的监控图表，进入实例的监控图表页面。
4. 单击监控图右上角的铃铛图标，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

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的云数据库MongoDB版，进入MongoDB监控列表页面。
3. 选中所需实例后，单击列表下方的设置报警规则按钮，即可批量添加报警规则。

· 参数说明

- 产品：例如云服务器ECS、RDS、OSS 等。
- 资源范围：报警规则的作用范围，分为全部资源、实例。
  - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.9 消息服务监控

云监控通过监控Message Service的延迟消息、无效消息、活跃消息等监控项，帮助您获取Message Service队列的使用情况。在您创建Message Service的消息队列后，云监控自动开始对其进行监控，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。

监控服务

· 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	5分钟
InactiveMessages	在该Queue中处于Inactive状态的消息总数	userId,region,bid,queue	个	5分钟
DelayMessage	在该Queue中处于Delayed状态的消息总数	userId,region,bid,queue	个	5分钟
SendMessageCount	发送消息请求量	userId,region,queue	个	60分钟
BatchSendMessageCount	批量发送消息请求量	userId,region,queue	个	60分钟
ReceiveMessageCount	接收消息请求量	userId,region,queue	个	60分钟
BatchReceiveMessageCount	批量接收消息请求量	userId,region,queue	个	60分钟
BatchDeleteMessageCount	批量删除消息请求量	userId,region,queue	个	60分钟
ChangeMessageVisibilityCount	更改消息可见性计数	userId,region,queue	个	60分钟

- 查看监控数据

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的消息服务，进入消息服务监控列表页面。
  3. 单击队列名称或操作中的监控图表，进入监控图表页面。
  4. （可选）单击大小图切换按钮，切换大图显示。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的消息服务，进入消息服务监控列表页面。
  3. 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。
  4. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、queue维度。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - queue维度：表示该规则只作用在某个具体消息队列上。

- 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。例如规则描述为延迟消息5分钟平均值>=10个，则报警服务会5分钟检查一次5分钟内的数据是否满足平均值>=10个。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.10 分析型数据库监控

云监控通过提供Analytic DB的磁盘额定容量、磁盘已用容量、磁盘使用率等监控信息，帮助您获取Analytic DB服务的使用情况。在您开通Analytic DB服务后，云监控自动开始对其进行监控。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

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的分析型数据库，进入分析数据库监控列表页面。
3. 单击实例名称或操作中的监控图表，进入监控图表页面。
4. (可选)单击大小图切换按钮，切换大图显示。

报警服务

- 设置报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的分析型数据库，进入分析数据库监控列表页面。
3. 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。
4. 单击右上角的创建报警规则，选择资源范围，根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明
  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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。

  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50M。

- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人

- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.11 日志服务监控

云监控通过监控日志服务的出入流量、总体QPS、日志统计方法等监控项，帮助您获取日志服务的使用情况。在您创建日志服务后，云监控自动开始对其进行监控。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。

监控服务

- 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

监控项	含义	维度	单位	最小监控粒度
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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的日志服务，进入日志服务监控列表页面。
  3. 单击列表操作中的监控图表，进入监控图表页面。
  4. （可选）单击大小图切换按钮，切换大图显示。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的日志服务，进入日志服务监控列表页面。
  3. 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。
  4. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  说明:

  - 设置报警规则时，服务状态指标中可指定具体的状态，status字段包括：200 、400 、401 、403 、405 、500 、502。

- 操作次数指标中可选择具体的方法，method字段包括：PostLogStoreLogs 、GetLogtailConfig 、 PutData、 GetCursorOrData、 GetData 、GetLogStoreHistogram 、GetLogStoreLogs、 ListLogStores、 ListLogStoreTopics。

- 产品：例如云服务器ECS、RDS、OSS 等。
- 资源范围：报警规则的作用范围，分为全部资源、project维度。
  - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - project维度：表示该规则只作用在具体project上。

- 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。例如规则描述为总体QPS1分钟采样计数值>=70个，则报警服务会1分钟检查一次1分钟内的数据是否满足采样计数值>=70个。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.12 容器服务监控

云监控通过监控容器服务的 CPU 使用率、内存使用率等监控项，帮助您获取容器服务的使用情况。在您创建容器服务后，云监控自动开始对其监控。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

说明:

- 监控数据最多保存31天。
- 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。
  2. 单击左侧导航栏中云服务监控下的容器服务，进入容器服务集群列表页面。
  3. 单击操作中的监控图表即可进入实例监控图表页面，查看各项指标。
  4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续 14 天的监控数据。
  5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的容器服务，进入容器服务集群列表页面。
  3. 单击操作中的监控图表，即可进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的容器服务，进入容器服务集群列表页面。
  3. 选中所需实例后，单击列表下方的批量设置报警，即可对所选实例批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、资源维度。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 资源维度：表示该规则只作用在指定资源上。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.13 共享带宽

云监控通过监控共享带宽的网络出入带宽等监控项，帮助您监测共享带宽的网络使用情况，并支持您对监控项设置报警规则。在您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

- 监控项说明

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	bit/s	1分钟
带宽包网络流出带宽	用户维度、实例维度	bit/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

说明:

- 监控数据最多保存 31 天。
- 最多可连续查看 7 天的监控数据。

- 查看监控数据

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的共享带宽，进入共享带宽页面。
3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面，查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续7天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的共享带宽，进入共享带宽页面。
  3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的共享带宽，进入共享带宽页面。
  3. 选中所需实例后，单击列表下方的设置报警规则，即可对所选实例批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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。例如规则描述为流入带宽1分钟监控值>=10Mbit/s，则报警服务会1分钟检查一次1分钟内的数据是否满足监控值>=10Mbit/s。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.14 全球加速

云监控通过监控全球加速的网络出入带宽等监控项，帮助您监测全球加速的网络使用情况，并支持您对监控项设置报警规则。在您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

· 监控项说明

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	bit/s	1分钟
网络流出带宽	用户维度、实例维度	bit/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

说明:

- 监控数据最多保存 31 天。
- 最多可连续查看 7 天的监控数据。

· 查看监控数据

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的全球加速，进入全球加速页面。
3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面，查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续7天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的全球加速，进入全球加速页面。
  3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的全球加速，进入全球加速页面。
  3. 选中所需实例后，单击列表下方的设置报警规则，即可对所选实例批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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。例如规则描述为流入带宽1分钟监控值>=10Mbit/s，则报警服务会1分钟检查一次1分钟内的数据是否满足监控值>=10Mbit/s。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.15 时序时空数据库 TSDB

云监控通过监控时序时空数据库 TSDB的磁盘使用率、时间线数量、时间点增量等监控项，帮助您监测TSDB使用情况，并支持您对监控项设置报警规则。在您购买TSDB后，云监控会自动对TSDB的监控项收集数据。

监控服务

- 监控项说明

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
时间点增量	用户维度、实例维度	%	20秒

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的TSDB，进入TSDB页面。
3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面，查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的TSDB，进入TSDB页面。
  3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的TSDB，进入TSDB页面。
  3. 选中所需实例后，单击列表下方的设置报警规则，即可对所选实例批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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。例如规则描述为磁盘使用率1分钟监控值>=30%，则报警服务会1分钟检查一次1分钟内的数据是否满足监控值>=30%。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.16 VPN网关

云监控通过监控VPN网关的网络出入带宽等监控项，帮助您监测VPN网关的网络使用情况，并支持您对监控项设置报警规则。在您购买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

- 监控项说明

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	bit/s	1分钟
带宽包网络流出带宽	用户维度、实例维度	bit/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

说明:

- 监控数据最多保存 31 天。
- 最多可连续查看 7 天的监控数据。

- 查看监控数据

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的VPN网关，进入VPN网关页面。
3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续7天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的VPN网关，进入VPN网关页面。
  3. 单击实例名称或操作中的监控图表即可进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的VPN网关，进入VPN网关页面。
  3. 选中所需实例后，单击列表下方的设置报警规则，即可对所选实例批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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。例如规则描述为流入带宽1分钟监控值>=1Mbit/s，则报警服务会1分钟检查一次1分钟内的数据是否满足监控值>=1Mbit/s。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.17 API网关监控

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，帮助您获取API网关服务的使用情况。在您开通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信息。

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	Byte	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	Byte	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

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的API网关，进入API网关监控列表页面。
3. 单击实例名称或操作中的监控图表，进入监控图表页面，查看各项指标。
4. (可选)单击大小图切换按钮，切换大图显示。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的API网关，进入API网关监控列表页面。
  3. 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。
  4. 单击右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、API维度。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - API维度：表示该规则只作用在某个具体API上。

- 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。例如规则描述为流入带宽1分钟总计>=1024KBytes，则报警服务会1分钟检查一次1分钟内的数据是否满足总计>=1024KBytes。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.18 DDoS高防IP

云监控通过DDoS高防IP的流出带宽监控项，帮助您监测DDoS高防IP的使用情况，并支持对监控项设置报警规则。当您购买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

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

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的DDoS高防IP，进入DDoS高防IP页面。
3. 单击实例名称或操作中的监控图表即可进入实例监控图表页面，查看各项指标。
4. 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。
5. 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
  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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。例如规则描述为高防IP入流量1分钟只要有一次>=2Mbit/s，则报警服务会每分钟检查一次1分钟内的高防IP入流量是否>=2Mbit/s。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

· 设置单条报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的DDoS高防IP，进入DDoS高防IP页面。
3. 单击实例名称或操作中的监控图表即可进入实例监控图表页面。
4. 单击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。

7.19 邮件推送监控

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。帮助您实时监控邮件推送服务的服务状态，并支持您对监控项设置报警规则。在您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

· 监控项说明

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

说明:

- 监控数据最多保存 31 天。
- 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。
  2. 单击左侧导航栏中云服务监控下的邮件推送，进入邮件推送页面，您可以查看邮件推送服务的监控信息。

报警服务

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

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的邮件推送，进入邮件推送页面。
  3. 单击报警规则页签，进入报警规则列表页后，单击页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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SMTP认证失败QPS1分钟监控值>=10Count/min，则报警服务会1分钟检查一次1分钟内的数据是否满足监控值>=10Count/min。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.20 Elasticsearch监控

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，帮助您监测Elasticsearch服务的使用情况，并支持您对监控项设置报警规则。在您购买Elasticsearch后，云监控会自动对上述监控项收集数据。

监控服务

- 监控项说明

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
节点FullGc次数	节点维度	Count	1分钟
节点Exception次数	节点维度	Count	1分钟
集群快照状态	集群维度	-1代表没有快照； 0代表成功； 1代表进行中； 2代表失败	1分钟

说明:

- 监控数据最多保存 31 天。
- 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。
  2. 单击左侧导航栏中云服务监控下的Elasticsearch，进入Elasticsearch监控列表页面。
  3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面，查看各项指标。
  4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
  5. （可选）单击监控图右上角的放大按钮，可查看监控大图。

报警服务

- 设置报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的Elasticsearch，进入Elasticsearch监控列表页面。
  3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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。例如规则描述为节点CPU使用率1分钟平均值>=50%，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>=50%。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.21 弹性伸缩

云监控通过监控弹性伸缩组的最小实例数、最大实例数等监控项，帮助您监测伸缩组的实例状态，并支持您对监控项设置报警规则。在您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

- 监控项说明

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

说明:

- 监控数据最多保存31天。
- 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。
  2. 单击左侧导航栏中云服务监控下的弹性伸缩，进入弹性伸缩监控列表页面。
  3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面，查看各项指标。
  4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
  5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的弹性伸缩，进入弹性伸缩监控列表页面。
  3. 单击伸缩组名称或操作中的监控图表，即可进入该伸缩组监控图表页面。
  4. 单击监控图右上角的铃铛按钮或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的弹性伸缩，进入弹性伸缩监控列表页面。
  3. 选中所需伸缩组后，单击列表下方的设置报警规则，即可对所选伸缩组批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、伸缩组。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 伸缩组：表示该规则只作用在某个具体伸缩组上。

- 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。例如规则描述为最大实例数5分钟平均值>=10个，则报警服务会5分钟检查一次5分钟内的数据是否满足平均值>=10个。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.22 E-MapReduce监控

云监控通过监控 E-MapReduce 集群的 CPU 空闲率、内存容量、磁盘容量等监控项，帮助您监测集群的运行状态，并支持您对监控项设置报警规则。在您购买 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

- 监控项说明

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	bit/s	30s
网络流出速率	用户维度、集群维度、角色维度	bit/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	Byte	30s
磁盘总容量	用户维度、集群维度、角色维度	Byte	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	Byte	30s
总内存容量	用户维度、集群维度、角色维度	Byte	30s
数据包流入速率	用户维度、集群维度、角色维度	个/秒	30s

监控项	维度	单位	最小监控粒度
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、角色维度	个	30s
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	Byte	30s
MemNonHeapCommittedM	用户维度、集群维度、角色维度	Byte	30s
MemNonHeapMaxM	用户维度、集群维度、角色维度	Byte	30s
MemHeapUsedM	用户维度、集群维度、角色维度	Byte	30s
MemHeapCommittedM	用户维度、集群维度、角色维度	Byte	30s
MemHeapMaxM	用户维度、集群维度、角色维度	Byte	30s
MemMaxM	用户维度、集群维度、角色维度	Byte	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

监控项	维度	单位	最小监控粒度
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
ReceivedByte	用户维度、集群维度、角色维度	-	30s
SentByte	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

监控项	维度	单位	最小监控粒度
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、角色维度	-	30s
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
ByteRead	用户维度、集群维度、角色维度	-	30s
ByteWritten	用户维度、集群维度、角色维度	-	30s

监控项	维度	单位	最小监控粒度
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
ReplaceBlockOpAvgTime	用户维度、集群维度、角色维度	ms	30s
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

监控项	维度	单位	最小监控粒度
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

监控项	维度	单位	最小监控粒度
AvailableMB	用户维度、集群维度、角色维度	-	30s
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

说明:

- 监控数据最多保存31天。
- 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。
2. 单击左侧导航栏中云服务监控下的E-MapReduce，进入E-MapReduce监控列表页面。
3. 单击集群ID或操作中的监控图表，进入监控图表页面，可查看各项监控指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）单击监控图右上角的放大按钮，可查看监控大图。

