Web 应用防火墙

常见问题

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

常见问题
- 产品咨询相关
- 接入相关
  - 源站相关
  - 端口支持相关
  - 域名相关
  - CNAME 相关
  - 关联产品相关
- 使用相关
- 权限相关

版权所有：腾讯云计算（北京）有限责任公司

常见问题
产品咨询相关

最近更新时间：2025-06-10 10:56:33

WAF 是否支持跨账号使用、跨账号配置迁移、跨账号共享?

WAF 暂不支持跨账号使用，不支持跨账号配置迁移，也不支持跨账号共享。

非腾讯云内的服务器能否使用 WAF?

- SAAS-WAF 支持云外机房用户接入，可以保护任何公网的服务器，包括但不限于腾讯云，包括其他厂商的云，IDC 等。
- CLB-WAF 仅支持腾讯云上业务负载均衡用户接入使用。

> ⚠ **注意：**
> 在中国内地（大陆）地区接入的域名必须按照工信部要求进行 ICP 备案。

WAF 是否支持 HTTPS 防护?

SAAS-WAF 及 CLB-WAF 全面支持 HTTPS 业务。用户只需根据提示将 SSL 证书及私钥上传，或者选择腾讯云托管证书，WAF 即可防护 HTTPS 业务流量。

WAF 的 QPS 限制规格是针对整个实例，还是配置的单个域名的 QPS 上限?

SAAS-WAF 及 CLB-WAF 的 QPS 限制规格是针对整个实例。若配置防护三个域名，则这三个域名累加的 QPS 不能超过规定上限。如果超过已购买的实例的 QPS 限制，将触发限速，导致丢包。

WAF 可以直接使用 DDoS 高防包么?

可以，在 DDoS 高防包控制台配置页面直接选择 SAAS-WAF 实例 或 CLB-WAF 实例的 IP 即可让 Web 应用防火墙具备高防能力。详情请参见 DDoS 高防包接入实践 。

上传 SSL 证书私钥是否有风险?

腾讯云对 SSL 证书的密钥托管体现出极高的安全性，主要从以下三个维度来看：

上传阶段

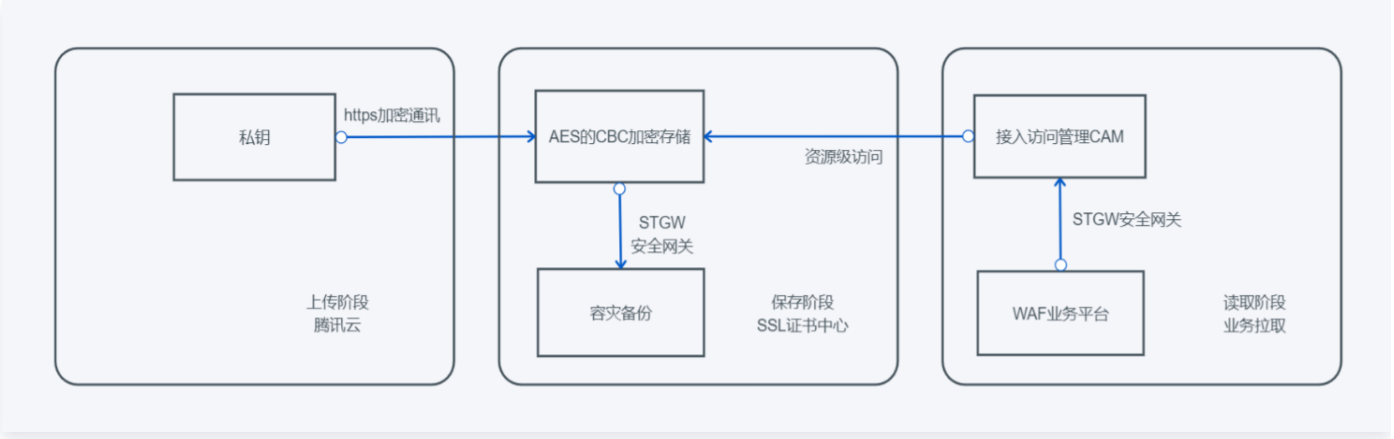
用户在上传阶段跳转到腾讯云托管证书平台配置证书，操作全程使用 HTTPS 加密通讯和企业型 SSL 证书，保证通讯数据的安全。

