ALIBABA CLOUD

阿里云

云防火墙

日志

文档版本：20210610

阿里云

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

目录

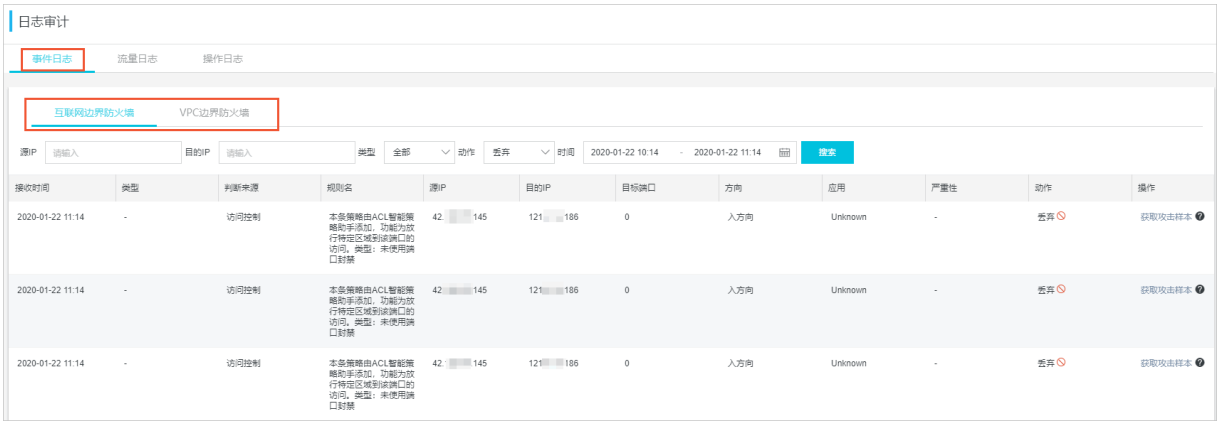
1.日志审计

通过云防火墙的所有流量会在**日志审计**页面记录下来，包括流量日志、事件日志和操作日志，帮助您实时审计您的网络流量，并为您对可疑流量进行相应的处理提供依据。云防火墙日志审计默认保留7天。

云防火墙还提供日志分析功能，可存储6个月内的日志数据。如果您有等保合规的需求，建议开通日志分析服务。日志分析的费用说明请参见日志分析计费方式。

事件日志

事件日志包括经过互联网边界防火墙和VPC边界防火墙的流量相关的事件日志。您可以单击**互联网边界防火墙**或**VPC边界防火墙**页签查看相应事件的日志详情，包括事件的时间、威胁类型、源IP和目的IP、应用类型、严重性等级以及动作状态等信息。

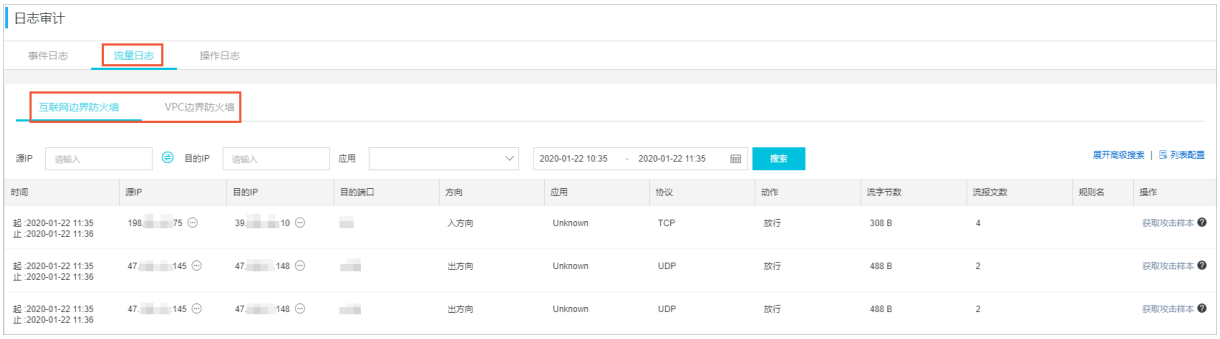


您可在**事件日志**列表上方输入源IP、目的IP、类型、动作或自定义时间范围等信息检索您需要查看的日志。

> **说明** 可设置的自定义时间为7天以内。

流量日志

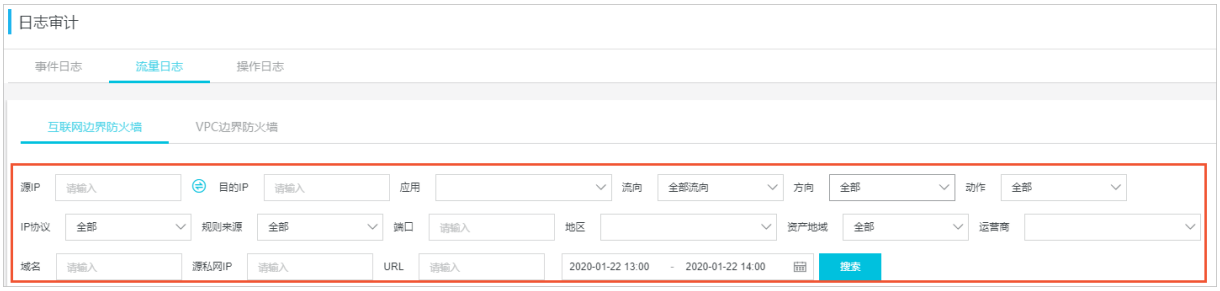
流量日志包括经过互联网边界防火墙和VPC边界防火墙的流量的日志记录。您可以单击**互联网边界防火墙**或**VPC边界防火墙**页签查看相应流量日志详情，包括访问流量开始和结束的时间、源IP和目的IP、应用类型、源端口、应用、支持的协议、动作状态、字节数以及报文数等信息。



