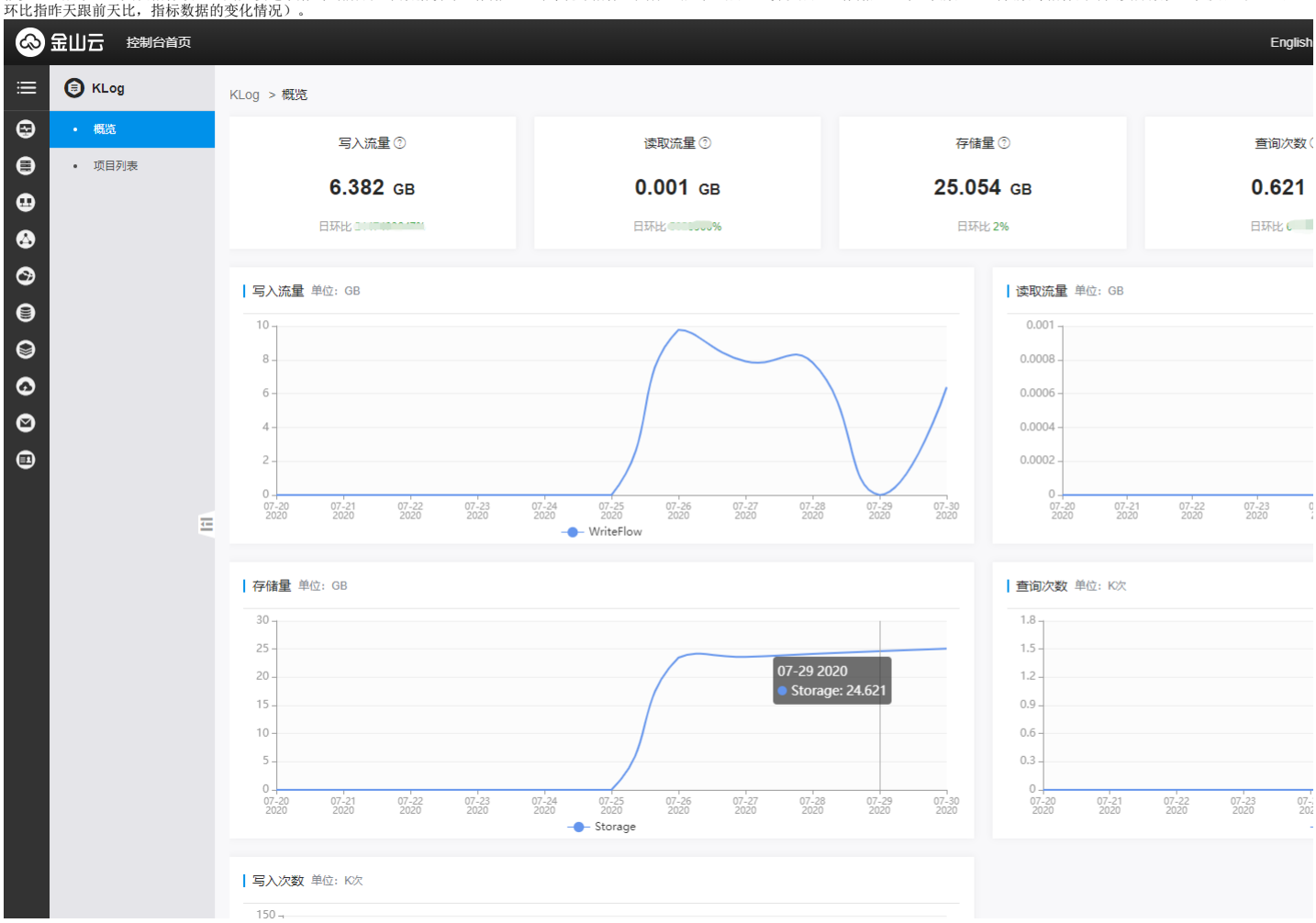
目录

概览

简介

概览通过展示一些关键指标项，让用户快速了解到当前账户下数据读写、存储、查询等统计指标。具体包括写入流量、读取流量、存储量、写入次数、查询次数等指标的昨天实际数值、以及日环比（日环比指昨天跟前天比，指标数据的变化情况）。



项目

简介

项目是基本业务组织单元，用户可以为不同业务在指定Region下创建不同的项目。每个项目都包含日志池、日志搜索、仪表盘、监控告警等模块。 项目组成员具有在该项目下创建日志池、写入读取数据、执行日志查询等权限。

创建项目

1. 登录金山云日志服务Klog控制台。
2. 点击导航**项目列表**，进入到**项目列表页**。
3. 在项目列表中点击**创建项目**，进入到创建项目页面。
   - 项目名称：按照格式要求自定义项目名称，名称创建后不支持修改
   - 地域：选择项目所属地域，选择后不支持修改
   - 备注：填写项目的描述信息，保存后支持修改 点击**确定**，完成项目创建。

项目详情

1. 登录金山云日志服务Klog控制台。
2. 点击导航**项目列表**，进入到**项目列表页**。
3. 在项目列表中，点击项目名称，进入到该**项目详情页**。
   - 访问域名：产品提供内网和外网两种访问域名，外网访问会产生外网流量。
   - 日志池：当前项目下的日志池，日志池相关操作详见日志池。

日志池

简介

日志池是日志服务的最小存储单元。日志服务支持用户自定义创建日志池以及定义日志池的分区数（分区数范围2-64）、日志数据存储周期（1-3000天），并允许用户根据业务实际数据流量来调整日志池的分区数。日志服务会自动删除超出存储周期的日志数据。日志池支持存储TEXT、LONG、DOUBLE、DATE等数据类型。

创建日志池

1. 登录金山云日志服务Klog控制台。
2. 在控制台点击**项目列表** > **项目详情页** > **概览**，点击**创建日志池**进入到创建页面。
   - 名称：按照格式要求自定义日志池名称，名称保存后不支持修改
   - 存储周期：范围支持1-3000天，保存后支持修改
   - 分区数：范围支持2-64天，保存后支持修改 点击“确定”完成日志池创建。

编辑日志池

1. 登录金山云日志服务Klog控制台。
2. 在控制台点击**项目列表** > **项目详情页** > **概览**，选中某一日志池，点击**编辑**进入到编辑页面。
   - 存储周期：修改存储周期后，存储周期会在第二天生效，比如今天把存储周期从6天调整为2天后，超出存储周期的4天数据不会被立即删除，会在第二天对超出存储周期范围的数据做删除操作。

- 分区数：修改分区数后会立即生效。

删除日志池

删除日志池后，日志池中的所有日志数据以及日志池相关联的告警、图表会被一起清除，且不可恢复，请谨慎操作。

klog-filebeat

klog-filebeat介绍

Filebeat是由Elastic开发的一款开源日志采集软件，使用者可以将其部署到需要采集日志的机器上对日志进行采集，并输出到指定的日志接收端如elasticsearch、kafka、logstash等等。KLog团队对开源Filebeat进行了二次开发并提供新增特性，我们称之klog-filebeat，其新增特性如下：

- 支持输出日志到klog：
  - 支持输出到多个项目和日志池
  - 可为每个日志池配置过滤器，让只有符合条件的日志条目输出到对应的日志池
  - 可选择仅输出部分字段
  - 支持动态加载access_key、secret_key
- 支持通过grok方式解析日志，将普通文本解析为json对象。