保存阶段

1. 上传后证书落库保存，对于证书私钥，使用 AES 的 CBC 模式进行加密，有效防范私钥被暴力破解。
2. 证书数据库做了容灾备份。保证证书数据的高可用性与高安全性，无对外暴露接口，由腾讯云内部 STGW 安全网关保证安全。
3. 证书后台部署有多台服务器，通过负载均衡接入，保证接口的稳定性。

证书的操作与读取

1. 客户进行证书操作，腾讯云 SSL 证书中心以“资源级”接入访问管理（Cloud Access Management，CAM），拥有完善的权限管理体系。客户可以对于不同的证书授予不同子账号不同的权限，防止恶意吊销、删除操作。
2. WAF 拉取证书，同样由腾讯云安全网关保证安全，业务按需拉取证书，同时对请求来源进行鉴别与鉴权，避免非法与不必要的访问。



SaaS 型和负载均衡型 WAF 是否都支持 SSL 双向认证?

SaaS 型 WAF 不支持 SSL 双向认证，负载均衡型 WAF 支持 SSL 双向认证。

Web 应用防火墙（WAF）与云防火墙区别是什么?

Web 应用防火墙（WAF）与云防火墙的区别如下：

类型	腾讯云 Web 应用防火墙（WAF）		腾讯云防火墙（CFW）
	SAAS 型 WAF	负载均衡型 WAF（CLB WAF）	
防护对象	网站和 API 服务。	网站和 API 服务。	全部暴露到互联网的业务。
适用场景	有等保或重保需求的客户，关注 Web 和 API 安全防护，关注应用层防护和机器防刷。	有等保或重保需求的客户，关注 Web 和 API 安全防护，关注应用层防护和机器防刷，且腾讯云上已使用或计划使用七层负载均衡的客户。	有等保或重保需求客户，或关注 CVM 主机及网络安全的客户。

核心防护能力	• Web 漏洞和未知威胁防护，自助漏报和误报处理。 • CC 攻击防护。 • API 安全和业务安全防护。 • 防泄漏/防篡改。	• Web 漏洞和未知威胁防护，自助漏报和误报处理。 • CC 攻击防护 。 • API 安全和业务安全防护。 • 网站 IPv6 防护。	IPS 的虚拟补丁能力，无需 CVM 安装实体补丁，无需重启。含 OWASP TOP 10 Web 基础漏洞防护。 自动发现失陷主机，对 CVM 的恶意外联行为进行自动阻断。 支持基于域名的主动外联控制。
核心优势	适用范围广阔，广泛覆盖腾讯云上和非腾讯云上用户。	云原生接入，接入无需调整现有的网络架构。 网站业务转发和安全防护分离，一键 bypass，保障网站业务安全、稳定可靠，支持多地域接入，仅覆盖腾讯云上用户。	云原生防火墙，一键开启，对客户业务无任何影响。 集成了 IPS、威胁情报、漏扫等安全能力，等保及重保场景必备，仅覆盖腾讯云上用户。
如何选择	云上和本地 IDC 均有网站和 API 防护需求的客户，推荐使用 SAAS 型 WAF。	腾讯云上已使用或计划使用七层负载均衡的用户，推荐使用负载均衡型 WAF。	对于关注 CVM 的防护效果，关注 CVM 是否失陷，特别是业务对外除了 Web 服务，还暴露了其他公网服务，推荐选择云防火墙。

WAF 的策略生效优先级是怎么命中的?

WAF 命中规则优先级为：精准白名单 > IP 白名单 > IP 黑名单 > API 限流 > 地域封禁、小程序防护、访问控制、CC 规则、BOT 防护、Web 防护（规则引擎）、AI 引擎 > 防篡改、防敏感。

版权所有：腾讯云计算（北京）有限责任公司

接入相关
源站相关

最近更新时间：2025-06-10 10:56:33

WAF 的源站 IP 可以填写腾讯云 CVM 内网 IP 吗?