您可在**流量日志**列表中输入源IP、目的IP、应用和自定义时间范围等信息搜索流量日志。

> **说明** 可设置的自定义时间为7天以内。

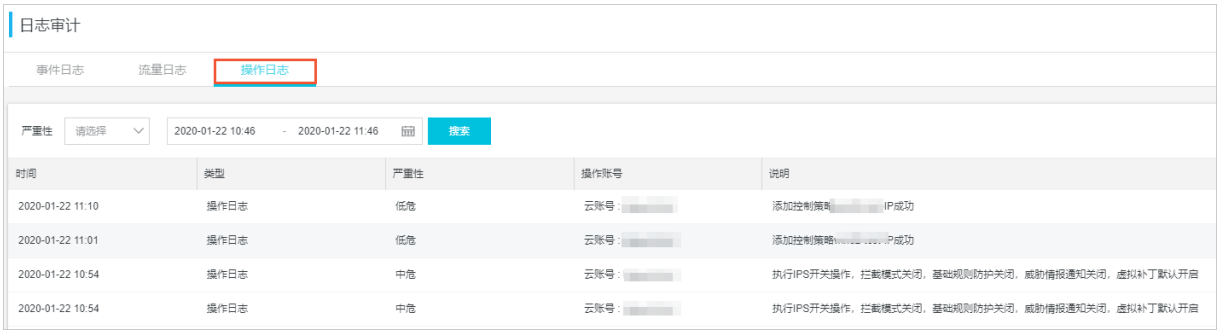
单击搜索栏右侧的**展开高级搜索**，可以通过**方向**、**规则来源**、**端口**、**资产地域**等高级搜索条件精确定位您的筛选范围。



说明 如果流量匹配中了访问策控制策略或IPS入侵防御策略，流量日志**规则名**一栏会展示匹配中的策略的名称；未匹配中策略的流量**规则名**一栏则为空。

操作日志

操作日志记录云防火墙中的所有操作执行的时间、操作类型、严重性以及具体操作信息。



您可在**操作日志**列表中选择**严重性**等级来筛选对应的操作记录。

您也可设置自定义时间范围搜索相关的日志。可设置的自定义时间为7天以内。

2.日志分析

2.1. 概述

阿里云云防火墙与日志服务打通，对外开放访问流量日志，提供云防火墙日志实时分析服务。

云防火墙日志实时分析可以实时地自动采集并存储出入方向的流量日志，并基于日志服务，输出查询分析、报表、报警、下游计算对接与投递等能力，帮助您专注于分析，远离琐碎的查询和整理工作。

功能优势

云防火墙日志实时查询分析服务具有以下功能优势：

- **等保合规**：存储网站六个月以上的访问日志，助力网站符合等保合规要求。
- **配置灵活**：轻松配置即可实现互联网流量日志的实时采集。
- **实时分析**：依托日志服务产品，提供实时日志分析能力、开箱即用的报表中心，让您对经过云防火墙的互联网流量以及用户访问细节了如指掌。
- **实时告警**：支持基于特定指标定制准实时的监测与告警，确保在关键业务发生异常时能第一时间响应。

前提条件与限制

要使用云防火墙进行日志实时分析，必须满足以下前提条件：

- 开通阿里云日志服务。
- 开通阿里云云防火墙（高级版、企业版或旗舰版），并购买了日志分析服务。

云防火墙所存储的日志库属于专属日志库，有如下限制：

- 用户无法通过API/SDK等方式写入数据，或者修改日志库的属性（例如存储周期等）。

  > **说明** 支持其他日志库功能（例如查询、统计、报警、流式消费等），且与一般日志库无差别。

- 日志服务不对专属日志库计费，但日志服务本身需处于可用状态（不超期欠费）。
- 内置报表可能会发生更新和升级。

应用场景

- 追踪互联网流量日志，溯源安全威胁。
- 实时查看互联网请求活动，洞察状态与趋势。
- 快速了解安全运营效率，及时反馈处理。
- 输出日志到自建数据与计算中心。

2.2. 日志分析计费方式

云防火墙日志服务根据您选择的日志存储时长和日志存储容量进行计费，采用预付费（包年包月）的方式。

您可以在云防火墙购买页面中，选择开通日志服务，并根据实际需要选择日志存储时长和日志存储容量的规格。云防火墙将根据您选定的日志存储规格和云防火墙实例的购买时长来计算费用。

日志存储规格

云防火墙日志服务不同的日志存储规格收费如下：

日志存储时长	日志存储容量	适用带宽	推荐使用的版本	中国内地地域实例	
				包月费用	包年费用8.5折
180天	1 TB	适用月带宽不高于10 Mbps的业务场景	高级版	500元	5,100元
	5 TB	适用月带宽不高于50 Mbps的业务场景	企业版	2,500元	25,500元
	20 TB	适用月带宽不高于200 Mbps的业务场景	旗舰版	10,000元	102,000元

说明 如您需要扩展带宽，每增加10 Mbps带宽建议扩展1 TB的日志存储空间。

日志存储容量满额说明

如果您购买的日志存储容量已经满额，系统将自动提醒您升级容量。您可以随时通过**升级容量**的方式进行扩容。

注意

- 云防火墙基础版和免费试用版不支持日志分析功能。如果您使用的是云防火墙基础版或免费试用版，控制台将不会展示日志存储容量。如何开通云防火墙服务的日志分析功能，请参见开通日志分析服务。
- 如果日志存储容量已满的时候您未及时升级容量，云防火墙将停止向日志分析服务的专属日志库写入新的日志数据，日志库中已存储的日志数据会被保留。如果您的日志数据存储超过180天或者日志分析服务到期7天后未续费，日志库中的所有日志数据将自动释放。日志数据释放后将无法恢复。

购买时长

云防火墙日志服务的购买时长与您购买的云防火墙包年包月实例绑定。

- **新购**：在新购云防火墙包年包月实例时，系统将根据您选择的实例购买时长计算日志服务的费用。
- **升级**：通过升级已购买的云防火墙包年包月实例开通日志服务时，系统将根据您现有云防火墙实例的剩余时长（精确到分钟级别）计算日志服务的费用。

服务到期说明

如果您购买的云防火墙实例即将到期，日志分析服务也将同时到期。

- 服务到期后，云防火墙将停止向日志分析服务的专属日志库写入日志数据。
- 服务到期后，云防火墙日志服务中的日志数据将为您保留7天。7天内完成续费您可以继续使用云防火墙日志服务功能；如未能及时完成续费，所有已存储的云防火墙日志将被清空。

相关文档

日志相关问题

2.3. 开通日志分析服务

开通云防火墙服务后，您可以在云防火墙控制台开通日志分析功能。

适用范围

云防火墙**日志分析**功能可自动采集实时的互联网流量日志，并对采集到的日志数据进行实时检索与分析，以丰富的仪表盘形式展示查询结果。您可以在购买开通云防火墙日志服务时，根据实际需要选择**日志存储容量**大小。