报警服务

· 设置报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的E-MapReduce，进入E-MapReduce监控列表页面。
3. 单击集群ID或操作中的监控图表，进入监控图表页面。
4. 单击监控图右上角的铃铛图标或右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

· 参数说明

- 产品：例如云服务器ECS、RDS、OSS 等。
- 资源范围：报警规则的作用范围，分为全部资源、集群。
  - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率

大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 集群：表示该规则只作用在某个具体集群上。

- 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空闲率5分钟平均值>=10%，则报警服务会5分钟检查一次5分钟内的数据是否满足平均值>=10%。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.23 高速通道

云监控通过监控高速通道实例的网络流入流量、网络流出流量等监控项，帮助您监测高速通道服务的网络使用情况，并支持您对监控项设置报警规则。在您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

- 监控项说明

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	Byte	1分钟
网络流出流量	用户维度、实例维度	Byte	1分钟
网络流入带宽	用户维度、实例维度	bit/s	1分钟
网络流出带宽	用户维度、实例维度	bit/s	1分钟
时延	用户维度、实例维度	ms	1分钟
丢包率	用户维度、实例维度	%	1分钟

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的高速通道，进入高速通道监控列表页面。
3. 单击实例名称或操作中的监控图表，即可进入实例监控图表页面，查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的高速通道，进入高速通道监控列表页面。
  3. 单击实例名称或操作中的监控图表，进入实例监控图表页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的高速通道，进入高速通道监控列表页面。
  3. 选择所需实例后，单击列表下方的设置报警规则按钮，即可对所选实例批量设置报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、对象Id。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 对象Id：表示该规则只作用在某个具体对象Id上。

- 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。例如规则描述为流入带宽5分钟监控值>=100Mbits/s，则报警服务会5分钟检查一次5分钟内的数据是否满足监控值>=100Mbits/s。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.24 函数计算监控

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，帮助您实时监控函数计算服务的服务状态，并支持您对监控项设置报警规则。在您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

- 监控项说明

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

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的函数计算，进入函数计算监控页面，您可以查看函数计算服务的整体监控概况。
3. 单击 Service列表页签，可以查看Service或Function级别的监控信息。

报警服务

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

· 设置单条报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的函数计算，进入函数计算监控页面。
3. 单击报警规则页签，进入报警规则列表页，单击右上角的创建报警规则按钮，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

· 设置批量报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中云服务监控下的函数计算，进入函数计算监控页面。
3. 单击Service列表页签。
4. 在Service列表中选择所需服务后，单击列表下方的设置报警规则按钮，即可对所选服务批量设置报警规则。

· 参数说明

- 产品：例如云服务器ECS、RDS、OSS 等。
- 资源范围：报警规则的作用范围，分为全部资源、Service。
  - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - Service：表示该规则只作用在Service维度。

- 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。例如规则描述为最大内存使用1分钟监控值>=1024MBytes，则报警服务会1分钟检查一次1分钟内的数据是否满足监控值>=1024MBytes。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.25 流计算

云监控通过监控流计算的业务延迟等监控项，帮助您监测流计算服务的业务运行情况，并支持您对监控项设置报警规则。在您购买流计算服务后，云监控会自动对上述监控项收集数据。

监控服务

- 监控项说明

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

说明:

- 监控数据最多保存31天。
- 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。
2. 单击左侧导航栏中云服务监控下的流计算，进入Project列表页面。
3. 单击实例名称或操作中的监控图表，进入实例监控详情页面，查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的流计算，进入Project列表页面。
  3. 单击实例名称或操作中的监控图表，进入实例监控详情页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的流计算，进入Project列表页面。
  3. 选择所需实例后，单击列表下方的设置报警规则按钮，即可对所选实例批量设置报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.26 云数据库HybridDB for PostgreSQL

云监控通过监控 HybridDB for PostgreSQL 的 CPU 使用率、内存使用率等监控项，帮助您监测 HybridDB for PostgreSQL 实例的使用情况，并支持您对监控项设置报警规则。在您购买 HybridDB for PostgreSQL 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	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

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的 HybridDB for PostgreSQL，进入HybridDB监控列表页面。
3. 单击实例ID或操作中的监控图表，进入实例监控详情页面，可查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续 14 天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的 HybridDB for PostgreSQL，进入HybridDB监控列表页面。
  3. 单击实例ID或操作中的监控图表，进入实例监控详情页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的 HybridDB for PostgreSQL，进入HybridDB监控列表页面。
  3. 选择所需实例后，单击列表下方的设置报警规则按钮，即可对所选实例批量设置报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、集群名称。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 集群名称：表示该规则只作用在某个具体集群上。例如设置了集群粒度的CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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5分钟平均值>=90%，则报警服务会5分钟检查一次5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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.27 NAT网关监控

云监控通过监控NAT网关的SNAT连接数等监控项，帮助您监测NAT网关服务的网络使用情况，并支持您对监控项设置报警规则。在您购买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

· 监控项说明

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	bit/s	1分钟
带宽包网络流出带宽	用户维度、实例维度	bit/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

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的NAT网关，进入NAT网关列表页面。
3. 单击实例名称或操作中的监控图表，进入实例监控详情页面，可查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的NAT网关，进入NAT网关列表页面。
  3. 单击实例名称或操作中的监控图表，进入实例监控详情页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择资源范围、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的NAT网关，进入NAT网关列表页面。
  3. 选择所需实例后，单击列表下方的设置报警规则按钮，即可对所选实例批量设置报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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SNAT连接数1分钟只要有一次>=100Count/min，则报警服务会1分钟检查一次1分钟内的数据是否满足只要有一次>=100Count/min。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.28 营销引擎监控

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 等监控指标，帮助您实时了解营销引擎服务的服务状态，并支持您对监控项设置报警规则。在您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

- 监控项说明

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 有效人群请求量	用户维度	次/天	1小时

说明:

- 监控数据最多保存 31 天。
- 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。
  2. 单击左侧导航栏中云服务监控下的营销引擎，进入营销引擎页面，您可以查看营销引擎服务的整体监控概况。
  3. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续 14 天的监控数据。
  4. （可选）单击监控图右上角的放大按钮，可查看监控大图。

报警服务

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

设置报警规则

- 方法一

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的营销引擎，进入营销引擎页面。
  3. 单击监控图右上角的铃铛图标，进入创建报警规则页面，选择关联资源、根据参数设置报警规则，选择通知方式，单击确认即可。

- 方法二

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的营销引擎，进入营销引擎页面。
  3. 单击报警规则页签。
  4. 在报警规则列表页，单击右上角的创建报警规则，选择关联资源、根据参数设置报警规则，选择通知方式，单击确认即可。

参数说明

- 产品：例如云服务器ECS、RDS、OSS 等。
- 资源范围：报警规则的作用范围，分为全部资源、实例。
  - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80% ，就会发送报警通知。

- 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（DSP）RTB竞价PV1分钟总计>=100个，则报警服务会1分钟检查一次1分钟内的数据是否满足1分钟总计>=100个。

  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50M 。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.29 阿里云OpenAPI监控

云监控通过监控阿里云OpenAPI的调用次数、错误次数、错误率等监控项，帮助您监测阿里云OpenAPI的使用情况，并支持您对监控项设置报警规则。在您使用阿里云OpenAPI后，云监控会自动对上述监控项收集数据。

监控服务

- 监控项说明

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	次	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	次	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

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的阿里云OpenAPI，进入阿里云OpenAPI页面。
3. 单击实例名称或操作中的监控图表，进入实例监控详情页面，可查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的阿里云OpenAPI，进入阿里云OpenAPI页面。
  3. 单击实例名称或操作中的监控图表，进入实例监控详情页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择关联资源、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的阿里云OpenAPI，进入阿里云OpenAPI页面。
  3. 选择所需实例后，单击列表下方的设置报警规则按钮，即可对所选实例批量设置报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、产品。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 产品：表示该规则只作用在某个具体产品上。

- 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。例如规则描述为调用次数1分钟平均值>=100次，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>=100次。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.30 开放搜索监控

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，帮助您监测开放搜索服务的使用情况，并支持您对监控项设置报警规则。在您购买开放搜索后，云监控会自动对上述监控项收集数据。

监控服务

- 监控项说明

监控项	维度	单位	最小监控粒度
存储容量	APP维度	Byte	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

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的开放搜索，进入开放搜索页面。
3. 单击应用名称或操作中的监控图表，进入监控详情页面，可查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的开放搜索，进入开放搜索页面。
  3. 单击应用名称或操作中的监控图表，进入监控详情页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择关联资源、根据参数设置报警规则，选择通知方式，单击确认即可。

- 设置批量报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的开放搜索，进入开放搜索页面。
  3. 选择所需应用，单击列表下方的设置报警规则按钮，即可对所选应用批量添加报警规则。

- 参数说明

  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、应用名。

    ■ 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

  - 应用名：表示该规则只作用在某个具体应用上。

- 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。例如规则描述为查询QPS5分钟只要有一次>=10次/秒，则报警服务会5分钟检查一次5分钟内的数据是否满足只要有一次>=10次/秒。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。
- 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。

7.31 云数据库HybridDB for MySQL

云监控通过监控云数据库 HybridDB for MySQL 实例的磁盘使用量、网络流入带宽、网络流出带宽等多个监控项，帮助您监测 HybridDB for MySQL 的实例状态，并支持您对监控项设置报警规则。在您购买云数据库 HybridDB for MySQL 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	维度	单位	最小监控粒度
磁盘使用量	用户维度、实例维度	GB	60分钟
网络流入带宽	用户维度、实例维度	KByte/Second	5分钟
网络流出带宽	用户维度、实例维度	KByte/Second	5分钟
每秒请求数	用户维度、实例维度	次/秒	5分钟
子节点CPU使用率	用户维度、实例维度	%	8分钟
子节点磁盘使用量	用户维度、实例维度	GB	8分钟
子节点IOPS	用户维度、实例维度	次/秒	8分钟

说明:

- 监控数据最多保存 31 天。
- 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。
2. 单击左侧导航栏中云服务监控下的HybridDB for MySQL，进入HybridDB for MySQL列表页面。
3. 单击实例名称或操作中的监控图表，进入实例监控详情页面，可查看各项指标。
4. 单击页面上方的时间范围快速选择按钮或自定义时间范围，监控数据最长支持查看连续14天的监控数据。
5. （可选）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
  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的HybridDB for MySQL，进入HybridDB for MySQL列表页面。
  3. 单击实例名称或操作中的监控图表，进入实例监控详情页面。
  4. 单击监控图右上角的铃铛图标或页面右上角的创建报警规则，选择关联资源，根据参数设置报警规则，选择通知方式，单击确认即可。
- 设置批量报警规则
  1. 登录云监控控制台。
  2. 单击左侧导航栏中云服务监控下的HybridDB for MySQL，进入HybridDB for MySQL列表页面。
  3. 选择所需实例后，单击列表下方的设置报警规则，即可对所选实例批量设置报警规则。
- 参数说明
  - 产品：例如云服务器ECS、RDS、OSS 等。
  - 资源范围：报警规则的作用范围，分为全部资源、实例。
    - 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。例如设置了全部资源粒度的MongoDB CPU使用率大于80%报警，则只要用户名下有MongoDB CPU使用率大于80%，就会发送报警通知。资源范围选择全部资源时，报警的资源最多1000个，超

过1000个可能会导致达到阈值不报警的问题，建议您使用应用分组按业务划分资源后再设置报警。

- 实例：表示该规则只作用在某个具体实例上。例如设置了实例粒度的主机 CPU 使用率大于80%报警，则只要这个实例 CPU使用率大于80%，就会发送报警通知。

- 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。例如规则描述为磁盘使用量60分钟平均值>=1GB，则报警服务会60分钟检查一次60分钟内的数据是否满足平均值>=1GB。

  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50M。
- 通道沉默时间：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。
- 连续几次超过阈值后报警：连续几次报警的探测结果符合您设置的规则描述，才会触发报警。例如规则描述为“CPU使用率 1分钟内平均值>80%,连续3次超过阈值后报警”，则连续出现3次 CPU使用率 1分钟内平均值>80%的情况，才会触发报警。
- 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。
- 报警级别：

  - 电话+短信+邮件+钉钉机器人
  - 短信+邮件+钉钉机器人
  - 邮件+钉钉机器人
- 邮件主题：默认为产品名称+监控项名称+实例ID。
- 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。

- **报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。**

8 访问控制

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。

 说明:

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

Action	含义
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

9 应用分组

9.1 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。

说明:

- 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。

9.2 创建应用分组

本文旨在为您介绍如何通过创建应用分组将业务相关的服务器、数据库等资源添加到应用分组中，在应用分组维度管理报警规则。

背景信息

随着互联网的发展，越来越多的企业用户购买使用各种阿里云产品，随之而来的是如何管理和监控各云产品资源的使用和运行情况。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。

创建应用分组的准备工作

创建应用分组支持动态模式和静态模式两种方式：

- 动态模式是指创建应用分组时，设置动态匹配实例名称的命名规则后，会自动将满足规则的实例添加到应用分组中。后续需要向应用分组移入或移出实例时，只需修改实例名称，无需再手动将实例移入或移出应用分组。目前动态模式支持云服务器ECS实例、云数据库RDS版实例和负载均衡实例。
- 静态模式是指创建应用分组时，手动将具体的实例加入到分组。

创建应用分组的实施步骤

注意事项

说明:

- 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。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。

3. 单击右上角的创建组，进入创建应用分组页面。

4. 填写基本信息：输入应用分组名称，选择联系人组（联系人组用于接收报警通知）。
5. 设置监控报警：选择报警模板（可选，用于对组内的实例初始化报警规则）和报警级别。启用初始化安装监控插件，系统将会对本组的服务器批量安装上监控插件，以便采集监控数据。
6. 设置事件监控： 勾选订阅事件通知后，分组内相关资源产生严重级别和警告级别事件时，将发送报警通知。
7. 设置动态添加实例：通过制定动态匹配规则自动添加ECS实例。支持根据ECS实例名称进行字段的“包含”、“前缀”、“后缀”匹配，符合匹配规则的实例会自动加入到当前应用分组中（包括以后创建的实例）。最多可以添加三条动态匹配规则，规则之间可以是“与”、“或”关系。点击添加产品，可继续制定云数据库RDS版和负载均衡的动态匹配规则。其他产品实例可在应用分组创建完成后进行添加。
8. 单击 创建应用分组按钮，即可完成应用分组的创建。