关于Filebeat自身的详细特性，可以参考filebeat官方文档。

前提条件

1. 已创建项目和日志池。更多信息，请参见项目和日志池。
2. 已开通服务器的80端口和443端口。
3. 已完成Klog-Filebeat环境配置。

下载

- 最新Linux版本的klog-filebeat可以点击此处下载。
- 或直接在您的服务器上下载：

```
wget "https://ks3-cn-beijing.ksyun.com/klog/filebeat/klog-filebeat.latest.tar.gz"
```

安装

安装比较简单，解压缩到您需要的路径即可：

```
tar xvf klog-filebeat.latest.tar.gz
```

运行

执行如下命令，运行klog-filebeat。

```
./filebeat -e
```

采集器配置

klog-filebeat需要2个配置文件，分别是filebeat.yml和credential.ini，这两个配置文件均在klog-filebeat压缩包中，解压后即可看到。

credential.ini

这个配置文件的内容是您的金山云access_key和secret_key。内容示例：

```
[klog]
access_key = AKLT6-bcdesfg-ajsIjfiejI9
secret_key = Jf2390j9E9finfiDIOFJFD8483+dfsDVdOCTFazCnDEAw+mxA/7Lfeh3ugErwoKKb5wNOIei==
```

filebeat.yml

这个是主配置文件，内容示例如下：

```
filebeat.inputs:
- type: log
  enabled: true
  paths:
    # 需要采集的日志文件
    - /var/log/*.log

output.klog:
  endpoint: https://klog-cn-beijing.ksyun.com
  credential:
    path: credential.ini
    check_interval: 60
  targets:
    - project_name: yourProjectName
      pool_name: yourPoolName
      fields:
        - key: message
```

关于output.klog的详细配置说明可参考下面的yml文件完整配置。其余详细配置可参考filebeat官方文档。

注意：在输出到klog的情况下，filebeat的modules功能无法使用。

yml文件完整配置

文件完整示例以及配置项含义分别如下：

```
# ------------------------------ Filebeat Input ------------------------------
filebeat.inputs:
- type: log
  enabled: true

  # 需要采集的日志文件
  paths:
    - /your/app/log/path.log

  # 如果您的日志是以json形式打印的，则可设为true或false，这样filebeat会自动解析json内容。
  # 设置为false时，解析出来的map对象存在于filebeat事件对象的名为json的字段中。
  # 设置为true时，解析出来的map对象的各字段直接存在于filebeat事件对象中。
  # 删除这个配置项时，日志作为普通文本，存在于filebeat事件对象的message字段中。
  json.keys_under_root: false

# ------------------------------ KLog Output -------------------------------

# klog-filebeat特有配置。表示将采集到的日志发送到klog服务端。
output.klog:
  # klog服务的日志接收地址。如果使用内网域名，请使用http协议
  endpoint: https://klog-cn-beijing.ksyun.com

  # 最大批量条数，默认为2048
  bulk_max_size: 2048

  # 用于发送的协程数，默认为1
  worker_num: 1

  # 发送时使用的压缩传输方式，默认为lz4。取消压缩写none
```

```
  compress_method: lz4

  # 从哪个文件读取您在金山云的 access_key 和 secret_key
  credential:
    # 文件路径
    path: credential.ini

    # 每隔多少秒检查一次ini文件的修改时间。如果发生改变，则重新加载ini
    check_interval: 60

  # 发送到指定的klog项目和日志池。每个target代表一对项目和日志池。
  # 可以设置多个target, 各target之间支持重复设置项目和日志池。
  targets:
      # 目标项目名称
    - project_name: yourProjectName

      # 使用字段yourField1的值作为目标项目名称。
      # project_name和project_name_from_field可以只配置其中一项。如果两项同时配置，则优先使用project_name_from_field。
      # project_name_from_field: yourField1

      # 目标日志池名称
      pool_name: yourPoolName

      # 使用字段yourField2的值作为目标日志池名称。
      # pool_name和pool_name_from_field可以只配置其中一项。如果两项同时配置，则优先使用pool_name_from_field。
      # pool_name_from_field: yourField2

      # 需要发送的段，可以设置多个，不设置则为发送事件的所有字段。
      fields:

        # 需要发送的字段名。字段名里面不可有"."
        - key: message

          # 该字段是map类型时，如果设置为true，则表示只发送它的后代字段。默认为false。
          skip_root: false

      # 过滤器。可以设置多个。匹配所有过滤器的日志条目将会发送到该target。未配置filters的，会全部发送。
      filters:
          # 对哪个字段过滤
        - key: message

          # 阈值。支持字符串和数值。所有数值在内部都转换成float64
          value: ""

          # 比较符。支持的计算有：>, >=, <, <=, ==, !=, exists, not_exists, contains（仅字符串）, not_contain（仅字符串）
          operator: "!="

# ------------------------------ Klog新增的处理器 -------------------------
  processors:

  #grok处理器可以把普通文本日志解析为json对象。
  #由于grok是基于正则表达式的，所以开启该选项会增加filebeat的资源消耗。
  - grok:
      # 解析哪个字段
      source_field: message

      # 解析结果保存到哪个字段
      target_field: yourField3

      # 用于解析的表达式
      pattern: "%{IPORHOST:client} %{WORD:method} %{URIPATHPARAM:request} %{INT:size} %{NUMBER:duration}"

      # 用于解析的自定义表达式，不是必填的
      patterns:
        MYPATTERN: "\\d+"
```

- 说明：数据解析时，如果存在需要跳过的字符，对字符做解析后不设置字段名称即可，具体示例如下。 原始日志数据内容如下：

  ```
  127.0.0.1 - - [26/Mar/2020:19:09:19 -0400] "GET / HTTP/1.1" 401 - "" "Mozilla/5.0 Gecko" "-"
  ```

  数据解析表达式如下：

  ```
  pattern: "%{IPORHOST}\s-\s-\s\[%{HTTPDATE:timestamp}\]"
  ```

  通过如上表达式，只解析出timestamp字段对应的内容”26/Mar/2020:19:09:19 -0400“。

filebeat事件

filebeat事件是原生Filebeat数据处理过程中的重要概念。

Filebeat采集到的每条日志，在Filebeat内部都表示为一条事件数据。 Filebeat对日志数据字段的读取、转换和新增都是对事件字段的操作。一条简单的事件数据如下：

```
{
    "@timestamp": "2020-09-21T03:08:07.682Z",
    "@metadata": {
        "beat": "filebeat",
        "type": "_doc",
        "version": "7.9.1"
    },
    "log": {
        "offset": 423019,
        "file": {
            "path": "/path/to/your.log"
        }
    },
    "message": "2020-09-21 03:08:07.682 [INFO][47] ipsets.go 304: Finished resync family=\"inet\" numInconsistenciesFound=0 resyncDuration=2.18885ms",
    "input": {
        "type": "log"
    },
    "ecs": {
        "version": "1.5.0"
    },
    "host": {
        "name": "filebeat-cwssh"
    },
    "agent": {
        "name": "filebeat-cwssh",
        "type": "filebeat",
        "version": "7.9.1",
        "hostname": "filebeat-cwssh",
        "ephemeral_id": "decf7010-9f78-41f7-85b6-7a0cc5ba4115",
        "id": "7b2bc79a-9da8-4038-ba55-993af4d9ac71"
    }
}
```

filebeat使用字段massage保存日志原始内容。 在配置filebeat.yml时，可以使用诸如"message"、"log.file.path"、"host.name"、"json.field1"等形式表示事件的字段。