WAF 添加域名时，填写的源站地址必须是公网 IP 或者域名。其中公网 IP 包括 CVM 公网 IP、CLB 公网 IP 或者其他本地 IDC 的出口 IP，不支持填写 CVM 的内网 IP。

回源 IP 的作用是什么?

回源 IP 是 SaaS 型 WAF 配置防护域名后自动分配的，Web 应用防火墙把流量转发到客户源站时，将使用这些回源 IP 地址作为源地址，因此，需要用户在服务器端设置 WAF 回源 IP 地址为可信 IP。为达到更好的防护效果，建议源站服务器仅允许接受来自 Web 应用防火墙回源 IP 的访问流量。

WAF 一个防护域名可以设置多少个源站 IP?

WAF 一个防护域名最多可以设置50个源站 IP。

WAF 配置多个源站时如何负载?

如果配置了多个回源 IP，WAF 采用轮询的方式对访问请求进行负载均衡。

WAF 是否会自动将回源 IP 段加入安全组?

不会自动将高防回源 IP 段添加到安全组。请参考 快速入门 将相应的回源 IP 加入到安全组。

端口支持相关

最近更新时间：2025-06-10 10:56:33

SaaS 型 WAF 支持哪些端口?

SaaS 型 WAF 套餐端口支持情况，可以在控制台进行查看并配置。

1. 登录 Web 应用防火墙控制台 ，在左侧导航中，选择**资产中心** > **接入管理**，默认进入域名接入页面。
2. 在域名接入页面，单击**添加域名**，进入添加域名页面。
3. 在添加域名页面的**服务器配置**中，选择对应的协议查看并配置端口，一个域名最多可配置5个端口。
   - WAF 高级版默认　持 HTTP（80/8080）和 HTTPS（443/8443）标准端口防护，不支持非标端口。
   - WAF 企业版和旗舰版套餐中除了默认　持 HTTP（80/8080）和 HTTPS（443/8443）标准端口防护外，还支持非标端口。 企业版和旗舰版支持的所有端口详情如下：

协议名称	端口
HTTP 协议	80、81、82、83、84、85、86、87、88、89、97、800、805、808、1000、1090、2020、3333、3501、3601、5000、5222、6001、6666、7000、7001、7002、7003、7004、7005、7006、7007、7008、7009、7010、7011、7012、7013、7014、7015、7016、7018、7019、7020、7021、7022、7023、7024、7025、7026、7040、7070、7081、7082、7083、7088、7097、7510、7621、7777、7800、8000、8002、8003、8004、8005、8006、8007、8008、8009、8010、8011、8012、8020、8021 、8022、8025、8026、8060、8077、8078、8080、8081、8082、8083、8086、8087、8088、8089、8090、8106、8181、8182、8184、8210、8215、8334、8336、8445、8686、8800、8888、8889、8999、9000、9001、9002、9003、9021、9023、9027、9037、9080、9081、9082、9180、9182、9200、9201、9205、9207、9208、9209、9210、9211、9212、9213、9898、9908、9916、9918、9919、9928、9929、9939、10000、10001、10080、10083、12601、20080、20083、25060、28080、33702、48800、52301
HTTPS 协议	443、4443、5100、5200、5443、6443、7443、8084、8085、8091、8442、8443、8553、8663、9443、9550、9553、9663、10803、18980

说明：

- 针对旗舰版用户，如果您需要防护的端口不在所支持的 HTTP 协议或 HTTPS 协议列表中，WAF 支持为您提供非标端口定制服务（范围为1 - 65535），套餐内所有域名非标端口定制总数不多于5个，如有需要可以 提交工单 处理。
- 已在 HTTP 协议或 HTTPS 协议列表中的端口不支持跨协议定制。
- 选择 HTTP 和 HTTPS 非标端口需要 提交工单 进行加白处理。

版权所有：腾讯云计算（北京）有限责任公司

版权所有：腾讯云计算（北京）有限责任公司

域名相关

最近更新时间：2024-07-16 16:51:41

如何接入域名?

