ALIBABA CLOUD

阿里云

Web应用防火墙

安全服务

文档版本：20220318

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.概述

安全服务帮助您解决Web应用防火墙使用过程中遇到的问题，协助您完成网站接入、防护配置、安全分析等任务。

根据服务形式和计费方式的不同，Web应用防火墙提供以下安全服务。

名称	描述	是否收费	适用场景或对象	交付方式	开通方式
安全专家指导服务	您可以加入阿里云企业安全服务钉钉群或者创建企业专属的安全服务钉钉群，免费享受安全专家通过钉钉为您提供的一对一指导服务，解决产品使用过程中遇到的困难或紧急问题。	否	日常咨询	安全服务钉钉群或者企业专属钉钉群	开通Web应用防火墙后，通过控制台加入安全服务钉钉群。
WAF产品托管服务	您可以通过预付费方式开通WAF产品托管服务，享受阿里云原厂安全服务团队提供的全面的Web应用防火墙技术支持，例如接入设置、防护策略优化、监控与告警设置、安全报表定制等。 使用该服务时，您需要开通服务授权，允许阿里云安全服务专家查看您的业务场景数据，以便提供有针对性的防护咨询和日志数据深度分析建议。更多信息，请参见开通WAF安全服务授权。	是	需要外包专业人员协助进行安全产品服务运营的用户、企业级用户、国际用户	企业专属钉钉群、电话会议、邮件等	在WAF产品托管服务售卖页购买。

> **说明** 关于钉钉聊天应用，请参见阿里云钉钉官网首页。

2.安全专家指导服务

阿里云Web应用防火墙支持通过钉钉服务群为您提供免费的一对一专家指导服务。您在使用Web应用防火墙过程中遇到任何问题时，都可以通过Web应用防火墙管理控制台的专家指导服务入口获取7*24的Web应用防火墙产品帮助服务。

前提条件

- 已经开通过Web应用防火墙服务。更多信息，请参见开通Web应用防火墙。
- 已经在手机移动端安装并注册使用钉钉聊天应用。更多信息，请参见阿里巴巴钉钉官网。

背景信息

安全专家指导服务支持以下两种方式：

- 加入阿里云官方钉钉服务群咨询问题：适合咨询相对简单的问题，加入临时的官方产品服务群，不需要多个业务相关人员参与提问。
- 创建并使用企业专属钉钉服务群咨询问题：适合企业级用户，可以创建7*24的专属服务群，随时咨询产品使用过程中的任何问题，支持邀请多个企业业务相关人员共同参与提问。

加入阿里云官方钉钉服务群咨询问题

1. 登录Web应用防火墙控制台。
2. 在**总览**页面右上角，单击**有问题，找专家**。

   > **说明** 只有已经开通过Web应用防火墙服务后，才会显示**有问题，找专家**。

3. 打开手机钉钉应用，扫描显示的二维码，申请加入WAF紧急事件处理群。
   成功加入WAF紧急事件处理群后，您可以在群里直接咨询使用Web应用防火墙时遇到的问题。钉钉群内的安全专家将通过钉钉为您提供一对一指导服务，帮助您妥善解决Web应用防火墙产品使用过程中遇到的任何问题。

创建并使用企业专属钉钉服务群咨询问题

> **说明** 目前该入口仅向2020年6月后首次开通Web应用防火墙服务的用户开放。如果您在2020年6月之前已经开通过Web应用防火墙服务，则不支持通过Web应用防火墙控制台创建企业专属钉钉服务群，建议您通过阿里云官方钉钉服务群联系我们帮助您创建专属钉钉服务群。更多信息，请参见加入阿里云官方钉钉服务群咨询问题。