API上传数据

简介

日志服务KLog产品为用户提供数据上传的API，API文档详见Putlogs。接下来介绍如何把原始日志数据序列化成如下格式的Protocol Buffer数据流，然后才能通过API写入服务端。

步骤一、定义Protocol格式

按照如下格式，生成一个klog.proto文件

```
syntax = "proto3";
package klog;

message Log
{
    message Content
    {
        required string key   = 1; // 每组字段的 key
        required string value = 2; // 每组字段的 value
    }
    required int64 time = 1; // 时间戳，UNIX时间格式
    repeated Content contents = 2; // 一条日志里的多个kv组合
}
message LogGroup
{
    repeated Log    logs        = 1; // 多条日志合成的日志数组
    optional string reserved    = 2; // 目前暂无效用
    optional string filename    = 3; // 日志文件名
    optional string source      = 4; // 日志来源，一般使用机器IP
}
```

- 说明：关于Protocol Buffer格式的更多信息请参见Github首页。

步骤二、编译Protocol Buffers

根据上面的内容，定义数据的报文格式后，运行Protocol Buffer编译器，把上面的klog.proto文件编译成特定语言的类。这些类提供了简单的方法访问每个字段，像是访问类的方法一样将结构序列化或反序列化。

- 说明：如需安装编译器，可前往Protobuf版本页选择版本和语言。

这里使用proto编辑器生成Java语言的文件，在klog.proto文件的同一目录下，执行如下编辑命令

```
protoc.exe --java_out=./ klog.proto
```

- 说明：--java_out=./表示编译成 Java 格式并输出当前目录下，./klog.proto表示位于当前目录下的 klog.proto 描述文件。

编辑成功后，输出对应语言的代码文件，这里会生成klog.java文件。

步骤三、调用

将生成的klog.Java和klog.proto文件复制到工程目录下参与编译就可以。

简介

在使用KLog进行日志数据检索、SQL查询分析之前，请先配置索引规则。字段索引规则包括全文索引、字段索引两部分。

索引类型	说明
全文索引	以文本形式为所有字段的Value创建索引，并根据分词符对Value进行分词。
字段索引	配置字段索引后可根据指定字段做数据查询、聚合统计。

说明

- 同时配置全文索引和指定字段索引的情况下，以指定字段索引的配置为准。
- 当某个字段配置了字段索引时，则该字段的全文索引仍会生效。
- 如果字段不配置字段索引，该字段不能进行聚合统计等查询操作。

索引配置

配置索引

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**日志搜索**，选择某一日志池。

3. 点击页面右上角的**配置索引**，开始配置索引。

- 索引状态

  默认开启状态，开启状态下，支持全文索引和字段查询索引两种；关闭状态下，无法进行全文检索和字段检索，但可以使用SQL查询进行数据筛选。

- 全文索引

参数	说明
区分大小写	关闭区分大小写，查询时关键词不区分大小写；开启区分大小写，查询时关键词区分大小写
分词符	根据指定分词符，将日志数据的Value切分成多个关键词

- 字段查询

参数	说明
字段名称	日志字段名称，必填项
数据类型	必选项，日志字段值的数据类型，支持text、long、double、date四种数据类型
别名	选填项，字段的别名，可以使用别名进行数据查询，多个字段的数据别名可以相同，相同情况下，会按照别名进行跨字段查询

区分大小写 默认关闭，关闭区分大小写，查询时关键词不区分大小写；开启区分大小写，查询时关键词区分大小写
分词符 字段数据类型为text时，支持设置分词符对Value进行分词；根据指定的分词符，将日志数据的Value切分成多个关键词

4. 点击**确定**，完成索引属性配置。

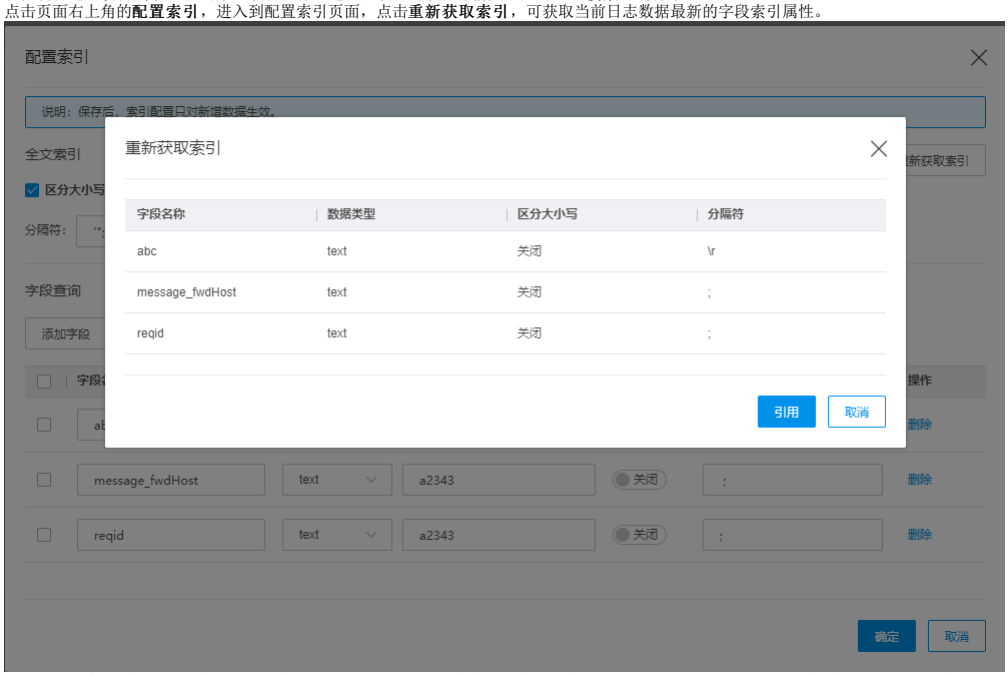
   说明

   - 保存索引配置后，索引配置只对保存配置后写入的数据生效。如需查询历史数据，需根据历史索引配置进行查询。

重新获取索引

当实际日志数据发生改变时，之前保存的索引配置已经无法满足当前的数据查询需求，需要重新配置索引规则。

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**日志搜索**，选择某一日志池。
3. 点击页面右上角的**配置索引**，进入到配置索引页面，点击**重新获取索引**，可获取当前日志数据最新的字段索引属性。



4. 重新获取的索引属性不支持修改，如需修改，可以先点击**引用**，把索引属性自动加载到**配置索引**页面后，再根据业务情况自定义配置索引。
5. 点击**确定**，完成索引配置。