后续操作

以下介绍创建应用分组后的一些后续操作：

- 在应用分组中添加资源。
- 将报警模板应用到分组。

9.3 查看应用分组

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 ECS、 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。

说明:

- 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。

说明:

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。

> 说明:
> 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。
  - 正常状态：规则关联的资源全部正常。
  - 报警状态：规则关联的实例至少有一个实例正在报警。
  - 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”。
  - 修改：修改报警规则。
  - 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。
  - 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。
  - 删除：删除报警规则。
  - 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。

> 说明:
> 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。

> 说明:
> 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

产品类别	监控项	展现形式	备注
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

9.4 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。

说明:

- 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。

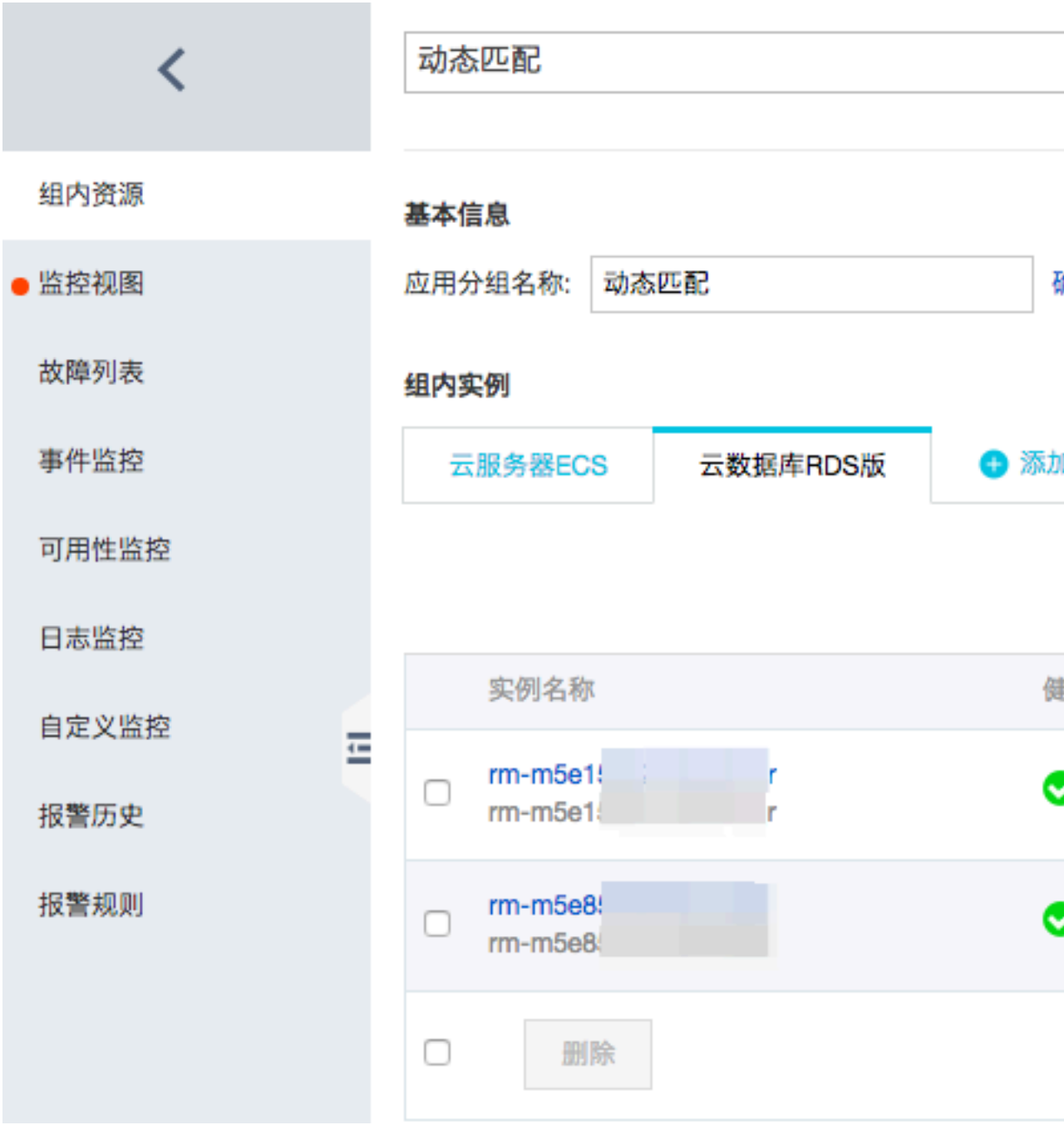
修改基本信息

进入应用分组详情页面后，鼠标悬浮于分组名称或联系人组信息上时，会出现编辑标志，点击后可直接修改并保存。

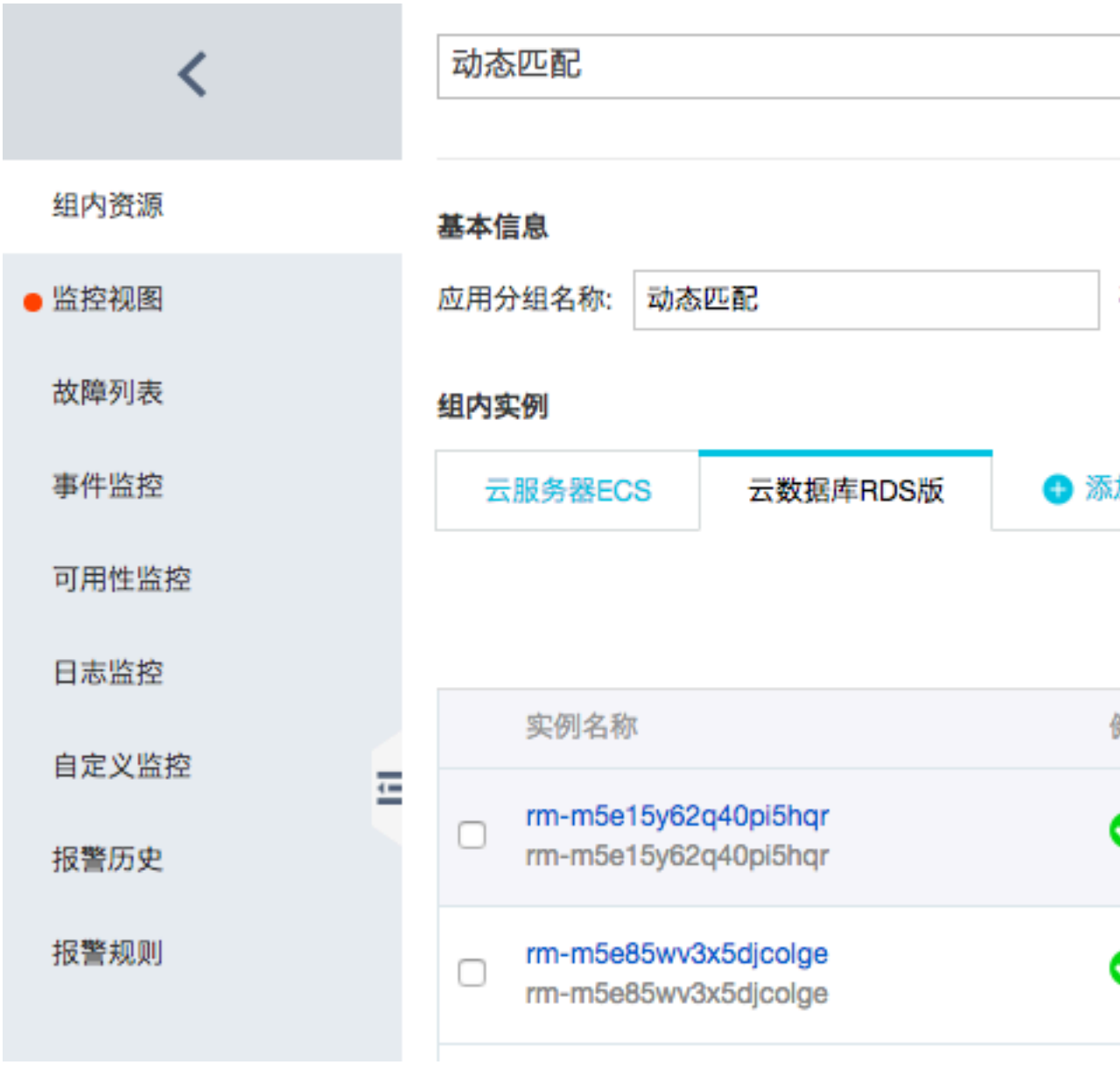

动态匹配
组内资源
监控视图
故障列表
事件监控
基本信息
应用分组名称: 动态匹配
组内实例
云服务器ECS
添加产品

增减组内实例

1. **删除实例：选择需要删除实例的产品，在操作中点击删除即可。**



2. 添加实例：选择需要添加实例的产品，点击右上角的添加实例按钮，进入页面勾选要添加的实例。



添加新产品

进入分组详情页后，点击添加产品后进入添加页面，选择需要添加的具体资源。

9.5 在应用分组中添加资源

本文为您介绍如何在应用分组中添加资源，以便在分组维度管理报警规则，查看监控数据。

背景信息

由于目前创建应用分组动态模式仅支持云服务器ECS实例、云数据库RDS版实例和负载均衡实例。除此之外的实例，需要您手动将具体的实例加入到分组。本文将为您介绍如何手动将实例加入到应用分组中。

在应用分组中添加资源的前提条件

- 准备需要添加到应用分组的实例。
- 已经创建应用分组，如还未创建应用分组请参考创建应用分组。

在应用分组中添加资源的实施步骤

注意事项

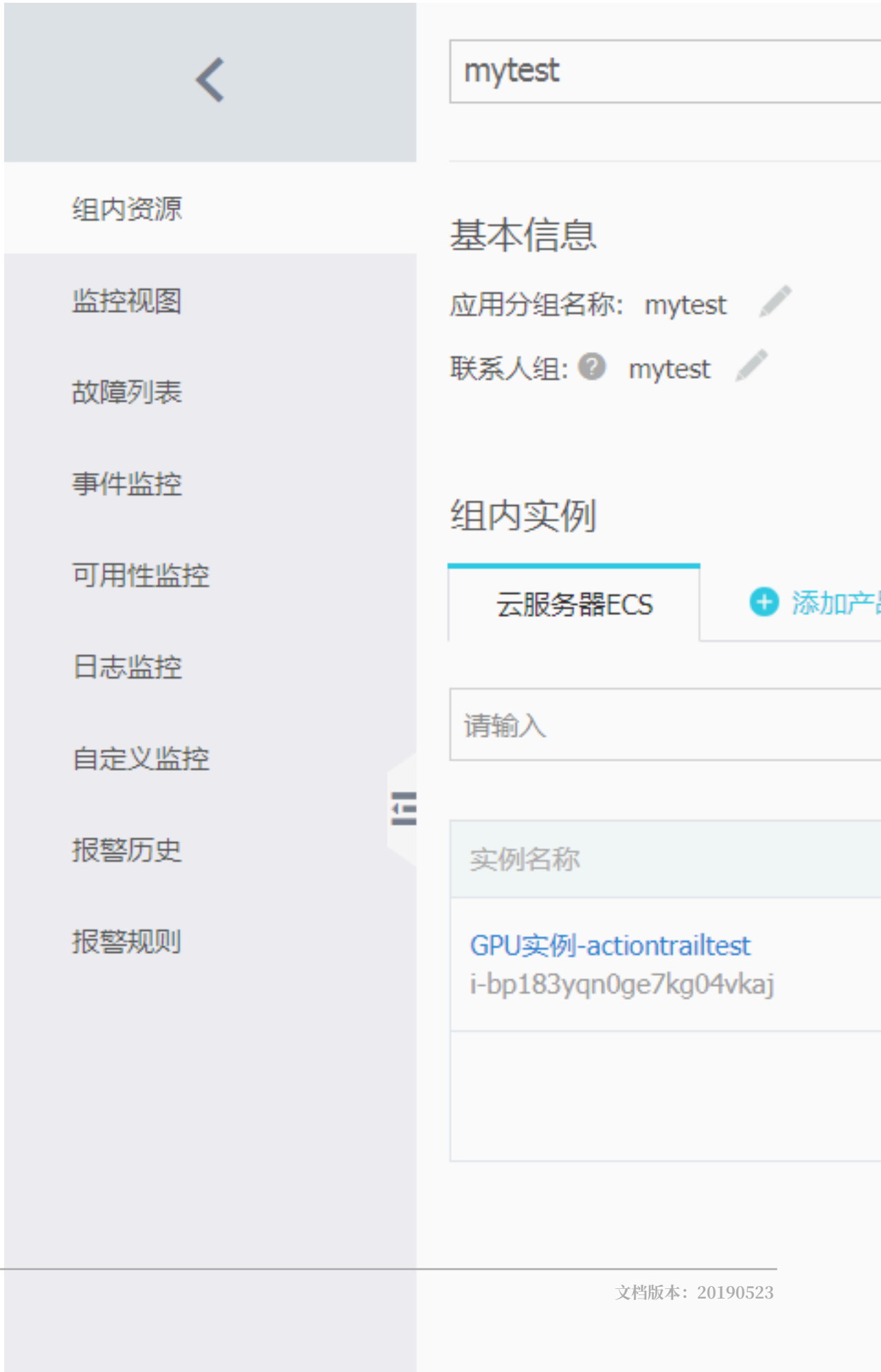
说明:

每个应用分组最多可添加1000个资源实例。

添加产品的操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择要添加资源的分组，单击分组名称，进入组内资源页面。