您可以在 WAF 控制台 中接入域名，详情请参见 域名添加 。

WAF 是否支持泛域名接入?

支持，如需接入泛域名，直接在 WAF 控制台 添加泛域名即可。

> **说明：**
> - 若泛域名（如 `*.test.com` ）在云 WAF 接入后，支持其他账号接入该泛域名的子域名。
> - 若您同时添加了泛域名和精确域名（例如： `*.test.com` ， `a.test.com` ），WAF 优先使用精确域名所配置防护策略。

域名 DNS 解析状态（防护状态）更新需要多长时间?

请检查您的网站域名 CNAME 配置是否正确，在 DNS 处完成 CNAME 记录添加后，状态更新时间预计10 – 20分钟，请耐心等待。若您设置完成后，等待时间超过30分钟，防护状态仍未更新，您可及时 提交工单 联系我们协助您处理。

域名回源 IP 地址会变更吗?

WAF 在维护、升级等情况下，可能会变更域名回源 IP 地址。如果变更，我们会提前通过短信、邮件或站内信的方式通知您。具体回源 IP 地址，以控制台 域名列表 中所查看到的回源 IP 地址为准。

SaaS 型 WAF 实例域名接入的服务 VIP 地址是否会变化?

为了提供多地以及同地多机房容灾能力， WAF 在维护、升级等情况下，可能会变更服务 VIP 地址。为保障客户业务的稳定性，WAF 只提供 CNAME 方式接入，以支持灵活、弹性的迁移和扩容、缩容能力，不支持直接解析到 VIP 地址或业务应用上直接绑定 WAF 实例的服务 VIP 地址。

SaaS 型 WAF 实例域名接入的服务 VIP 地址可以申请更新吗?

SaaS 型 WAF 实例不支持申请变更域名的服务 VIP 地址。如果该实例绑定的域名出现服务异常，请先关注是否被 DDoS 攻击；同时可以 提交工单 联系我们，我们会及时为您处理。

版权所有：腾讯云计算（北京）有限责任公司

接入 WAF 的域名有什么要求吗?

如果接入 WAF 防护源站域名地域属于中国大陆地区，源站业务内容必须合法，并且完成工信部备案。

- 若源站未备案，则需要通过腾讯云完成工信部备案，备案流程可参见 如何快速备案您的网站 。
- 若源站在腾讯云上，但是工信部备案在其他服务商完成，则需要在腾讯云再次接入备案，备案流程可参见 备案资料填写流程 。

> **注意：**
> 若接入实例为 SAAS-WAF 实例，还需要您修改接入源站的 DNS 为 WAF 的 Cname 地址。

域名回源支持哪些方式?

支持域名回源和 IP 回源，您可以根据需要进行选择和配置，详情可参见 域名添加 。

域名接入 WAF 之后，如何绑定 CNAME?

您可以参考 修改 DNS 解析，在您的 DNS 服务商处绑定 CNAME。

域名删除后重新添加， CNAME 会发生变化吗?

域名在控制台删除后重新添加都会发生变化，具体取值可在 WAF 控制台域名列表 中，实例信息处中查看。

WAF 添加域名时，使用的回源域名应该如何填写?

回源域名需填写其他代理给出的 CNAME 地址或其他域名，域名不能和 WAF 添加的域名相同，不需要填写协议类型信息（HTTP 或 HTTPS）。

CNAME 相关

最近更新时间：2024-04-24 14:15:41

如何配置 CNAME?

- CNAME 域名不能直接访问，您需要在域名服务提供商处完成 CNAME 配置，配置生效后，WAF 将对域名进行防护，具体 CNAME 配置步骤，可参见 修改 DNS 解析 。
- 若已完成 CNAME 配置，在您的域名接入 WAF 后，系统会为您自动分配一个以 `.qcloudxxx.com` (如 `.qlcoudcjpj.com` 、 `qcloudwzgj.com` 等)为后缀的 CNAME 域名，可在 WAF 控制台域名列表 中，实例信息处进行查看。

关联产品相关

最近更新时间：2024-06-19 10:20:11

WAF 如何同 CDN 或 DDoS 高防包 一起接入?

