ALIBABA CLOUD

阿里云

Web应用防火墙

日志管理

文档版本：20211111

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.日志服务

1.1. 概述

WAF日志服务帮助您采集并存储接入WAF防护的网站域名的Web访问及攻击防护日志，并基于阿里云日志服务，输出查询分析、统计图表、报警服务、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。

适用对象

- 对云上资产的主机、网络以及安全日志有存储合规需求的大型企业与机构，例如金融公司、政府类机构等。
- 拥有自己的安全运营中心，需要收集安全告警等日志进行中央运营管理的企业，例如大型地产、电商、金融公司、政府类机构等。
- 拥有较强技术能力，需要基于云上资产的日志进行深度分析，对告警进行自动化处理的企业，例如IT、游戏、金融公司等。
- 对云上业务安全事件有溯源需求，需要定期输出安全周报、月报和年报，或者拥有三级以上等保合规需求的用户。

应用场景

- 追踪Web攻击日志，溯源安全威胁。
- 查看Web请求活动，了解请求状态与趋势。
- 快速了解安全运营效果，及时反馈和处理异常。
- 输出安全网络日志到自建数据与计算中心。

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Web访问及攻击防护日志的采集。
  - 支持自定义日志存储的时长和容量，设置需要采集日志的网站。
  - 支持根据您的业务需求修改或者自定义符合业务或安全需求的报表模板，帮助您快速感知网站业务和安全状态。
- 实时分析：依托阿里云日志服务产品，提供实时日志分析能力、开箱即用的报表中心与交互挖掘支持，从传统几十分钟级别到秒级别，让您对网站业务的各种Web攻击状况以及Web访问细节了如指掌。
- 实时告警：支持基于特定指标定制监控与告警，确保在关键业务发生异常时能第一时间响应。
- 生态体系：支持对接其他生态如实时计算、云存储、可视化等方案，进一步挖掘数据价值。

计费与开通服务

高级版及以上版本的WAF包年包月实例、WAF按量计费实例均支持WAF日志服务。

WAF日志服务必须单独开通后才可以使用。WAF日志服务按照您所需日志存储空间容量计费。具体计费信息，请参见计费方式。

关于如何开通WAF日志服务，请参见开通WAF日志服务。

功能概览

功能	说明
WAF日志采集	开通WAF日志服务后，您可以为已接入WAF防护的域名开启日志采集。只有开启日志采集后，WAF才会采集并存储域名的相关日志数据，供您进行查询与分析。关于WAF日志数据包含的字段信息，请参见WAF日志字段。 您可以修改默认日志存储设置，包括日志存储时长、要存储的日志字段类型、存储日志类型（全量日志、仅拦截日志）。相关操作，请参见修改日志设置。
日志查询与分析	使用查询分析语句，对采集到的日志数据进行查询与分析。 查询分析语句由日志服务专用查询语句（Search）和SQL92标准分析语句（Analytics）组成，查询和分析语句间使用竖线（|）分隔。分析语句执行后，默认以表格形式展示分析结果，您还可以选择以折线图、柱状图、饼图等多种统计图表方式查看结果。 您可以基于查询分析语句创建告警。创建告警后，日志服务将定期检查查询与分析结果，并在检查结果满足预设条件时，向您发送告警通知，实现实时的服务状态监控。相关操作，请参见日志告警。
日志分析仪表盘	仪表盘是日志服务提供的实时数据分析大盘。您可以在仪表盘查看多个基于查询与分析结果的统计图表。 WAF日志服务基于常见的业务及防护查询场景，为您预置了运营中心、访问中心、安全中心仪表盘，方便您无需输入查询与分析语句，仅通过修改查询时间，即可快速查询您关心的网站业务和安全数据。 您还可以使用订阅仪表盘功能，通过邮件或者钉钉群消息将仪表盘内容定时推送给指定对象。
管理日志存储空间	您可以定期查询日志存储空间的使用情况，并根据实际业务需要，升级存储空间容量或者清空已存储的日志。
集成WAF日志到Syslog系统	您可以使用Python Program将WAF日志集成到Syslog日志系统中，以实现合规、审计等要求，也方便您在安全操作中心统一管理所有相关日志。

1.2. 计费方式

WAF日志服务根据您设置的日志存储容量进行计费。

概述

WAF日志服务支持在包年包月（高级版及以上）和按量计费WAF实例中开通和使用。开通方法如下：

- 包年包月（预付费）：在Web应用防火墙购买页选择开启**日志服务**，并根据实际需要选择**日志存储容量**。WAF将根据您选择的日志存储容量和WAF实例的购买时长计算费用。

- 按量计费（后付费）：在Web应用防火墙控制台的**账单与套餐中心**页面，设置**日志存储容量**（大于0即表示开通日志服务）。开通WAF日志服务后，按量计费账单中会包含日志服务对应的规格系数。具体价格信息，请参见按量计费2.0。

关于开通WAF日志服务的具体操作，请参见开通WAF日志服务。

日志存储规格

规格名称	是否影响计费	说明	开通WAF日志服务后，是否支持修改
日志存储容量	是	• 包年包月实例： 开通WAF日志服务时，您可以选择特定的日志存储容量（单位：TB）。您选择的存储容量随实例一起按照包年包月方式计费。不同存储容量的具体价格，以Web应用防火墙购买页为准。 • 按量计费实例： 支持在1~100（TB）整数范围内设置日志存储容量（大于0即表示开通WAF日志服务）。每TB存储容量的具体价格，以**账单与套餐中心**页面的信息为准。	• 包年包月实例： 支持通过升级实例提升日志存储容量。具体操作，请参见升级。 • 按量计费实例： 支持在**账单与套餐中心**页面修改日志存储容量。具体操作，请参见账单与套餐中心（按量2.0版本）。 **注意** 如果日志存储容量已满，但您未及时升级容量，WAF将停止向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将保留，直到该日志数据因超出日志存储时长被自动删除。
日志存储时长	否	• 包年包月实例：默认为180天。 • 按量计费实例：默认为7天。	只有企业版及以上版本的包年包月实例，支持在30~360天范围内自定义日志存储时长。具体操作，请参见修改日志设置。

如何选择日志存储容量？

您可以根据日志存储配置和网站业务的日常QPS，选择您需要的日志存储容量。

日志存储配置包括：

- 日志存储类型：分为存储全量日志、只存储攻击拦截日志。存储全量日志所需日志存储容量更大。
- 日志存储时长：存储时长越长，所需日志存储容量越大。
- 日志包含的字段：WAF日志字段分为必选字段（日志中必须包含的字段）和可选字段（日志中可以自定义是否包含的字段）。启用的可选字段越多，所需日志存储容量越大。

首次开通WAF日志服务后，默认日志存储配置为：存储全量日志、存储时长为180天、日志只包含必选字段。
您可以通过**日志设置**功能修改日志存储配置。相关操作，请参见修改日志设置。
以默认日志存储配置为例，您可以参考以下信息，根据网站业务的日常QPS，选择所需日志存储容量：

- 日均QPS不大于80的业务防护场景，推荐选择3 TB存储容量。
- 日均QPS在80~120范围的业务防护场景，推荐选择5 TB存储容量。
- 日均QPS在120~260范围的业务防护场景，推荐选择10 TB存储容量。
- 日均QPS在260~350范围的业务防护场景，推荐选择15 TB存储容量。
- 日均QPS在350~500范围的业务防护场景，推荐选择20 TB存储容量。
- 日均QPS在500~1200范围的业务防护场景，推荐选择50 TB存储容量。

说明 如果您需要自定义日志存储配置，可以在以上信息基础上估算需要的日志存储容量。

计费时长

WAF日志服务的计费时长与您开通WAF日志服务的方式有关。具体说明如下：

- 如果您在购买包年包月WAF实例时开通WAF日志服务，则WAF日志服务的计费时长与您选择的购买时长一致。
- 如果您通过升级已购买的WAF包年包月实例开通WAF日志服务，则WAF日志服务的计费时长等于当前WAF实例的剩余有效期时长（精确到分钟）。
- 如果您为按量计费WAF实例开通WAF日志服务，则WAF日志服务随按量计费实例一起计费。

服务到期说明

当您购买的WAF实例到期时，WAF日志服务将同时到期。WAF日志服务到期的影响如下：

- WAF日志服务到期后，WAF将停止向专属日志库写入日志数据。
- WAF日志服务到期后，WAF日志数据将为您保留7天。
  如果您在7天内完成续费，则可以继续使用WAF日志服务；如果您未能及时完成续费，则所有已存储的WAF日志将被自动清空。

1.3. WAF日志字段

本文介绍了WAF日志中包含的专有字段的说明。

字段检索表

下表描述了WAF日志支持的专有字段。您可以通过字段名称检索您需要了解的字段。

首字母	字段
a	account_action | account_rule_id | account_test | acl_action | acl_rule_id | acl_rule_type | acl_test | algorithm_action | algorithm_rule_id | algorithm_test | antifraud_action | antifraud_test | antiscan_action | antiscan_rule_id | antiscan_rule_type | antiscan_test
b	block_action | body_bytes_sent | bypass_matched_ids
c	cc_action | cc_rule_id | cc_rule_type | cc_test | content_type
d	deeplearning_action | deeplearning_rule_id | deeplearning_rule_type | deeplearning_test | dlp_action | dlp_rule_id | dlp_test
f	final_action | final_plugin | final_rule_id | final_rule_type
h	host | http_cookie | http_referer | http_user_agent | http_x_forwarded_for | https
i	intelligence_action | intelligence_rule_id | intelligence_test
m	matched_host
n	normalized_action | normalized_rule_id | normalized_rule_type | normalized_test
q	querystring
r	real_client_ip | region | remote_addr | remote_port | request_body | request_length | request_method | request_path | request_time_msec | request_traceid
s	scene_action | scene_id | scene_rule_id | scene_rule_type | scene_test | server_port | server_protocol | ssl_cipher | ssl_protocol | status
t	time

首字母	字段
u	ua_browser | ua_browser_family | ua_browser_type | ua_browser_version | ua_device_type | ua_os | ua_os_family | upstream_addr | upstream_response_time | upstream_status| user_id
w	waf_action | waf_rule_id | waf_rule_type | waf_test | wxbb_action | wxbb_invalid_wua | wxbb_rule_id | wxbb_test

WAF防护类字段

防护类字段表示客户端请求触发了WAF不同防护模块下的防护规则（包含放行类、拦截类等规则），由WAF基于防护逻辑生成的日志字段，帮助您分析业务受攻击情况。

WAF防护动作（action）说明

名称	说明	取值示例
account_action	客户端请求命中的账户安全规则对应的防护动作。取值仅有*block*，表示拦截。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
account_rule_id	客户端请求命中的账户安全规则的ID。	151235
account_test	客户端请求命中的账户安全规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
acl_action	客户端请求命中的IP黑名单、自定义防护策略（ACL访问控制）规则对应的防护动作。取值： • *block*：表示拦截。 • *captcha_strict*：表示严格滑块验证。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 • *captcha_strict_pass*：表示客户端通过了严格滑块验证，WAF放行客户端请求。 • *captcha_pass*：表示客户端通过了普通滑块验证，WAF放行客户端请求。 • *js_pass*：表示客户端通过了JS验证，WAF放行客户端请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
acl_rule_id	客户端请求命中的IP黑名单、自定义防护策略（ACL访问控制）规则的ID。	151235
acl_rule_type	客户端请求命中的IP黑名单、自定义防护策略（ACL访问控制）规则的类型。取值： • *custom*：表示自定义防护策略（ACL访问控制）规则。 • *blacklist*：表示IP黑名单规则。	custom
acl_test	客户端请求命中的IP黑名单、自定义防护策略（ACL访问控制）规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false

名称	说明	取值示例
algorithm_action	客户端请求命中的典型爬虫行为识别规则对应的防护动作。取值： • *block*：表示拦截。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 • *captcha_pass*：表示客户端通过了普通滑块验证，WAF放行客户端请求。 • *js_pass*：表示客户端通过了JS验证，WAF放行客户端请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
algorithm_rule_id	客户端请求命中的典型爬虫行为识别规则的ID。	151235
algorithm_test	客户端请求命中的典型爬虫行为识别规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
antifraud_action	客户端请求命中的数据风控规则对应的防护动作。取值： • *pass*：表示放行。 • *block*：表示拦截。 • *captcha*：表示普通滑块验证。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
antifraud_test	客户端请求命中的数据风控规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
antiscan_action	客户端请求命中的扫描防护规则对应的防护动作。取值仅有*block*，表示拦截。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
antiscan_rule_id	客户端请求命中的扫描防护规则的ID。	151235
antiscan_rule_type	客户端请求命中的扫描防护规则的类型。取值： • *highfreq*：表示高频Web攻击封禁规则。 • *dirscan*：表示目录遍历防护规则。 • *scantools*：表示扫描工具封禁规则。 • *collaborative*：表示协同防御规则。	highfreq
antiscan_test	客户端请求命中的扫描防护规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false