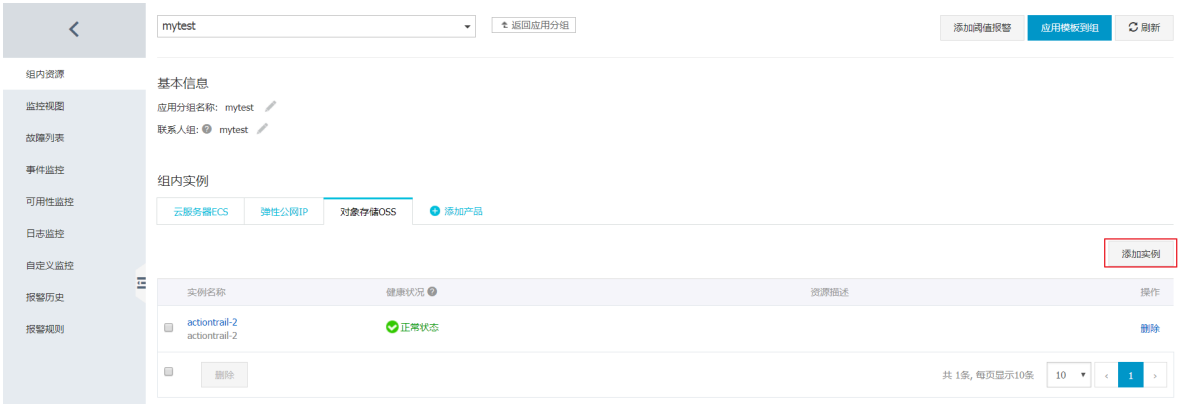
4. 单击添加产品，进入添加资源页面。



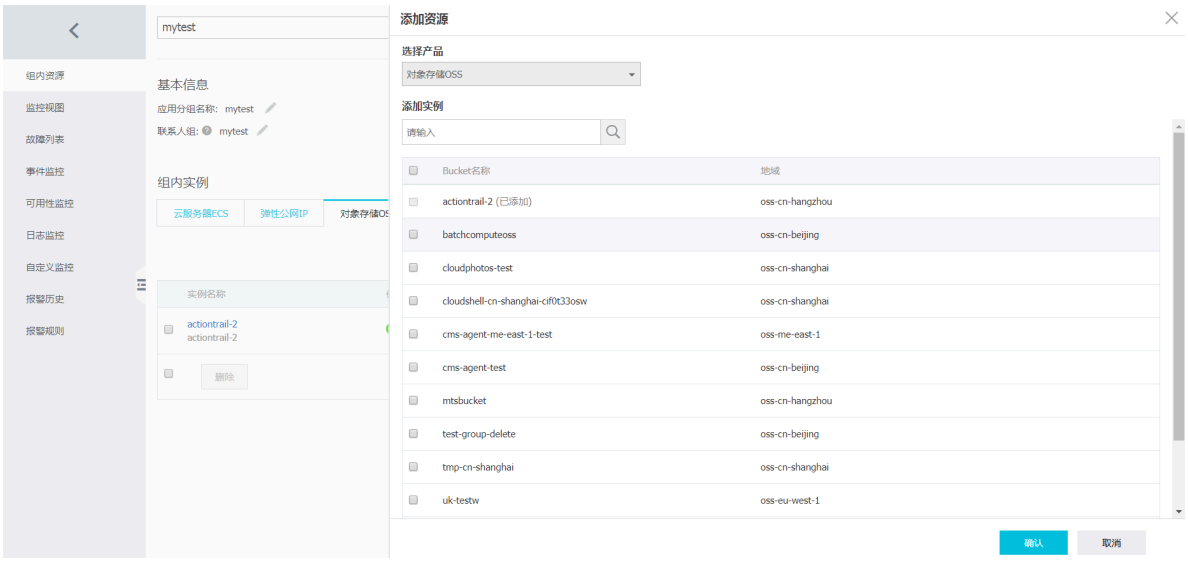
5. 在产品下拉列表中选择产品，然后在该产品的实例列表中选择要添加的实例，单击确认按钮即可。

添加实例的操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择要添加资源的分组，单击分组名称，进入组内资源页面。



4. 单击要添加实例的产品页签，例如对象存储OSS。
5. 单击添加实例按钮，进入添加资源页面。



6. 在实例列表中选择要添加的实例，然后单击确认按钮即可。

9.6 将报警模板应用到分组

本文为您介绍如何将报警模板应用到应用分组上，为业务模块快速创建好报警规则。

背景信息

如果您有大量云资源（ECS、RDS、SLB、OSS等），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，这样可极大简化报警规则的创建和维护过程。

报警模板需要与应用分组配合使用，您可以将报警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。

将模板应用到分组前的准备工作

将模板应用到分组需要先创建报警模板，如何创建报警模板请参见创建报警模板。

将模板应用到分组的实施步骤

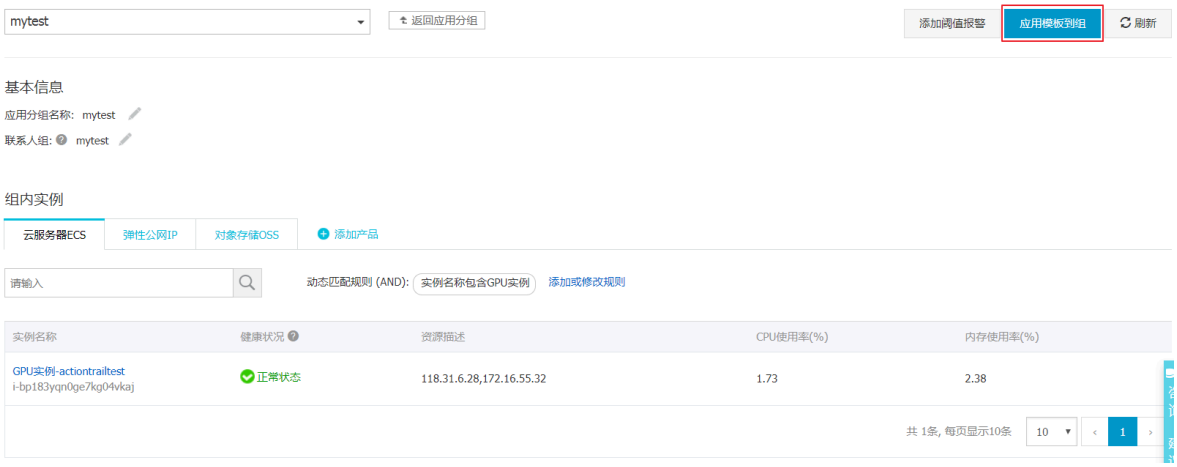
注意事项

报警模板需要与应用分组配合使用，因此建议您按照业务应用对云资源创建应用分组和报警模板。

> **说明:**
> 选择报警模板应用到指定分组后，云监控将删除您的应用分组原有的报警规则，然后根据所选模板内容为您创建新的报警规则。

操作步骤

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 选择需要应用报警模板的分组，单击分组名称，进入分组详情页面。



4. 单击右上角的应用模板到组，进入应用模板到分组页面。

5. 选择需要使用的报警模板，点击确认即可将所选模板应用到当前分组。

9.7 管理报警规则

您可以在应用分组内对阈值报警规则进行创建、查看、修改、删除、启用和禁用等操作。

> **说明:**
> 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。

创建报警规则

1. 登录云监控控制台。
2. 单击左侧导航栏中的的应用分组，进入应用分组页面。
3. 选择需要创建报警规则的分组，单击分组名称，进入分组详情页面。
4. 单击右上方的添加阈值报警，进入添加报警页面。
5. 选择产品类型、添加报警规则、设置报警机制、选择联系人组，点击添加即可。

通过报警模板创建报警规则

1. 登录云监控控制台。
2. 选择页面左侧菜单的应用分组。
3. 选择需要创建报警规则的分组，单击分组名称，进入分组详情页面。

4. 单击右上方的应用模板到组。
5. 选择需要使用的报警模板，单击确认完成创建。

删除报警规则

1. 登录云监控控制台。
2. 选择页面左侧菜单的应用分组。
3. 选择需要删除报警规则的分组，单击分组名称，进入分组详情页面。
4. 单击左侧导航栏中的报警规则，进入分组的报警规则页面。
5. 在报警规则列表右侧操作栏中，单击对应的删除，可删除该报警规则。或者勾选多条报警规则后，单击列表下方的删除按钮，即可删除所选报警规则。

修改报警规则

1. 登录云监控控制台。
2. 选择页面左侧菜单的应用分组，进入应用分组页面。
3. 选择需要修改报警规则的分组，单击分组名称，进入分组详情页面。
4. 单击左侧导航栏中的报警规则，进入分组的报警规则页面。
5. 在报警规则列表右侧操作栏中，单击对应的修改，可修改该报警规则。

禁用或启用分组的报警规则

当您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
  1. 登录云监控控制台。
  2. 单击左侧导航栏中的应用分组，进入应用分组页面。
  3. 选择相应的分组名称，在右侧操作栏中单击更多。
  4. 选择禁用所有报警规则即可。
- 启用分组中全部报警规则
  1. 登录云监控控制台。
  2. 单击左侧导航栏中的应用分组，进入应用分组页面。
  3. 选择相应的分组名称，在右侧操作栏中单击更多。
  4. 选择启用所有报警规则即可。

- 禁用分组中部分报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中的应用分组，进入应用分组页面。
  3. 选择相应的报警规则分组，单击分组名称，进入分组详情页面。
  4. 单击左侧导航栏中的报警规则，进入分组的报警规则页面。
  5. 在报警规则列表右侧操作栏中，单击对应的禁用，禁用该报警规则。或者勾选多条报警规则后，单击列表下方的禁用按钮，禁用所选报警规则。

- 启用分组中部分报警规则

  1. 登录云监控控制台。
  2. 单击左侧导航栏中的应用分组，进入应用分组页面。
  3. 选择需要创建报警规则的分组，单击分组名称，进入分组详情页面。
  4. 单击左侧导航栏中的报警规则，进入分组的报警规则页面。
  5. 在报警规则列表右侧操作栏中，单击对应的启用，启用该报警规则。或者勾选多条报警规则后，单击列表下方的启用按钮，启用所选报警规则。

10 事件监控

10.1 事件监控概览

事件监控汇集了云产品故障、运维事件以及用户业务异常事件，提供按产品、级别、名称、应用分组汇总统计事件，便于关联业务与问题复盘。支持自定义事件通知对象、通知方式，避免关键事件被忽略，并可以记录事件详情，帮您快速分析定位问题。

云产品事件

事件监控为您提供各类云产品产生的系统事件的统一查询和统计入口，使您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。

同时还为您提供了事件的报警功能，您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，使您第一时间知晓严重事件并及时进行处理，形成线上自动化运维闭环。

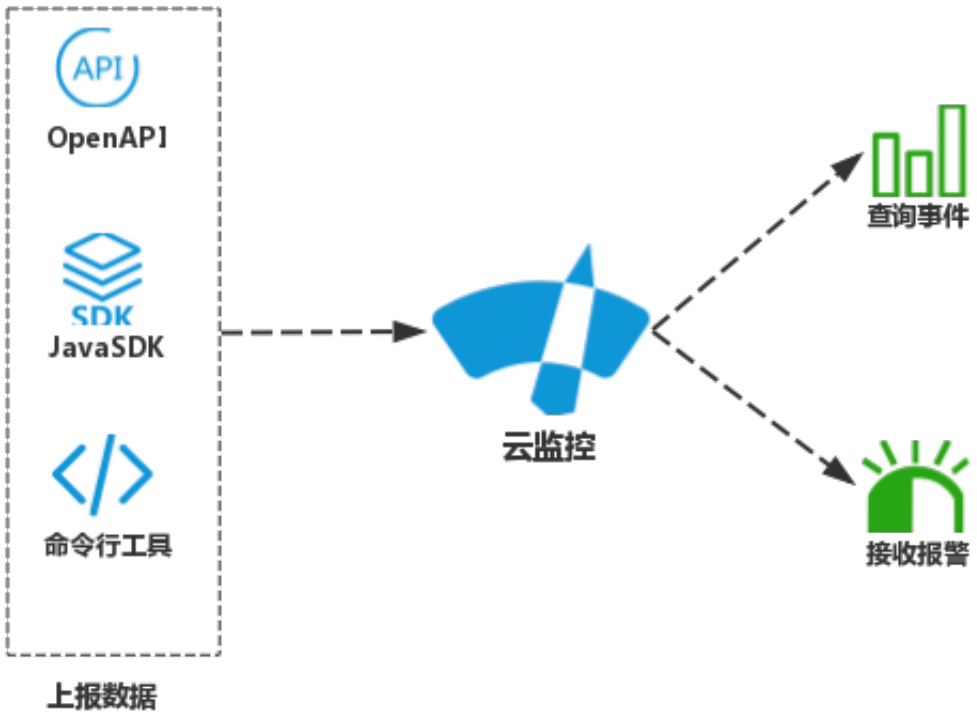
事件监控为您提供云产品故障、运维事件的查询及报警服务。

- ECS事件：支持系统错误或实例错误引发的重启、磁盘性能受损等重要ECS系统事件。
- SLB事件：HTTPS证书过期事件。
- OSS事件：Bucket上、下行带宽超过流控阈值或汇报阈值。
- 弹性伸缩事件：弹性伸缩扩、缩容成功、失败。
- E-MapReduce事件：集群创建失败、超时、服务组件状态。

更多云产品事件请参考云产品事件。

自定义事件

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。



自定义事件监控与自定义监控的区别：

- 自定义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。

报警服务与自动化运维

事件监控支持多种报警方式，便于您进行自动化运维。

- 报警通知：支持语音电话、短信、邮件、钉钉群等通知方式。
- 消息队列服务：事件可写入您的消息服务队列中，您可通过消息服务与自有运维系统进行对接。
- 函数计算：事件触发您的函数服务，进行后续运维逻辑处理。
- 报警回调：通过HTTP协议的POST请求推送报警通知到您指定的公网URL（已有运维体系或消息通知体系），您在接收到报警通知后，可以根据通知内容做进一步处理。