- WAF 可直接将 DDoS 高防包叠加，CDN 的源站指向 WAF 实例的 IP 即可。推荐部署架构：客户端 > CDN > WAF+高防包 > 负载均衡 > 源站。
- 在客户需要 CDN 和高防能力时，只要将 Web 应用防火墙接入后提供的 CNAME 配置为 CDN 的源站即可，同时可以将 DDoS 高防包叠加到 WAF 实例上。即可实现用户流量经过 CDN 之后，被转发至 WAF，同时具备大流量 DDoS 的清洗能力，最终转发至源站，对源站进行全面的安全防护。

若已经接入 CDN 域名在 WAF 如何接入?

若已经接入 CDN 域名，将 WAF 为域名分配的 CNAME 地址作为 CDN 的源站即可，流量按照用户 > CDN > WAF > 负载均衡 > 源站的架构回源。同时您可以登录 WAF 控制台，在 添加域名页面，将代理情况勾选为是，此时 WAF 会根据 HTTP 头部中的 XFF 字段，获取客户端的真实 IP，保证 WAF 正常防护。

使用相关

最近更新时间：2025-04-11 14:24:52

如何下载180天的访问日志?

访问日志功能用于记录 Web 应用防火墙防护域名的访问日志信息，提供防护域名在用户自定义的日志保存天数内（最大180天）的访问日志查询和下载功能。如需下载180天访问日志，请开启相关域名访问日志开关，并于控制台设置存储180天访问日志。详情参见 访问日志 。

WAF 是否支持健康检查?

SaaS型 WAF 支持四层健康检查机制，支持企业版及以上版本于域名接入时开启，开启后对所有源站 IP 每隔3秒主动探测源站健康状态。如需了解更多的健康检查机制，请 提交工单 咨询了解。

WAF 是否支持会话保持?

WAF 支持开启会话保持，如需开启，请 提交工单 联系我们协助您处理。

域名列表 WAF 开关关闭后，还会记录日志吗?

WAF 的开关关闭后，WAF 所有的防护功能将会关闭，并进入纯流量转发模式，且不会记录日志。

更改接入配置后大约需要多少时间生效?

一般情况下，更改后的配置在10s内即可生效。

> **说明**
> 此处为修改接入配置相关（如源站地址、链接方式，是否启用 HTTP2.0 等），并非防护配置。

WAF 防护域名的 VIP 地址因为 DDoS 封堵如何处理?

WAF 的 VIP 默认具备 DDoS 基础防护能力（防护能力为2Gbs），如果在 DDoS 基础防护中发生封堵，急需恢复业务请购买 DDoS 高防包 实例并绑定 WAF 的 VIP 地址。

如果上传文件被拦截，那使用 HTTPS 或者 SFTP 上传文件是否仍会拦截呢?

若没有使用 WAF 不会被拦截，如果使用 WAF 并且开启了拦截模式，使用 HTTP 或 HTTPS 上传恶意文件将会被拦截。但使用 SFTP 上传文件则不会被拦截，SFTP 是非 HTTP 或 HTTPS 协议，WAF 不支持防护。

WAF 更换证书长连接会话是否会断开?

不会。更新证书会 reload nginx，等旧的请求会话结束才会回收线程，所以不会断开。

SaaS 型 WAF 支持的加密套件有哪些?