日志搜索

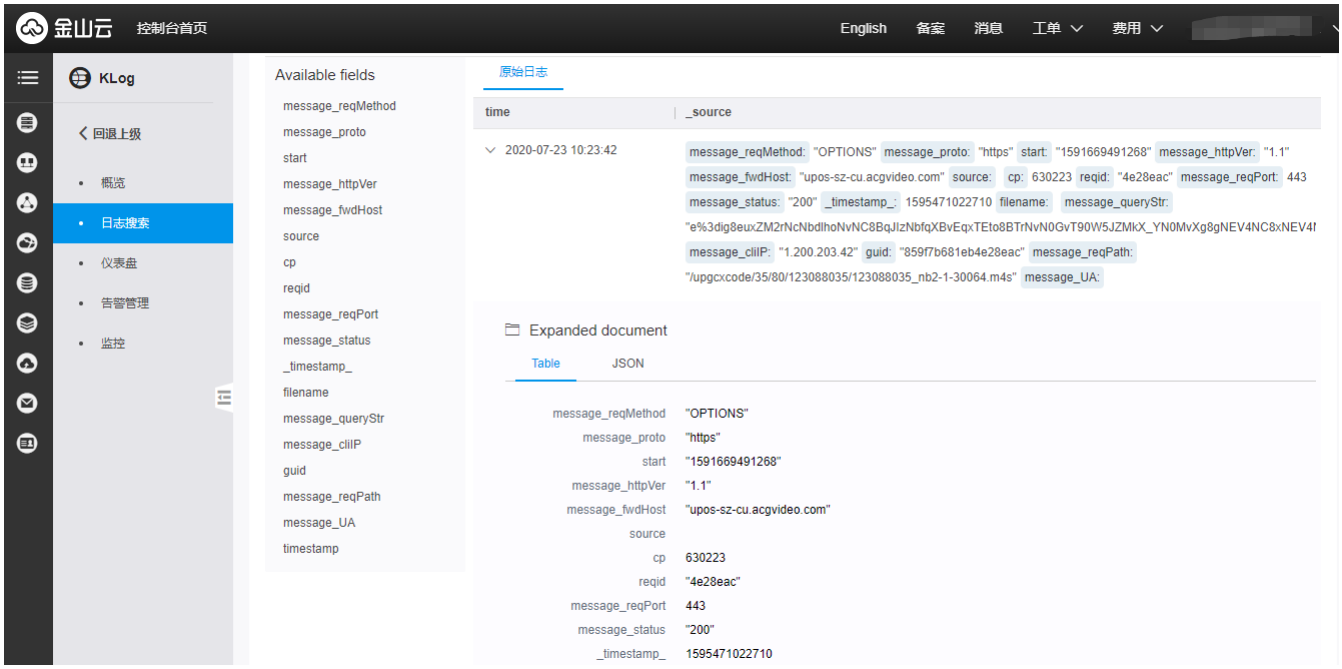
查询数据

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**日志搜索**，进入到日志搜索页面。
3. 选择日志池、查询时间范围，并输入查询语句，并点击**查询**，即可在下方查看到返回的数据结果。
   - 产品支持全文检索、键值对检索和SQL查询，用户可以在输入框中输入检索语句或者SQL语句，通过检索语句检索并返回原始日志；通过SQL语句查询并返回聚合或者筛选后的数据表格。具体详见查询语法。
   - 查询语句中的使用限制详见使用限制。