10.2 云产品事件

10.2.1 云产品事件

本文为您介绍目前事件监控支持哪些云产品的系统事件。

ECS系统事件

ECS系统事件含义详情介绍，请参见事件通知列表。

事件名称	事件含义	事件类型	事件状态	事件等级	备注
Instance:InstanceFailure.Reboot	因实例错误实例重启开始	Exception	Executing	CRITICAL	
Instance:InstanceFailure.Reboot	因实例错误实例重启结束	Exception	Executed	CRITICAL	
Instance:SystemFailure.Reboot	因系统错误实例重启开始	Exception	Executing	CRITICAL	
Instance:SystemFailure.Reboot	因系统错误实例重启结束	Exception	Executed	CRITICAL	
Instance:SystemMaintenance.Reboot	因系统维护实例计划重启	Maintenance	Scheduled	CRITICAL	
Instance:SystemMaintenance.Reboot	因系统维护实例计划重启已规避	Maintenance	Avoided	CRITICAL	
Instance:SystemMaintenance.Reboot	因系统维护实例计划重启执行中	Maintenance	Executing	CRITICAL	
Instance:SystemMaintenance.Reboot	因系统维护实例计划重启已完成	Maintenance	Executed	CRITICAL	
Instance:SystemMaintenance.Reboot	因系统维护实例计划重启已取消	Maintenance	Canceled	CRITICAL	

事件名称	事件含义	事件类型	事件状态	事件等级	备注
Instance:SystemMaintenance.Reboot	因系统维护实例计划重启已失败	Maintenance	Failed	CRITICAL	
Disk:Stalled	磁盘性能受到严重影响开始	Exception	Executing	CRITICAL	
Disk:Stalled	磁盘性能受到严重影响结束	Exception	Executed	CRITICAL	
Instance:StateChange	实例状态改变通知	StatusNotification	Normal	INFO	事件详情中会展示实例的具体状态，状态包括Running（运行中）、Stopped（已停止/已过期/即将过期/已锁定/欠费回收中/等待释放）、Deleted（实例已释放），具体的实例生命周期说明请参考实例生命周期
Instance:PreemptibleInstanceInterruption	抢占式实例中断通知	StatusNotification	Normal	WARN	导致抢占式实例进入待回收状态的原因，包括市场价格高于您的出价或者资源供需关系发生变化等，具体请参考抢占式实例
Snapshot:CreateSnapshotCompleted	磁盘快照创建完成	StatusNotification	Normal	INFO	

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3天后到期	WARN
CertKeyExpired_7	证书将在7天后到期	WARN
CertKeyExpired_15	证书将在15天后到期	WARN
CertKeyExpired_30	证书将在30天后到期	WARN
CertKeyExpired_60	证书将在60天后到期	WARN

OSS系统事件

事件名称	事件含义	事件等级	说明
BucketEgressBandwidth	Bucket下行带宽超过汇报阈值	INFO	云用户所有Bucket下行带宽之和超过128Mbps汇报阈值即触发该事件。
BucketEgressBandwidthThresholdExceeded	Bucket下行带宽超过流控阈值	WARN	该Bucket受到区域流控限流影响。（指定区域内所有Bucket的下行带宽之和超过流控设置，则触发触发流控。大陆公共云默认每个区域是10Gbps，香港和海外默认是5Gbps，Bucket级别不设置默认流控）。
BucketIngressBandwidth	Bucket上行带宽超过汇报阈值	INFO	云用户所有Bucket上行带宽之和超过128Mbps汇报阈值即触发该事件。

事件名称	事件含义	事件等级	说明
BucketIngressBandwidthThresholdExceeded	Bucket上行带宽超过流控阈值	WARN	该Bucket受到区域流控限流影响。（指定区域内所有Bucket的上行带宽之和超过流控设置，则触发触发流控。大陆公共云默认每个区域是10Gbps，香港和海外默认是5Gbps，Bucket级别不设置默认流控）
UserEgressBandwidth	User下行带宽超过汇报阈值	INFO	云用户所有Bucket下行带宽之和超过128Mbps汇报阈值即触该发事件。
UserEgressBandwidthThresholdExceeded	User下行带宽超过流控阈值	WARN	指定区域内所有Bucket的下行带宽之和超过流控设置，则会触发该事件（大陆公共云默认每个区域是10Gbps，香港和海外默认是5Gbps，Bucket级别不设置默认流控）。
UserIngressBandwidth	User上行带宽超过汇报阈值	INFO	云用户所有Bucket上行带宽之和超过128Mbps汇报阈值即触发该事件。
UserIngressBandwidthThresholdExceeded	User上行带宽超过流控阈值	WARN	指定区域内所有Bucket的下行带宽之和超过流控设置，则会触发该事件（大陆公共云默认每个区域是10Gbps，香港和海外默认是5Gbps，Bucket级别不设置默认流控）。

ESS弹性伸缩系统事件

事件名称	事件含义	事件状态	事件等级
AUTOSCALING:SCALE_IN_ERROR	弹性伸缩组缩容伸缩活动失败	Unnormal	CRITICAL
AUTOSCALING:SCALE_IN_SUCCESS	弹性伸缩组缩容伸缩活动成功	Normal	INFO
AUTOSCALING:SCALE_OUT_ERROR	弹性伸缩组扩容伸缩活动失败	Unnormal	CRITICAL
AUTOSCALING:SCALE_OUT_SUCCESS	弹性伸缩组扩容伸缩活动成功	Normal	INFO
AUTOSCALING:SCALE_REJECT	弹性伸缩组伸缩活动执行被拒绝	Warn	WARN
AUTOSCALING:SCHEDULE_TASK_EXPIRING	定时任务到期提醒	Warn	WARN
AUTOSCALING:SCALE_OUT_START	弹性伸缩组扩容伸缩活动开始	normal	INFO
AUTOSCALING:SCALE_IN_START	弹性伸缩组缩容伸缩活动开始	normal	INFO

物联网套件系统事件

事件名称	事件含义	事件类型	事件状态	事件等级
Account_Connect_QPS_Limit	当前账号每秒最大连接请求数达到上限。	Exception	Fail	WARN
Account_Downlink_QPS_Limit	当前账号每秒发给设备的请求数达到上限。	Exception	Fail	WARN
Account_RuleEngine_DataForward_QPS_Limit	当前账号每秒到达规则引擎的请求数达到上限。	Exception	Fail	WARN
Account_Uplink_QPS_Limit	当前账号每秒发布请求数达到上限。	Exception	Fail	WARN

事件名称	事件含义	事件类型	事件状态	事件等级
Device_Downlink_QPS_Limit	任一设备下行消息QPS达到上限。	Exception	Fail	WARN
Device_Uplink_QPS_Limit	任一设备上行消息QPS达到上限。	Exception	Fail	WARN

智能接入网关系统事件

事件名称	事件含义	事件状态	事件等级
AccessGatewayFailover	接入点切换	Agwfailover	INFO
Connection Disconnect	网络连接断开	Disconnect	CRITICAL
DeviceHacked	设备被攻击	Hacked	CRITICAL
DeviceOffline	设备离线	Offline	CRITICAL
DeviceOnline	设备上线	Online	INFO

云监控系统事件

事件名称	事件含义	事件状态	事件等级
Group_AddResourcesFailed_QuotaReached	超过资源上限，动态添加机器到分组失败	Failed	CRITICAL
Agent_Status_Stopped	心跳检查失败	Stopped	CRITICAL
Agent_Status_Running	心跳检查恢复	Running	CRITICAL

数据库备份DBS事件

事件名称	事件含义	事件状态	事件等级
CloseContBackup	关闭增量日志备份	Failed	INFO
ContBackupFail	增量备份异常	Failed	WARN
DataRestoreFail	数据恢复异常	Failed	WARN
DataRestoreSuccess	数据恢复成功	Running	WARN
FullBackupFail	全量备份异常	Failed	WARN

事件名称	事件含义	事件状态	事件等级
InstancePause	备份计划暂停	Failed	INFO
InstanceStart	备份计划启动	Running	INFO
OpenContBackup	开启增量日志备份	Running	INFO

RDS系统事件

事件名称	事件含义	事件状态	事件等级
Instance_Failover	实例主备切换	Executed	WARN
Instance_Failure_Start	实例故障开始	Executing	CRITICAL
Instance_Failure_End	实例故障结束	Executed	CRITICAL

Redis系统事件

事件名称	事件含义	事件状态	事件等级
Instance_Failover	实例主备切换	Executed	WARN
Instance_Failure_Start	实例故障开始	Executing	CRITICAL
Instance_Failure_End	实例故障结束	Executed	CRITICAL

MongoDB系统事件

事件名称	事件含义	事件状态	事件等级
Instance_Failure_Start	实例故障开始	Executing	CRITICAL
Instance_Failure_End	实例故障结束	Executed	CRITICAL

分析型数据库事件

事件名称	事件含义	事件等级
StorageUsage	磁盘使用率超过80%。	CRITICAL
InsertFailureRate	插入失败率10%。	CRITICAL
SelectFailureRate	查询失败率10%。	CRITICAL

边缘节点服务ENS事件

事件名称	事件含义	事件分类	事件状态	事件等级
EnsRegion:NetworkDown:Executing	节点网络失联。	Exception	Executing	CRITICAL
EnsRegion:NetworkDown:Executed	节点网络恢复。	Exception	Executed	CRITICAL
EnsRegion:NetworkMigration:Scheduled	边缘节点网络割接计划。	Maintenance	Scheduled	WARN
EnsRegion:NetworkMigration:Executing	边缘节点网络割接执行。	Maintenance	Executing	CRITICAL
EnsRegion:NetworkMigration:Executed	边缘节点网络割接完成。	Maintenance	Executed	INFO
EnsRegion:NetworkMigration:Canceled	边缘节点网络割接取消。	Maintenance	Canceled	INFO
Instance:SystemFailure.Reboot:Executing	实例重启执行中（系统问题导致）。	Exception	Executing	CRITICAL
Instance:SystemFailure.Reboot:Executed	实例重启完成（系统问题导致）。	Exception	Executed	CRITICAL

10.2.2 查看云产品事件

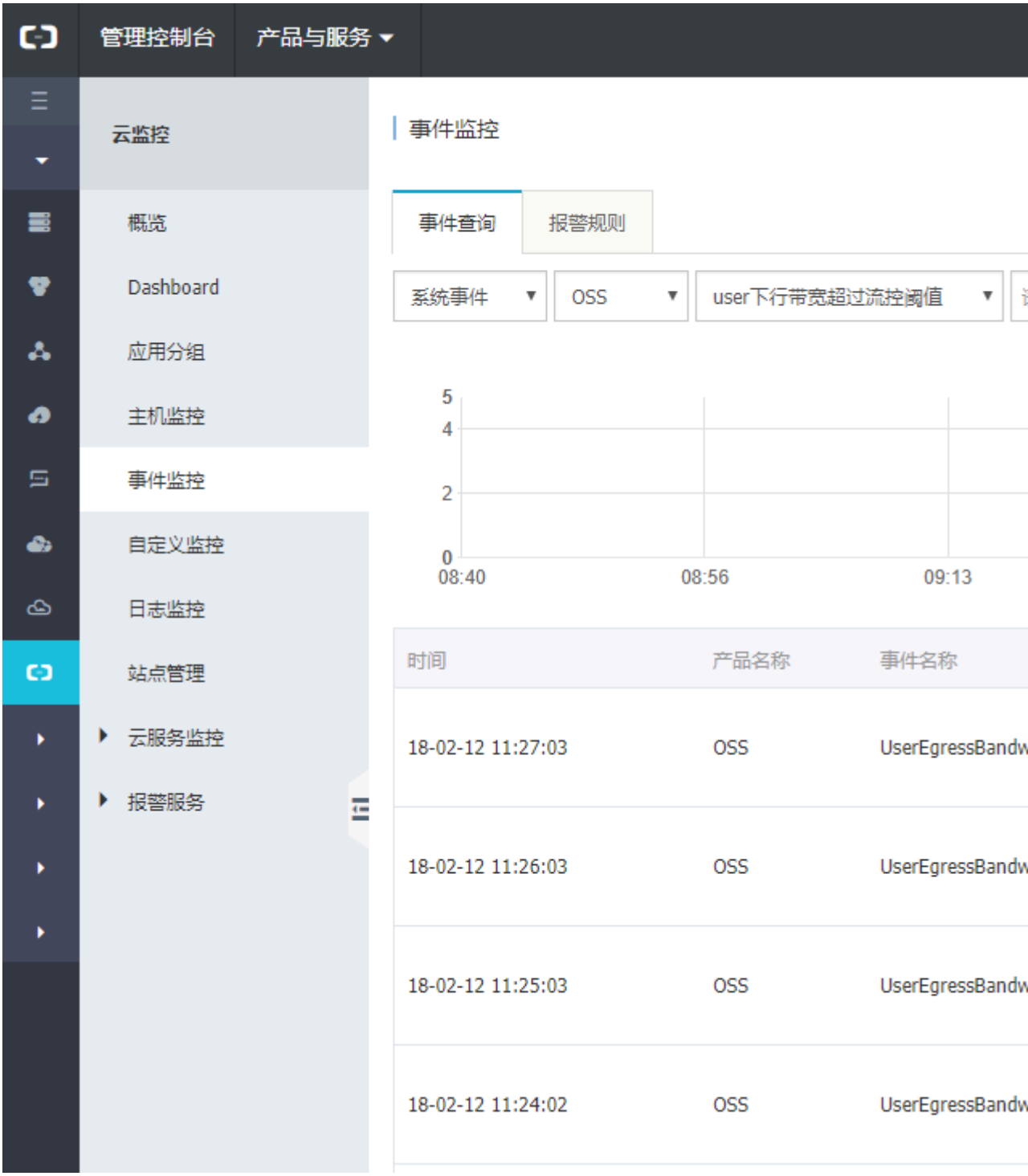
事件监控为您提供各类云产品产生的系统事件的统一查询和统计入口，使您明确知晓云产品的使用状态，让云更透明。

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。

按产品查看系统事件

1. 登录云监控控制台。
2. 点击左侧导航栏中的事件监控，进入事件监控页面。在下拉框中选择系统事件，然后产品下拉框选择产品，事件下拉框选择事件，选择时间即可查看指定时间内发生的事件。

3. 单击操作栏中的查看详情，即可查看相关事件的详细信息。



按分组查看系统事件

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。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。

3. 单击分组名称，进入分组的详情页面。
4. 在分组详情页面，单击左侧导航栏中的事件监控，进入事件监控页面，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。

10.2.3 使用云产品事件报警功能

本文为您介绍如何使用云产品事件报警功能，实现系统异常时进行报警的目的。

背景信息

当阿里云产品发生系统异常时，事件监控的报警能力为您提供以下两种通知能力，方便您及时知晓事件发生、自动化处理异常：

- 提供通过语音电话、短信、邮件、钉钉群的方式，对事件发生进行报警。
- 将事件分发到您的消息服务队列、函数计算、日志服务、URL回调，以便您根据业务场景自动化处理异常事件。