- SaaS 型 WAF 中，支持的加密套件和所属 TLS 协议版本如下：

加密套件名称	支持协议版本	安全加密套件	通用加密套件
DES-CBC3-SHA	TLSv1.0 TLSv1.1 TLSv1.2	否	是
ECDHE-RSA-DES-CBC3-SHA		否	是
AES256-SHA		是	是
AES128-SHA		是	是
ECDHE-RSA-AES256-SHA		是	是
ECDHE-ECDSA-AES256-SHA		是	是
ECDHE-RSA-AES128-SHA		是	是
ECDHE-ECDSA-AES128-SHA		是	是
AES256-SHA256	TLSv1.2	是	是
AES256-CCM8		是	是
AES128-SHA256		否	是
AES256-CCM		是	是
AES256-GCM-SHA384		是	是
ECDHE-RSA-AES256-SHA		是	是
ECDHE-RSA-AES256-SHA384		是	是
ECDHE-RSA-AES256-GCM-SHA384		是	是
AES128-CCM8		是	是
AES128-CCM		是	是

版权所有：腾讯云计算（北京）有限责任公司

AES128-GCM-SHA256		是	是
ECDHE-RSA-AES128-SHA256		是	是
ECDHE-RSA-CHACHA20-POLY1305		是	是
ECDHE-RSA-AES128-GCM-SHA256		是	是
TLS-AES-128-GCM-SHA256		是	是
TLS-CHACHA20-POLY1305-SHA256		是	是
TLS-AES-256-GCM-SHA384		是	是

- WAF 支持的 TLS 版本说明：
  - 协议版本：TLSv1 TLSv1.1 TLSv1.2 TLSv1.3。
  - 密码套件 EECDH+CHACHA20:EECDH+AES128:RSA+AES128:EECDH+AES256:RSA+AES256:EECDH+3DES:RSA+3DES:!MD5。

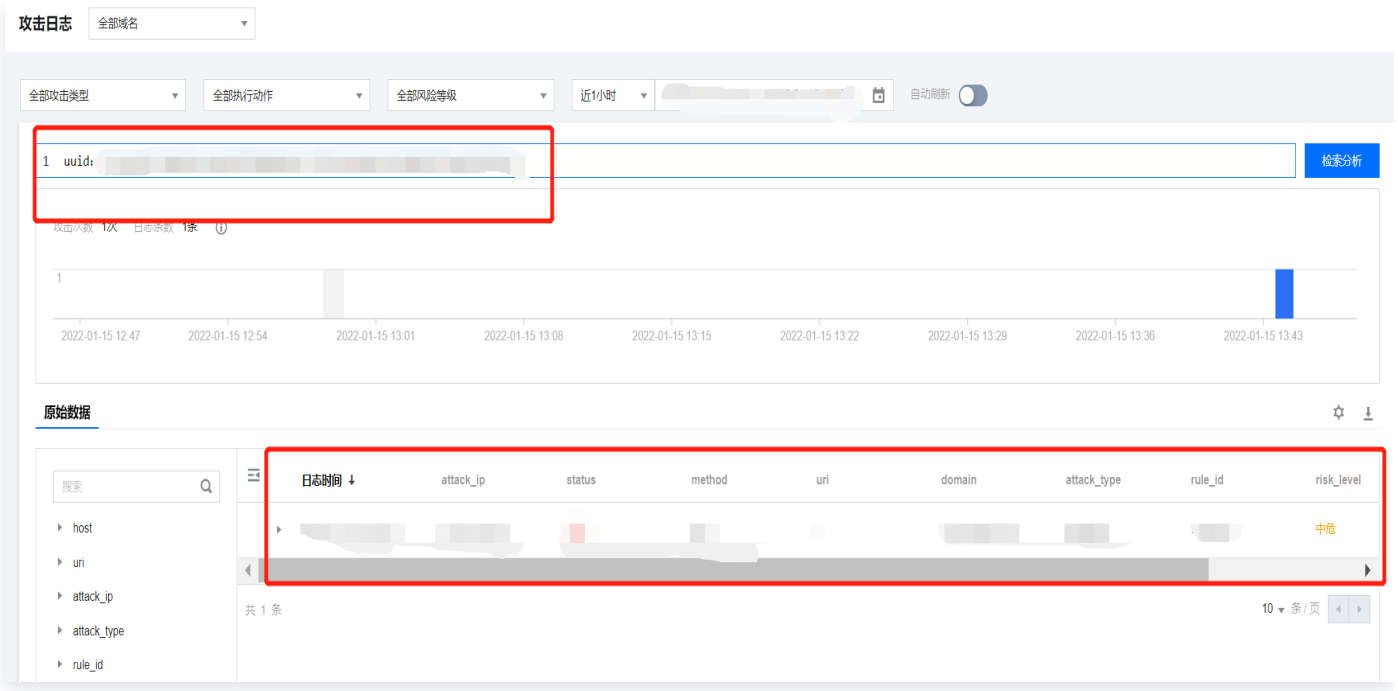
> **说明**
> - SaaS WAF 默认支持 ECDHE 的密码套件（如 TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA）。
> - 负载均衡型 WAF 协议加密套件依赖 CLB、云原生 API 网关、用户自定义网关自身的 TLS 协议支持情况。