名称	说明	取值示例
block_action	注意 由于WAF功能升级，该字段已失效。新增字段final_plugin用于替代该字段。如果您在业务中使用了block_action，请尽快将其替换成final_plugin。 触发了拦截动作的WAF防护类型。取值： • *tmd*：表示CC攻击防护，对应final_plugin取值*cc*。 • *waf*：表示Web攻击防护，对应final_plugin取值*waf*。 • *acl*：表示精准访问控制，对应final_plugin取值*acl*。 • *deeplearning*：表示深度学习引擎，对应final_plugin取值*deeplearning*。 • *antiscan*：表示扫描防护，对应final_plugin取值*antiscan*。 • *antifraud*：表示数据风控，对应final_plugin取值*antifraud*。 • *antibot*：表示防爬封禁，对应final_plugin取值*intelligence*、*algorithm*、*wxbb*、*scene*。	waf
bypass_matched_ids	客户端请求命中的WAF放行类规则的ID，具体包括白名单规则、设置了放行动作的自定义防护策略规则。 如果请求同时命中了多条放行类规则，该字段会记录所有命中的规则ID。多个规则ID间使用半角逗号（,）分隔。	283531
cc_action	客户端请求命中的CC安全防护、自定义防护策略（CC攻击防护）规则对应的防护动作。取值： • *block*：表示拦截。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 • *captcha_pass*：表示客户端通过了普通滑块验证，WAF放行客户端请求。 • *js_pass*：表示客户端通过了JS验证，WAF放行客户端请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
cc_rule_id	客户端请求命中的CC安全防护、自定义防护策略（CC攻击防护）规则的ID。	151234
cc_rule_type	客户端请求命中的CC安全防护、自定义防护策略（CC攻击防护）规则的类型。取值： • *custom*：表示自定义防护策略（CC攻击防护）规则。 • *system*：表示CC安全防护规则。	custom
cc_test	客户端请求命中的CC安全防护、自定义防护策略（CC攻击防护）规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
deeplearning_action	客户端请求命中的深度学习引擎规则对应的防护动作。取值仅有*block*，表示拦截。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
deeplearning_rule_id	客户端请求命中的深度学习引擎规则的ID。	151238

名称	说明	取值示例
deeplearning_rule_type	客户端请求命中的深度学习引擎规则的类型。取值： • *xss*：表示跨站脚本防护规则。 • *code_exec*：表示代码执行防护规则。 • *webshell*：表示webshell防护规则。 • *sqli*：表示SQL注入防护规则。 • *lfilei*：表示本地文件包含防护规则。 • *rfilei*：表示远程文件包含防护规则。 • *crlf*：表示CRLF注入防护规则。 • *other*：表示其他防护规则。	xss
deeplearning_test	客户端请求命中的深度学习引擎规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
dlp_action	客户端请求命中的防敏感信息泄露规则对应的防护动作。取值： • *block*：表示拦截。 • *mask*：表示脱敏敏感信息。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	mask
dlp_rule_id	客户端请求命中的防敏感信息泄露规则的ID。	151245
dlp_test	客户端请求命中的防敏感信息泄露规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
final_action	WAF对客户端请求最终执行的防护动作。取值： • *block*：表示拦截。 • *captcha_strict*：表示严格滑块验证。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。 如果一个请求未触发任何防护模块（包括命中了放行类规则、客户端完成滑块或JS验证后触发放行的情况），则不会记录该字段。 如果一个请求同时触发了多个防护模块，则仅记录最终执行的防护动作。防护动作的优先级由高到低依次为：拦截（*block*）> 严格滑块验证（*captcha_strict*）> 普通滑块验证（*captcha*）> JS验证（*js*）。	block

名称	说明	取值示例
final_plugin	WAF对客户端请求最终执行的防护动作（final_action）对应的防护模块。取值： • waf：表示规则防护引擎。 • deeplearning：表示深度学习引擎。 • dlp：表示防敏感信息泄露。 • account：表示账户安全。 • normalized：表示主动防御。 • acl：表示IP黑名单、自定义防护策略（ACL访问控制）。 • cc：表示CC安全防护、自定义防护策略（CC攻击防护）。 • antiscan：表示扫描防护。 • scene：表示场景化配置。 • antifraud：表示数据风控。 • intelligence：表示爬虫威胁情报。 • algorithm：表示典型爬虫行为识别。 • wxbb：表示App防护。 您可以在Web应用防火墙控制台的**防护配置 > 网站防护**页面，配置以上防护模块。关于不同防护模块的介绍，请参见网站防护配置概述。 如果一个请求未触发任何防护模块（包括命中了放行类规则、客户端完成滑块或JS验证后触发放行的情况），则不会记录该字段。 如果一个请求同时触发了多个防护模块，则仅记录最终执行的防护动作（final_action）对应的防护模块。	waf
final_rule_id	WAF对客户端请求最终应用的防护规则的ID，即final_action对应的防护规则的ID。	115341
final_rule_type	WAF对客户端请求最终应用的防防护规则（final_rule_id）的子类型。 例如，在`final_plugin:waf`类型下有`final_rule_type:sqli`、`final_rule_type:xss`等细分的规则类型。	xss/webshell
intelligence_action	客户端请求命中的爬虫威胁情报规则对应的防护动作。取值： • *block*：表示拦截。 • *captcha_strict*：表示严格滑块验证。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 • *captcha_strict_pass*：表示客户端通过了严格滑块验证，WAF放行客户端请求。 • *captcha_pass*：表示客户端通过了普通滑块验证，WAF放行客户端请求。 • *js_pass*：表示客户端通过了JS验证，WAF放行客户端请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
intelligence_rule_id	客户端请求命中的爬虫威胁情报规则的ID。	152234
intelligence_test	客户端请求命中的爬虫威胁情报规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false

名称	说明	取值示例
normalized_action	客户端请求命中的主动防御规则对应的防护动作。取值： • *block*：表示请求异常，主动防御模块拦截请求。 • *continue*：表示请求中未检测出异常，主动防御模块放行请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
normalized_rule_id	客户端请求命中的主动防御规则的ID。	151266
normalized_rule_type	客户端请求命中的主动防御规则的类型。取值： • *User-Agent*：表示User-Agent基线规则（即请求头的User-Agent字段不在基线范围。其他规则类型的含义与此类似）。 • *Referer*：表示Referer基线规则。 • *URL*：表示URL基线规则。 • *Cookie*：表示Cookie基线规则。 • *Body*：表示Body基线规则。	User-Agent
normalized_test	客户端请求命中的主动防御规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
scene_action	客户端请求命中的场景化配置规则对应的防护动作。取值： • *block*：表示拦截。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 • *captcha_pass*：表示客户端通过了普通滑块验证，WAF放行客户端请求。 • *js_pass*：表示客户端通过了JS验证，WAF放行客户端请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
scene_id	客户端请求命中的场景化配置规则对应的场景ID。	151235
scene_rule_id	客户端请求命中的场景化配置规则的ID。	153678
scene_rule_type	客户端请求命中的场景化配置规则的类型。取值： • *bot_aialgo*：表示AI智能防护规则。 • *js*：表示简单脚本过滤规则。 • *intelligence*：表示爬虫威胁情报库匹配、IDC黑名单封禁规则。 • *sdk*：表示App（已集成SDK）签名异常、设备特征异常规则。 • *cc*：表示IP限速、自定义会话限速规则。	bot_aialgo
scene_test	客户端请求命中的场景化配置规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false

名称	说明	取值示例
waf_action	客户端请求命中的规则防护引擎规则对应的防护动作。取值仅有*block*，表示拦截。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
waf_rule_id	客户端请求命中的规则防护引擎规则的ID。	113406
waf_rule_type	客户端请求命中的规则防护引擎规则的类型。取值： • *xss*：表示跨站脚本防护规则。 • *code_exec*：表示代码执行防护规则。 • *webshell*：表示webshell防护规则。 • *sqli*：表示SQL注入防护规则。 • *lfilei*：表示本地文件包含防护规则。 • *rfilei*：表示远程文件包含防护规则。 • *crlf*：表示CRLF注入防护规则。 • *other*：表示其他防护规则。	xss
waf_test	客户端请求命中的规则防护引擎规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false
wxbb_action	客户端请求命中的App防护规则对应的防护动作。取值： • *block*：表示签名验证失败，App防护模块拦截请求。 • *captcha*：表示普通滑块验证。 • *js*：表示JS验证。 • *continue*：表示签名验证通过，App防护模块放行请求。 关于WAF防护动作的具体说明，请参见WAF防护动作（action）说明。	block
wxbb_invalid_wua	客户端请求被App防护规则判定为异常的原因。取值： • *wxbb_simulator*：表示使用模拟器。 • *wxbb_proxy*：表示使用代理。 • *wxbb_root*：表示Root设备。 • *wxbb_hook*：表示存在Hook行为。 • *wxbb_antireplay*：表示签名串（*wToken*）重放攻击。 • *wxbb_virtual*：表示设备上应用（集成了WAF SDK）多开。 • *wxbb_debugged*：表示设备处于调试模式。 • *wxbb_invalid_sign*：表示签名验证失败。 常见失败原因包括： ◦ 请求没有携带签名。 ◦ 加签时的传参与WAF收到的实际内容不一致，例如，加签传参为 `a=1&b=2` ，WAF实际收到的请求参数为 `b=2&a=1` ；加签传参内容未经过编码，WAF实际收到的请求经过了Base64编码等。	wxbb_invalid_sign
wxbb_rule_id	客户端请求命中的App防护规则的ID。	156789

名称	说明	取值示例
wxbb_test	客户端请求命中的App防护规则对应的防护模式。取值： • *true*：表示观察模式，即仅记录日志，不触发拦截等防护动作。 • *false*：表示防护模式，WAF对命中防护规则的请求执行拦截等防护动作。	false

非防护类字段

非防护类字段包含WAF从客户端请求提取的与请求逻辑相关的字段（例如，常用的请求头部字段等）以及WAF对请求进行分析处理后生成的与请求行为相关的补充字段（例如，请求的真实客户端IP、源站响应码等）。

名称	说明	取值示例
body_bytes_sent	客户端请求体的字节数。单位：Byte。	1111
content_type	被请求的内容类型。	application/x-www-form-urlencoded
host	客户端请求头部的Host字段，表示被访问的域名（基于您的业务设置，也可能是IP地址）。	api.example.com
http_cookie	客户端请求头部的Cookie字段，表示访问来源客户端的Cookie信息。	k1=v1;k2=v2
http_referer	客户端请求头部的Referer字段，表示请求的来源URL信息。 如果请求无来源URL信息，则该字段显示 `-` 。	http://example.com
http_user_agent	客户端请求头部的User-Agent字段，包含请求来源的客户端浏览器标识、操作系统标识等信息。	Dalvik/2.1.0 (Linux; U; Android 10; Android SDK built for x86 Build/QSR1.200715.002)
http_x_forwarded_for	客户端请求头部的X-Forwarded_For（XFF）字段，用于识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址。	101.XX.XX.120
https	是否是HTTPS请求。取值： • *on*：表示是HTTPS请求。 • *off*：表示是HTTP请求。	on
matched_host	客户端请求匹配到的已接入WAF进行防护的域名。 **说明** 由于WAF网站接入中支持配置泛域名，所以客户端请求可能匹配到某个泛域名配置。例如，假设已接入WAF防护的域名是*.aliyun.com，当被请求的URL是www.aliyun.com时，可能匹配到*.aliyun.com。	*.aliyun.com