数据查询结果

原始日志

在输入框中输入检索语句后，在“原始日志”查看到返回的原始日志数据内容。点击左侧的下拉按钮，数据以表格和json方式展示内容详情。

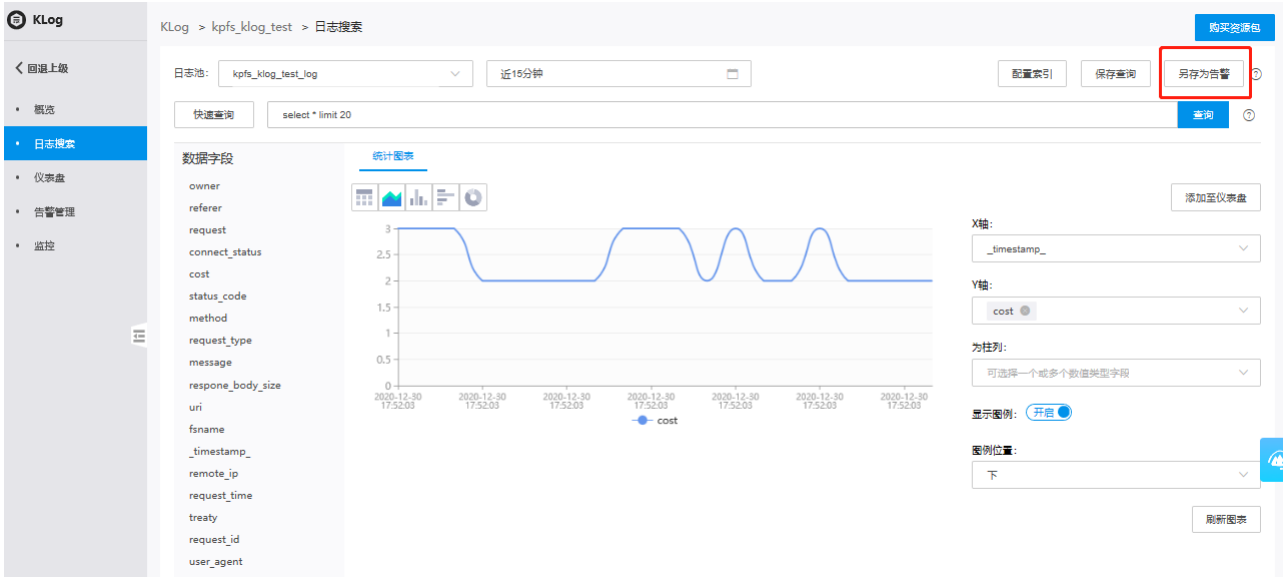


统计图表

使用SQL语句查询数据后，在“统计图表”查看到数据返回结果，默认显示表格样式。可以修改图表类型（比如折线图, 柱状图，饼图等）。具体详见图表。

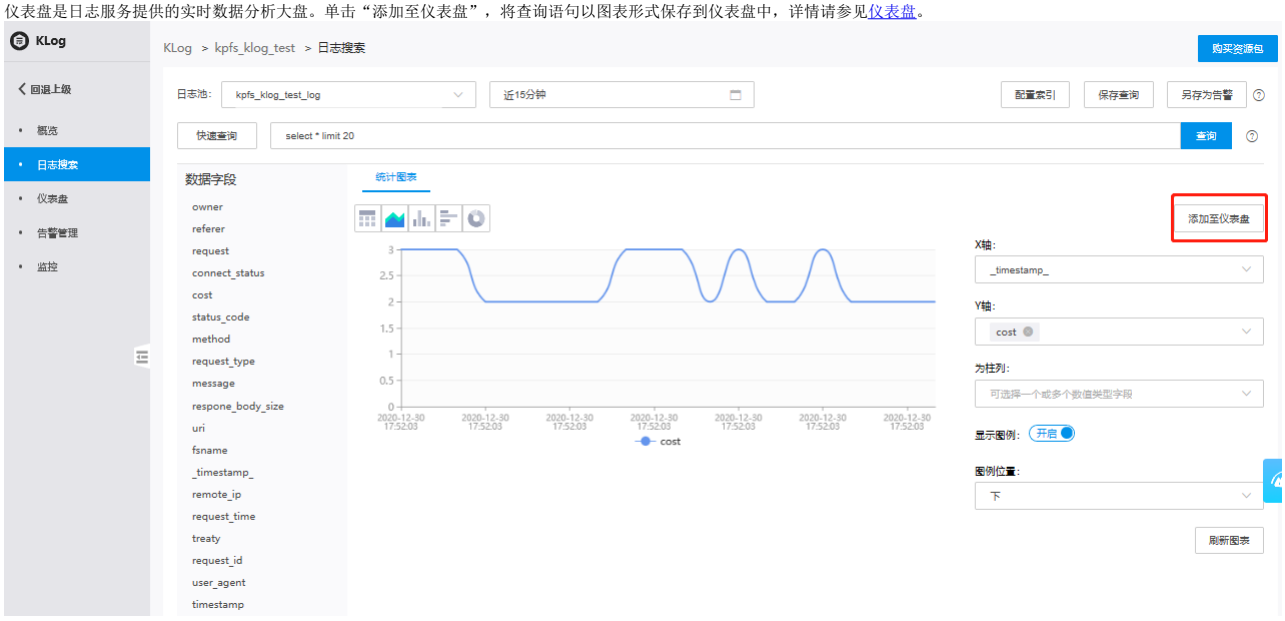
另存为告警

在查询分析页面上，单击**另存为告警**，可为查询结果设置告警。



添加至仪表盘

仪表盘是日志服务提供的实时数据分析大盘。单击“添加至仪表盘”，将查询语句以图表形式保存到仪表盘中，详情请参见仪表盘。



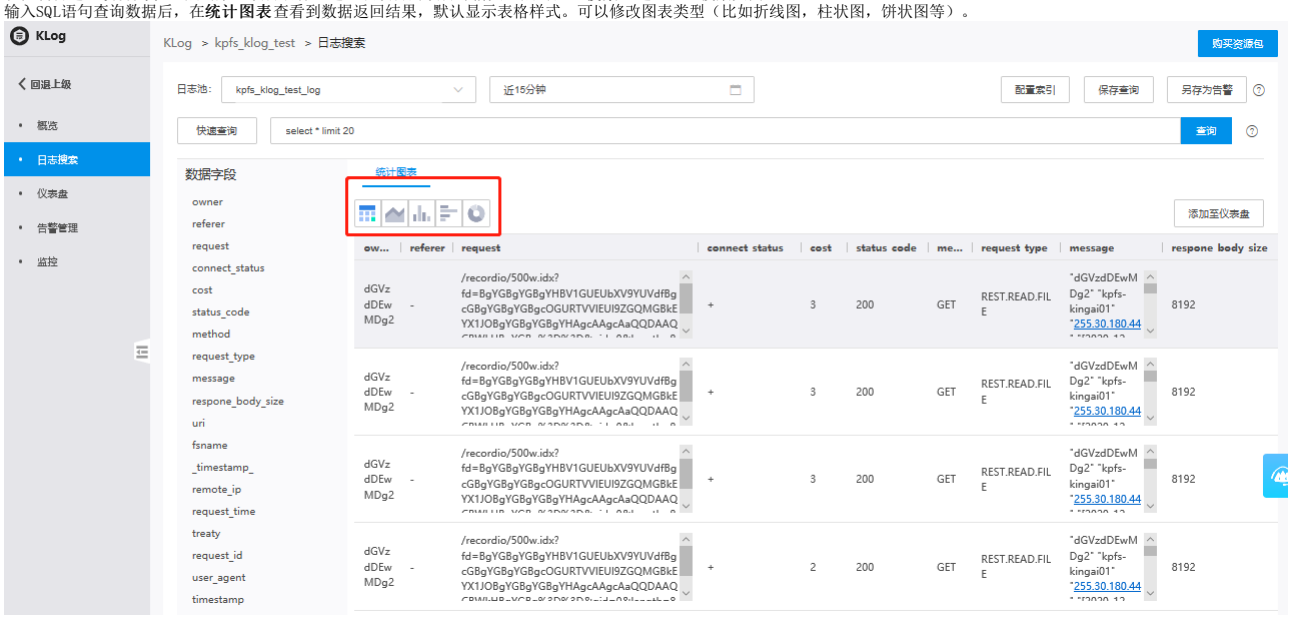
统计图表

前提条件

已对当前日志池配置索引规则。 **注意：** 只有在日志搜索时使用SQL分析语句，才能根据统计结果为您展示图表。

统计图表

1. 登录[金山云日志服务Klog控制台](#)。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**日志搜索**，进入日志搜索页面。
3. 输入SQL语句查询数据后，在**统计图表**查看到数据返回结果，默认显示表格样式。可以修改图表类型（比如折线图，柱状图，饼状图等）。

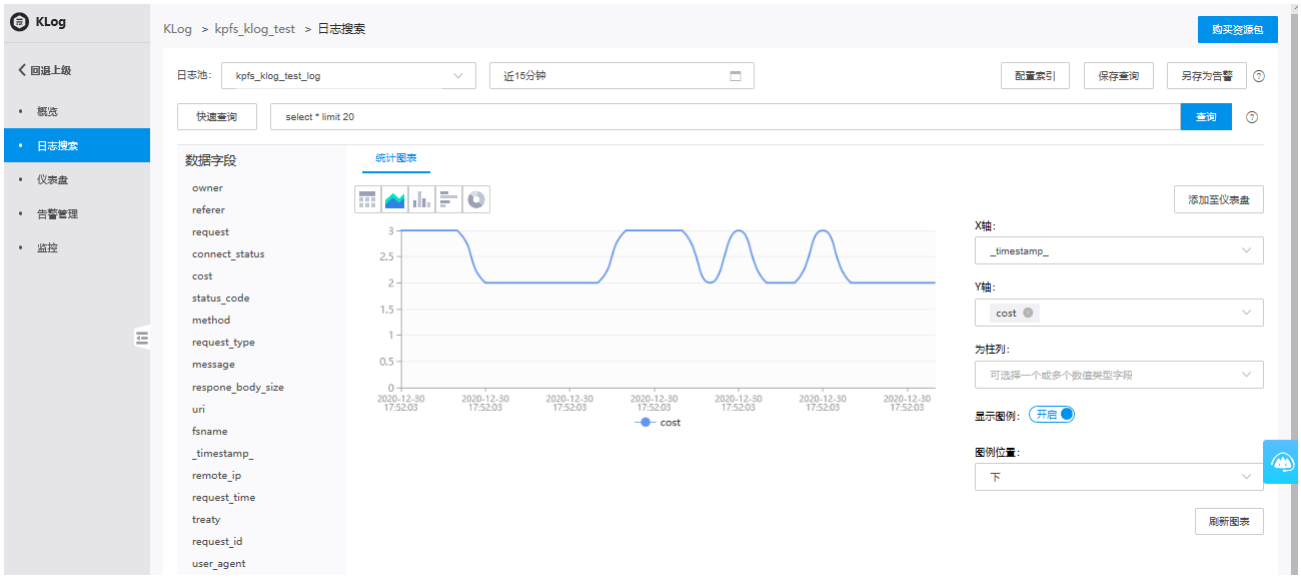


select * limit 20

ow...	referer	request	connect status	cost	status code	me...	request type	message	respone body size
dGVz dDEw MDg2	-	/recordio/500w.idx? fd=BgYGBgYGBgYHBV1GUEUbXV9YUVdfBg cGBgYGBgYGBgcOGURTVVIEUI9ZGQMGBkE YX1JOBgYGBgYGBgYHAgcAAgcAaQQDAAQ	+	3	200	GET	REST.READ.FILE	"dGVzdDEwMDg2" "kpfs-kingai01" "255.30.180.44	8192
dGVz dDEw MDg2	-	/recordio/500w.idx? fd=BgYGBgYGBgYHBV1GUEUbXV9YUVdfBg cGBgYGBgYGBgcOGURTVVIEUI9ZGQMGBkE YX1JOBgYGBgYGBgYHAgcAAgcAaQQDAAQ	+	3	200	GET	REST.READ.FILE	"dGVzdDEwMDg2" "kpfs-kingai01" "255.30.180.44	8192
dGVz dDEw MDg2	-	/recordio/500w.idx? fd=BgYGBgYGBgYHBV1GUEUbXV9YUVdfBg cGBgYGBgYGBgcOGURTVVIEUI9ZGQMGBkE YX1JOBgYGBgYGBgYHAgcAAgcAaQQDAAQ	+	3	200	GET	REST.READ.FILE	"dGVzdDEwMDg2" "kpfs-kingai01" "255.30.180.44	8192
dGVz dDEw MDg2	-	/recordio/500w.idx? fd=BgYGBgYGBgYHBV1GUEUbXV9YUVdfBg cGBgYGBgYGBgcOGURTVVIEUI9ZGQMGBkE YX1JOBgYGBgYGBgYHAgcAAgcAaQQDAAQ	+	2	200	GET	REST.READ.FILE	"dGVzdDEwMDg2" "kpfs-kingai01" "255.30.180.44	8192