如何查询拦截页面命中模块?

1. 当恶意用户对防护域名进行非法访问时，Web 应用防火墙会对请求进行拦截并返回拦截页面，页面会返回唯一标识码（uuid）。

2. 复制当前标识码在 攻击日志页面 检索该标识码可以查看拦截包信息。

> **说明**
>
> - 检索时请检查时间范围。
> - 拦截包主要分为几个字段：“attack_type”攻击类型，“rule_id”规则ID，“attack_content”攻击字段内容。根据上述字段可以查询得知命中的规则，方便后续用户操作。


攻击日志
全部域名
全部攻击类型
全部执行动作
全部风险等级
近1小时
自动刷新
1 uuid:
检索分析
攻击次数 1次
日志条数 1条
1
2022-01-15 12:47
2022-01-15 12:54
2022-01-15 13:01
2022-01-15 13:08
2022-01-15 13:15
2022-01-15 13:22
2022-01-15 13:29
2022-01-15 13:36
2022-01-15 13:43
原始数据
搜索
host
uri
attack_ip
attack_type
rule_id
日志时间
attack_ip
status
method
uri
domain
attack_type
rule_id
risk_level
中危
共 1 条
10 条/页

权限相关

最近更新时间：2025-04-11 14:24:52

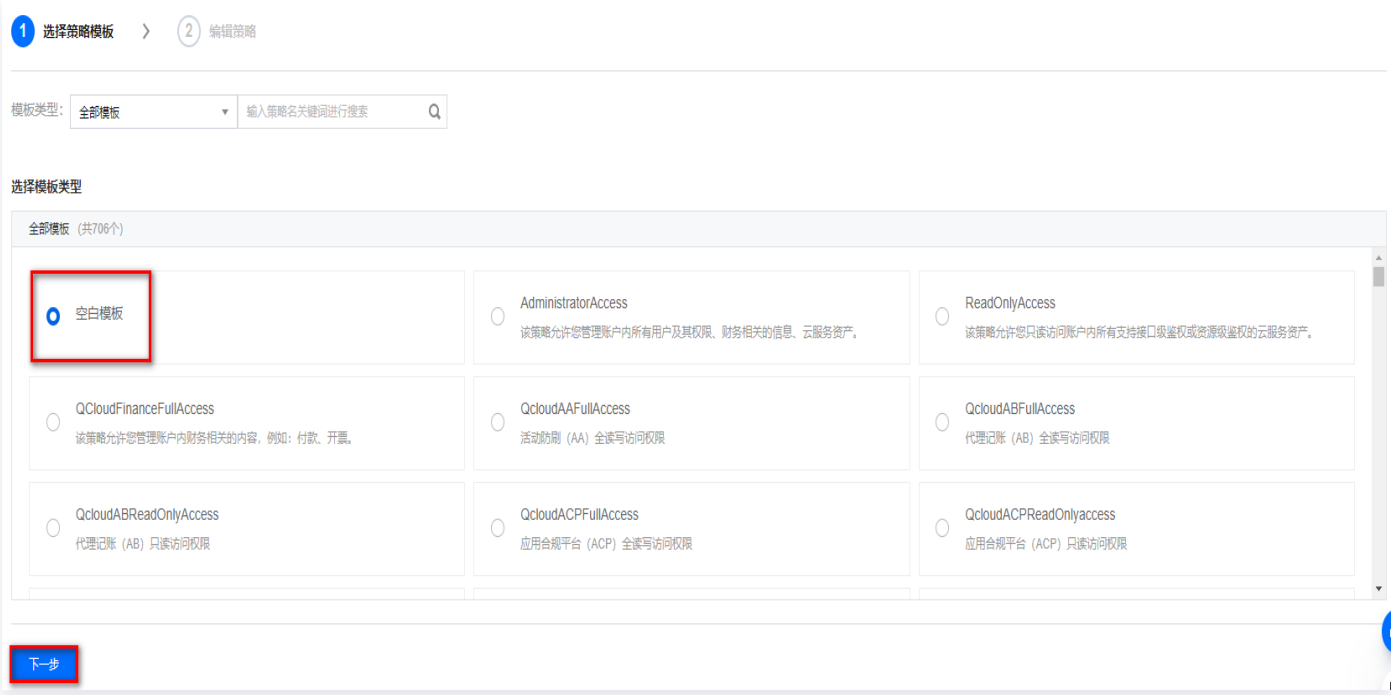
日志投递服务开通后，出现子账号权限异常报错怎么处理?