> **说明** 云防火墙**日志分析**功能对云防火墙高级版、企业版、旗舰版开放。

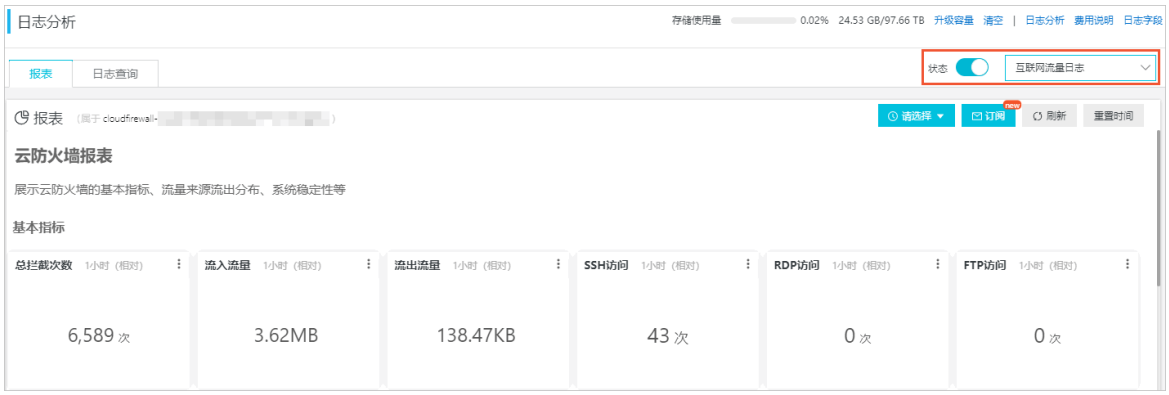
开通云防火墙日志分析功能

1. 登录云防火墙控制台。
2. 在左侧导航栏，单击**日志 > 日志分析**。
3. 单击**立即开通**。

4. 在**日志分析**模块单击*是*，并根据您的业务需要选择**日志存储容量**，单击**去支付**完成支付。

> **说明** 关于云防火墙日志服务收费标准，参考计费方式。

5. 在云防火墙控制台**日志分析**页面，选择已接入云防火墙防护的**互联网流量日志**，单击**状态**开关，开启云防火墙互联网流量日志的采集功能。



日志分析将实时采集云防火墙记录的所有出/入方向的互联网流量日志，并根据采集到的日志数据进行实时检索与分析。

2.4. 日志采集

您可以在云防火墙管理控制台为云防火墙开启日志采集功能。

前提条件

- 已购买开通云防火墙。

- 已开通云防火墙日志分析服务。

背景信息

请勿随意删除或修改日志服务为您创建的默认Project、Logstore、索引和仪表盘设置。日志服务将不定期更新、升级云防火墙日志查询与分析功能，专属日志库中的索引与默认报表也会自动更新。

日志服务支持实时采集**阿里云云防火墙**出入方向的互联网流量日志，并支持对采集到的日志数据进行实时检索与分析，以仪表盘形式展示查询结果。您可以通过日志对网站的访问和攻击行为进行即时分析研究，从而协助安全管理人员制定防护策略。

开通云防火墙日志分析后，日志服务会在您的账号下自动创建一个专属日志库和专属Logstore（cloudfirewall-logstore），云防火墙自动将日志实时导入该专属日志库中，该日志库不支持通过包括API或SDK在内的任何方式写入其他数据。专属日志库和专属Logstore等默认配置请参见默认配置。

如果您的子账号需要使用云防火墙日志查询分析功能，需要为其授予日志服务相关权限。具体操作方式请参见子账号日志查询分析授权。

日志服务对专属日志库不进行任何收费，但您账号中的日志服务产品需处于正常使用状态。

> **说明** 当您的日志服务产品出现欠费时，云防火墙日志采集功能将暂停工作，及时补缴欠款后采集功能将自动恢复。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏，选择**日志 > 日志分析**。
3. 在**日志分析**页面单击右上角**状态**开关开启日志采集功能。

日志分析默认配置

默认配置项	配置内容
Project	云防火墙自动为您创建日志分析的Project。Project名称根据您的云防火墙实例的地域决定。 ○ 中国内地地域的云防火墙实例的Project名称：cloudfirewall-project-*阿里云账户ID*-cn-hangzhou ○ 杭州金融云用户默认Project名称：cloudfirewall-project-*阿里云账户ID*-cn-hangzhou-finance ○ 除中国内地地域和金融云以外其他地域的云防火墙实例的Project名称：cloudfirewall-project-*阿里云账户ID*-ap-southeast-1

默认配置项	配置内容
Logstore	默认为您创建Logstore（ cloudfirewall-logstore ）。 云防火墙日志采集到的所有日志数据都将保存在该Logstore中。专属日志库的存储周期等基本设置不支持修改。 **说明** 专属日志库在查询、统计、报警、流式消费等功能上均无特殊限制。
地域	○ 云防火墙实例地域为中国内地地域的，默认Project保存在杭州地域。 ○ 云防火墙实例地域为其他地域的，默认Project保存在新加坡地域。
Shard	默认为您创建2个Shard，并开启自动分裂Shard功能。
仪表盘	默认为您创建的仪表盘。

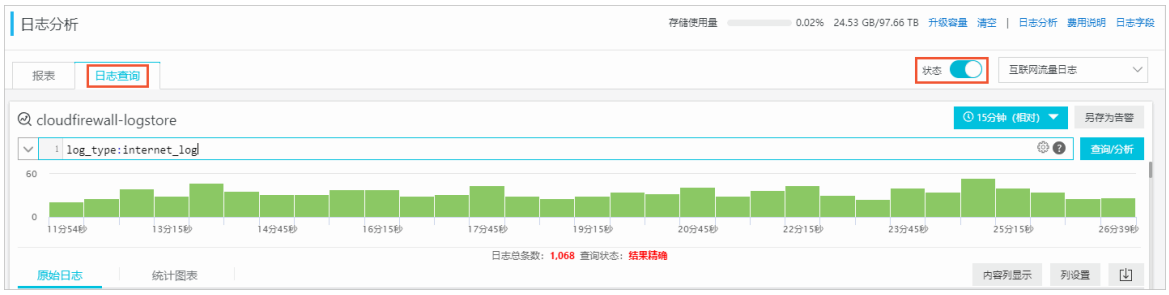
说明 日志分析的默认配置项不支持修改。

2.5. 日志查询

在云防火墙管理控制台开通日志服务后，即可在日志服务实时查询分析功能页面，对采集到的日志数据进行实时查询与分析、查看或编辑仪表盘、设置监控告警等操作。

操作步骤

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**日志 > 日志分析**。
3. 单击**日志查询**页签切换到日志查询页面。
4. 开启右侧的**状态**开关。