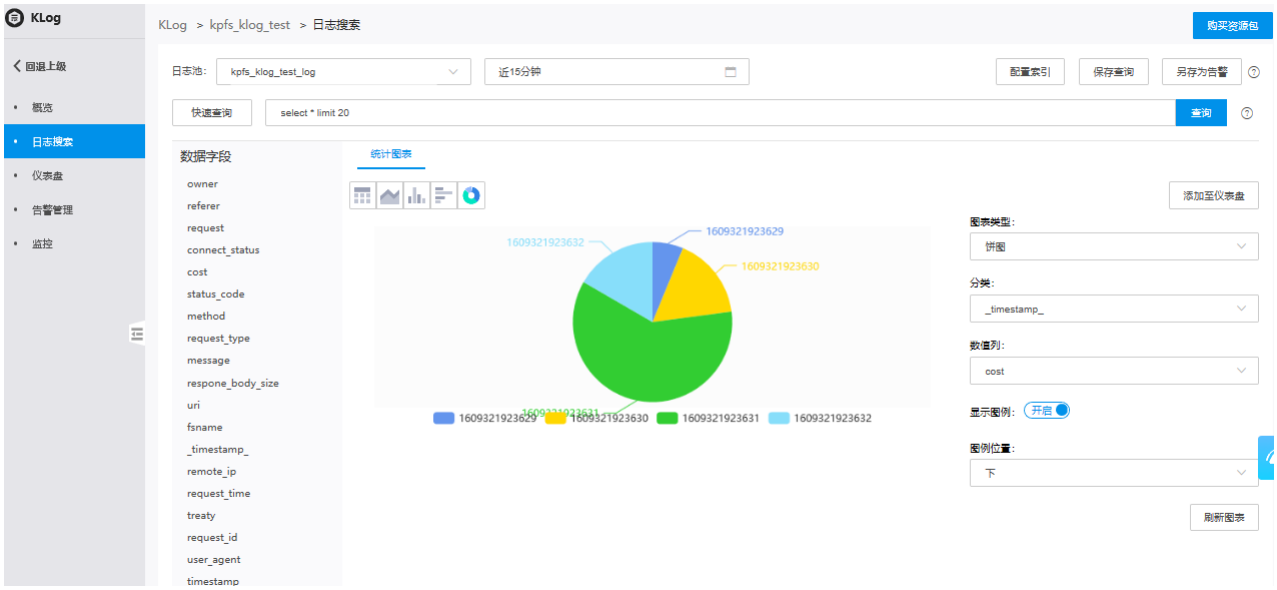
制作图表

折线图： 选择图表类型为**折线图**，在右侧设置X轴、Y轴字段，X轴只需要选中一列字段，Y轴可以选中多个字段，每个字段会对应显示一个折线。

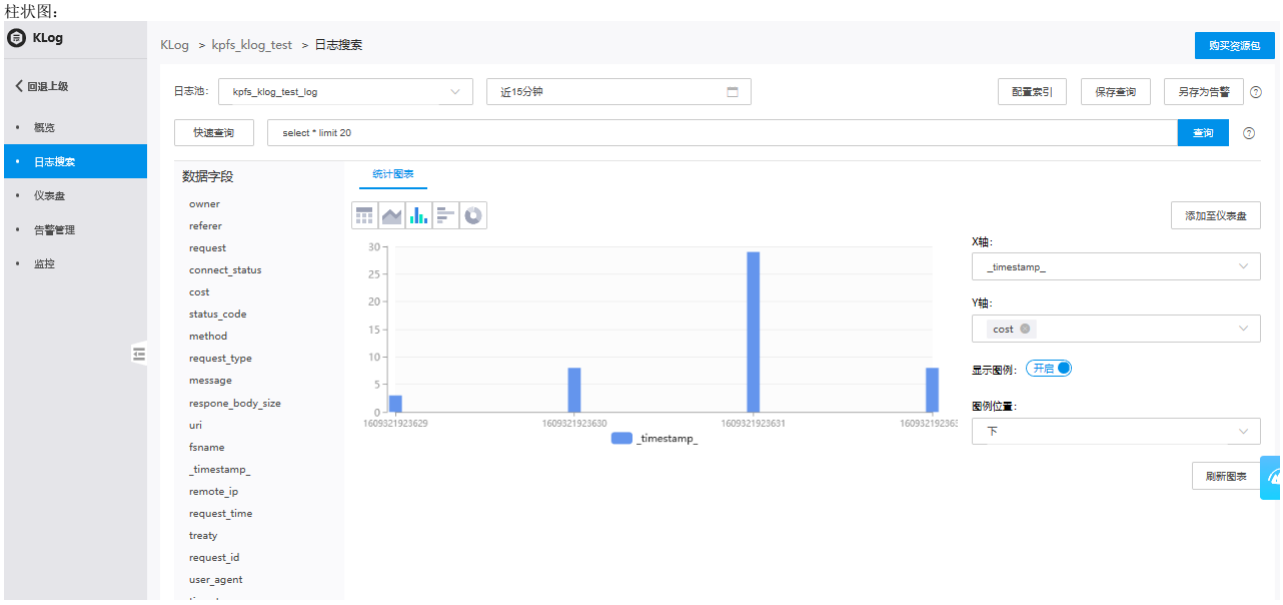


通过类似的操作，还可以制作饼图、柱状图等。

饼状图：



柱状图：



添加至仪表盘

制作完图表后，如需保留图表以便于随时查看该图表，可点击**添加至仪表盘**，填写新仪表盘名称或者选择已有仪表盘，填写图表名称后，即可把当前图表保存到指定仪表盘中。

仪表盘

创建仪表盘

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**仪表盘**进入到仪表盘列表页。页面显示当前项目下已有的仪表盘。
3. 点击创建仪表盘按钮来创建新的仪表盘。您也可以在日志搜索页面，点击图标右侧的添加至仪表盘来创建新的仪表盘。

修改仪表盘

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**仪表盘**进入到仪表盘列表页。
3. 点击某一仪表盘名称，进入该仪表盘详情页。点击**修改仪表盘**，该仪表盘进入到编辑状态。