名称	说明	取值示例
querystring	客户端请求中的查询字符串，具体指被请求URL中问号（?）后面的部分。	title=tm_content%3Darticle&pid=123
real_client_ip	WAF对客户端请求进行分析后，判定发起该请求的真实客户端IP，便于您在业务中直接使用。 WAF无法判定真实客户端IP时（例如，由于用户通过代理服务器访问、请求头中IP字段有误等），该字段显示 `-` 。	1.XX.XX.1
region	WAF实例的地域ID。取值： • *cn*：表示中国内地。 • *int*：表示海外地区。	cn
remote_addr	与WAF建立连接的IP。 如果WAF与客户端直接连接，该字段等同于客户端IP；如果WAF前面还有其他七层代理（例如，CDN），该字段表示上一级代理的IP。	1.XX.XX.1
remote_port	与WAF建立连接的端口。 如果WAF与客户端直接连接，该字段等同于客户端端口；如果WAF前面还有其他七层代理（例如，CDN），该字段表示上一级代理的端口。	80
request_body	访问请求体。	i am the request body, encrypted or not!
request_length	客户端请求的字节数，包含请求行、请求头和请求体。单位：Byte。	111111
request_method	客户端请求的请求方法。	GET
request_path	被请求的相对路径，具体指被请求URL中域名后面且问号（?）前面的部分（不包含查询字符串）。	/news/search.php
request_time_msec	WAF处理客户端请求所用的时间。单位：毫秒。	44
request_traceid	WAF为客户端请求生成的唯一标识。	7837b1171541038694343700 9ea1f0
server_port	被请求的目的端口。	443
server_protocol	源站服务器响应WAF回源请求的协议及版本号。	HTTP/1.1
ssl_cipher	客户端请求使用的加密套件。	ECDHE-RSA-AES128-GCM-SHA256
ssl_protocol	客户端请求使用的SSL/TLS协议和版本。	TLSv1.2
status	WAF响应客户端请求的HTTP状态码。例如，*200*（表示请求成功）。	200

名称	说明	取值示例
time	客户端请求的发起时间。按照ISO 8601标准表示，并需要使用UTC时间，格式为 yyyy-MM-ddTHH:mm:ss+08:00 。	2018-05-02T16:03:59+08:00
ua_browser	发起请求的浏览器的名称。	ie9
ua_browser_family	发起请求的浏览器所属系列。	internet explorer
ua_browser_type	发起请求的浏览器的类型。	web_browser
ua_browser_version	发起请求的浏览器的版本。	9.0
ua_device_type	发起请求的客户端的设备类型。	computer
ua_os	发起请求的客户端的操作系统类型。	windows_7
ua_os_family	发起请求的客户端所属的操作系统系列。	windows
upstream_addr	源站服务器的IP地址和端口。格式为 IP:Port 。多个记录间使用半角逗号（,）分隔。	1.XX.XX.1:443
upstream_response_time	源站服务器响应WAF回源请求的处理时间。单位：秒。	0.044
upstream_status	源站服务器响应WAF回源请求的HTTP状态码。例如，*200*（表示请求成功）。	200
user_id	当前WAF实例所属的阿里云账号ID。	17045741********

1.4. 快速上手

1.4.1. 步骤1：开通WAF日志服务

WAF日志服务通过阿里云日志服务准实时地采集已接入WAF防护的网站业务的全量日志，支持对采集到的日志数据进行查询与分析、以丰富的仪表盘形式展示查询结果，满足等保合规要求和网站业务的防护及运营需求。本文介绍了首次开通WAF日志服务的操作方法。

前提条件

- 已开通**高级版**及以上规格的WAF包年包月实例，或者已开通WAF按量计费实例。
  相关操作，请参见开通Web应用防火墙。
- 已将网站域名接入WAF进行防护。
  如果您还没有将网站域名接入WAF进行防护，即使开通WAF日志服务，也不会产生日志数据，建议您先将网站域名接入WAF防护，再开通WAF日志服务。关于网站接入的相关操作，请参见使用教程。
- 已开通阿里云日志服务。
  首次登录日志服务控制台时，您可以根据页面提示开通日志服务。

包年包月实例

如果您使用WAF包年包月实例，可以参照以下步骤，开通WAF日志服务：

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 在**日志服务**页面，单击**立即升级**，并按照页面提示完成升级。

> **说明** 如果您在购买WAF实例时已经开启了**日志服务**（如下图所示），则无需进行升级操作，请跳过该步骤。

升级操作步骤：

i. 在**变配**页面，开启**日志服务**，并根据您的业务需要选择**日志存储容量**。

关于日志服务相关参数的具体说明，请参见开通Web应用防火墙。

ii. 单击**去支付**，并完成支付。

5. 授权WAF访问相关云服务。

WAF需要访问阿里云日志服务，才能够存储WAF日志，并向您提供日志查询与分析服务。因此，在使用WAF日志服务前，您必须授权WAF访问相关云服务。

> **注意** 使用WAF过程中，您只需完成一次云服务访问授权。完成授权后，WAF将获得服务关联角色（AliyunServiceRoleForWAF）权限，用于访问其他的云服务资源。如果WAF已经拥有该角色权限，则您无需重复授权。您可以在RAM控制台的**RAM角色管理**页面，查询WAF服务关联角色。更多信息，请参见授权WAF访问云服务。

授权操作步骤：

i. 在**日志服务**页面，单击**立即授权**。

ii. 在**提示**对话框，单击**确定**。

开通WAF日志服务后，阿里云日志服务将自动为当前阿里云账号创建专属的WAF日志项目和日志库，完成日志数据采集前的准备工作。关于WAF专属日志项目及日志库的默认配置，请参见WAF专属日志项目及日志库。

按量计费实例

如果您使用WAF按量计费实例，可以参照以下步骤，开通WAF日志服务：

1. 登录Web应用防火墙控制台。
2. 在左侧导航栏，选择**日志管理 > 日志服务**。
3. 在**日志服务**页面，单击**立即升级**，并参照以下步骤完成升级：

i. 在**修改套餐**页面，定位到**系统规格**区域，设置**日志存储容量**（单位：TB）。

日志存储容量大于0，即表示开通日志服务。

ii. 单击**确认修改**。

4. 授权WAF访问相关云服务。

WAF需要访问阿里云日志服务，才能够存储WAF日志，并向您提供日志查询与分析服务。因此，在使用WAF日志服务前，您必须授权WAF访问相关云服务。

> **注意** 使用WAF过程中，您只需完成一次云服务访问授权。完成授权后，WAF将获得服务关联角色（AliyunServiceRoleForWAF）权限，用于访问其他的云服务资源。如果WAF已经拥有该角色权限，则您无需重复授权。您可以在RAM控制台的**RAM角色管理**页面，查询WAF服务关联角色。更多信息，请参见授权WAF访问云服务。

授权操作步骤：

i. 在**日志服务**页面，单击**立即授权**。

ii. 在**提示**对话框，单击**确定**。

开通WAF日志服务后，阿里云日志服务将自动为当前阿里云账号创建专属的WAF日志项目和日志库，完成日志数据采集前的准备工作。关于WAF专属日志项目及日志库的默认配置，请参见WAF专属日志项目及日志库。

后续步骤

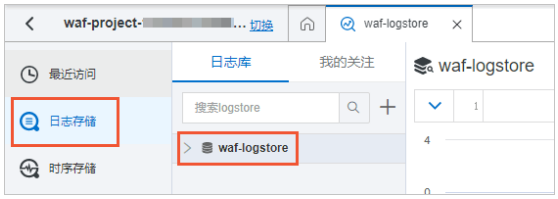
开通WAF日志服务后，您只需为已接入WAF防护的网站域名开启日志采集，WAF就会存储该域名的日志数据，并为您提供查询与分析服务。关于开启日志采集的具体操作，请参见步骤2：开启日志采集。

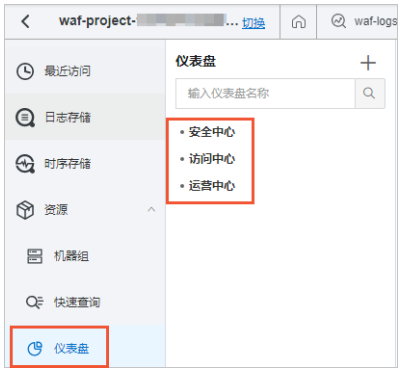
WAF专属日志项目及日志库

下表描述了阿里云日志服务自动创建的WAF专属日志项目（Project）及日志库（Logstore）的默认配置。

> **注意** 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WAF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。

资源类型	说明
Project	日志服务自动为WAF创建一个日志项目（Project）。日志项目的具体信息如下： • 中国内地WAF实例：日志项目名称为 `waf-project-阿里云账号ID-cn-hangzhou`，所属地域为华东1（杭州）。 • 海外地区WAF实例：日志项目名称为 `waf-project-阿里云账号ID-ap-southeast-1`，所属地域为新加坡。 您可以在日志服务控制台的首页查询WAF专属日志项目，单击项目名称可以进入项目。  关于Project的更多介绍，请参见管理Project。

资源类型	说明
Logstore	WAF日志项目下默认已创建一个日志库（Logstore）。WAF日志库名称为 `waf-logstore` 。WAF采集到的所有日志都将存储到该日志库。您可以在WAF日志项目中查询WAF日志库。  WAF日志库不支持通过API、SDK等方式写入除WAF日志外的其他类型数据。该日志库在查询、统计、报警、流式消费等功能上无特殊限制。 日志服务不会对WAF日志库收费，但是只有当阿里云账号下的日志服务产品处于正常使用状态时，WAF日志库才可以正常使用。 **说明** 当您的日志服务产品出现欠费时，WAF日志采集功能将暂停工作。当您及时补缴欠款后，日志采集功能将自动恢复。 关于Logstore的更多介绍，请参见管理Logstore。
Shard	WAF日志库默认包含二个分区（Shard），并开启了自动分裂分区功能。您可以通过**Logstore基本信息**查询分区属性。  关于Shard的更多介绍，请参见管理Shard。

资源类型	说明
仪表盘	WAF日志项目下默认包含三个预置的仪表盘，分别为**运营中心**、**访问中心**、**安全中心**。 您可以在WAF日志项目中查询WAF日志仪表盘。 关于WAF日志仪表盘的更多介绍，请参见查看日志分析仪表盘。 

1.4.2. 步骤2：开启日志采集

开通WAF日志服务后，您可以为已接入WAF防护的网站域名开启日志采集。只有开启日志采集，网站相关的日志数据才会自动存储到WAF专属日志库，并支持查询与分析。本文介绍了为网站开启日志采集的操作方法。

前提条件

- 已开通WAF日志服务。相关操作，请参见步骤1：开通WAF日志服务。
- 网站域名已接入WAF进行防护。相关操作，请参见使用教程。

背景信息

WAF日志服务只会存储已开启日志采集的网站相关日志。如果网站未开启日志采集，WAF不会存储其日志数据。

网站域名开启日志采集后，WAF将按照下表描述的默认配置，自动存储网站域名的日志数据。

默认配置	是否支持修改默认配置
默认存储网站域名的全量日志（包含WAF放行请求和拦截请求的日志）。	是，可以修改为仅存储拦截日志。
默认存储180天内的日志数据。	是，可以修改日志存储时长，可选范围：30~360天。 **注意** 仅企业版及以上版本的包年包月WAF实例支持修改日志存储时长。
WAF日志由WAF支持的日志字段组成，默认包含全部必选字段和部分可选字段。	是，可以修改WAF日志中包含哪些可选字段。

如果您需要修改以上默认配置，请参见修改日志设置。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 从域名下拉列表中选择要开启日志采集的网站域名，打开右侧的**状态**开关，为该网站域名开启日志采集。

域名下拉列表仅包含已接入WAF防护的网站域名。如果您还没有将网站域名接入WAF防护，请先完成网站接入。相关操作，请参见使用教程。

网站域名开启日志采集后，WAF将自动采集该域名的日志，并将日志数据存储到WAF专属日志库。您可以参照该步骤，为其他网站域名开启日志采集。

后续步骤

网站域名开启日志采集后，您就可以在**日志服务**页面查询与分析网站的日志数据。具体操作，请参见步骤3：查询和分析日志。

1.4.3. 步骤3：查询和分析日志

为网站域名开启日志采集后，您可以在日志服务页面查询和分析网站的日志数据。本文介绍了通过WAF日志服务页面查询和分析日志的操作方法。

前提条件

已为接入WAF防护的网站域名开启日志采集。相关操作，请参见步骤2：开启日志采集。

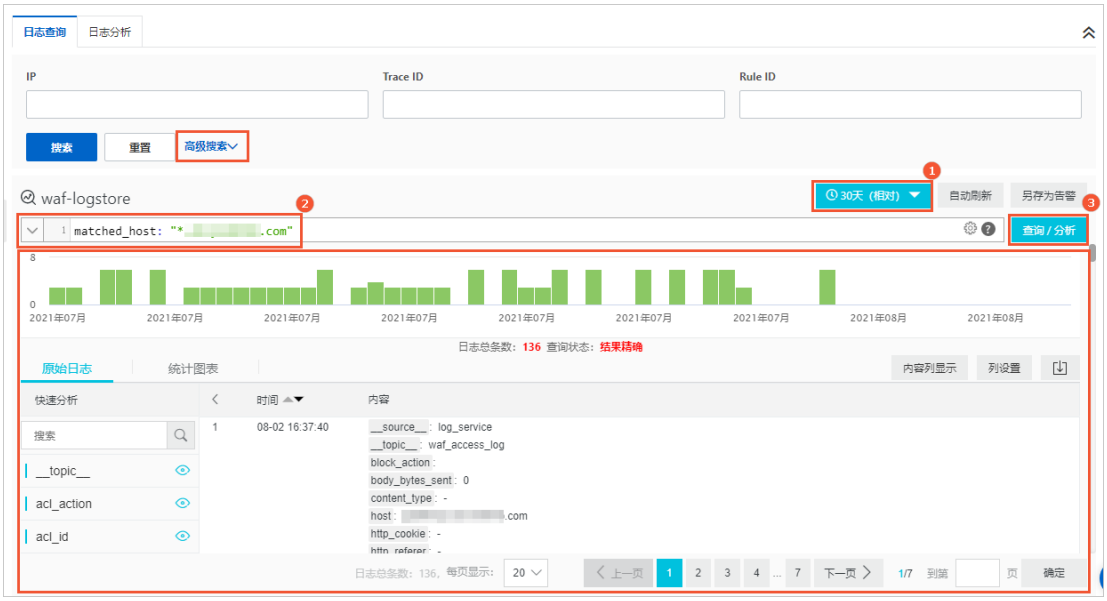
只有开启日志采集后，WAF才会采集与网站域名有关的日志数据，供您进行查询与分析。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 在**日志服务**页面上方，选择要操作的网站域名。