1. 登录Web应用防火墙控制台。
2. 在**总览**页面右上角，单击**有问题，找专家**。

   > **说明** 只有已经开通过Web应用防火墙服务后，才会显示**有问题，找专家**。

3. 创建企业专属钉钉服务群 。
   i. 单击**使用钉钉注册手机号**。

   > **说明** 只有在2020年6月后首次开通Web应用防火墙服务，才会显示**使用钉钉注册手机号**。

ii. 填写企业专属钉钉服务群的注册信息。

参数	说明
钉钉注册手机号	填写成功注册了钉钉应用的中国手机号码。
钉钉昵称	填写使用当前手机号码注册的钉钉名称。
企业名称	填写您的公司简称。示例：阿里云。

iii. 单击**提交**。
提交申请后，钉钉会立即为您创建专属的阿里云企业安全服务群，群名称默认为“【安全】*企业名称*企业服务群”。

> **说明** 如果您收到申请建群失败的提示，建议您通过扫描二维码的方式联系我们，安全专家收到您的问题后将会第一时间与您沟通。更多信息，请参见加入阿里云官方钉钉服务群咨询问题。

成功创建并加入阿里云企业安全服务群后，您可以在群里直接咨询使用Web应用防火墙时遇到的问题。钉钉群内的安全专家将通过钉钉为您提供一对一指导服务，帮助您快速解决Web应用防火墙产品使用过程中遇到的任何问题。

4. （可选）邀请企业中其他业务相关业务人员加入企业专属安全服务群。

i. 单击**使用钉钉注册手机号**。

ii. 填写要加入企业专属安全服务群的钉钉用户的信息。

参数	说明
钉钉注册手机号	填写成功注册了钉钉应用的中国手机号码。
钉钉昵称	填写使用当前手机号码注册的钉钉名称。

iii. 单击**提交**。

提交申请后，您申请的钉钉用户将自动加入到企业专属安全服务群，并可以在群内直接提问。

3.WAF产品托管服务

云盾Web应用防火墙（WAF）支持产品托管服务。开通WAF产品托管后，您可以在阿里云安全产品专家的帮助下完成WAF接入配置、防护策略优化，并享有安全事件响应、安全咨询、安全培训与案例分享、安全报告分析等服务。

概述

WAF产品托管由阿里云原厂安全服务团队提供技术支持，面向云盾WAF用户提供产品托管服务。WAF产品托管帮助您更有效地使用WAF保护Web资产、降低业务安全风险、减少运维人力投入。

WAF产品托管适用于已开通阿里云Web应用防火墙，但缺乏业务持续监控能力和缺少可应对安全漏洞风险的安全工程师的业务场景。该服务适合需要外包专业人员协助来进行安全产品服务运营的用户。

> **说明** 由于托管服务的部分工作内容（包括但不局限于防护策略优化、监控和预警设置、安全报告定制等）需要使用WAF日志服务，如果您未购买WAF日志服务，上述托管服务可能存在无法交付的风险。建议您在选购WAF产品托管服务的同时，购买WAF日志服务功能。更多信息，请参见步骤1：开通WAF日志服务。

服务内容

WAF安全托管为您提供完整的WAF接入和使用支持，下表描述了具体的服务内容。

服务类型	描述
接入配置	• 在WAF上配置保护对象的域名策略。 • 协助用户配置和上传HTTPS证书（用户可自行上传）。 • 协助用户配置ECS和SLB的源站保护策略。 • 产品适配和访问测试验证。 • 用户保护域名变化时，调整相关配置。
防护策略优化	• 在WAF上的业务出现异常时，提供诊断和排错服务。 • 基于攻防日志，优化用户安全防护策略和配置。 • 安全事件响应时，调整防护策略和提供方案，帮助用户缓解事件影响。 • 提供故障处理、CC防护规则、精准访问控制规则、数据风控等WAF防护配置建议。
监控和预警	• 系统自动化监控WAF集群可用性故障。 • 系统自动化监控安全高危事件和攻击导致的异常事件。 • 人工在线判断和过滤监控事件预警。
安全报告	• 根据用户要求提供定制化安全报告内容。 • 提供服务日报和服务月报，其中日报包括当天操作信息，月报包括操作数据和攻防数据分析。