编辑图表

鼠标移入某个图表右上角的更多图标，点击**编辑图表**，弹出图表编辑框。填写图表信息后，点击**刷新图表**加载出编辑后的图表效果，点击**确定**完成编辑。

- 说明：编辑图表后，需点击页面右上角的**保存**，当前修改的内容才会保存到仪表盘中

删除图表

如需删除仪表盘中的图表，点击图表右上角的**删除图表**，即可删除当前图表。

简介

日志服务支持为查询或分析结果设置告警。设置告警后，日志服务定期检查查询或分析结果，当检查结果满足预设条件时发送告警通知，实现实时的服务状态监控。

告警限制

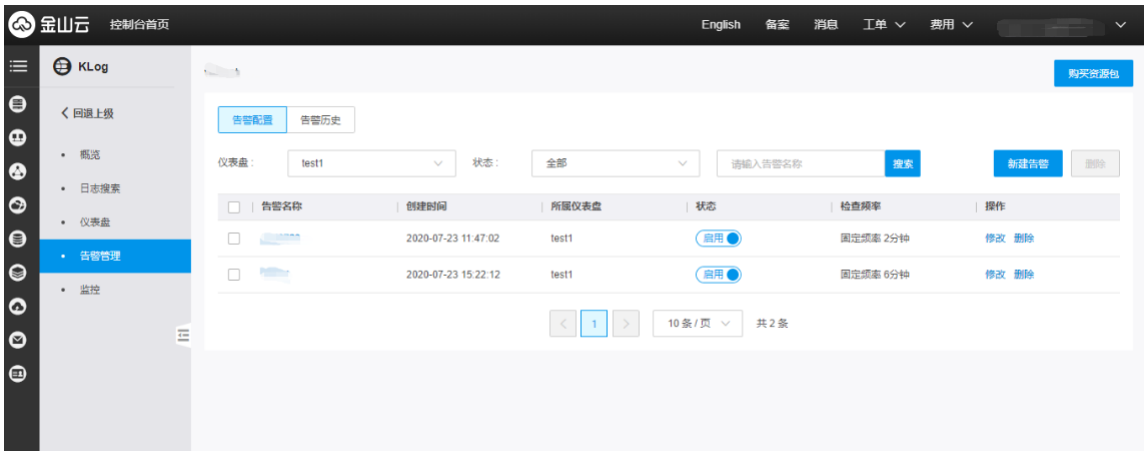
日志服务告警相关限制说明如下表所示。

限制项	说明
告警名称	支持2-64个字符，仅允许字母、中文、数字和-_@#.
图表名称	支持小写字母、数字、连字符（-）和下划线（_），需要以数字或小写字母为开头和结尾
检查频率	支持检测周期和检测间隔的自由组合，其中，检测周期可选固定间隔、每天、每周、每小时，而检测间隔则可选择小时/分钟/天
触发条件	支持加(+)、减(-)、乘(*)、除(/)、4种基础运算符和>、>=、<、<=、==、!= 6种比较运算符，&&、2种逻辑运算
通知方式	提供短信和邮件两种通知方式

告警管理

告警列表

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**告警管理**，进入到告警列表页。



用户可通过筛选仪表盘、告警状态以及输入告警名称来查询指定的告警。

修改告警状态

在告警列表中的状态一栏，点击**禁用**或者**启动**来修改当前告警的状态。 启动状态下，服务会按照执行频率定时执行告警规则。当满足触发告警通知时，以短信、邮件方式实时发送告警消息。 禁用状态下，则不再执行告警规则，也不会触发告警。

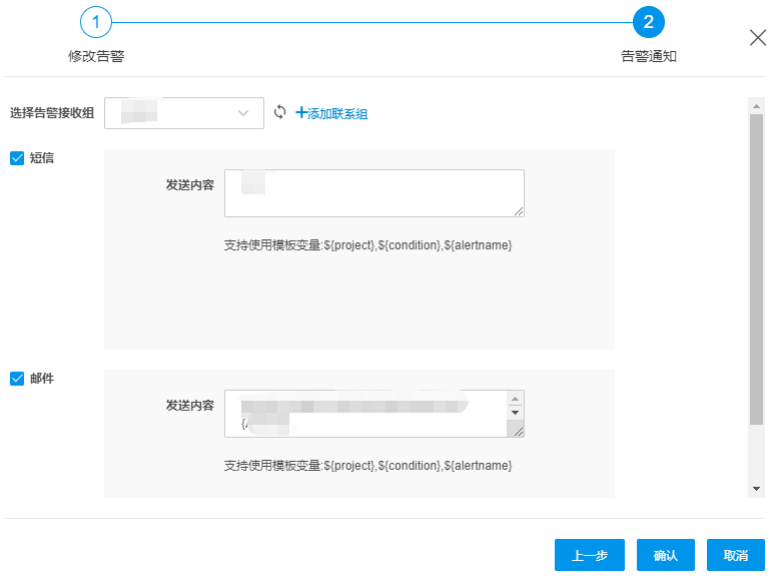
新建告警

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**告警管理**，进入到告警列表页。
3. 在告警列表页，点击**新建告警**，进入到新建告警页面。

- 告警名称：必填项，名称支持2-64个字符，仅允许字母中文数字-_@#.
- 仪表盘：必选项，选择当前已有仪表盘
- 关联图表：基于所选图表的数据内容来配置告警出发规则，支持关联同一仪表盘下的多个图表；每个图表具备一个序列号，例如：第一个图表的序列号为0，第二个图表序列号为1，以此类推。
- 检查频率：该告警执行数据查询的频率，支持固定间隔和crontab模式。其中，固定间隔支持分钟、小时、天粒度的间隔。

  cron表达式说明如下：
  0/5 从0分钟开始，每隔5分钟发送一次
  0 0/1 *从0点0分开始，每隔1小时发送一次*
  0 18 每天18点0分发送一次
  0 0 1 每月1日0点0分发送一次

- 触发条件：通过表达式来设置触发告警的条件，支持加(+)、减(-)、乘(*)、除(/)、4种基础运算符和>、>=、<、<=、==、!= 6种比较运算符,&&、|| 2种逻辑运算
- 触发次数阈值：触发告警的次数上限，当某次执行中查询到满足表达式的数据，累计1次，当累计值达到触发次数阈值时，会触发告警。
- 通知间隔：发送告警通知的时间间隔。比如设置5分钟间隔时，会每隔5分钟查看当前累计触发次数是否超出阈值，超出时则发送告警。 点击下一步，设置告警通知方式。



- 选择告警接收组：告警通知会发送给接受组下的用户。如果没有接受组，需先添加联系组。
- 短信和邮件：选中发送通知方式，并填写报警内容，内容支持使用模板变量。 点击”确定“完成告警创建。

修改告警

修改告警后，会按照修改后的告警规则来执行告警判断。修改告警中各项配置项的逻辑请参照上面的创建告警。

告警详情

点击某一告警名称，进入到告警详情页。

- 告警统计：告警次数是指昨天触发告警的次数之和；通知成功次数是指昨天告警通知发送成功的次数之和；日环比是昨天跟前天的环比。
- 告警历史：告警规则执行的历史记录。