5. 输入需要查询的分析语句，选择日志时间范围后，单击**查询/分析**。

更多操作说明

在日志分析页面，您还可以对查询到的日志数据进行以下操作：

- **自定义查询与分析**

  日志服务定义了一系列查询语法和分析语法，支持多种复杂场景下的日志查询。更多详细介绍，请参考自定义查询与分析。

- **查看日志的时间分布**

  搜索框下方展示了符合查询时间和查询语句的日志的时间分布情况，以时间为横轴、数量为纵轴的柱状图形式展示。并显示查询到的日志总数。

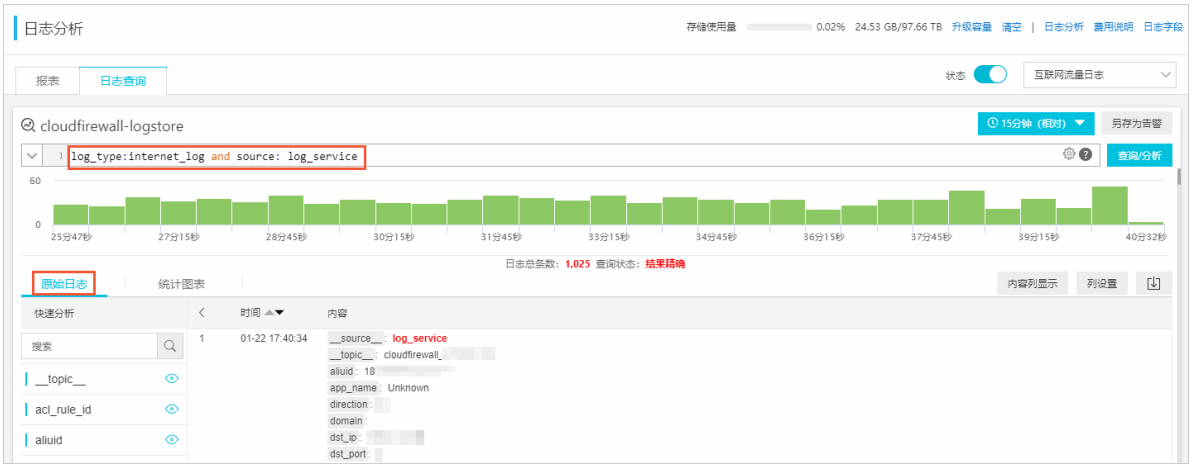
  > **说明** 您可以在柱状图上按住鼠标左键拖拽选择更小范围的时间区域，`时间选择器`将自动更新为选择的时间范围，并展示所选择时间范围内的结果。

- **查看原始日志**

  在**原始日志**页签中，以分页的形式展示每一条日志的详细内容，包括时间、内容以及其中的各个字段。您可以单击**内容列显示**设置内容列中长字符的显示效果（**整行**或**换行**）、单击**列设置**选择特定的字段进行展示或单击日志下载按钮 将当前查询结果下载至本地。

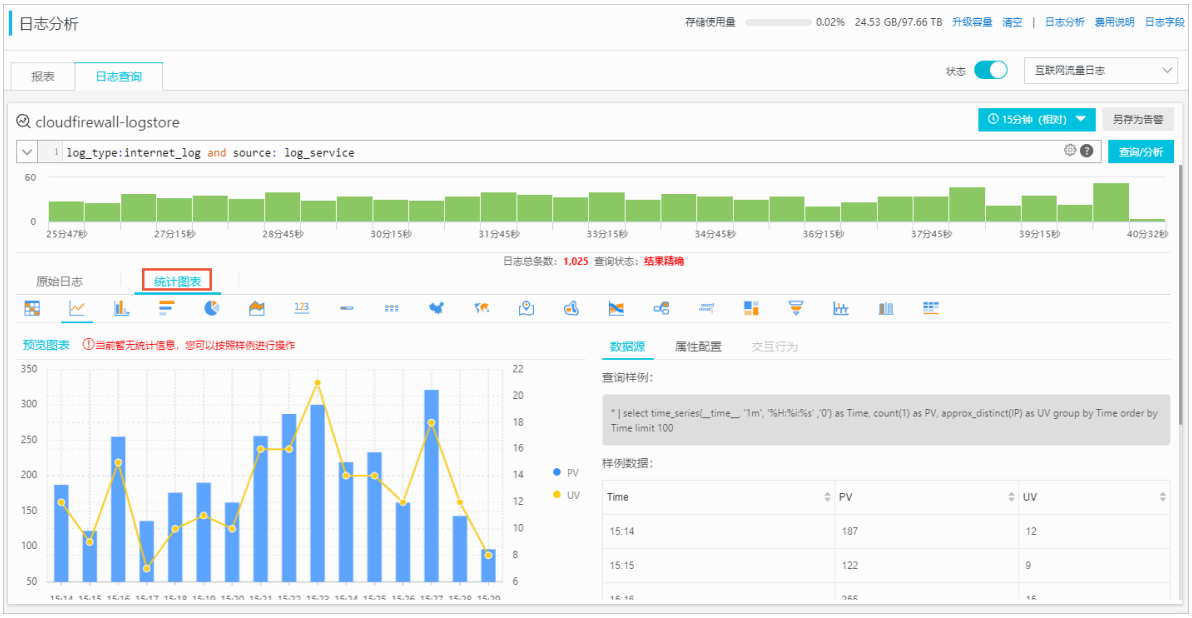
  同时，在内容列中单击相应字段的值或分词，搜索框中将自动增加相应的搜索条件。例如，单击`__source__: log_service`中的值`log_service`，搜索框中将自动增加更新为以下查询语句，并展示相应的查询结果：

  ```
  原来的搜索语句 and source: log_service
  ```



