Web应用防火墙（WAF）

产品文档



目录

Web应用防火墙（WAF） 3
- 产品简介 3
  - 产品概述 3
  - 产品优势 5
  - 产品分类 7
  - 应用场景 10
- 快速入门 11
  - 新手常见问题 11
  - 快速入门 12
- 操作指南 23
  - 租户端功能清单 23
  - 负载均衡WAF域名接入 25
  - 规则引擎 29
  - CC防护设置 34
  - 自定义策略 40
  - 网页防篡改 43
  - 防信息泄露 45
  - 地域封禁 47
  - 黑白名单管理 49
    - 功能介绍 49
    - IP白名单 50
    - 精准白名单管理 55
    - 规则白名单 57
    - IP黑名单 59
  - 攻击日志 62
  - IP管理 67
  - 常见操作 71
    - 场景1：创建实例 71
    - 场景2：添加clb-waf型防护域名 75
    - 场景3：添加saas-waf型防护域名 78
    - 场景4：删除防护域名 81
    - 场景5：删除实例 82
    - 场景6：添加自定义规则 84
    - 场景7：添加CC防护规则 86
    - 场景8：检查域名是否处于被防护状态 88
    - 场景9：应急预案 91
- 最佳实践 94
  - 搭建负载均衡型WAF测试环境 94
  - 搭建SaaS型WAF源站 114
- 常见问题 133
  - 常见问题 133
- API文档 135
  - 网站管家（waf） 135
    - 版本（2018-01-25） 135
      - API 概览 135
      - 调用方式 137
        - 接口签名v1 137
        - 接口签名v3 144
        - 请求结构 153
        - 返回结果 154
        - 公共参数 157
      - 其他接口 159
        - 增加自定义规则 159
        - 获取系统版本 161
        - 获取规则版本 163
        - waf获取白名单列表 165
        - 购买WAF 167
        - WafGetDomainEngineType 170
      - 日志服务相关接口 172
        - 创建攻击日志下载任务 172
        - 删除下载记录 174
      - 防护设置相关接口 176
        - 增加规则引擎白名单 176
        - 查询用户白名单名字重复 178
        - Waf 会话定义 Delete接口 180
        - 删除全局白名单 182
        - 获取自定义策略列表 184
        - 获取主类及子类信息 186
        - 获取特征规则更新动态 188
        - 获取用户规则引擎类型 190
        - 获取用户防护规则等级 192
        - 获取用户特征规则列表 194
        - 获取全局白名单 196
        - 获得webshell切换状态 198
        - 切换自定义规则的开关 200
        - 修改用户防护规则等级 202
        - 修改用户防护规则 204
        - 变更全局白名单 206
        - 切换webshell切换状态 208
      - 数据结构 210
      - 错误码 255

产品简介
产品概述

什么是 Web 应用防火墙

Web 应用防火墙（Web Application Firewall，WAF）是一款基于 AI 的一站式 Web 业务运营风险防护方案。通过 AI+规则双引擎识别恶意流量，保护网站安全，提高 Web 站点的安全性和可靠性。

WAF 提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF，两种 WAF 提供的安全防护能力基本相同，接入方式不同。

- SaaS 型 WAF 通过 DNS 解析，将域名解析到 WAF 集群提供的 CNAME 地址上，通过 WAF 配置源站服务器 IP，实现域名恶意流量清洗和过滤，将正常流量回源到源站，保护网站安全。
- 负载均衡型 WAF 通过和负载均衡集群进行联动，将负载均衡的 HTTP/HTTPS 流量镜像到 WAF 集群，WAF 进行旁路威胁检测和清洗，将用户请求的可信状态同步到负载均衡集群进行威胁拦截或放行，实现网站安全防护。

  WAF 可以有效防御 SQL 注入、XSS 跨站脚本、木马上传、非授权访问等 OWASP 攻击。此外还可以有效过滤 CC 攻击、DNS 链路劫持检测、提供 0day 漏洞补丁、防止网页篡改等，通过多种手段全方位保护网站的系统以及业务安全。