出现权限异常报错后可以在 访问管理 > **策略**中新建自定义策略来修复。具体示例如下：

> **说明**
> - 更多详情可参见 创建自定义策略 和 子账号授权指引 。
> - 请使用主账号进行授权。

1. 登录 访问管理控制台 ，在左侧导航中，选择选择**策略**。
2. 在策略页面，单击**新建自定义策略**，选择**按策略语法创建**。

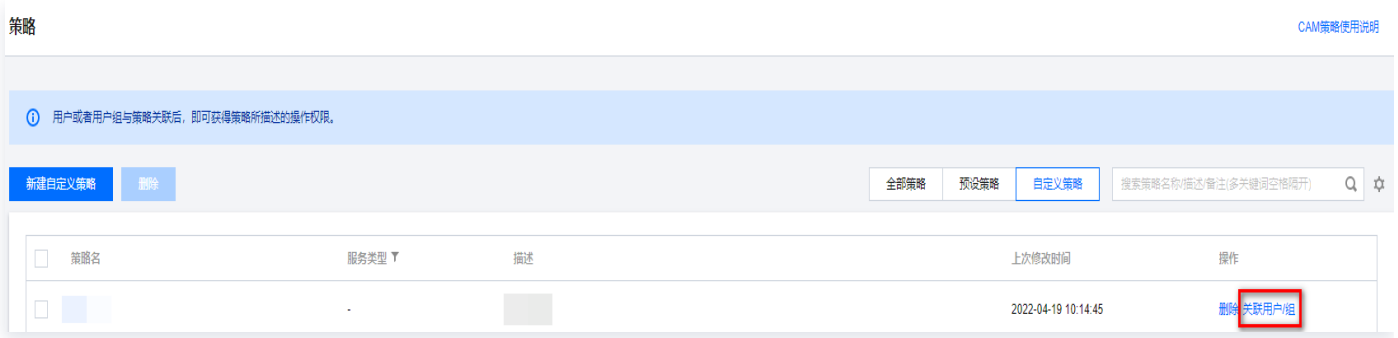
3. 在选择策略模板页面，选择**空白模板**，单击**下一步**。



4. 在编辑策略页面，输入策略名称和描述，并在策略内容中输入如下代码：

```
{
  "version": "2.0",
  "statement": [
 {
   "action": [
     "cls:DescribeTopics",
     "ckafka:DescribeInstanceAttributes",
     "ckafka:DescribeTopic",
     "ckafka:DescribeRoute",
     "ckafka:DescribeInstances",
     "ckafka:DescribeInstancesDetail"
   ],
   "resource": "*",
   "effect": "allow"
 }
  ]
}
```

5. 单击**完成**，返回至策略页面，选择刚刚创建策略，单击操作列的**关联用户/组**。



6. 在关联用户/组弹窗中，勾选所需的用户/组，单击**确定**。