安全事件响应时间

开通WAF安全托管后，当您遇到安全事件需要紧急协助时，服务团队响应您的时间遵循下表描述。

序号	优先级	定义	响应时间
1	危险	用户核心业务严重受损或完全不可用	15分钟
2	紧急	用户核心业务出现非全局异常	30分钟
3	高	用户非核心业务严重受损或不可用	2小时
4	中	用户非核心业务出现非全局异常	4小时
5	低	用户日常技术咨询	8小时

服务交付方式

下表描述了WAF产品托管的服务交付方式。

类别	描述
服务交付方式	远程在线服务
服务语言	中文和英语
服务周期	与用户购买周期一致
支持的服务渠道	• 电子邮件 • 钉钉 • 电话

定价和售卖方式

WAF产品托管服务支持通过预付费方式开通，并且可按月或者按年续费。购买WAF产品托管服务，请前往WAF产品托管服务售卖页。

> **注意** 由于服务支持系统和服务人力资源投入的特殊性，WAF产品托管服务在支付购买后暂不支持退款。

4.产品托管服务授权

4.1. 开通WAF安全服务授权

通过WAF安全专家服务，您将获得阿里云安全服务专家和第三方安全专家为您提供的针对您业务场景的WAF产品安全服务，帮助您基于业务实际情况更好地使用WAF产品功能，保障您业务的网络应用安全。

背景信息

安全专家可以为您提供WAF中的域名接入咨询服务，同时通过对您的业务日志数据进行深度分析，有针对性地为您提供WAF防护配置的相关建议。

购买WAF产品安全服务后，您需要开通服务授权，阿里云安全服务专家和第三方安全专家才能通过阿里云安全服务平台为您提供产品服务。

> **注意** 您必须已购买或开通云盾Web应用防火墙产品，才能享受WAF安全专家服务。

操作步骤

1. 登录渗透测试（安全服务）管理控制台。
2. 在左侧导航栏，单击**服务授权**。
3. 在授权列表，查看您的WAF产品安全服务订单的授权情况。

   新创建的安全服务订单的**授权状态**为**未授权**。

4. 单击**查看授权协议**，阅读并同意授权书内容后，单击**确定**。

5. 单击**授权**，跳转到服务订单对应的云资源RAM角色授权页面，单击**同意授权**。

> **说明** 为了确保与安全专家的交流，请确认您已申请并开通与安全专家的专属钉钉服务群。

完成授权后，服务订单的**授权状态**将更新为**已授权**。

这时，您的专属安全专家将可以通过阿里云安全服务平台，直接查看您的WAF中相应的业务数据及配置数据，为您的业务提供专属的安全策略和建议。

> **说明** 安全专家通过阿里云安全服务平台查看您WAF控制台的所有操作都将产生相应的操作日志，您可以随时查看安全专家的操作记录。相关操作，请参见查看安全专家操作日志。