> 注意 域名必须已经开启日志采集（即**状态**开关已打开），否则WAF不会采集其日志数据，也不提供查询与分析服务。

5. 在**日志查询**页签，通过查询与分析语句，对WAF日志数据进行查询与分析。



具体步骤如下：

i. 通过时间选择器（图示①），修改日志查询时间范围。

ii. 在语句输入框（图示②），输入查询语句。

查询语句采用阿里云日志服务专用语法，关于该语法的详细介绍，请参见查询语法。查询语句中使用WAF日志包含的字段作为查询字段，关于支持使用的查询字段，请参见WAF日志字段。
如果您不了解日志查询语法，推荐您使用**高级搜索**。您只需在语句输入框上方展开**高级搜索**，设置搜索条件并单击**搜索**，语句输入框即可自动生成与搜索条件匹配的日志查询语句。

下表描述了高级搜索支持设置的搜索条件。

搜索条件	说明
IP	发起请求的客户端的IP地址。
Trace ID	WAF为客户端请求生成的唯一标识。WAF向客户端返回拦截页面或者滑块验证响应时会提供该ID，用于问题分析与故障排查。
Rule ID	请求命中的WAF防护规则ID。您可以在**安全报表**或者**系统管理 > 防护规则组**页面，获取规则ID信息。
服务器响应状态码	源站服务器响应WAF回源请求的HTTP状态码。
WAF返回客户端响应码	WAF响应客户端请求的HTTP状态码。
拦截规则	请求命中的WAF防护规则的类型。关于WAF防护模块的介绍及不同模块防护规则的配置方法，请参见概述。

iii. 如果您需要对查询结果进行计算和统计分析，可以在语句输入框（图示②）已输入的查询语句后，输入分析语句；如果您只需要查询满足条件的日志数据，可以跳过该步骤。

分析语句和查询语句间使用竖线（|）分隔。分析语句采用标准的SQL92语法，关于分析语句的更多介绍，请参见分析概述。

iv. 单击**查询/分析**（图示③）。
查询与分析结果（即命中查询条件的WAF日志数据）将会显示在页面下方，包含日志分布直方图、**原始日志**及**统计图表**。您可以基于查询结果进行快速分析、生成统计图表、设置告警等，相关操作，请参见操作查询与分析结果、创建告警。

更多关于日志查询与分析的案例，请参见查询与分析案例。

6. 在**日志分析**页签，查看WAF基于日志数据为您整合的日志分析仪表盘。

日志分析仪表盘是WAF基于日志数据，预先设置的一系列图形报表，方便您直接查询网站业务及安全防护的相关数据。日志分析仪表盘包含：

- **运营中心**：展示网站的业务运营指标，包含请求趋势、攻击概况等。

- **访问中心**：展示网站的访问指标、客户端分布、流量与性能等。
- **安全中心**：展示网站的被攻击指标、趋势、来源分布等。

您只需设置查询时间，即可直接查询相关仪表盘，并可以创建订阅，通过邮件等方式定期接收仪表盘数据报表。关于日志分析仪表盘包含的具体图表数据以及如何创建订阅，请参见查看日志分析仪表盘。

更多内容

如果您的RAM用户需要使用WAF日志查询与分析功能，您需要为其授予日志服务相关权限。具体操作，请参见为RAM用户授予日志查询分析权限。

如果您需要了解更多关于WAF日志查询与分析的应用，请参见日志应用教程。

如果您需要修改WAF日志存储规则、存储容量等设置，请参见日志存储管理。

1.5. 日志应用教程

1.5.1. 日志查询

为网站域名开启WAF日志采集后，您可以使用日志查询功能对采集到的日志数据进行实时查询与分析，并基于查询与分析结果生成统计图表、创建告警等。

前提条件

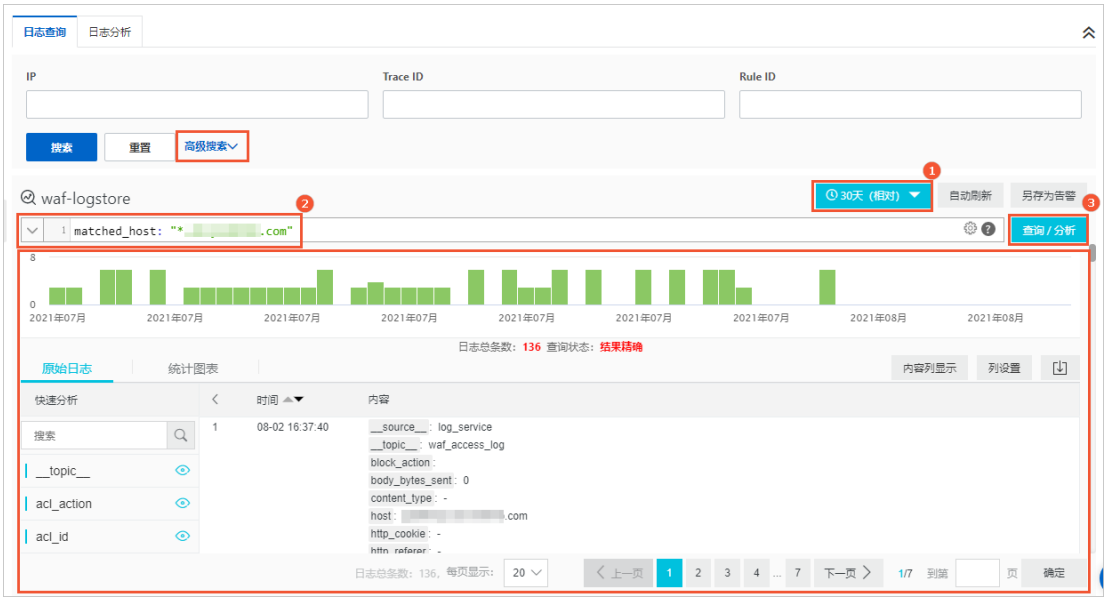
- 已开通WAF日志服务。相关操作，请参见步骤1：开通WAF日志服务。
- 已为接入WAF防护的网站域名开启日志采集。相关操作，请参见步骤2：开启日志采集。

查询和分析日志

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 在**日志服务**页面上方，选择要操作的网站域名。

> **注意** 域名必须已经开启日志采集（即**状态**开关已打开），否则WAF不会采集其日志数据，也不提供查询与分析服务。

5. 在**日志查询**页签，使用查询分析语句对WAF日志数据进行查询与分析：



i. 通过时间选择器（图示①），修改日志查询时间范围。

ii. 在语句输入框（图示②），输入查询语句。

查询语句采用阿里云日志服务专用语法，关于该语法的详细介绍，请参见查询语法。查询语句中使用WAF日志包含的字段作为查询字段，关于支持使用的查询字段，请参见WAF日志字段。
如果您不了解日志查询语法，推荐您使用**高级搜索**。您只需在语句输入框上方展开**高级搜索**，设置搜索条件并单击**搜索**，语句输入框即可自动生成与搜索条件匹配的日志查询语句。

下表描述了高级搜索支持设置的搜索条件。

搜索条件	说明
IP	发起请求的客户端的IP地址。
Trace ID	WAF为客户端请求生成的唯一标识。WAF向客户端返回拦截页面或者滑块验证响应时会提供该ID，用于问题分析与故障排查。
Rule ID	请求命中的WAF防护规则ID。您可以在**安全报表**或者**系统管理 > 防护规则组**页面，获取规则ID信息。
服务器响应状态码	源站服务器响应WAF回源请求的HTTP状态码。
WAF返回客户端响应码	WAF响应客户端请求的HTTP状态码。
拦截规则	请求命中的WAF防护规则的类型。关于WAF防护模块的介绍及不同模块防护规则的配置方法，请参见概述。

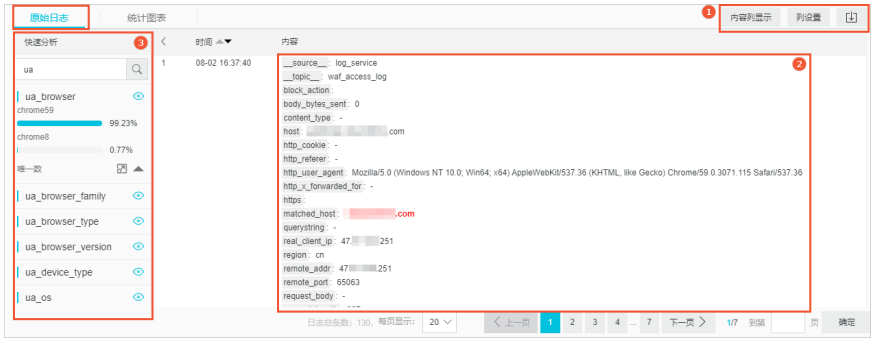
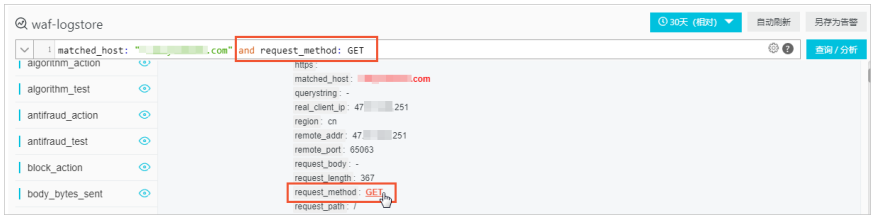
iii. 如果您需要对查询结果进行计算和统计分析，可以在语句输入框（图示②）已输入的查询语句后，输入分析语句；如果您只需要查询满足条件的日志数据，可以跳过该步骤。

分析语句和查询语句间使用竖线（|）分隔。分析语句采用标准的SQL92语法，关于分析语句的更多介绍，请参见分析概述。

iv. 单击**查询/分析**（图示③）。
查询与分析结果（即命中查询条件的WAF日志数据）将会显示在页面下方，包含日志分布直方图、**原始日志**及**统计图表**。您可以基于查询结果进行快速分析、生成统计图表、设置告警等，相关操作，请参见操作查询与分析结果、创建告警。

关于查询与分析语句的案例，请参见查询与分析案例。

操作查询与分析结果

结果类型	说明
日志分布直方图	日志分布直方图位于语句输入框下方，展示了查询到的日志数据在时间上的分布。  您可以在该区域执行以下操作： • 将光标放置在某个日志数据（即绿色数据块）上，查看该日志数据的产生时间范围和日志记录次数。 • 单击某个日志数据，查看该日志数据产生时间范围内的日志分布直方图。
原始日志	**原始日志**位于日志分布直方图下方，以分页形式展示每一条日志的详细内容（即日志包含的Key-Value字段信息）。  您可以在原始日志右上角（图示①区域）执行以下操作： • **内容列显示**：修改原始日志**内容**列的显示方式，例如是否换行显示、是否隐藏默认字段、JSON默认展开层级、长字符串折叠设置等。 • **列设置**：原始日志默认只显示**内容**列，您可以通过**列设置**，将指定的字段设置为以列形式显示。 • 日志下载：单击  图标，可以将日志下载到本地计算机，支持**直接下载**、**通过Cloud Shell下载**、**通过命令行工具下载**等方式。具体操作，请参见下载日志。 基于原始日志字段快速查询（图示②区域） 您可以在原始日志的**内容**列，单击某个字段的值，查询具有该字段属性的日志。例如，单击 `request_method: GET` 的值 `GET` ，语句输入框中将自动增加 `and request_method: GET` 查询语句（表示在原有查询基础上，查询 `request_method` 为 `GET` 的日志），并展示相应的查询结果。  **快速分析**（图示③区域） 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。操作说明如下： 1. 单击某个字段右侧的 