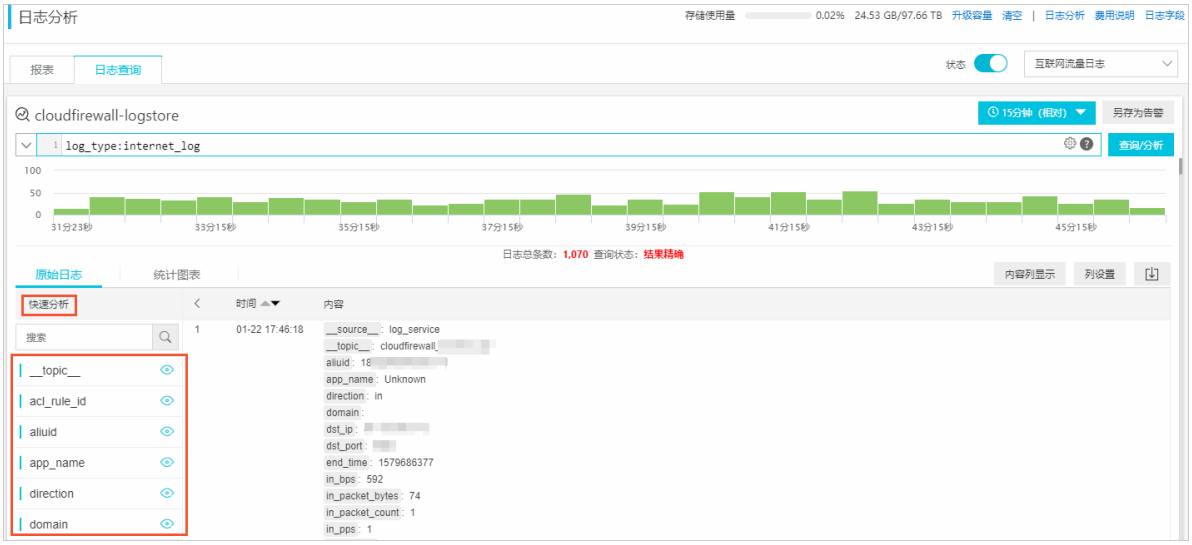
- **查看分析图表**

  日志服务支持以图表形式展示分析结果，您可以在**统计图表**页面根据需要选择不同的图表类型。更多详细介绍，请参考分析图表。



- **快速分析**

  原始日志页签中的快速分析功能为您提供一键交互式查询体验，帮助您快速分析某一字段在一段时间内的分布情况，减少索引关键数据的时间成本。更多详细介绍，请参考快速分析。



自定义查询分析

日志查询语句由查询语法（Search）和分析语法（Analytics）两个部分组成，中间通过 | 进行分割：

```
$Search | $Analytics
```

类型	说明
查询（Search）	查询条件，由关键词、模糊、数值、区间范围和组合条件等产生。如果为空或 * ，则代表查询所有数据。
分析（Analytics）	对查询结果或全量数据进行计算和统计。

> **说明** 查询和分析两部分均为可选。
> - 当Search部分为空时，代表针对该时间段所有数据不进行任何过滤，直接对结果进行统计。
> - 当Analysis部分为空时，代表只返回查询结果，不进行统计。

查询语法

日志服务查询语法支持**全文查询**和**字段查询**，查询框支持换行显示、语法高亮等功能。

- **全文查询**

  无需指定字段，直接输入关键字进行全文查询。您可以用双引号（""）包裹关键字查询包含该完整关键字的日志，也可以用空格或 and 分割查询多个关键字。

  示例

  - **多关键字查询**

    搜索包含所有 www.aliyun.com 和 error 的日志。

    www.aliyun.com error 或者 www.aliyun.com and error

- **条件查询**

  搜索所有包含 `www.aliyun.com`，并且包含 `error` 或者 `404` 的日志。

  ```
  www.aliyun.com and (error or 404)
  ```

- **前缀查询**

  搜索所有包含 `www.aliyun.com`，并且以 `failed_` 开头的日志。

  ```
  www.aliyun.com and failed_*
  ```

  > **说明** 查询中只支持后缀添加 `*`，但不支持以 `*` 作为前缀（如 `*_error`）。

- **字段查询**

  基于字段进行更精准的查询。

  字段查询支持数值类型字段的比较查询，格式为 `字段: 值` 或 `字段 >= 值`。同时，通过 `and`、`or` 等可进行组合查询，并支持与全文搜索组合使用。

  > **说明** 云防火墙日志服务支持基于字段查询。关于日志中各个字段的含义、类型、格式等信息，请参考云防火墙日志字段说明。

  示例

  - **查询多字段**

    如果要搜索指定客户端 `1.2.3.4` 访问目的地址 `1.1.1.1` 的访问日志，您可以设置以下查询条件：

    ```
    src_ip: 1.2.3.4 and dst_ip: 1.1.1.1
    ```

    > **说明** 本示例中的 `src_ip` 字段和 `dst_ip` 都是云防火墙记录的日志字段。

  - **查询字段是否存在**
    - 查询包含 `total_pps` 字段的日志。

      ```
      total_pps: *
      ```

    - 查询不包含 `total_pps` 字段的日志。

      ```
      not total_pps: *
      ```

关于日志服务支持的查询语法完整说明，请参考索引与查询。

分析语法

您可以使用SQL/92语法对日志数据进行分析与统计。

关于日志服务支持的语法与函数说明，请参考实时分析。

> **说明**
> - 分析语句中可以省略SQL标准语法中的 `from 表格名` 语句，即 `from log` 语句。
> - 日志数据默认返回前100条，您可以通过LIMIT 语法修改返回范围。

查询分析示例

基于日志时间的查询分析

每一条云防火墙记录的日志都存在 `time` 字段，用于表示日志的时间，格式为 `年-月-日T时:分:秒+时区` 。例如， `2018-05-31T20:11:58+08:00` ，其中时区为 `UTC+8` 区，即北京时间。

同时，每条日志都拥有一个内置字段， `__time__` 。该字段也表示该条日志的时间，以便在统计时进行基于时间的计算，其格式为*Unix时间戳*，其本质是一个自从1970-1-1 0:0:0 UTC时间开始的累计经过的秒数。因此在实际使用时，经过可选的计算后，需要经过格式化才能进行展示。

- **选择并展示时间**
- **计算时间**
- **基于特定时间分组统计**

> **说明** 您也可以使用折线图方式进行展示。

更多关于时间解析的函数，例如将一个时间格式转化为另外一个格式，需要使用 `date_parse` 与 `date_format` 函数，相关具体说明，请参考日期和时间函数。

2.6. 日志报表

云防火墙日志分析报表为您展示日志分析功能采集到的流量基本指标、流量流入和流出分布等数据。您可通过修改时间范围、订阅日志报表、设置刷新等操作，查看多种筛选条件下的仪表盘数据。

前提条件

查看日志报表前，请确认**日志分析**页面右侧的日志**状态**为**开启**。日志**关闭**状态下您将无法查看日志报表。

操作步骤

1. 登录云防火墙控制台。

2. 在左侧导航栏，选择**日志 > 日志分析**。
3. 在**报表**页面单击右上角**请选择**。

4. 在**时间**页面设置云防火墙的互联网流量日志报表显示的时间范围。支持选择**相对时间**、**整点时间**或**自定义**时间段。

时间类型	描述
相对时间	展示距离当前时刻、过去的某个时间段内（精确到秒）的日志数据。例如：2019-10-17 23:07:00~2019-10-17 23:08:00表示距离当前时刻（2019-10-17 23:08:00）过去1分钟内的日志数据。 支持自定义时间段（可精确到天、小时、分钟、秒）。
整点时间	展示距离当前整点时刻、过去的某个整点时间段内的日志数据。例如：2019-10-10 00:00:00~2019-10-17 00:00:00表示距离当前整点时刻过去的一周内的日志数据。 支持自定义时间段（可精确到天、小时、分钟）。
自定义时间	展示自定义的时间段内的日志数据。支持时间设置精确到分钟。