主要功能

功能	简介
AI + Web 应用防火墙	基于 AI + 规则的 Web 攻击识别，防绕过、低漏报、低误报、精准有效防御常见 Web 攻击，如 SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造，Webshell 木马上传等 OWASP 定义的十大 Web 安全威胁攻击
0day 漏洞虚拟补丁	安全团队 7 * 24 小时监测，主动发现并响应，24 小时内下发高危 Web 漏洞，0day 漏洞防护虚拟补丁，受护用户无需任何操作即可获取紧急漏洞，0day 漏洞攻击防护能力，大大缩短漏洞响应周期
网页防篡改	用户可设置将核心网页内容缓存云端，并对外发布缓存中的网页内容，实现网页替身效果，防止网页篡改给组织带来负面影响
数据防泄漏	通过事前服务器应用隐藏，事中入侵防护及事后敏感数据替换隐藏策略，防止后台数据库被黑客窃取

功能	简介
CC 攻击防护	智能CC防护，综合源站异常响应情况（超时、响应延迟）和网站行为大数据分析，智能决策生成防御策略。多维度自定义精准访问控制、配合人机识别和频率控制等对抗手段，高效过滤垃圾访问及缓解 CC 攻击问题

为何需要 Web 应用防火墙

在以下场景中，使用 WAF 均可有效防御以及预防，保障企业网站的系统以及业务安全。

- 数据泄露（核心信息资产泄露）
  Web 站点作为很多企业信息资产的入口，黑客可以通过 Web 入侵进行企业信息资产的盗取，对企业造成不可估量的损失。
- 恶意访问和数据抓取（无法正常服务，被对手利用数据）
  黑客控制肉鸡对 Web 站点发动 CC 攻击，资源耗尽而不能提供正常服务。恶意用户通过网络爬虫抓取网站的核心内容（文学博客、招聘网站、论坛网站、电商内的评论）电商网站被竞争对手刻意爬取商品详情进行研究。羊毛党们试图搜寻低价商品信息或在营销大促前提前获取情报寻找套利的可能。
- 网站被挂马被篡改（影响公信力和形象）
  攻击者在获取 Web 站点或者服务器权限后，通过插入恶意代码来让用户执行恶意程序、赚取流量、盗取账号、炫技等；植入“黄、赌、非”链接；篡改网页图片和文字；对网站运行造成很大影响，损坏网站运营者的形象。对外公信力和形象蒙受损失。
- 框架漏洞（补丁修复时段被攻击）
  很多 Web 系统基于常见的开源框架如 Structs2、Spring、WordPress 等，这些框架常常爆出安全漏洞，但等待安装补丁的维护时段，则是一段艰难和危险的过程，很多攻击会漏洞公布之后一天内就遍地开花。

产品优势

多种接入防护方式

- 开通 WAF 后，无需进行业务变更即可完成防护接入，一键绑定TCloudFinanceZone负载均衡实现网站旁路检测和威胁清洗，同时提供一键 bypass 功能，实现业务转发和安全防护分离，稳定可靠。
- 通过 CNAME 接入 WAF，隐藏用户真实源站，将可信流量回源，覆盖TCloudFinanceZone和非TCloudFinanceZone上用户。
- 防护集群资源多地部署、动态扩展，按需使用，避免冗余及单点故障。

AI+规则双引擎防护

- 在安全规则引擎进行 OWASP Top 10防御（如SQL 注入、非授权访问、XSS 跨站脚本、CSRF 跨站请求伪造、命令行注入等）的基础上，引入 AI 防御能力，通过交叉验证持续学习，精准有效捕捉各类常规 Web 攻击、0day 攻击及其它新型未知攻击。
- 通过不断学习海量业务数据特征，生成基于业务的个性化防护策略，避免误报，用户可基于 AI 引擎实现自助误报和漏报处理，提升运营效率。