结果类型	说明
	图标，分析该字段取值的分布情况，返回占比最高的前10个结果。例如，单击 ua_browser 字段后的  图标，分析日志数据中占比最高的前10个浏览器类型。 2. 单击  图标，将上一步使用的分析语句添加到语句输入框，并跳转到**统计图表**页签，查看更详细的分析图表。 如果字段取值数量超过10个，您可以单击**唯一数**，分析字段取值的去重统计数量。
统计图表	关于快速分析的更多介绍，请参见快速分析。 **统计图表**位于日志分布直方图下方，以图表的形式为您展示了分析结果。您必须在语句输入框中输入SQL92分析语句，才可以在**统计图表**页签查看对应的统计图表。  统计图表区域支持以下操作： • 切换图表类型（图示①区域）：选择不同的图表类型来查看分析结果。关于不同图表类型的介绍，请参见图表设置。 • 预览图表（图示②区域）：切换图表类型后，查看图表预览效果。 单击**添加到仪表盘**，可以将当前图表添加到仪表盘。单击**下载日志**，可以将日志下载到本地计算机，支持**直接下载**、**通过Cloud Shell下载**、**通过命令行工具下载**等方式。具体操作，请参见下载日志。 • 修改统计图表配置（图示③区域）： ○ **属性配置**：用于配置图表的显示属性，包括X轴、Y轴数据源、边距、字号等，不同的图表属性不同。适用于所有的查询分析场景。 ○ **数据源**：用于设置占位符变量，如果有图表的下钻行为是跳转到这个图表所在的仪表盘，那么当变量名一致的情况下，会将单击触发下钻的数据替换为此处设置的占位符变量，重新执行分析。适用于下钻场景中的目的仪表盘。具体操作，请参见设置交互事件。 ○ **交互行为**：用于设置该图表的下钻动作，设置后，在仪表盘中单击该图表中的值，即可执行指定的下钻动作。适用于下钻场景中的触发下钻图表。具体操作，请参见设置交互事件。 关于统计图表的更多介绍，请参见统计图表概述。

创建告警

您可以基于当前查询与分析语句创建告警。创建告警后，日志服务将定期检查查询与分析结果，并在检查结果满足预设条件时，向您发送告警通知，实现实时的服务状态监控。

在查询语句输入框右上方，单击**另存为告警**，并完成**创建告警**配置向导，即可创建告警。具体操作，请参见设置告警。

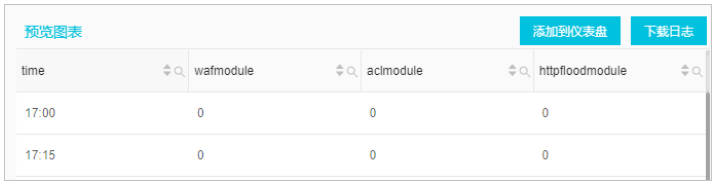
查询与分析案例

- 以15分钟为步长，分析在整点时刻由不同WAF防护模块拦截的攻击请求的数量，展示时间（time）、WAF

规则防护引擎拦截请求数（wafmodule）、IP黑名单及自定义防护策略（ACL访问控制）拦截请求数（aclmodule）、CC安全防护及自定义防护策略（CC攻击防护）拦截请求数（httpfloodmodule）。

```
* |
SELECT
 time_series(__time__, '15m', '%H:%i', '0') as time,
 COUNT_if(final_plugin = 'waf') as "wafmodule",
 COUNT_if(final_plugin = 'acl') as "aclmodule",
 COUNT_if(final_plugin = 'cc') as "httpfloodmodule"
GROUP by
 time
ORDER by
 time
```

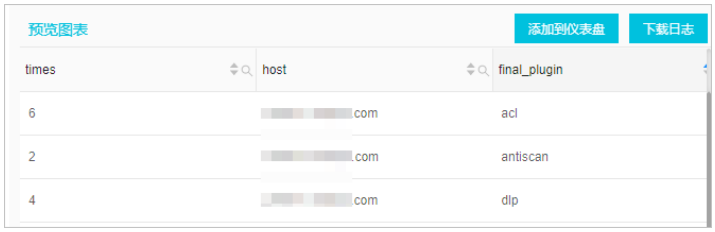
统计图表如下图所示。



- 分析触发了WAF最终防护动作的防护模块类型（final_plugin）的分布情况，展示命中次数（times）、被请求域名（host）和最终防护模块（final_plugin）。

```
* |
SELECT
 count(*) as times,
 host,
 final_plugin
GROUP by
 host,
 final_plugin
ORDER by
 times desc
```

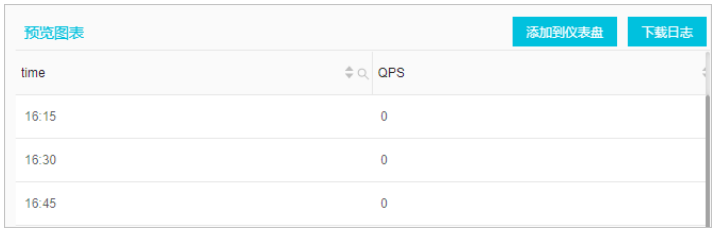
统计图表如下图所示。



- 以15分钟为步长，分析整点时刻的QPS，展示时间（time）和QPS（QPS）。

```
* |
SELECT
 time_series(__time__, '15m', '%H:%i', '0') as time,
 count(*) / 900 as QPS
GROUP by
 time
ORDER by
 time
```

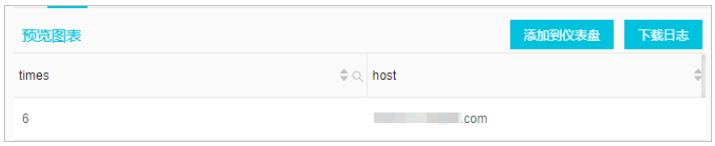
统计图表如下图所示。



- 分析受CC攻击次数最多的域名，展示CC攻击拦截次数（times）和被访问域名（host）。

```
*
and acl_action :block |
SELECT
 count(*) as times,
 host
GROUP by
 host
ORDER by
 times desc
```

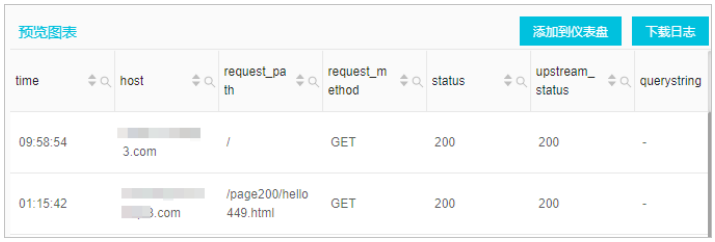
统计图表如下图所示。



- 以秒为步长，分析网站请求日志的详情，展示时间（time）、被访问域名（host）、被访问路径（request_path）、请求方法（request_method）、WAF响应客户端请求的HTTP状态码（status）、源站响应WAF回源请求的HTTP状态码（upstream_status）、查询字符串（querystring）。

```
* |
SELECT
 date_format(date_trunc('second', __time__), '%H:%i:%s') as time,
 host,
 request_path,
 request_method,
 status,
 upstream_status,
 querystring
LIMIT
 10
```

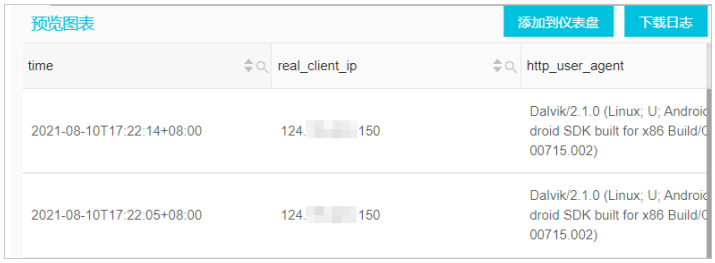
统计图表如下图所示。



- 查询网站（*your_domain_name*）遭受的最近10条攻击请求记录，展示请求发起时间（time）、真实客户端IP（real_client_ip）和客户端类型（http_user_agent）。

```
matched_host: your_domain_name
and final_action: block |
SELECT
 time,
 real_client_ip,
 http_user_agent
ORDER by
 time desc
LIMIT
 10
```

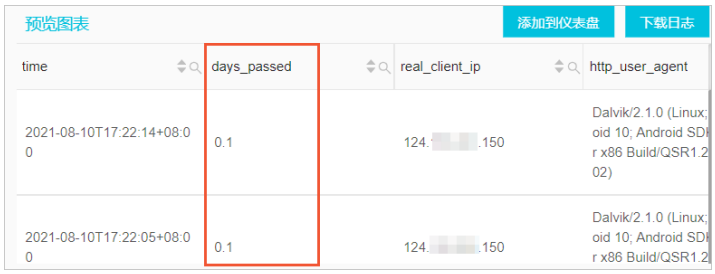
统计图表如下图所示。



- 分析网站（*your_domain_name*）遭受的攻击请求被WAF拦截后经过的天数（days_passed，保留1位小数）。

```
matched_host: your_domain_name
and final_action: block |
SELECT
 time,
 round((to_unixtime(now())-__time__) / 86400, 1) as "days_passed",
 real_client_ip,
 http_user_agent
ORDER by
 time desc
LIMIT
 10
```

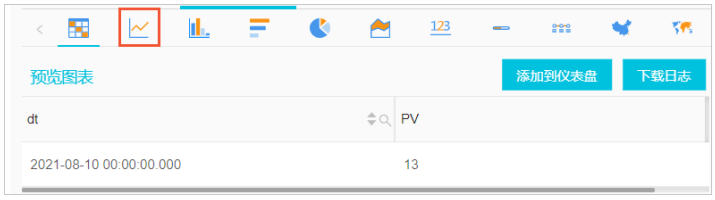
统计图表如下图所示。



- 分析网站（*your_domain_name*）遭受的攻击请求次数按天的变化趋势。

```
matched_host: your_domain_name
and final_action: block |
SELECT
 date_trunc('day', __time__) as dt,
 count(1) as PV
GROUP by
 dt
ORDER by
 dt
```

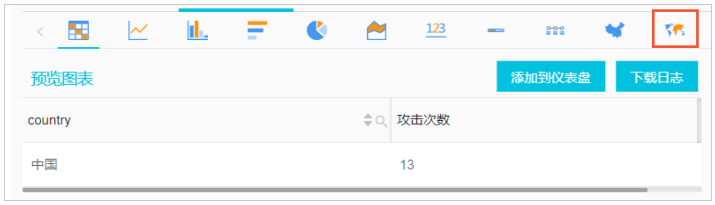
date_trunc函数用于对当前时间进行按天对齐分组。关于该函数的更多介绍，请参见日期和时间函数。
统计图表如下图所示。推荐您使用线图方式查看分析结果。



- 分析网站（*your_domain_name*）遭受的攻击请求的来源国家（country）分布。

```
matched_host: your_domain_name
and final_action: block |
SELECT
 ip_to_country(
  if(real_client_ip = '-', remote_addr, real_client_ip)
 ) as country,
 count(1) as "攻击次数"
GROUP by
 country
```

WAF日志中 real_client_ip 字段表示真实客户端IP。如果由于用户通过代理服务器访问或请求头中IP字段有误等原因无法获取真实客户端IP（ real_client_ip 取值为 - ），也可以直接使用 remote_addr 字段（表示直连客户端IP）作为真实客户端IP。
统计图表如下图所示。推荐您使用世界地图方式查看分析结果。

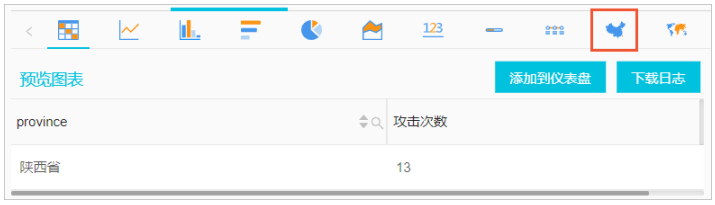


- 分析网站（*your_domain_name*）遭受的攻击请求的来源省份（province）分布。

```
matched_host: your_domain_name
and final_action: block |
SELECT
 ip_to_province(
  if(real_client_ip = '-', remote_addr, real_client_ip)
 ) as province,
 count(1) as "攻击次数"
GROUP by
 province
```

ip_to_province函数用于获取真实客户端IP对应的省份信息。关于该函数的更多介绍，请参见IP函数。

统计图表如下图所示。如果攻击IP均属于中国，推荐您使用中国地图方式查看分析结果。



1.5.2. 查看日志分析仪表盘

日志分析仪表盘是以图表形式展示的日志查询与分析结果。WAF日志服务基于常见的业务及防护查询场景，为您预置了运营中心、访问中心、安全中心仪表盘，方便您无需输入查询与分析语句，仅通过修改查询时间，即可快速查询您关心的网站业务和安全数据。