设置时间范围后，报表页面的所有仪表盘模块均会刷新展示该时间范围内的流量数据。

仪表盘模块说明请参见日志报表仪表盘。

> **说明** 时间选择器仅在当前页面临时生效，系统不保存该设置。您下次重新打开该报表页面时，仪表盘将恢复到默认时间范围。

5. （可选）在**报表**页面，操作单个仪表盘模块。您可单击目标仪表盘模块右上角的  按钮，打开其选项菜单。

   仪表盘模块的选项菜单支持以下操作：

   - **选择时间区域**：选择相对时间、整点时间或自定义时间后，该仪表盘会展示所选定时间范围内的基本指标数据。具体操作请参见时间设置。
   - **下载日志**：单击**下载日志**直接保存日志的Excel文件至本地计算机。
   - **下载图表**：单击**下载图表**直接保存图表的PNG图片至本地计算机。
   - **预览查询语句**：单击  ，查看仪表盘对应基本指标的查询语句。您可以使用该查询语句在日志查询页签中查询对应的日志数据。有关日志查询的详细内容请参见日志查询。

6. （可选）订阅日志报表，按照您设置的时间通过邮件或钉钉群机器人给您发送日志信息。

   单击页面右上角的**订阅**，在**新建订阅**页面添加互联网流量日志报表的订阅。

   i. 在**订阅配置**页签，进行以下配置。

配置项名称	描述
订阅名称	日志报表的订阅名称。系统显示默认设置，可自定义。
频率	订阅的日志报表发送通知的频率。可选值： ■ **每小时**：每小时发送一次订阅通知。 ■ **每天**：每天的某个整点时间（00:00~23:00）发送一次订阅通知。 ■ **每周**：每周的某天中某个整点时间（00:00~23:00）发送一次订阅通知。 ■ **固定间隔**：自定义的固定间隔时间，可选择**天**或**小时**。 ■ **Cron**：使用Cron表达式自定义订阅频率。Cron表达式的最小精度为分钟，格式为24小时制。您可参考界面举例自定义频率。
添加水印	图片自动加载通知渠道地址（邮箱或钉钉群机器人WebHook地址）作为水印。

ii. 单击**下一步**，设置通知类型。

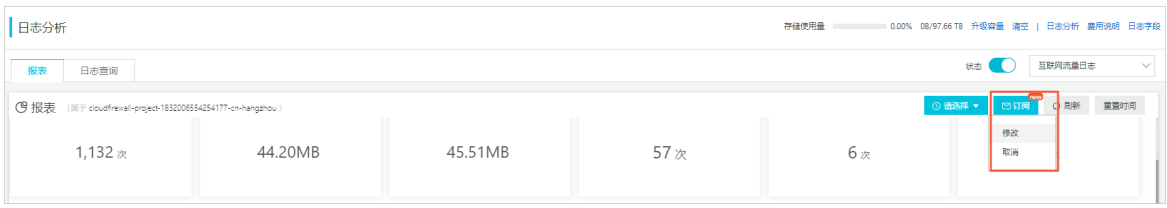
通知类型	参数名称	描述
邮件	**收件人**	收件人邮箱地址，支持添加多个收件人。
	主题	邮件主题，系统显示默认设置，可自定义。
WebHook-钉钉机器人	**请求地址**	WebHook请求地址。地址获取方法请参见配置钉钉机器人通知。
	标题	WebHook标题，系统显示默认设置，可自定义。

iii. 单击**提交**完成订阅创建。

iv. 单击**确定**确认订阅配置修改情况。

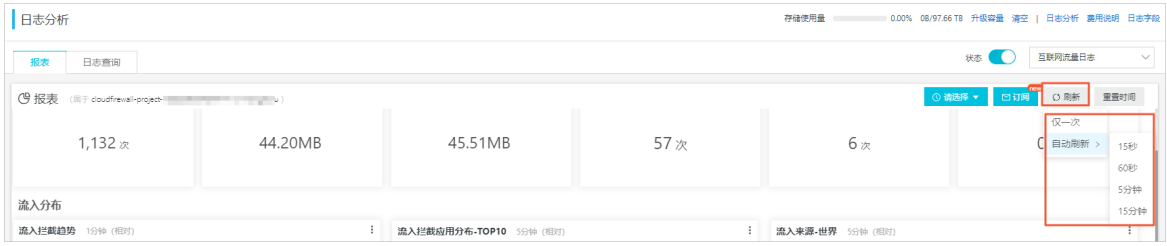
创建订阅后，鼠标移动至**报表**页面的**订阅**，可查看已创建的订阅信息。

单击**订阅**可**修改**订阅配置、通知类型，或**取消**订阅。



> **说明** 云防火墙仅支持创建一个订阅，**取消**已添加订阅后，可创建新的订阅。

7. （可选）单击**报表**页面右上角的**刷新**，设置日志报表刷新频率。



频率	描述
仅一次	立即触发一次刷新。
自动刷新	设置定时刷新频率。可选每15秒、60秒、5分钟或15分钟刷新一次。

日志报表仪表盘

云防火墙的日志报表提供了互联网流量相关的全局视图，包括流量的基本指标、流入和流出的趋势、分布等。下表描述了云防火墙支持的所有仪表盘。

图表	类型	默认时间范围	描述	样例
总拦截次数	数值	1小时（相对）	某个时间范围内，统计云防火墙拦截互联网的访问次数。	10次
流入流量	数值	1小时（相对）	某个时间范围内，统计互联网流入方向的流量值。	10 MB
流出流量	数值	1小时（相对）	某个时间范围内，统计互联网流出方向的流量值。	10 GB
SSH访问	数值	1小时（相对）	某个时间范围内，统计SSH的访问次数。	10次
RDP访问	数值	1小时（相对）	某个时间范围内，统计RDP的访问次数。	10次
FTP访问	数值	1小时（相对）	某个时间范围内，统计FTP的访问次数。	10次
流入拦截趋势	线图	1小时（相对）	某个时间范围内，流入方向拦截次数的变化趋势图。	无
流入拦截应用分布-TOP10	饼图	1小时（相对）	某个时间范围内，统计前10名流入方向拦截的应用类型（例如HTTP、SNMP、SIP、SSH等）分布情况。	无
流入来源-世界	地图（全球）	1小时（相对）	某个时间范围内，流入方向访问源的地理分布。	无