使用云产品事件报警的准备工作

如果您需要将系统事件分发到您的消息服务队列、函数计算、日志服务、URL回调，那么请准备消息服务队列、函数、日志服务以及报警回调URL。

使用云产品事件报警的实施步骤

您可以先创建事件报警规则，然后使用系统事件的调试功能，模拟系统事件的发生，以便验证报警规则中设置的消息服务队列是否能正常接收时间、函数计算的函数是否能正常被触发。

- 创建事件报警规则

1. 登录云监控控制台。
2. 在左侧导航栏选择事件监控。
3. 在报警规则页签，点击右上角的创建事件报警，弹出创建/修改事件报警对话框。
4. 在基本信息区域，填写报警规则名称。
5. 在事件报警规则区域，填写如下信息：

   a. 事件类型：选择系统事件

   b. 产品类型、事件等级、事件名称：按照实际情况填写

   c. 资源范围：选择全部资源时，任何资源发生相关事件，都会按照配置发送通知；选择应用分组时，只有指定分组内的资源发生相关事件时，才会发送通知。

6. 选择报警方式。目前支持报警通知、消息服务队列、函数服务、日志服务和URL回调等方式。

- 调试报警规则

1. 进入事件监控的报警规则列表页面。

2. 点击操作中的调试，进入调试页面。
3. 选择需要调试的事件，内容中会显示相应的事件内容，可以根据实际情况修改内容中的实例ID等字段。

4. 点击确定按钮，将根据内容发送一个事件，触发报警规则设置的报警通知、消息服务队列、函数计算、报警回调。

10.3 自定义事件

10.3.1 上报自定义事件数据

事件监控功能为您提供上报自定义事件的接口，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。

使用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

- 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：AccessKeyId: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

- 签名算法

  目前，上报事件数据只支持一种数字签名算法，即默认签名算法为hmac-sha1。

  1. 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。

  2. 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。

```
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	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

名称	定义	示例
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

上表中CanonicalizedHeaders 的构造方式如下：

a. 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。

b. 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。

c. 删除请求头和内容之间分隔符两端出现的任何空格。

d. 将所有的头和内容用 \n 分隔符组合成最后的 CanonicalizedHeaders。

上表中CanonicalizedResource 的构造方式如下：

a. 将 CanonicalizedResource 设置为空字符串（”“）。

b. 放入要访问的URI，如/event/custom/upload。

c. 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"
```

3. 生成请求的数字签名

默认签名算法为hmac-sha1，整个签名公式如下：

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

· 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
}
```

使用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);
```

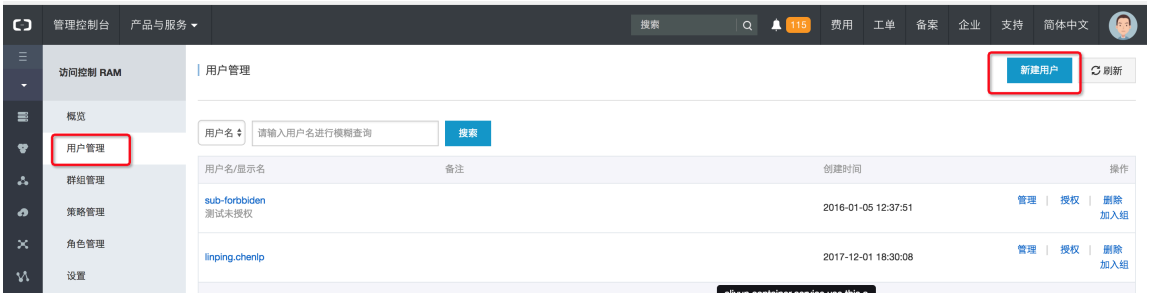
```
        }
```

使用阿里云命令行（CLI）上报数据

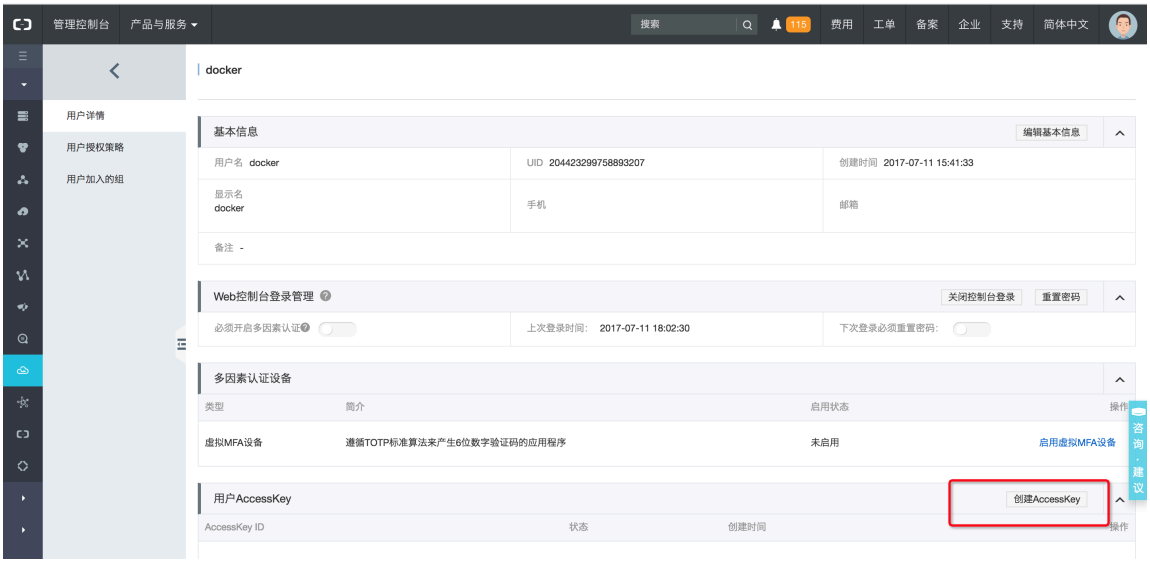
1. 准备工作

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）。

a. 创建子账号。



b. 为子账号生成accesskeyid， accesskeysecrret。



c. 为子账号授权云监控权限。

2. 安装CMS SDK

- **Windows安装方式如下：**

```
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 安装方式如下：

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

如果需要更新SDK，则使用如下命令：

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

3. 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

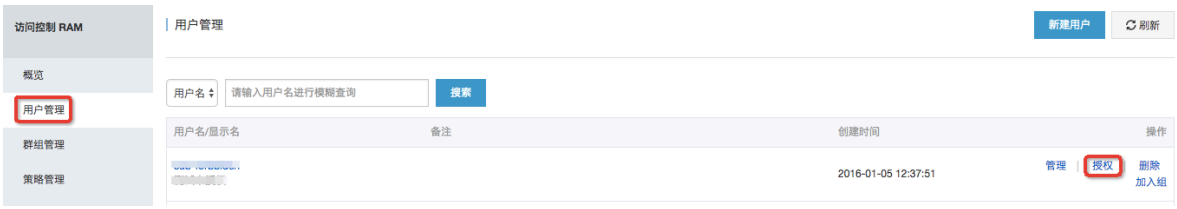
错误代码	含义
200	正常
400	客户端请求中的语法错误
403	校验失败、限速、没有授权
500	服务器内部错误

子账号授权说明

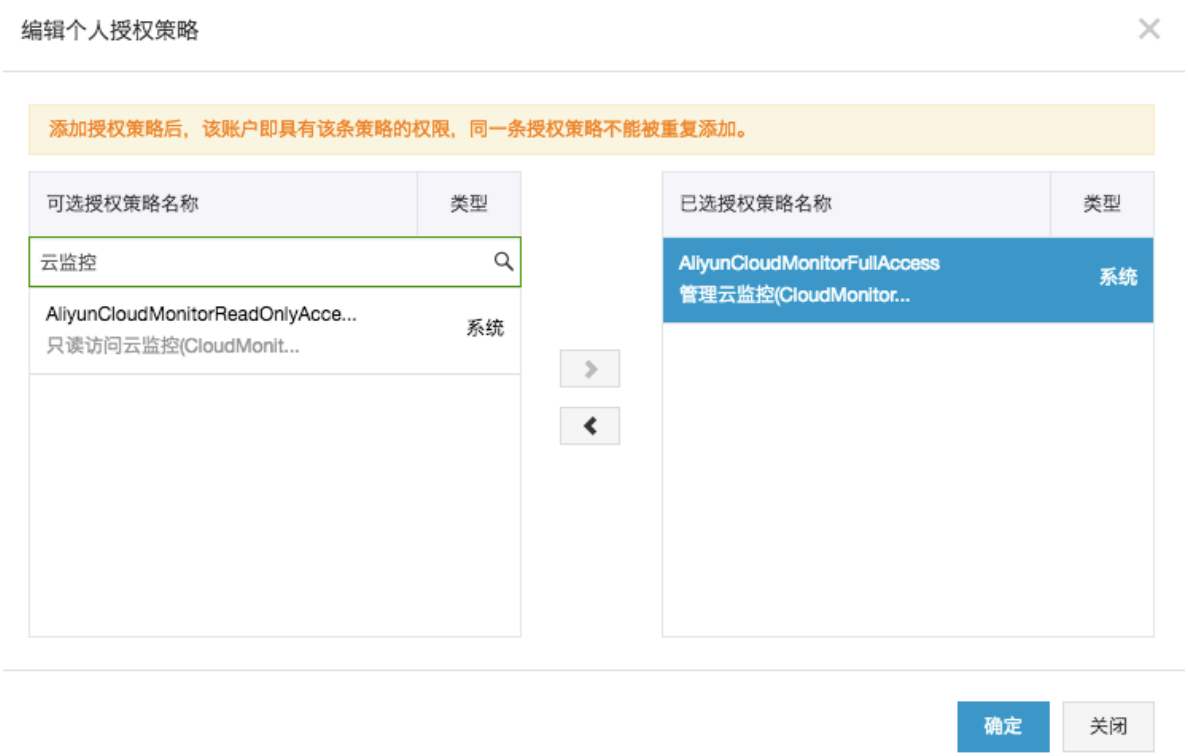
使用子账号的AK上报事件数据时，需要对相应子账号授权云监控管理权限。如果子账号未授权云监控管理权限，上报数据时会提示“cannot upload event, please use ram to auth”。

1. 登录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。



10.3.2 查看自定义事件

事件监控为您提供自定义事件的统一查询和统计入口，方便您对上报的自定义事件数据进行查看。

按事件级别查看自定义事件

1. 登录云监控控制台。
2. 单击左侧导航栏中的事件监控，进入事件监控页面。在下拉框中选择自定义事件，然后事件级别下拉框选择级别，事件下拉框选择事件，选择时间即可查看指定时间内发生的事件。
3. 单击操作栏中的查看详情，即可查看相关事件的详细信息。

按分组查看自定义事件

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自定义事件。

1. 登录云监控控制台。
2. 单击左侧导航栏中的应用分组，进入应用分组页面。
3. 单击分组名称，进入分组的详情页面。
4. 在分组详情页面，单击左侧导航栏中的事件监控，进入事件监控页面，在下拉框中选择自定义事件，页面中展示的自定义事件即为该分组中实例相关的自定义事件。

10.3.3 使用自定义事件报警功能

本文为您介绍如何使用自定义事件报警功能，实现对自定义事件进行报警的目的。

背景信息

当您上报的自定义事件数据发生异常时，事件监控的报警能力为您提供以下两种通知能力，方便您及时知晓事件发生、处理异常：

- 提供通过语音电话、短信、邮件、钉钉群的方式，对事件发生进行报警。
- 将事件分发到您的报警回调URL，以便您根据业务场景自动化处理异常事件。

使用云产品事件报警的实施步骤

1. 登录云监控控制台。
2. 单击左侧导航栏的事件监控，进入事件查询页面。

3. 单击报警规则页签，然后单击右上角的创建事件报警，弹出创建/修改事件报警对话框。

4. 在基本信息区域，填写报警规则名称。
5. 在事件报警规则区域，填写如下信息：
   a. 事件类型：选择自定义事件
   b. 所属应用分组：选择应用分组，只有指定分组内的资源发生相关事件时，才会发送通知。
   c. 事件名称：输入上报的事件名称。
   d. 规则描述：设置1~5分钟内累计发生次数。
   e. 通知方式：选择报警通知方式。
   f. 高级配置：设置生效时间和报警回调。
      - 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。
      - 报警回调：填写公网可访问的URL，云监控会将报警信息通过POST请求推送到该地址，目前仅支持HTTP协议。
   g. 设置完毕后，单击确定按钮，即可完成创建自定义事件报警规则。

当您上报的自定义事件达到报警条件时，将会触发报警通知。

10.3.4 自定义事件监控最佳实践

本文为您介绍如何利用云监控自定义事件监控功能实现系统在运行过程中出现异常时，记录异常情况并在满足特定条件时进行警通知。

背景信息

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。

准备工作

自定义事件监控提供了Java SDK和Open API两种上报数据的方式，本文为您介绍通过Java SDK上报异常数据。

1. 添加 Maven 依赖

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

```
</dependency>
```

2. 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);
```

3. 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 = CustomEven
tUploadRequest.builder();
        builder.setEventList(events);
        CustomEventUploadResponse response = cmsClient.putCustomE
vent(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);
    }
}
```

上报异常事件的演示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进行报警。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)
```