及时的补丁修复保障

- 可提供在 12h 内更新高危漏洞补丁，在 24h 内更新常见通用型漏洞补丁。
- 云端自动升级，秒级同步下发策略，帮助企业无忧 Web 漏洞隐患。

智能 CC 防护

- 可自定义 session，通过 session 维度进行 CC 防护，更加精确防护 CC 攻击，减少误报。
- 可实时查看 CC 封堵状态 IP，根据需要快速调整防护策略。
- 一键抗 DDoS联动，轻松应对敏感大流量 DDoS 攻击问题，无惧突发风险。

稳定的高可用业务保障

- 产品无需安装维护软硬件，提供用户便捷的接入。稳定的低延时高性能 VIP 专线服务，在隐藏保护源站 IP 的同时，优质加速线路可保障毫秒级业务延时与配置响应速度。

IPv6 安全防护

- 可使用云上 NAT64 实例，实现网站 IPv6 防护接入，无需对 IPv4 站点进行改造即可支持 IPv6 访问和防护。
- 通过和负载均衡进行联动，无缝处理 IPv4 和 IPv6 访问流量，使其具备同等安全防护能力，简单快捷。

产品分类

类型概述

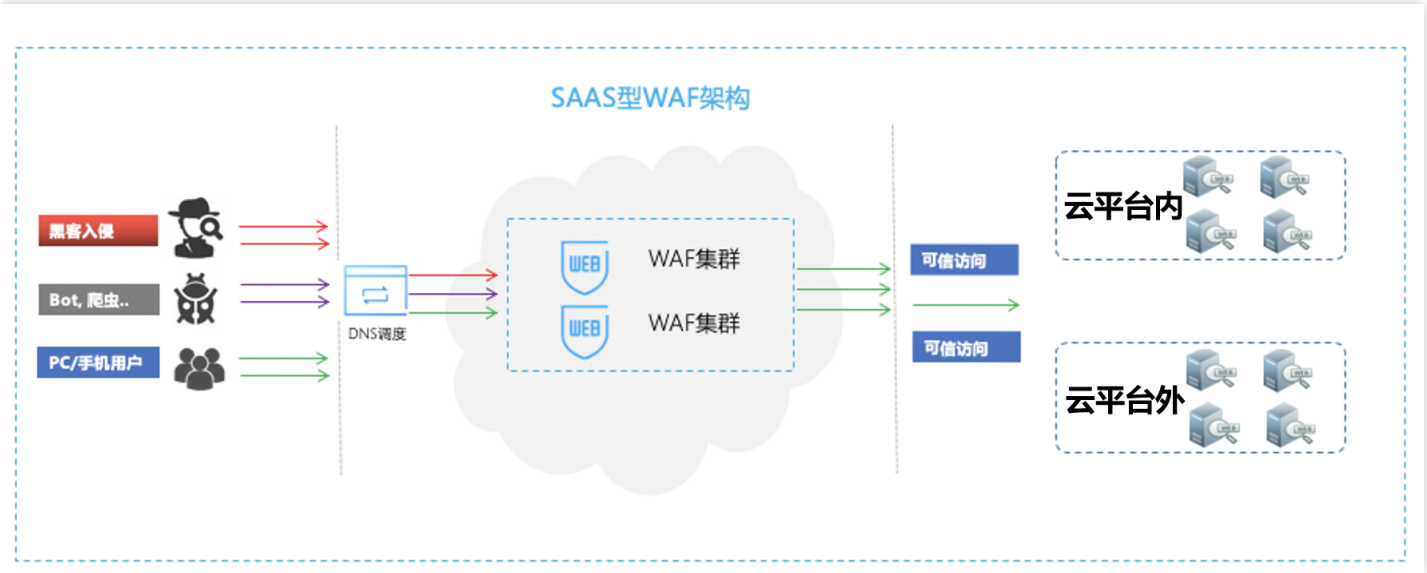
TCloudFinanceZone提供两种类型的云上 WAF，SaaS 型 WAF 和负载均衡型 WAF。两种 WAF 的安全防护能力基本相同，但接入方式不同，适用场景不同，您可以根据实际部署需求选择不同类型的 WAF。