前提条件

- 已开通WAF日志服务。相关操作，请参见步骤1：开通WAF日志服务。
- 已为接入WAF防护的网站域名开启日志采集。相关操作，请参见步骤2：开启日志采集。

背景信息

仪表盘是日志服务提供的实时数据分析大盘。您可以在仪表盘查看多个基于查询与分析结果的统计图表。开通WAF日志服务及开启日志采集后，您可以直接使用WAF为您预置的三个日志分析仪表盘（如下表所示），查看网站的业务和安全数据图表。

仪表盘	说明
运营中心	展示网站的流量防护过程数据及攻击概况等信息。
访问中心	展示网站的访问指标、趋势及请求分布等信息。
安全中心	展示网站的被攻击指标、趋势及攻击来源分布等信息。

仪表盘由一系列图表组成。关于WAF预置仪表盘包含的具体图表的介绍，请参见WAF预置仪表盘支持的图表。

您也可以根据业务相关的查询与分析场景，手动创建更多的日志分析仪表盘，并基于您常用的查询与分析语句在仪表盘添加自定义图表。更多信息，请参见可视化概述。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 在**日志服务**页面上方，选择要操作的网站域名。

> **注意** 域名必须已经开启日志采集（即**状态**开关已打开），否则WAF不会采集其日志数据，也不提供查询与分析服务。

5. 单击**日志分析**页签。

6. 单击**运营中心**、**访问中心**、**安全中心**页签，选择要查看的仪表盘，然后通过时间选择器设置查询时间，查看指定时间范围内的仪表盘图表。

关于不同仪表盘支持的图表类型的介绍，请参见WAF预置仪表盘支持的图表。
关于仪表盘支持的通用操作的介绍，请参见相关操作。

相关操作

操作	适用对象	说明
设置时间选择器	仪表盘、图表	每个仪表盘包含多种图表，这些图表是基于特定时间段内的原始日志数据生成的。您可以通过设置时间选择器，选择图表数据的时间范围。时间选择器分为以下类型： • 仪表盘时间选择器：适用于当前仪表盘下的所有图表。通过该选择器设置时间，表示使当前仪表盘内所有图表都按照该时间展示结果。 仪表盘时间选择器位于仪表盘右上角。每次进入**日志分析**页面时，默认未设置时间，此时时间选择器显示**请选择**。单击**请选择**，可以在**时间**面板为仪表盘所有图表设置时间范围。您可以选择相对时间、整点时间或自定义时间范围。 **说明** 仪表盘时间选择器设置仅适用于当前仪表盘。如果您切换了仪表盘，需要重新设置仪表盘时间选择器。 • 图表时间选择器：仅适用于仪表盘下的某个图表。 在某个图表区域，将光标放置在图表右上角的 ⋮ 图标，并单击**选择时间范围**，可以在**时间**面板为该图表设置时间范围。
创建订阅	仪表盘	您可以订阅仪表盘，即将仪表盘的图形报表，以邮件或者钉钉群消息的方式，定期自动发送给指定人员。 在仪表盘右上角单击**订阅**，并完成**创建订阅**配置向导，即可订阅当前仪表盘。 更多信息，请参见订阅仪表盘。

操作	适用对象	说明
图表数据下钻	图表	仪表盘中部分图表默认已经配置数据下钻，为您提供更多维度的详细统计数据。 在某个图表区域，将光标放置在图表右上角的 图标，如果在弹出的操作框中有  图标，表示该图表已经配置数据下钻操作。 对于已经配置数据下钻的图表，您可以单击图表中带有下划线的数字，查看该数字底层更详细的数据。例如，单击**安全中心**仪表盘**被攻击网站**图表中的数字，您可以快速查看到被攻击的具体网站域名和遭受的攻击次数。 **说明** 您也可以切换到**原始日志**页签，查看相关的原始日志。 更多信息，请参见设置交互事件。
下载日志	图表	在某个图表区域，将光标放置在图表右上角的 图标，在弹出的操作框中单击**下载日志**，可以将当前图表对应的数据以CSV文件的形式下载到本地计算机。
预览查询语句	图表	在某个图表区域，将光标放置在图表右上角的 图标，在弹出的操作框中单击  图标，可以预览当前图表对应的查询语句。

WAF预置仪表盘支持的图表

WAF日志服务预置了运营中心、访问中心、安全中心仪表盘，分别用于展示网站业务流量的运营状况、业务访问状况、业务被攻击状况。不同仪表盘提供不同的图表，具体说明如下：

- **运营中心**：展示网站的流量防护过程数据及攻击概况等信息，具体包含下表所罗列的图表。

图表名称	类型	默认时间范围	说明	示例值
用户请求	单值图	同比昨日	用户请求PV、UV数量。	48.3千次
流量峰值	单值图	同比昨日	互联网入方向、出方向流量的峰值及攻击流量的峰值，单位：KB/s。	4.6
有效请求率	单值图	环比1小时前	互联网流量经WAF分析后，其中有效请求的占比。	98.41%
有效流量	单值图	环比1小时前	WAF回源到Web业务服务器的有效流量大小（入方向、出方向），单位：MB。	10.7

图表名称	类型	默认时间范围	说明	示例值
请求趋势	线图	1周（相对）	请求次数与请求有效率的变化趋势、入方向及出方向网络带宽大小（单位：KB/S）的变化趋势。	无
攻击统计	单值图、世界地图、中国地图	环比1小时前	攻击的数量、流量大小（单位：KB）及其在世界地图、中国地图上的分布。	无
攻击者列表	表格	1小时（相对）	对网站业务发起攻击的IP列表。	无
被攻击网站Top 100	表格	1小时（相对）	遭受攻击最多的前100个网站域名。	无

- **访问中心**：展示网站的访问指标、趋势及请求分布等信息，具体包含下表所罗列的图表。

图表名称	类型	默认时间范围	说明	示例值
PV	单值图	1小时（相对）	请求总数。	100千次
UV	单值图	1小时（相对）	独立的访问客户端总数。	100次
流入流量	单值图	1小时（相对）	网站的入方向流量总和，单位：MB。	300 MB
网络in带宽峰值	单值图	今天（整点时间）	网站请求的入方向流量速率的峰值，单位：KB/s。	0.5 KB/s
网络out带宽峰值	单值图	今天（整点时间）	网站请求的出方向流量速率的峰值，单位：KB/s。	1.3 KB/s
流量带宽趋势	面积图	今天（整点时间）	网站流入、出方向流量趋势图，单位：KB/s。	无
PV/UV访问趋势	线图	今天（整点时间）	PV、UV趋势图，单位：次。	无
访问状态分布	流图	今天（整点时间）	访问请求响应状态（400、304、200等状态码）的趋势图，单位：个/小时。	无
访问来源	世界地图	1小时（相对）	访问请求的来源国家分布。	无
流入流量来源（世界）	世界地图	1小时（相对）	访问请求的入方向流量来源国家分布。	无
流入流量来源（中国）	中国地图	1小时（相对）	访问请求的入方向流量来源省份（中国）分布。	无
访问热力图	高德地图	1小时（相对）	访问请求来源在地理位置上的访问热力图。	无

图表名称	类型	默认时间范围	说明	示例值
来源网络提供商	饼图	1小时（相对）	访问请求来源的网络服务提供商（例如电信、联通、移动、教育网等）分布情况。	无
Referer	表格	1小时（相对）	经跳转次数最多的前100个Referer URL、主机及出现次数信息。	无
移动客户端类型分布	饼图	1小时（相对）	移动客户端请求的客户端类型分布情况。	无
PC端客户端类型分布	饼图	1小时（相对）	PC客户端请求的客户端类型分布情况。	无
请求内容类型分布	饼图	1小时（相对）	请求内容类型（例如HTML、Form、JSON、流数据等）分布情况。	无
访问域名	矩形树图	1小时（相对）	前30个被访问最多的网站域名。	无
访问最多的客户端	表格	1小时（相对）	发起请求次数最多的前100个客户端的信息，包括客户端IP、地域城市、网络、请求方法分布、流入流量、错误访问次数、攻击次数等。	无
响应最慢的URL	表格	1小时（相对）	前100个响应时间最长的URL信息，包括网站域名、URL、平均响应时间、访问次数等。	无

- **安全中心**：展示网站的被攻击指标、趋势及攻击来源分布等信息，具体包含下表所罗列的图表。

图表名称	类型	默认时间范围	说明	示例值
攻击峰值	单值图	1小时（相对）	遭受的攻击流量峰值，单位：Bps。	100 Bps
被攻击网站	单值图	今天（整点时间）	遭受攻击的网站个数。	3个
攻击来源国家	单值图	今天（整点时间）	攻击请求来源国家个数。	2个
攻击流量	单值图	1小时（相对）	攻击请求流量总和，单位：B。	1 B
攻击者UV	单值图	1小时（相对）	攻击请求来源的独立客户端个数。	40个
攻击类型分布	流图	今天（整点时间）	攻击请求的攻击类型分布。	无

图表名称	类型	默认时间范围	说明	示例值
攻击拦截	单值图	1小时（相对）	WAF拦截的攻击请求总次数。	100次
CC攻击拦截	单值图	1小时（相对）	WAF拦截的CC攻击请求次数。	10次
Web攻击拦截	单值图	1小时（相对）	WAF拦截的Web应用攻击请求次数。	80次
访问控制事件	单值图	1小时（相对）	被WAF自定义防护策略（ACL访问控制）拦截的请求次数。	10次
CC攻击（世界）	世界地图	1小时（相对）	CC攻击请求的来源国家分布。	无
CC攻击（中国）	中国地图	1小时（相对）	CC攻击请求的来源省份（中国）分布。	无
Web攻击（世界）	世界地图	1小时（相对）	Web应用攻击请求的来源国家分布。	无
Web攻击（中国）	中国地图	1小时（相对）	Web应用攻击请求的来源省份（中国）分布。	无
访问控制攻击（世界）	世界地图	1小时（相对）	WAFWAF自定义防护策略（ACL访问控制）拦截的攻击请求的来源国家分布。	无
访问控制攻击（中国）	中国地图	1小时（相对）	WAFWAF自定义防护策略（ACL访问控制）拦截的攻击请求的来源省份（中国）分布。	无
被攻击网站	矩形树图	1小时（相对）	遭受攻击最多的网站域名排名。	无
CC防护策略分布	饼图	1小时（相对）	触发的CC防护策略分布情况。	无
Web攻击类型分布	饼图	1小时（相对）	遭受的Web攻击类型分布情况。	无
攻击者列表	表格	1小时（相对）	前100位攻击者的IP、所在省份、网络运营商信息，以及发起的各类攻击次数和攻击流量。	无
攻击者Referer	表格	1小时（相对）	攻击请求的Referer统计信息，包括Referer URL、Referer主机、出现次数。	无

关于图表类型的介绍，请参见统计图表概述。

1.5.3. 为RAM用户授予日志查询分析权限

如果RAM用户需要使用WAF日志查询分析服务，需要由阿里云账号为其进行授权操作。

背景信息

开通和使用WAF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）	阿里云账号
授权WAF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）	• 阿里云账号 • 具备 `AliyunLogFullAccess` 权限的RAM用户 • 具备指定权限的RAM用户
使用日志查询分析功能	• 阿里云账号 • 具备 `AliyunLogFullAccess` 权限的RAM用户 • 具备指定权限的RAM用户

您也可以根据实际需求为RAM用户授予相关权限。

授权场景	授予权限	操作步骤
为RAM用户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，请参见为RAM用户授权。
阿里云账号开通WAF日志查询分析服务并完成授权操作后，为RAM用户授予日志查看权限。	授予只读权限 `AliyunLogReadOnlyAccess`	具体操作步骤，请参见为RAM用户授权。
仅为RAM用户授予开通和使用WAF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RAM用户授予该自定义授权策略。	具体操作步骤，请参见本文操作步骤章节。