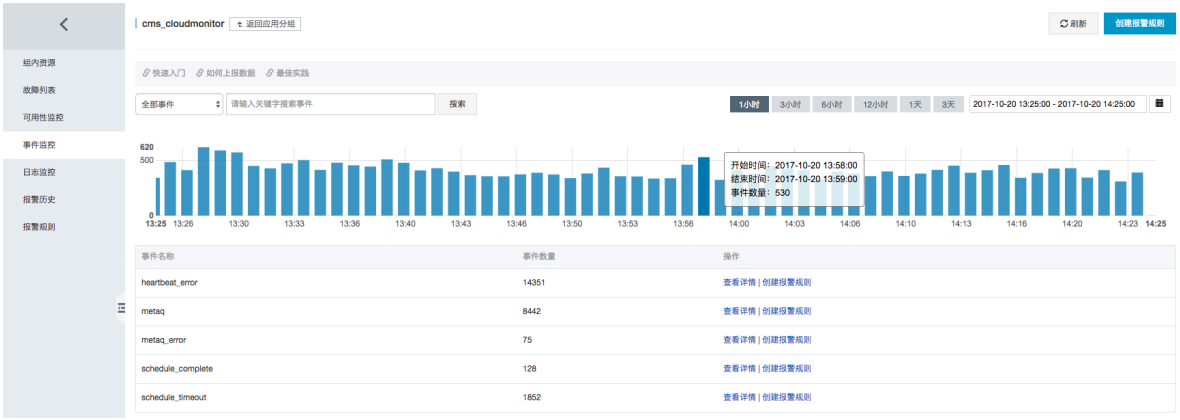
- Demo2：后台定时任务执行情况与消息消费情况的监控

  如同上面的HTTP请求事件，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.getReconsu
meTimes())); // 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));
```

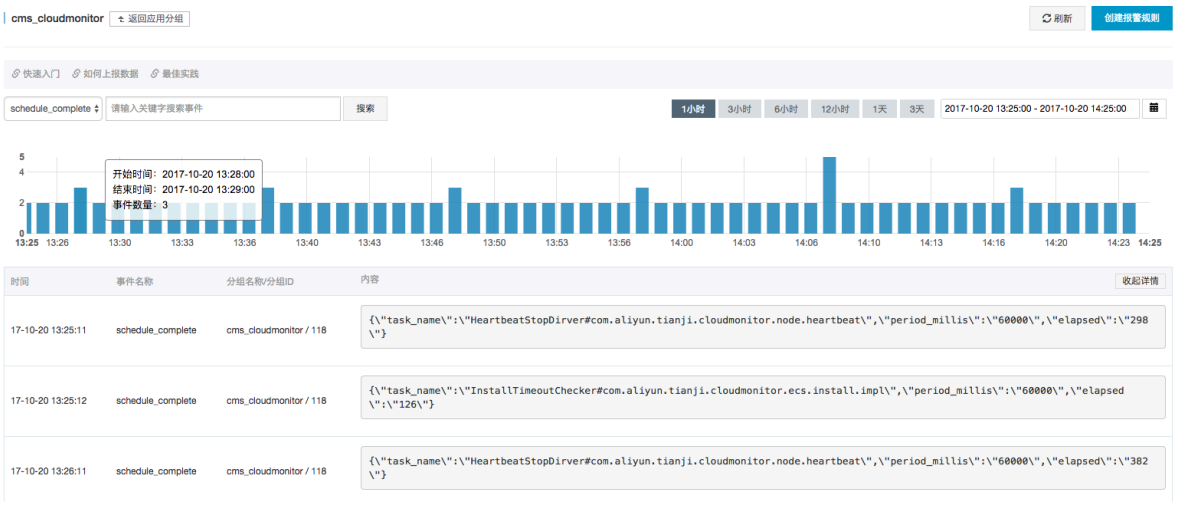
上报后查看事件



对消息队列消费异常设置报警

- **Demo 3：记录重要事件**

  自定义事件监控还有一种使用场景是用来记录一些重要的业务发生情况，但是不需要报警，方便日后查看。 例如重要业务的操作日志、修改密码、修改订单、异地登录等。



11 自定义监控

11.1 自定义监控概览

应用场景

自定义监控是提供给您自由定义监控项及报警规则的一项功能。您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，并根据处理结果进行报警。

事件监控与自定义监控的区别：

- 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

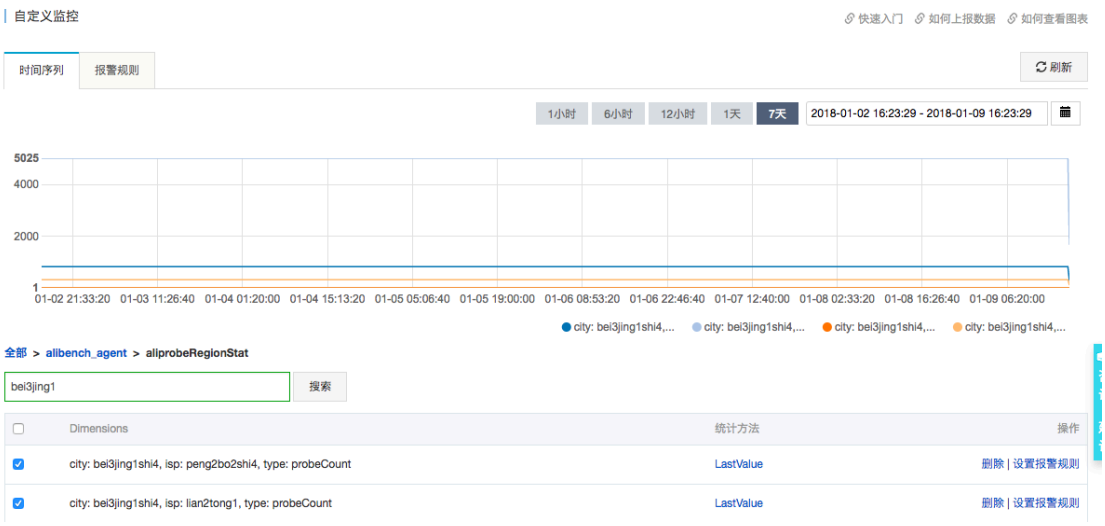
  请参见上报监控数据。

- 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。

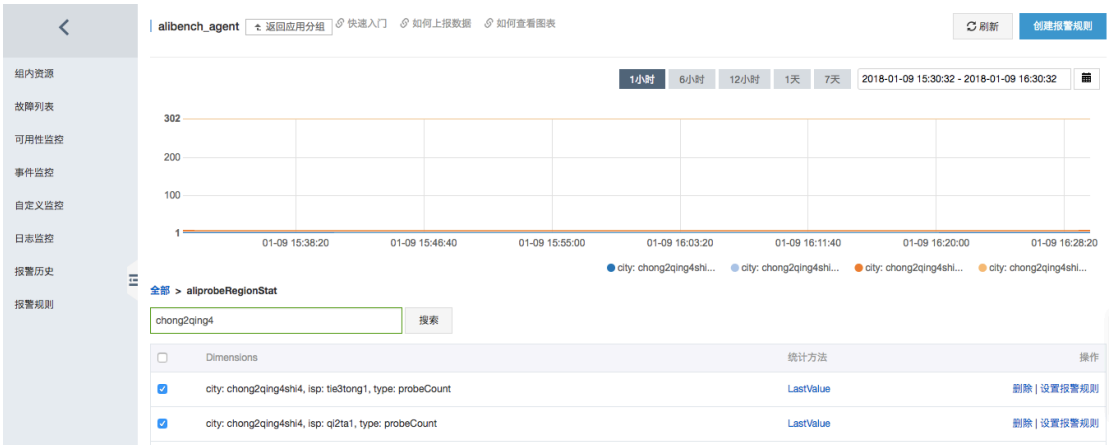
  - 查看所有自定义监控数据

    1. 登录云监控控制台。
    2. 点击左侧导航栏中的自定义监控，进入自定义监控页面。
    3. 选择对应的应用分组、监控项，进入时间序列详情页面。
    4. 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。
    2. 点击左侧导航栏中的应用分组，进入应用分组页面。
    3. 选择相应的应用分组，进入分组详情页。
    4. 点击自定义监控菜单，进入自定义监控详情页。
    5. 选择对应的监控项，进入时间序列详情页面。
    6. 选择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，设置报警规则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，可以按照如下方式设置报警规则。

  - 方式一：

    1. 登录云监控控制台。
    2. 点击左侧导航栏中的自定义监控，进入自定义监控页面。
    3. 选择对应的应用分组、监控项，进入时间序列详情页面。
    4. 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。
    5. 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。
    2. 点击左侧导航栏中的应用分组，进入应用分组页面。
    3. 选择相应的应用分组，进入应用分组内的自定义监控页面。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。

11.2 上报监控数据

本文为您介绍如何上报自定义监控的监控数据。

自定义监控为您提供了自由定义监控项及报警规则的功能，您可以针对自己关心的业务指标进行监控。通过上报监控数据的接口，将自己采集的时序数据上报到云监控，并可通过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

- 北京、上海、杭州地域QPS限制为200，张家口、深圳地域QPS限制为100，其余地域QPS限制为50。
- 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。
- 上报原始数据为付费功能，免费版可以上报聚合数据（即上报数据时，请求参数中type字段需传入1）。
- 其他限制请关注计费方式。

OpenAPI方式上报数据

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
- 服务地址

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

  内网服务地址如下：

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

地域	RegionId	服务地址
亚太东南 1（新加坡）	ap-southeast-1	http://metrichub-ap-southeast-1.aliyun.com
亚太东南3（吉隆坡）	ap-southeast-3	http://metrichub-ap-southeast-3.aliyun.com
亚太南部 1 （孟买）	ap-south-1	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}}]
```

- 签名算法

  目前，上报监控数据只支持一种数字签名算法，即默认签名算法为hmac-sha1。

  1. 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。

  2. 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。

```
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	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

名称	定义	示例
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

上表中CanonicalizedHeaders 的构造方式如下：

a. 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。

b. 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。

c. 删除请求头和内容之间分隔符两端出现的任何空格。

d. 将所有的头和内容用 \n 分隔符组合成最后的 CanonicalizedHeaders。

上表中CanonicalizedResource 的构造方式如下：

a. 将 CanonicalizedResource 设置为空字符串（”“）。

b. 放入要访问的URI，如/event/custom/upload。

c. 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"
```

3. 生成请求的数字签名

默认签名算法为hmac-sha1，整个签名公式如下：

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

· 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“_-./\”，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。

名称	类型	必选	描述
dimensions	object	是	维度map，key-value都为字符串，支持字母、数字、连接符“_-./\”，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。

名称	类型	必选	描述
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。

Java SDK方式上报数据

- Java SDK 安装

  通过maven进行安装，需要添加的依赖如下：

```
<dependency>
            <groupId>com.aliyun.openservices</groupId>
            <artifactId>aliyun-cms</artifactId>
            <version>0.2.4</version>
</dependency>
```

- 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
```

```
}
```

- 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 = CustomMetricUploadRe
quest.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.putCustomM
etric(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

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）
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 CMSMetricRegistryBui
lder();
        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();
                        }
                    });
```

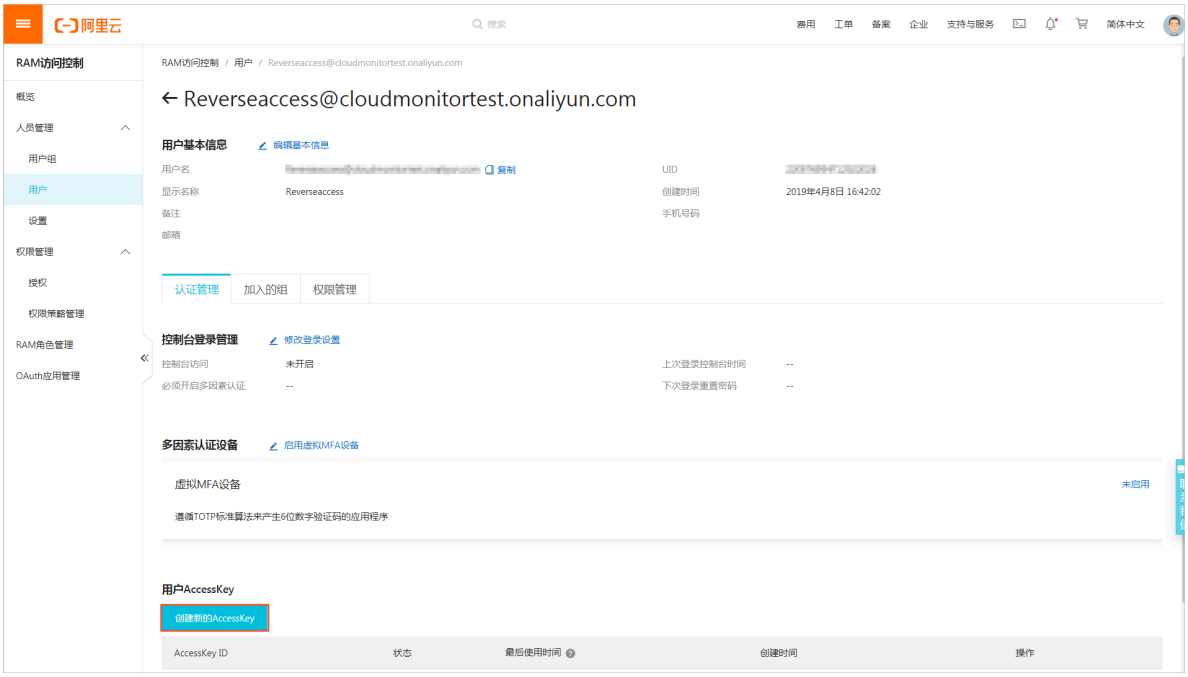
命令行（CLI）方式上报数据

准备阿里云账号

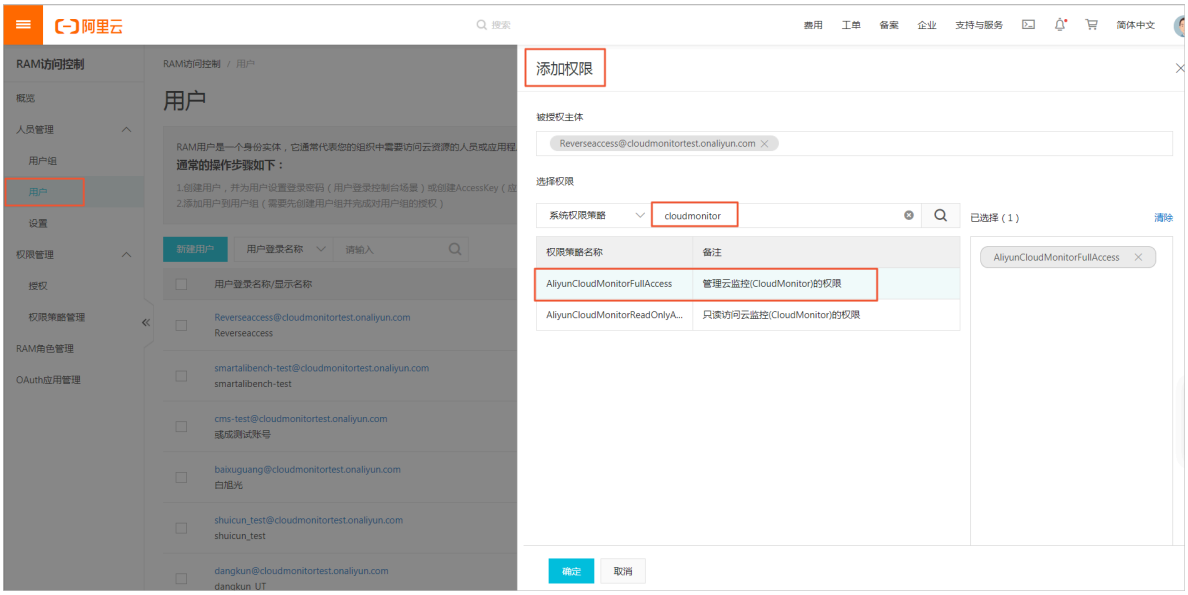
拥有阿里云账号，并生成具有云监控权限的子账号AK（使用子账号安全性更好）。

- 创建子账号

- 为子账号生成accesskeyid， accesskeysecrret



- 为子账号授权云监控权限



安装阿里云命令行（CLI）工具

系统要求：Linux、UNIX 或 Mac OS。

- 方式一：下载安装包

  您可以在阿里云CLI GitHub上下载最新版的CLI工具，解压后即可使用。支持Mac、Linux和Windows平台(x64版本）终端。 解压后，您可以将aliyun文件移至/usr/local/bin目录下，或添加到$PATH环境变量中。