图表	类型	默认时间范围	描述	样例
流入应用-TOP10	饼图	1小时（相对）	某个时间范围内，按访问次数统计前10名流入方向的应用类型（例如HTTP、SSH等）分布情况。	无
流入地域-TOP10	饼图	1小时（相对）	某个时间范围内，按访问次数统计前10名流入方向的访问源的地域分布情况。	无
流入端口-TOP20	矩形图	1小时（相对）	某个时间范围内，统计前20名流入方向的端口访问次数。	无
外联拦截趋势	线图	1小时（相对）	某个时间范围内，流出方向拦截次数的变化趋势图。	无
外联拦截应用分布-TOP10	饼图	1小时（相对）	某个时间范围内，统计前10名流出方向拦截的应用类型（例如HTTP、SSH等）分布情况。	无
外联端口-TOP20	矩形图	1小时（相对）	某个时间范围内，统计前20名流出方向的端口访问次数。	无
外联IP-TOP10	饼图	1小时（相对）	某个时间范围内，统计前10名流出方向的IP访问次数。	无
外联域名-TOP10	矩形图	1小时（相对）	某个时间范围内，统计前10名流出方向的域名访问次数。	无
外联应用-TOP10	饼图	1小时（相对）	某个时间范围内，统计前10名流出方向的应用类型（例如HTTP、SSH等）分布情况。	无

2.7. 日志字段说明

云防火墙详细记录出方向和入方向的流量日志。日志中包含多个字段，您可以根据需要选取相应的日志字段进行查询分析。

字段名称	含义及说明	取值示例
__time__	操作时间。	2018-02-27 11:58:15
__topic__	日志的主题。取值固定为 `cloudfirewall_access_log`，表示云防火墙的流量日志。	cloudfirewall_access_log
log_type	日志的类型。取值固定为 `internet_log`，表示互联网流量日志。	internet_log
aliuid	阿里云账号ID。	1233333333****
app_name	访问流量的应用名称。取值：`HTTPS`、`NTP`、`SIP`、`SMB`、`NFS`、`DNS`、`Unknown`（协议为未知类型）。	HTTPS

字段名称	含义及说明	取值示例
direction	流量的方向。取值： • in：入方向，表示来自互联网的其他资源或内网中的其他ECS访问您的ECS服务器。 • out：出方向，表示您的ECS服务器主动访问互联网上的其他资源或内网中的其他ECS。	in
domain	域名。	www.aliyun.com
dst_ip	访问流量的目的IP。	1.XX.XX.1
dst_port	访问流量的目的端口。	443
end_time	会话结束时间。使用Unix时间戳格式表示，单位：秒。	1555399260
in_bps	入方向总流量的大小。单位：bit/s	11428
in_packet_bytes	入方向总流量的字节数。	2857
in_packet_count	入方向总流量的报文数。	18
in_pps	入方向总流量的包数量。单位：packet/s。	9
ip_protocol	IP协议类型。取值：TCP、UDP。	TCP
out_bps	出方向总流量的大小。单位：bit/s。	27488
out_packet_bytes	出方向总流量的字节数。	6872
out_packet_count	出方向总流量的报文数。	15
out_pps	出方向总流量的大小。单位：packet/s。	7
region_id	访问流量所属的地域ID。关于不同地域ID的含义，请参见支持的地域。	cn-beijing
rule_result	访问流量命中云防火墙访问控制规则的结果。取值： • pass：允许流量通过云防火墙。 • alert：对该流量通过云防火墙提供告警提示。 • drop：丢弃流量，不允许该访问流量通过云防火墙。	pass
src_ip	访问流量的源IP。	1.XX.XX.1
src_port	访问流量的源端口，即发出流量数据的主机端口。	47915
start_time	会话开始时间。使用Unix时间戳格式表示，单位：秒。	1555399258

字段名称	含义及说明	取值示例
start_time_min	会话开始时间，分钟取整数。使用Unix时间戳格式表示，单位：分钟。	1555406460
tcp_seq	TCP序列号。	3883676672
total_bps	出入方向访问总流量的大小。单位：bit/s。	38916
total_packet_bytes	出入方向的访问总流量。单位：byte。	9729
total_packet_count	出入方向总流量的报文数。	33
total_pps	出入方向访问总流量的大小。单位：packet/s。	16
vul_level	漏洞风险等级。取值： • 1：表示低危漏洞。 • 2：表示中危漏洞。 • 3：表示高危漏洞。	1
url	您服务器访问的外部网页的地址。	http://www.test.com/index.html
src_private_ip	出方向访问流量中，源ECS服务器的私网IP地址。	192.168.0.0
acl_rule_id	访问流量命中的ACL规则的ID。	073a1475-6e11-43e2-8b28-98cee9c688c0
ips_rule_id	访问流量命中的IPS规则的ID。	073a1475-6e11-43e2-8b28-98cee9c688c0
ips_ai_rule_id	访问流量命中的AI规则的ID。	073a1475-6e11-43e2-8b28-98cee9c688c0
ips_rule_name	访问流量命中的IPS规则的中文名称。	主机存在挖矿行为
ips_rule_name_en	访问流量命中的IPS规则的英文名称。	Mining behavior on the host
attack_type_name	访问流量中包含的攻击类型的中文名称。	挖矿行为
attack_type_name_en	访问流量中包含的攻击类型的英文名称。	Mining Behavior

2.8. 导出日志

云防火墙日志分析功能支持将日志查询结果导出到本地，即支持下载本页日志（CSV格式）或全部日志（TXT格式）到本地。本文介绍了导出日志的具体操作。

操作步骤

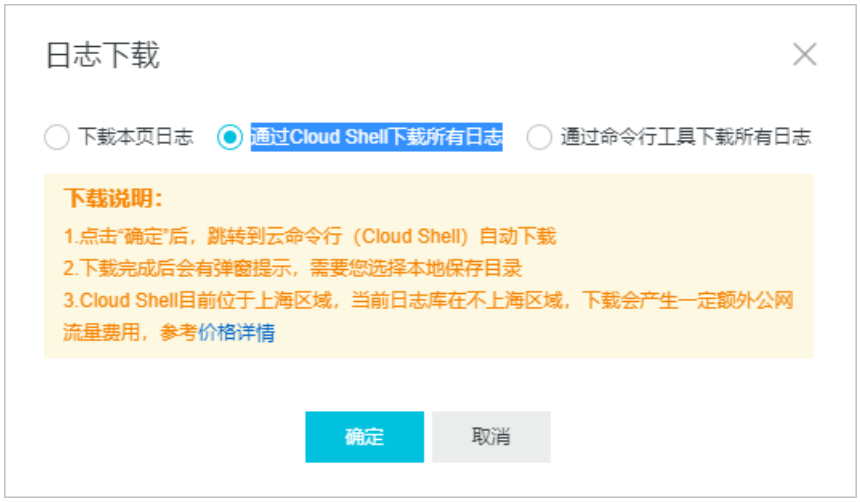
1. 登录云防火墙控制台。
2. 在左侧导航栏单击**日志分析 > 日志分析**。
3. 单击**日志查询**，并在该页面单击**原始日志**列表右侧的下载日志按钮