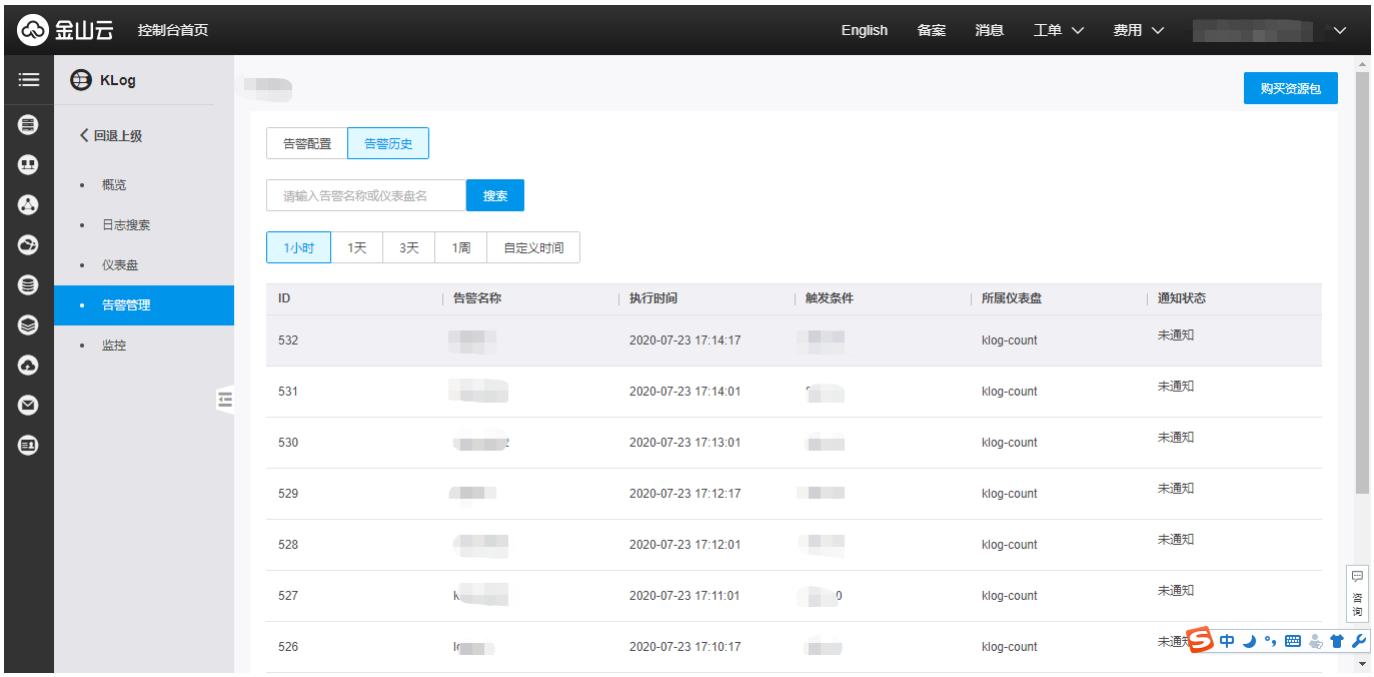
查看告警历史

告警历史

告警历史主要展示已有告警的执行历史记录。

1. 登录金山云日志服务Klog控制台。
2. 从控制台进入**项目列表**，点击某一项目名称，进入该项目的项目详情页，点击**告警管理**，进入到告警列表页。
3. 在告警列表页，点击**告警历史**。

告警历史页面显示当前项目下所有告警规则的执行记录。可通过告警名称、仪表盘名称、时间范围来筛选历史记录。



检索语法

检索规则

在进行日志搜索前，需先选择日志池、时间范围，以及在输入框中输入检索语句。产品支持全文检索、键值检索和模糊关键字检索。

全文检索

日志服务会根据分词符将每条日志数据拆分为多个词组，以支持您根据特定的关键字来检索日志。全文检索支持普通查询、短语查询和模糊查询。

- 普通查询：直接输入关键字，或者指定字段和关键字，将返回符合关键字的数据结果。例如 `method:GET and status=200` 表示查询 `method` 是 `GET` 并且 `status` 等于 `200` 的日志。
- 短语查询：如果需要查询的关键字中包含检索语法运算符或空格，可以将关键字用双引号（""）包裹，表示将双引号中的内容作为多个关键字查询。例如 `msg:"not avaliable"` 表示 `msg` 查询包含关键字 `not` 和 `avaliable` 的日志，等价于查询 `msg:service and msg:"not" and msg:avaliable`。 模糊查询：支持关键字中间或末尾加上模糊查询字符（ * 和 ?）。例如 `http_user:andr?` 表示在所有日志中查找 `http_user`字段包含以 `andr` 开头的词的日志。

键值检索

用户可以指定字段名称和字段内容进行查询。对于double和long类型的字段，可以指定数值范围进行查询。例如查询语句为count>5000 and Status:200，表示查询count值大于5000且Status字段值为200的日志。

运算符语法

语法	语义
key:value	键值搜索格式，默认开启所有字段的索引，其中 value 支持?、*模糊搜索
A and B	“与”逻辑，返回 A 与 B 的交集结果，如果多个单词间没有语法关键词，默认是 and 的关系
A OR B	“或”逻辑，返回 A 或 B 的并集结果
exists	返回结果中，需要有该字段
missing	返回结果中，不能含有该字段
?	匹配单个字符，用于替代单个字符
*	匹配0到多个字符
TO	range 用法，如status:[400 TO 499]，或status:[400 TO 499} ’}’为不包含499
>	返回字段下大于某个数值的日志
>=	返回字段大于或等于某个数值的日志
<	返回字段小于某个数值的日志
<=	返回字段小于或等于某个数值的日志
=	返回字段等于某个数值的日志
!a:b	返回a字段不包含b的数据

SQL语法

语法支持

日志服务支持基础的 SELECT 查询，具体查询语法是

```
select_expr [, select_expr] ...
[WHERE where_condition]
[GROUP BY {col_name | expr}, ... ]
[ORDER BY {col_name | expr} [ASC | DESC], ...]
[LIMIT [offset,] row_count]
```

说明：SQL查询语法使用限制详见使用限制。

运算符

比较函数

运算符	含义
<	小于
>	大于
<=	小于或等于
>=	大于或等于
=	等于
<>	不等于

|BETWEEN|查询处于两个参数之间的数据| |IS NULL/IS NOT NULL|判断参数是否是Null值|

逻辑运算函数

运算符	含义
AND	只有左右运算数都是true时，结果才为true
OR	左右运算数任一个为true，结果为true
NOT	右侧运算数为false时，结果才为true

真值表

a	b	a AND b	a OR b
TRUE	TRUE	TRUE	TRUE
TRUE	FALSE	FALSE	TRUE
TRUE	NULL	NULL	TRUE
FALSE	TRUE	FALSE	TRUE
FALSE	FALSE	FALSE	FALSE
FALSE	NULL	FALSE	NULL
NULL	TRUE	NULL	TRUE
NULL	FALSE	FALSE	NULL

数学计算函数

运算符	含义
+	两个参数相加
-	两个参数相减
*	两个参数相乘
/	两个参数相除求整数
%	两个参数相除求余数
log10(x)	返回以10为底，x的对数
round(x)	x四舍五入

聚合函数

运算符	含义	示例
avg(x)	计算x列的算数平均值	select avg(request_time) as avg_times
count(*)	表示所有的行数	select count(*) where method = GET
max(x)	返回最大值	select max(request_time) as max_times
min(x)	返回最小值	select min(request_time) as min_times
sum(x)	返回x列的和	select sum(request_time) as sum_times
stats(x)	返回x列的聚合计算结果，包括avg、max、min、sum等	-
data_histogram(x, interval)	根据指定间隔获取所有匹配的值	select data_histogram(timestamp) where status_code=200