- 方式二：编译源码

  请先安装并配置好Golang环境，并按照如下步骤下载源码并编译。

```
```
$ mkdir -p $GOPATH/src/github.com/aliyun
$ cd $GOPATH/src/github.com/aliyun
$ git clone http://github.com/aliyun/aliyun-cli.git
$ git clone http://github.com/aliyun/aliyun-openapi-meta.git
$ cd aliyun-cli
$ make install
```
```

配置CLI

在使用阿里云CLI前，您需要运行aliyun configure命令配置调用阿里云资源的AccessKey、地域、语言等。 您可以在阿里云控制台的AccessKey页面创建和查看您的AccessKey，或者联系您的系统管理员获取AccessKey。

```
$ aliyun configure
Configuring profile 'default' ...
Aliyun Access Key ID [None]: <Your AccessKey ID>
Aliyun Access Key Secret [None]: <Your AccessKey Secret>
Default Region Id [None]: cn-hangzhou
```

```
Default output format [json]: json
Default Language [zh]: zh
```

多用户配置：阿里云CLI支持多用户配置。您可以使用$ aliyun configure --profile user1命令指定使用哪个账号调用云产品的API。 执行`$ aliyun configure list`命令可以查看当前的用户配置， 如下表所示。其中在Profile后面有星号（*）标志的为当前使用的默认用户配置。

Profile	Credential	Valid	Region	Language
default *	AK:***f9b	Valid	cn-beijing	zh
aaa	AK:******	Invalid		
test	AK:***456	Valid		en
ecs	EcsRamRole: EcsTest	Valid	cn-beijing	en

阿里云CLI可通过在configure命令后增加--mode <authenticationMethod>参数的方式来使用不同的认证方式，目前支持的认证方式如下：

验证方式	说明
AK	使用AccessKey ID/Secret访问。
StsToken	使用STS Token访问。
RamRoleArn	使用RAM子账号的AssumeRole方式访问。
EcsRamRole	在ECS实例上通过EcsRamRole实现免密验证。

上报监控数据

使用`PutCustomMetric`接口上报监控数据，示例如下：

```
aliyun cms PutCustomMetric  --MetricList.1.MetricName cpu_total --
MetricList.1.Dimensions '{"sampleName1":"value1","sampleName2":"
value2"}' --MetricList.1.Time 1555390981421 --MetricList.1.Type 0
 --MetricList.1.Period 60 --MetricList.1.Values '{"value":10.5}' --
MetricList.1.GroupId "0"
```

上报成功后，返回状态码200。

```
{
  "Message": "success",
  "RequestId": "F69F5623-DDD6-42AE-AE59-87A2B841620B",
  "Code": "200"
}
```

错误编码

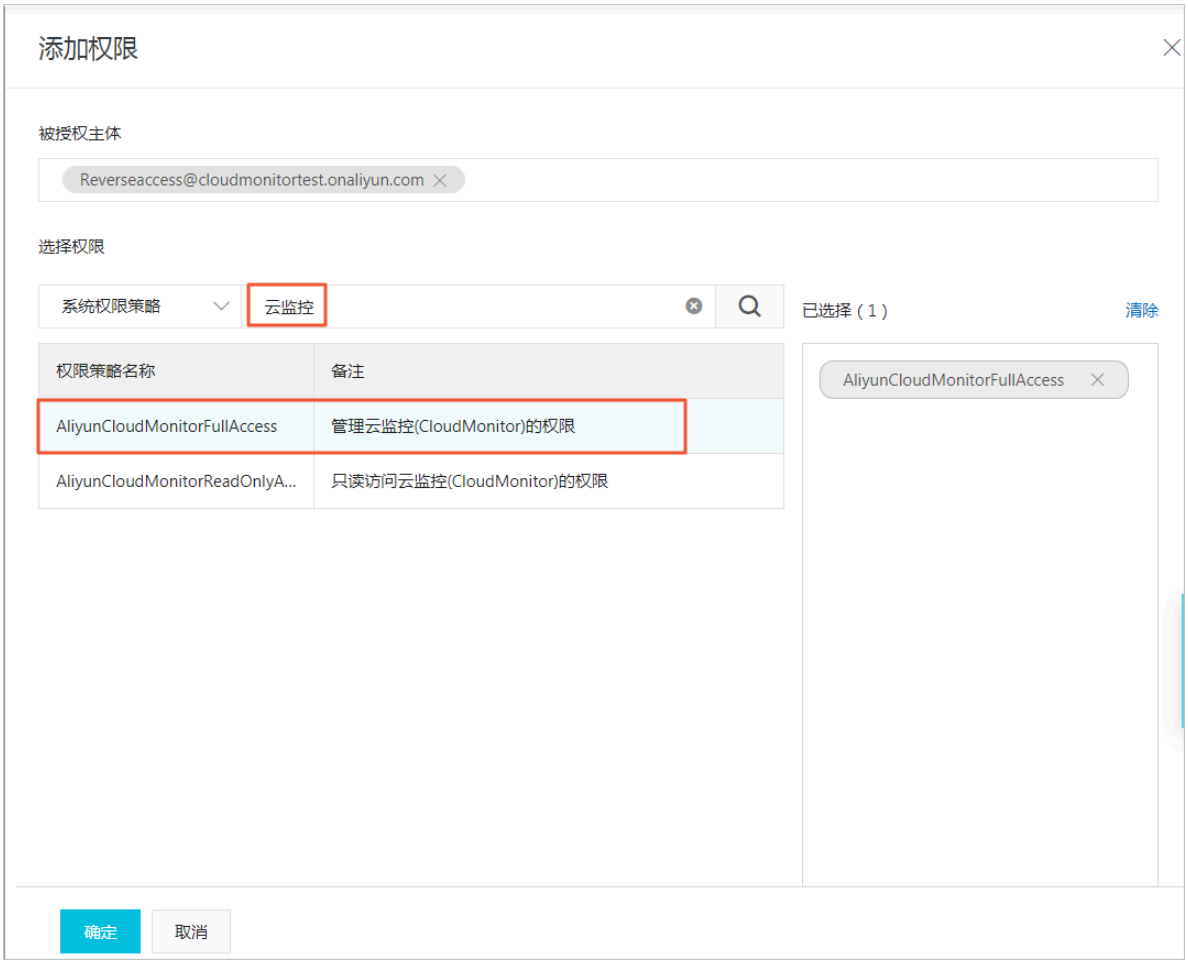
错误编码	含义
200	正常
206	部分成功 返回信息为“reach max time series num”，表示您的可以使用的时间序列配额已用完，需要购买更多配额或删除不再使用的时间序列 返回信息为“not allowed original value, please upgrade service”，表示您使用的是免费版，无法使用上报原始数据的功能。 返回信息为“type is invalid”，type参数错误，请检查是否传入了0或1以外的数值。
400	客户端请求中的语法错误
403	校验失败、限速、没有授权
500	服务器内部错误

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 data, please use ram to auth”。

1. 登录RAM控制台。
2. 单击左侧导航栏中的用户，进入用户页面。
3. 选择需要上报数据的子账号，在操作中单击添加权限。

4. 在添加权限页面中，选择管理云监控的权限，并单击确定保存授权即可。



11.3 查看自定义监控图表

本文为您介绍当您监控数据上报到自定义监控后，如何通过创建监控大盘并添加图表，来方便您查看自定义监控图表。

背景信息

当您想要针对自己关心的业务指标进行监控，您可以通过自定义监控功能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以图表形式进行呈现。

查看自定义监控图表的前提条件

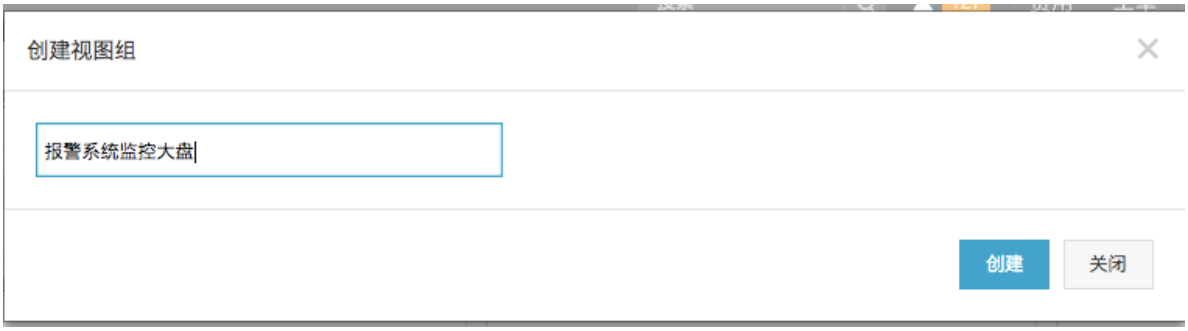
已成功上报监控数据。如何上报请参见上报监控数据。

查看自定义监控图表的实施步骤

创建监控大盘

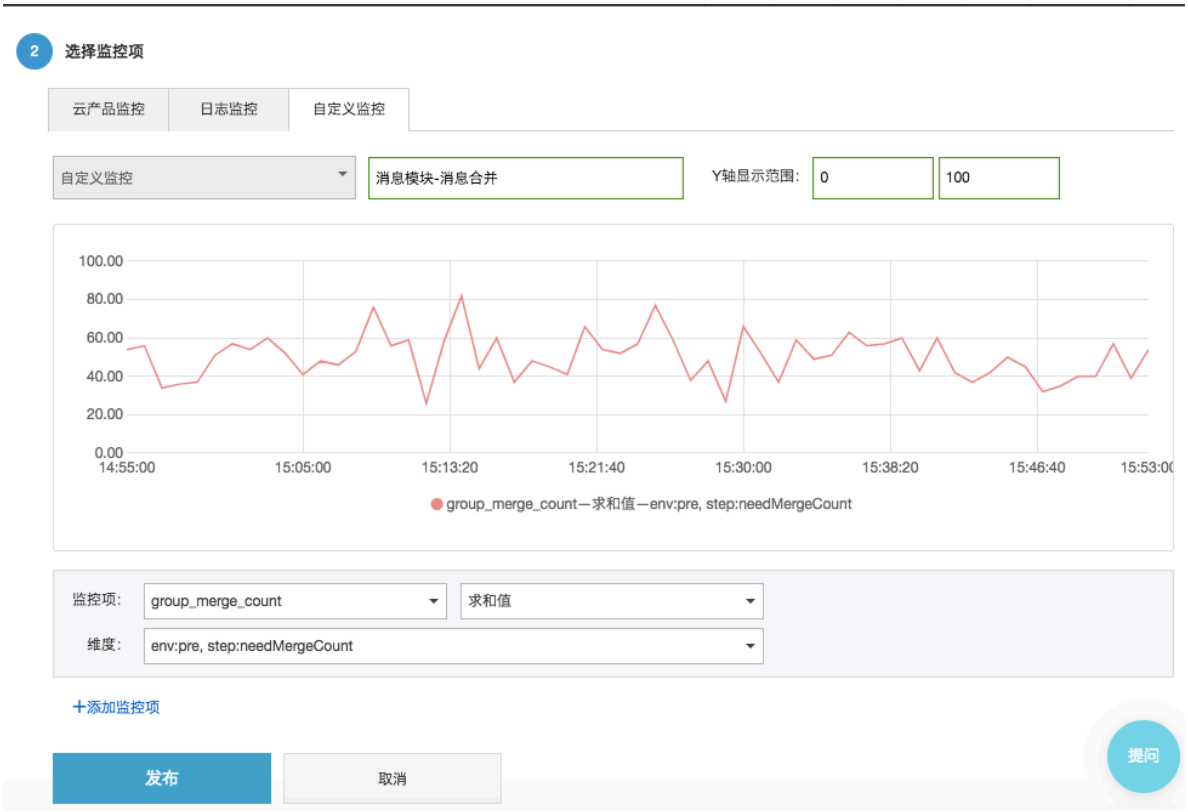
1. 登录云监控控制台。
2. 单击左侧导航栏中Dashboard下的自定义大盘，进入当前监控大盘页面。

3. 单击页面右上角的创建监控大盘按钮，填写监控大盘名称后，单击创建，即可创建新的监控大盘。



添加监控图表

1. 单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. 选择图表类型：从折线图、面积图、TopN表格、热力图、饼图中选择一种图表类型。
3. 单击自定义监控页签。



4. 填写图表名称，选择需要展示的监控项、统计方式、维度。

5. 单击发布按钮，即可完成添加图表。发布后即可看到自定义监控图表：