   。
4. 在**日志下载**对话框中，选择日志下载方式并保存日志。
   - 选择**下载本页日志**，并单击**确定**。

     云防火墙本页面的日志（CSV格式）会保存到本地。
   - 选择**通过Cloud Shell下载所有日志**下载所有日志。

     a. 单击**确定**跳转至Cloud Shell命令页面。
     b. 根据页面弹出的提示框要求，输入相关信息。
     c. 选择并确定日志文件保存到本地的路径。

     下载成功后，云防火墙的全部日志会保存到本地。

     > **说明** Cloud Shell目前位于上海区域，当前日志库如果不在上海区域，日志的下载会产生一定的公网流量费用。单击**价格详情**了解流量费用。
   - 选择**通过命令行工具下载所有日志**下载所有日志。

a. 单击下载日志对话框中的**帮助文档**，打开命令行工具安装说明页面。

b. 安装命令行工具。

c. 单击**安全信息管理**，查看并复制当前用户的密钥ID和KEY。

d. 单击**复制命令行**并用当前用户的密钥ID和KEY替换该命令行中`【步骤2中的密钥ID】`和`【步骤2中的密钥Key】`。

e. 在CLI命令行工具中执行该命令。

命令执行后，云防火墙全部日志将自动下载并保存到运行命令的当前目录下的download_data.txt文件中。

2.9. 子账号日志查询分析授权

如果子账号需要使用云防火墙日志查询分析服务，需要由主账号为其进行授权操作。

背景信息

开通和使用云防火墙日志查询分析服务，具体涉及以下权限：

操作类型	支持的操作账号类型
开通日志服务（全局一次性操作）。	主账号
授权云防火墙实时写入日志数据到日志服务的专属日志库（全局一次性操作）。	• 主账号 • 具备`AliyunLogFullAccess`权限的子账号 • 具备指定权限的子账号
使用日志查询分析功能。	• 主账号 • 具备`AliyunLogFullAccess`权限的子账号 • 具备指定权限的子账号

您也可以根据实际需求为子账号授予相关权限。

授权场景	授予权限	操作步骤
为子账号授予日志服务产品的所有操作权限。	授予日志服务全部管理权限 `AliyunLogFullAccess` 。	具体操作步骤，参考RAM用户管理。
主账号开通云防火墙日志查询分析服务并完成授权操作后，为子账号授予日志查看权限。	授予只读权限 `AliyunLogReadOnlyAccess` 。	具体操作步骤，参考RAM用户管理。
仅为子账号授予开通和使用云防火墙日志查询分析服务的权限，不授予日志服务产品的其他管理权限。	创建自定义授权策略，并为子账号授予该自定义授权策略。	具体操作步骤，参考本文档内容。

操作步骤

1. 登录 RAM 控制台。
2. 在**策略管理**中打开**自定义授权策略**页签。
3. 在页面右上角单击**新建授权策略**。
4. 单击**空白模板**，在模板中输入**策略名称**和以下**策略内容**。

> **说明** 将以下策略内容中的 `${Project}` 与 `${Logstore}` 分别替换为您的云防火墙日志服务专属Project和Logstore的名称。

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": "log:GetProject",
   "Resource": "acs:log:*:*:project/${Project}",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateProject",
   "Resource": "acs:log:*:*:project/*",
   "Effect": "Allow"
  },
{
   "Action": "log:ListLogStores",
   "Resource": "acs:log:*:*:project/${Project}/logstore/*",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateLogStore",
   "Resource": "acs:log:*:*:project/${Project}/logstore/*",
   "Effect": "Allow"
  },
{
   "Action": "log:GetIndex",
   "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
   "Effect": "Allow"
```

```
  },
  {
   "Action": "log:CreateIndex",
   "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
   "Effect": "Allow"
  },
  {
   "Action": "log:UpdateIndex",
   "Resource": "acs:log:*:*:project/${Project}/logstore/${Logstore}",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateDashboard",
   "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
   "Effect": "Allow"
  },
 {
   "Action": "log:UpdateDashboard",
   "Resource": "acs:log:*:*:project/${Project}/dashboard/*",
   "Effect": "Allow"
  },
 {
   "Action": "log:CreateSavedSearch",
   "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
   "Effect": "Allow"
  },
 {
   "Action": "log:UpdateSavedSearch",
   "Resource": "acs:log:*:*:project/${Project}/savedsearch/*",
   "Effect": "Allow"
  }
 ]
}
```

5. 单击**新建授权策略**。
6. 定位到**用户管理**页面，找到需要授权的子账号并单击对应的**授权**。
7. 添加您所创建的自定义授权策略，单击**确定**。
   被授权的子账号即可以开通和使用云防火墙日志查询分析服务，但无法对日志服务产品的其它功能进行操作。

2.10. 日志存储空间管理

开通云防火墙日志服务后，系统将根据您所选择的日志存储规格分配日志存储空间，您可以在云防火墙管理控制台的日志服务页面查看日志存储空间的使用情况。

查看日志存储空间使用情况

您可以在云防火墙控制台随时查看日志存储空间用量。

> **说明** 控制台中显示的日志存储空间用量并非实时更新，与实际使用情况间存在两个小时的延迟。因此，当日志存储空间即将占满时，请提前升级容量。

1. 登录云防火墙控制台。
2. 在左侧导航栏单击**日志 > 日志分析**。
3. 在**日志分析**页面右上方查看日志存储空间用量。

升级日志存储空间容量

如果您发现日志存储空间即将占满，您可以单击**日志分析**页面上方的**升级容量**，选择更大的日志存储容量规格，并支付相应的扩容费用。

> **说明** 为避免因日志存储空间容量占满，新的日志数据无法写入专属日志库而造成日志数据不完整的情况，请您及时升级日志存储空间容量。

清空日志存储空间

根据业务需要，您可以清空当前日志存储空间中的所有日志数据。例如，清空测试阶段产生的日志数据，从而充分利用日志存储空间记录有意义的生产数据。

单击**日志分析**页面上方的**清空**，确认清空您日志存储空间中的全部日志。

> **注意**
>
> - 日志清空后将无法复原，请谨慎使用清空功能。
> - 清空日志存储空间功能存在使用次数限制。