类别	SAAS型	负载均衡型
适用场景	适合所有用户（云上用户或本地 IDC 用户），通过 DNS 解析调度实现域名接入。	TCloudFinanceZone上已使用或计划使用七层负载均衡的用户。
核心优势	· 适用范围广阔，广泛覆盖TCloudFinanceZone上和非TCloudFinanceZone上用户。 · 支持源站隐藏，减少风险暴漏面	· 无感知接入，毫秒级延迟，WAF 接入不需要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。
如何选择	若用户在TCloudFinanceZone上和本地均有网站需要防护需求，或TCloudFinanceZone上未使用七层负载均衡，推荐使用 SAAS 型 WAF。	TCloudFinanceZone上已使用或计划使用七层负载均衡的用户，且有 Web 安全防护、合规保护、网站安全运营需求，推荐使用负载均衡型 WAF。

> 说明：
>
> 负载均衡型 WAF，当前灰度开放中，如需使用请提交申请，我们将尽快为您核实开通。

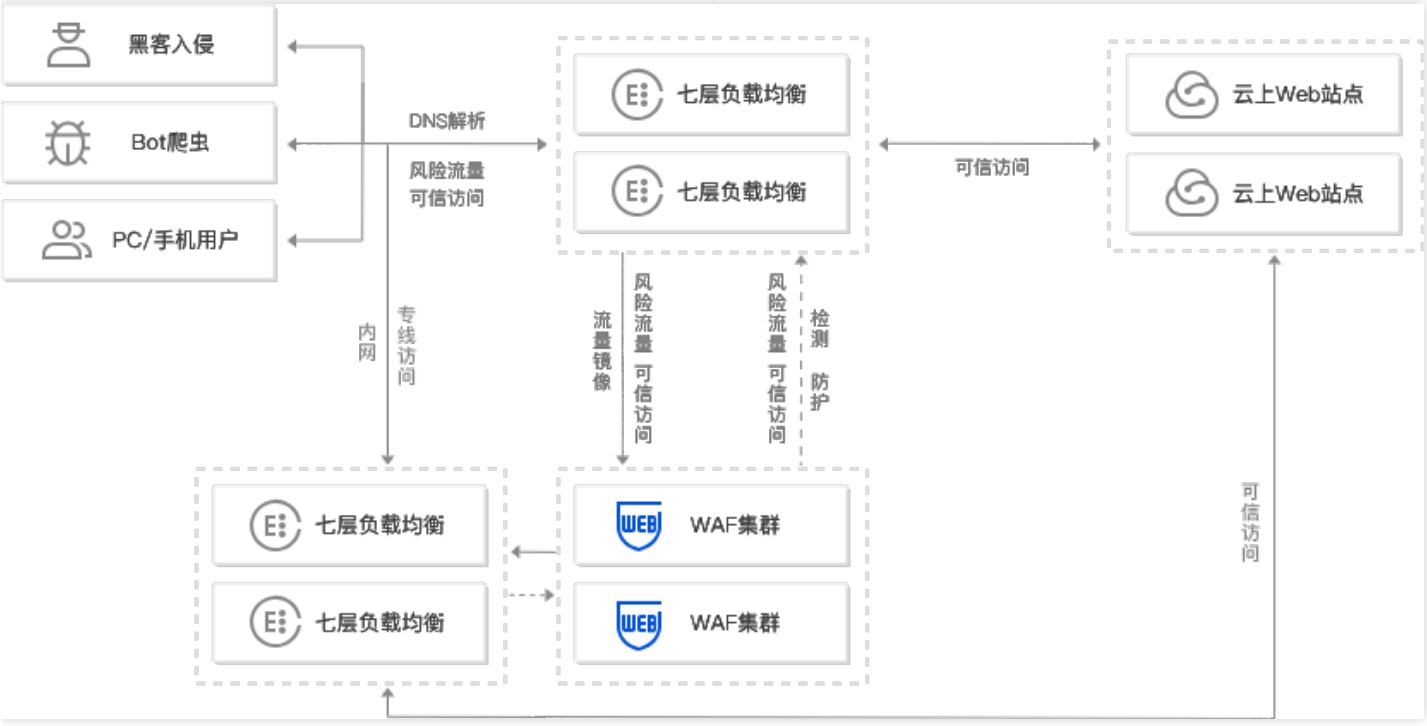
SaaS型WAF

Web 应用防火墙采用 SaaS 化模式交付，通过修改 DNS 引流设置，用户侧无需部署任何硬件设备，即可分钟级获取 Web 防护能力。WAF 集群对防护域名进行恶意流量检测和防护后，将正常流量回源到源站，保护网站安全。