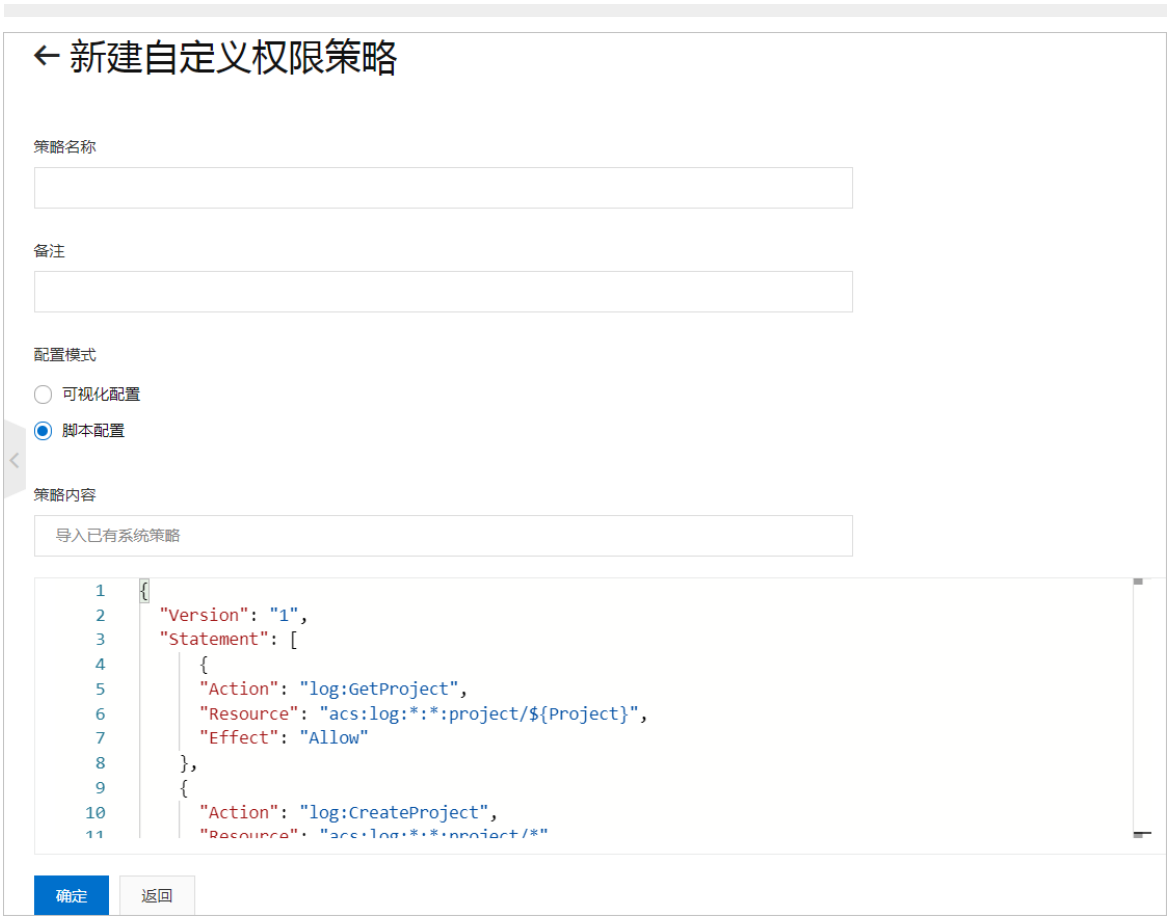
操作步骤

1. 使用阿里云账号登录RAM控制台。
2. 在左侧导航栏，选择**权限管理 > 权限策略**。
3. 在**权限策略**页面，单击**创建权限策略**。
4. 在**新建自定义权限策略**页面，输入**策略名称**和**备注**。
5. 选择**脚本配置**模式，输入以下**策略内容**。

> 注意 请将以下策略内容中的 `${Project}` 与 `${Logstore}` 分别替换为您的WAF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"
   }
  ]
}
```



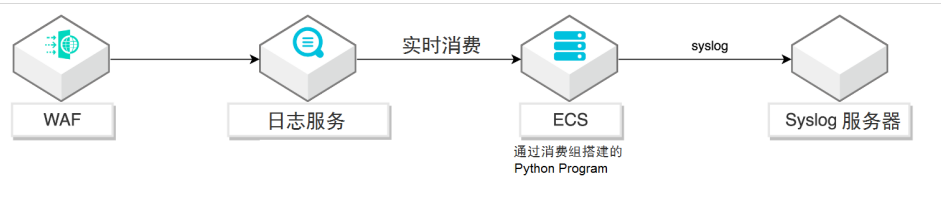
6. 单击**确定**。
7. 在**人员管理 > 用户**页面，找到需要授权的RAM用户，并单击操作列的**添加权限**。
8. 选择您所创建的自定义授权策略，单击**确定**。
   完成授权后，被授权的RAM用户将可以开通和使用WAF日志查询分析服务，但无法操作日志服务产品的其他功能。

1.5.4. 集成WAF日志到Syslog系统

本文介绍了如何使用Python Program将Web应用防火墙（WAF）的日志集成到Syslog日志系统中，以实现合规、审计等要求，也方便您在安全操作中心统一管理所有相关日志。

背景信息

该方案的整体集成架构如下图所示：



阿里云日志服务为日志数据提供一站式服务，被广泛应用于阿里巴巴集团的许多大数据场景中。日志服务在无需开发介入的前提下，帮助您快速完成数据采集、消费、投递、查询和分析，提高运维运营效率，建立DT时代海量数据的处理能力。Web应用防火墙集成了日志服务的能力，通过WAF日志服务功能提供网站访问日志的采集、查询、分析等服务。更多信息，请参见WAF日志服务概述。

Python Program是运行在ECS上的一段日志投递程序，帮助您将WAF日志投递到Syslog服务器。消费库（Consumer Library）是对LogHub消费者提供的高级模式，它使用消费组（Consumer Group）统一处理消费端问题。相比于直接使用SDK读取数据，消费库让您只关注业务逻辑，而无需在意日志服务的实施细节或多消费者间的容错问题。更多信息，请参见消费组消费。

Syslog服务器是一个集中的日志消息管理服务器，它可以从多个Syslog源接收数据。

前提条件

- 您已开通WAF日志服务并为网站域名开启日志采集。更多信息，请参见以下文档：
  - 步骤1：开通WAF日志服务
  - 步骤2：开启日志采集
- 您拥有一个Linux ECS服务器，该服务器满足以下推荐配置：
  - Ubuntu操作系统
  - 8核处理器，2.0 Ghz以上主频率
  - 32 GB内存
  - 可用磁盘空间大于2 GB（建议在10 GB以上）
- 您拥有一个Syslog服务器，并开放UDP协议514端口用来接收Syslog数据。

操作步骤

您需要先在ECS实例中安装日志服务的Python SDK，然后配置Python Program，投递WAF日志到Syslog服务器。具体操作步骤如下：

1. 通过SSH或ECS控制台远程连接ECS实例。具体操作请参见连接ECS实例。
2. 安装Python3、pip和aliyun-log-python-sdk。关于日志服务Python SDK的介绍，请参见用户指南。

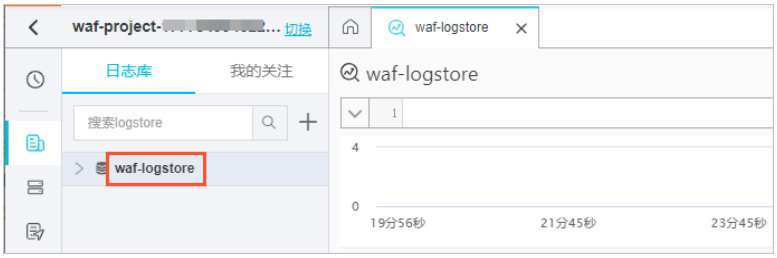
```
apt-get update
apt-get install -y python3-pip python3-dev
cd /usr/local/bin
ln -s /usr/bin/python3 python
pip3 install --upgrade pip
pip install aliyun-log-python-sdk
```

3. 执行以下命令，从GitHub下载最新的集成示例代码。

```
wget https://raw.githubusercontent.com/aliyun/aliyun-log-python-sdk/master/tests/consumer_group_examples/sync_data_to_syslog.py
```

4. 替换示例代码Python Program中与日志服务（SLS）、Syslog相关的配置参数，具体包括：

参数	释义	描述
SLS Project	日志项目名称	日志项目（Porject）是日志服务的资源管理单元，用来划分和操作资源。 您可以登录阿里云日志服务控制台查看WAF日志服务项目。 WAF日志服务项目的名称以 **waf-project** 开头。**华东1（杭州）**地域的项目表示中国内地WAF实例的日志项目，**新加坡**地域的项目表示海外地区WAF实例的日志项目。 

参数	释义	描述
SLS Endpoint	日志服务入口	日志服务入口是访问一个日志项目及其内部日志数据的URL。它和项目所在的阿里云地域及日志项目名称相关。要查看日志服务的入口URL，请参见服务入口。
SLS Logstore	日志库	日志库（Logstore）是日志服务用来采集、存储和查询日志数据的单元。每个日志库归属在一个项目下，每个项目可以拥有多个日志库。 您可以登录阿里云日志服务控制台，单击WAF日志服务项目后，在WAF日志服务项目中查看日志库的名称。 
SLS AccessKey ID和AccessKey Secret	访问密钥	访问密钥是您在使用API（而非控制台）访问云资源时的密码。您需要使用AccessKey为API请求内容签名，使其能够通过日志服务的安全认证。具体请参见访问密钥。 您可以登录用户信息管理控制台查看您的AccessKey信息。 
Syslog Host	Syslog主机	Syslog服务器的IP地址或主机名称。
Syslog Port	Syslog端口	接收Syslog的端口。UDP协议使用514，TCP协议使用1468。
Syslog protocol	Syslog协议	指定使用UDP或TCP协议来接收Syslog数据，具体取决于Syslog服务器的配置。
Syslog separator	Syslog分隔符	指定用于分隔Syslog键值对的分隔符。

以下是Python Program的配置示例。

- 日志服务配置

```
endpoint = os.environ.get('SLS_ENDPOINT', 'http://ap-southeast-1.log.aliyuncs.com')
accessKeyId = os.environ.get('SLS_AK_ID', '替换成您自己的AccessKey ID')
accessKey = os.environ.get('SLS_AK_KEY', '替换成您自己的AccessKey Secret')
project = os.environ.get('SLS_PROJECT', 'waf-project-548613414276****-ap-southeast-1')
logstore = os.environ.get('SLS_LOGSTORE', 'waf-logstore')
consumer_group = os.environ.get('SLS_CG', 'WAF-SLS')
```

- Syslog配置