4.2. 查看安全专家操作日志

安全专家通过阿里云安全服务平台查看您WAF控制台的所有操作都将产生相应的操作日志，您可以随时登录阿里云操作审计控制台查看相关操作记录，审计安全专家的操作行为。

操作步骤

1. 登录操作审计管理控制台，并选择**华东1（杭州）**地域。

> **说明** 目前，所有WAF安全服务的操作日志记录均存储在华东1（杭州）地域的操作审计服务中。

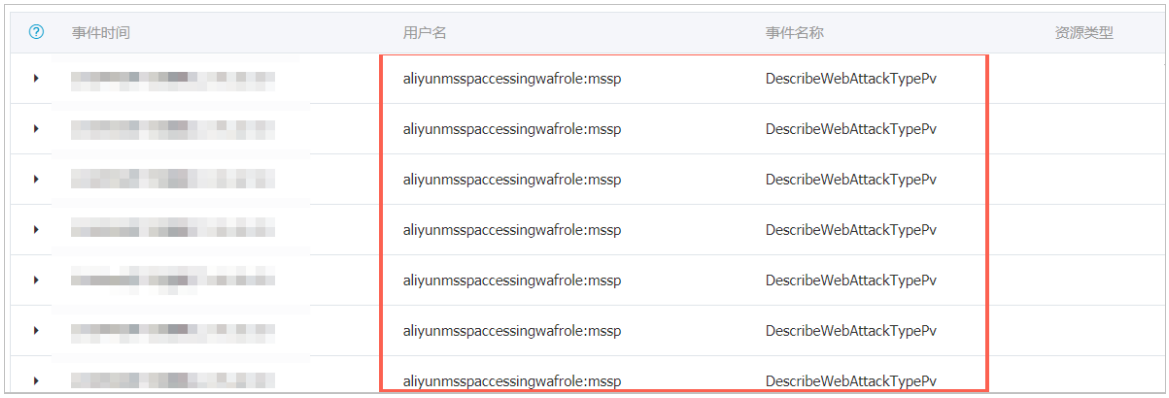
2. 定位到**历史事件查询**页面，设置以下查询条件，查询您的专属安全专家在WAF控制台中的操作记录日志。
   - **资源名称**：aliyunmsspaccessingwafrole
   - **事件类型**：所有类型

> **说明** 目前，WAF安全服务仅授权安全专家查看您WAF控制台中的数据，不具备更改配置等权限。因此，您也可以将事件类型条件设置为**读类型**，查询到的事件记录与选择所有事件类型得到的查询结果一致。

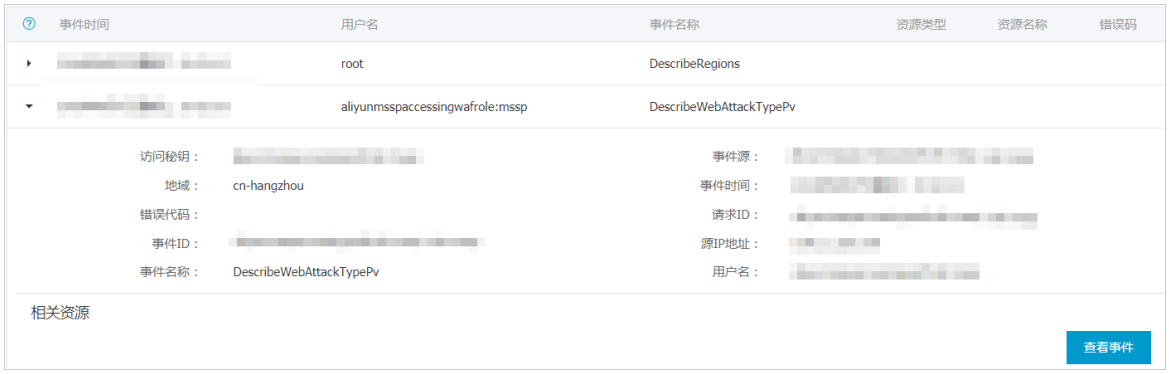
   - **时间**：选择您想查询的时间范围。

> **说明** 历史事件查询支持查看最近30天内的操作记录。

查询结果如下图所示。



3. 在事件列表中，单击操作记录可展开查看事件详情。



4. 单击**查看事件**可查看该事件的详细参数。

4.3. 取消WAF安全服务授权

WAF安全服务授权开通后，您可以随时在访问控制（RAM）控制台中删除WAF安全服务的授权角色，取消WAF安全服务授权。

操作步骤

1. 登录RAM控制台。
2. 定位到**角色管理**页面，找到授权服务订单时生成的MSSP安全产品服务的授权角色（AliyunMSSPAccessingWAFRole），单击**删除**。
3. 在**删除角色**对话框中，单击**确定**。

4. 获取并输入手机验证码，单击**确定**，通过手机验证。
   授权角色删除成功后，在云盾先知（安全情报）管理控制台的**服务授权**页面中相应服务订单的状态将变更为未授权。