负载均衡型WAF

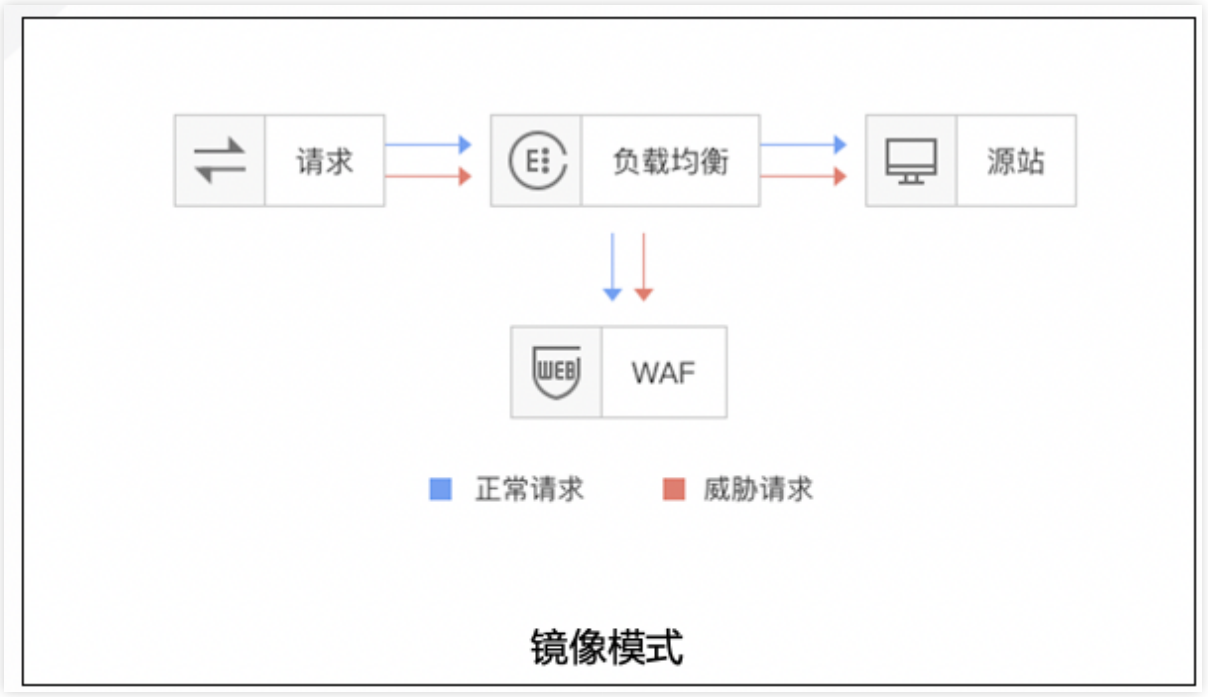
WAF 通过配置域名和TCloudFinanceZone各种网络环境下的七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP/HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离，最大限度减少安全防护对网站业务的影响，保护网站稳定运行。