```
settings = {
        "host": "1.2.xx.xx",
        "port": 514,
        "protocol": "udp",
        "sep": ",",
        "cert_path": None,
        "timeout": 120,
        "facility": syslogclient.FAC_USER,
        "severity": syslogclient.SEV_INFO,
        "hostname": None,
        "tag": None
      }
```

5. 启用Python Program。假设Python program被保存为 `sync_data_to_syslog.py` ，您可以使用以下命令启用它：

   ```
   python sync_data_to_syslog.py
   ```

   启用Python Program后，会显示成功投递日志到Syslog服务器。

   ```
   *** start to consume data...
   consumer worker "WAF-SLS-1" start
   heart beat start
   heart beat result: [] get: [0, 1]
   Get data from shard 0, log count: 6
   Complete send data to remote
   Get data from shard 0, log count: 2
   Complete send data to remote
   heart beat result: [0, 1] get: [0, 1]
   ```

完成以上操作后，您可以在Syslog服务器中查询WAF日志。

1.6. 日志存储管理

1.6.1. 修改日志设置

开通WAF日志服务后，您可以通过日志设置，修改日志存储时长、要存储的日志字段类型、日志存储类型（全量日志、仅拦截日志）。合理的日志设置可以帮助您更有效地利用日志存储容量，建议您根据业务防护及分析需要、等级保护合规要求等来修改日志设置。

前提条件

已开通WAF日志服务。相关操作，请参见步骤1：开通WAF日志服务。

背景信息

日志设置对所有已开启日志采集的网站域名生效。关于为域名开启日志采集的操作，请参见步骤2：开启日志采集。

目前，仅企业版及以上版本的包年包月WAF实例支持修改日志存储时长。自定义字段配置、修改日志存储类型无版本限制。

操作步骤

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。

3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 在**日志服务**页面右上角，单击**日志设置**。
5. 在**日志设置**页面，根据需要修改以下设置。

参数	说明
日志存储时长	要存储多长时间范围内的日志，单位：天，可选范围：30~360。 超过存储时长范围的日志将被删除，且不再支持查询与分析。例如，存储时长为180天，则180天以前的日志将被删除。 **说明** 仅企业版及以上版本的包年包月WAF实例支持修改日志存储时长。
自定义字段配置	WAF日志中要包含哪些WAF支持的日志字段。 WAF日志字段分为**必选字段**和**可选字段**。必选字段不支持修改，表示WAF日志中必须包含这些字段；可选字段支持修改，您可以根据需要配置要在WAF日志中包含哪些可选字段。关于WAF日志字段的说明，请参见WAF日志字段。 在**可选字段**区域，您可以从左侧**待选字段**框中，将需要在WAF日志中包含的可选字段添加到右侧**已选字段**框中。
存储类型	要存储的日志类型。可选项： ○ **全量日志**：表示存储所有日志，包含WAF放行请求和拦截请求的日志。 ○ **拦截日志**：表示仅存储WAF拦截请求的日志。

6. 单击**保存**。

执行结果

日志设置修改成功后，WAF将按照已保存的设置来存储相关日志。

1.6.2. 管理日志存储空间

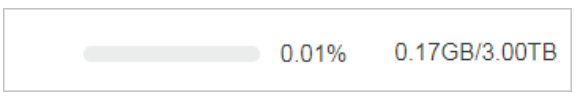
开通WAF日志服务后，系统将根据您所选择的日志存储规格分配日志存储空间，您可以在Web应用防火墙管理控制台的日志服务页面查看日志存储空间的使用情况。

前提条件

已开通WAF日志服务。相关操作，请参见步骤1：开通WAF日志服务。

查询存储使用量

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 日志服务**。
4. 在**日志服务**页面右上方，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。

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**日志服务**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。

> **说明** 开通WAF日志服务后，您总共有4次清空日志存储空间的机会。

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

> **警告** 日志清空后将无法复原，请务必谨慎使用清空功能。

2.全量日志（即将下线）

2.1. 使用全量日志

开启全量日志功能后，Web应用防火墙（WAF）将记录您网站的所有访问请求日志，您可以通过一键智能搜索快速定位请求记录，满足运维、安全方面的管理需求。

> 注意 全量日志功能仅对保有该功能的存量用户提供。新开通WAF时不再赠送全量日志功能。如果您需要使用网站访问日志，建议您开通WAF日志服务。更多信息，请参见步骤1：开通WAF日志服务。

背景信息

全量日志功能可以帮助您轻松地完成以下运维工作：

- 确认某个具体请求是否被WAF拦截或放行。
- 确认某个具体拦截是由Web攻击、CC攻击防护或是自定义的访问控制规则触发。
- 查询源站对于某个具体请求的响应时间，观察是否超时等。
- 通过源IP、URL关键字、Cookie、Referer、User-Agent、X-Forwarded-For、服务器响应状态码等条件组合查询具体的请求。

使用须知

- 开启全量日志即表示您允许阿里云记录您全部经过WAF的Web请求（POST数据不会被记录）。
- 全量日志只支持保存最近7天内的网站访问日志。

> 说明 如果您需要满足日志存储180天的等保要求，建议您开通WAF日志服务。更多信息，请参见步骤1：开通WAF日志服务。

- 一个WAF实例最多可以为100个域名开启全量日志。

开启全量日志

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**资产中心 > 网站接入**。
4. 定位到要操作的域名，开启**日志检索**开关。

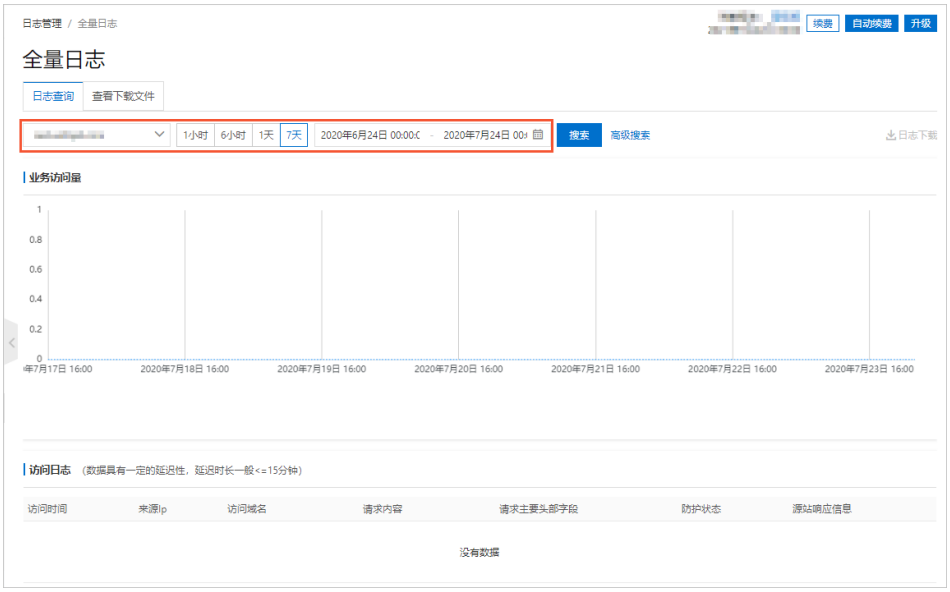
> 注意 只有保有全量日志功能的用户可以看到**日志检索**，否则您看到的是**日志服务**。关于日志服务的更多信息，请参见概述。

开启**日志检索**（即全量日志）后，WAF将开始记录当前网站的访问日志，并提供全量日志查询服务。如果您不需要全量日志服务，可以在**网站接入**页面为域名关闭**日志检索**开关。

> 注意 关闭**日志检索**后，网站的访问请求日志不会被记录。即使后续重新开启**日志检索**，您也无法查询到关闭期间的访问请求日志。

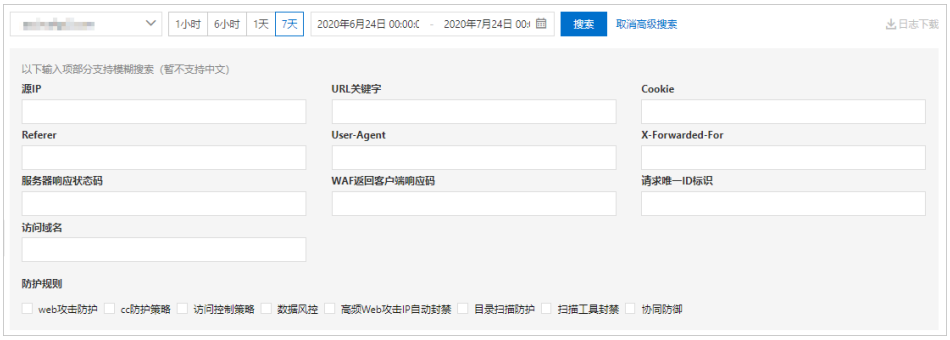
查询全量日志

1. 登录Web应用防火墙控制台。
2. 在顶部菜单栏，选择Web应用防火墙实例的资源组和地域（**中国内地**、**海外地区**）。
3. 在左侧导航栏，选择**日志管理 > 全量日志**。
4. 在**日志查询**页签下，选择要查询的域名，设置查询时间并单击**搜索**。

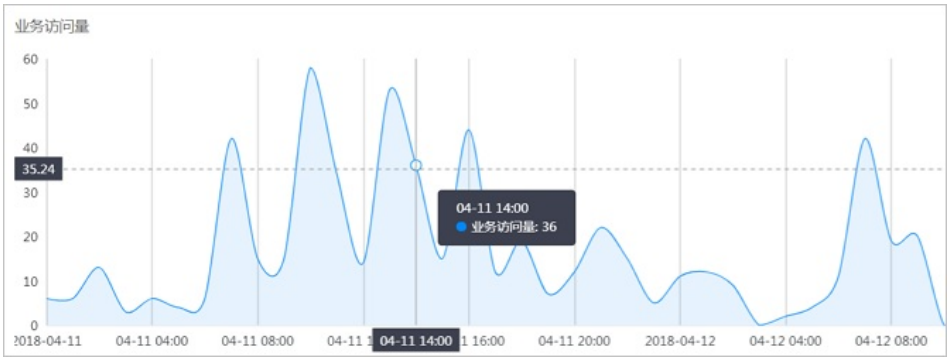


> **注意** 只支持查询最近7天的数据。

您也可以单击**高级搜索**，设置更详细的搜索条件。关于高级搜索支持的过滤字段，请参见高级搜索条件。



5. 查看日志搜索结果。
   - 在**业务访问量**区域，查看搜索时间范围内的访问请求量趋势图。



- 在**访问日志**列表，查看符合搜索条件的访问请求记录。
  例如，被访问控制策略拦截的访问请求记录如下图所示。关于日志字段的详细信息，请参见访问日志字段。

6. （可选）下载日志。

   您可以根据需要将当前搜索到的日志结果下载到本地。

   i. 单击**日志查询**页面右上方的**日志下载**。

   ii. 等待下载任务生成后，单击**查看下载文件**页签，将相应格式的日志文件下载到本地。

   > **说明** 单个下载任务最多支持导出2000万条日志。如果您需要导出的日志超过2000万条，建议您分多个任务进行导出。

高级搜索条件

字段	描述
源IP	访问的客户端来源IP。
URL关键字	访问请求URL。 **说明** 所填写的URL关键字支持包含正斜杠（/）符号。例如，您可以填写 `/ntis/cashier` 。
Cookie	访问请求头部中带有的访问来源客户端Cookie信息。
Referer	访问请求头部中带有的访问请求的来源URL信息。
User-Agent	访问请求头部中带有的访问来源客户端浏览器标识、操作系统标识等信息。
X-Forwarded-For	访问请求头部中带有的XFF头信息。
服务器响应状态码	源站服务器返回给WAF的响应状态信息。 状态码支持填写最多三位数字，且支持模糊搜索。例如，输入 `4*` 进行搜索，将查找所有以4开头的状态码。 **说明** • `*` 可以匹配0或多位数字，但不能以 `*` 开头。 • 支持填写 `-` ，查找无状态信息的访问请求。

字段	描述
WAF返回客户端响应码	WAF返回给客户端的响应状态信息。 响应码支持填写最多三位数字，且支持模糊搜索。例如，输入 `4*` 进行搜索，将查找所有以4开头的响应码。 **说明** • `*` 可以匹配0或多位数字，但不能以 `*` 开头。 • 支持填写 `-` ，查找无状态信息的访问请求。
请求唯一ID标识	指定访问请求。如果存在访问请求被拦截，可以填写拦截页面中的该请求的ID进行搜索。
访问域名	当您对泛域名启用全量日志功能，可以利用该字段对一级子域名进行搜索。
防护规则	选择命中的防护规则类型，包括**Web攻击防护**、**cc防护策略**、**访问控制策略**、**数据风控**、**高频Web攻击IP自动封禁**、**目录遍历防护**、**扫描工具封禁**、**协同防御**。

访问日志字段

名称	含义	描述
Time	访问时间	访问请求的发生时间，在所下载的日志文件中以UTC时间记录。
Domain	访问域名	访问请求的域名。
Source_IP	来源IP	访问的客户端来源IP。
IP_City	来源IP所属地区	访问来源IP所属地区，中国内地地区可精确到市级。
IP_Country	来源IP所属国家	访问来源IP所属国家。
Method	访问请求方法	访问的请求行中的请求类型。
URL	访问请求URL	访问请求行中的所访问的服务器资源。
Https	访问请求协议	访问请求行中的请求所使用的协议。
Referer	HTTP Referer字段	访问请求头部中带有的访问请求的来源URL信息。
User-Agent	HTTP User-Agent字段	访问请求头部中带有的访问来源客户端浏览器标识、操作系统标识等信息。
X-Forwarded-For	HTTP X-Forwarded-For字段	访问请求头部中带有的XFF头信息，用于识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址。
Cookie	HTTP Cookie字段	访问请求头部中带有的访问来源客户端Cookie信息。

名称	含义	描述
Attack_Type	防护状态	WAF对该访问请求的处理结果： • 0：表示未发现攻击。 • 1：表示触发Web应用攻击防护规则。 • 2：表示触发CC安全防护规则。 • 3：表示触发精准访问控制规则。 • 4：表示触发地区封禁防护策略。 • 5：表示触发数据风控防护策略。 • 6：表示触发高频扫描攻击封禁规则。 • 7：表示触发目录遍历扫描防护规则。 • 8：表示触发协同防护策略。 • 9：表示触发扫描工具封禁规则。
Status	响应状态码	WAF返回给客户端的响应状态信息。
Upstream_Status	源站响应状态码	源站返回给WAF的响应状态。如果返回 `-` ，表示没有响应，例如该请求被WAF拦截或源站响应超时。
Upstream_IP	源站响应IP	访问请求所对应的源站IP。例如，WAF回源到ECS的情况，该参数即返回源站ECS的IP。
Upstream_Time	源站响应时间	源站响应WAF请求的时间。如果返回 `-` ，表示响应超时。