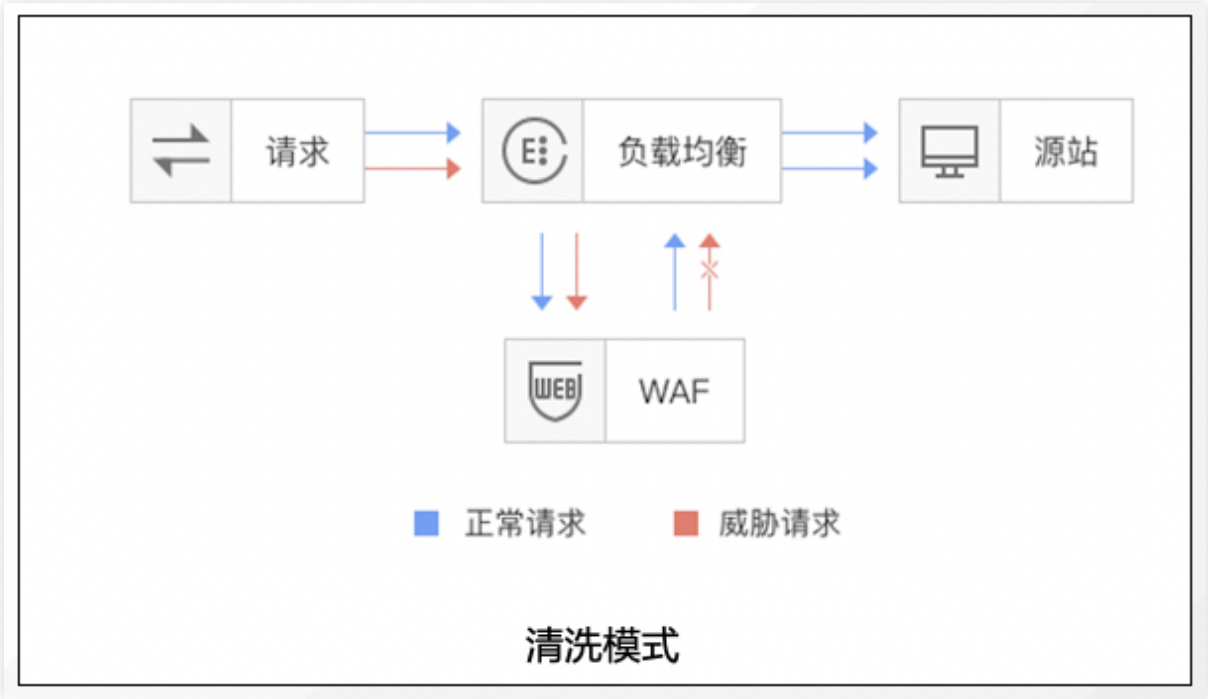
负载均衡型 WAF 提供两种流量处理模式：

- 镜像模式：通过域名进行关联，CLB 镜像流量到 WAF 集群，WAF 进行旁路检测和告警，不返回请求可信状

态。



- 清洗模式：通过域名进行关联，CLB 镜像流量到 WAF 集群，WAF 进行旁路检测和告警，同步请求可信状态，CLB 集群根据状态对请求进行拦截或放行处理。



应用场景

金融网站防护

- 一键接入防护，可跟大流量 DDoS 防御有机结合，同时具备 Web 安全防护。
- 有效监测 DNS 链路劫持，防止网站流量被恶意指向。
- 可有效检测撞库等异常访问，保护用户信息不外泄。
- 云端资源优势，自动伸缩，轻松应对业务突发，大流量 CC 攻击。

政务网站防护

- 一键接入防御，轻松配置，隐藏并保护源站，保证网站内容不会被黑客入侵、篡改。保障网站信息正确，政府服务正常可用，民众访问满意畅通。

电商网站防护

- 持续优化防护规则、精准拦截 Web 攻击，全面抵御 OWASP Top 10 Web 应用风险。
- 在高并发抢购场景下，可智能过滤恶意攻击及垃圾访问，保障正常访问业务流畅。

防数据泄密

- 避免因黑客的注入入侵攻击，导致网站核心数据被拖库泄露。
- 防 CC 攻击：防恶意 CC（http get flood），通过在四层和七层阻断海量的恶意请求，保障网站可用性。

快速入门
新手常见问题

WAF接入方式？

WAF分为两种类型，SaaS 型 WAF 和负载均衡型 WAF，两种类型 WAF 域名接入方式不同，请根据实际情况完成接入。

WAF 是否支持 HTTPS 防护？

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，WAF 即可防护 HTTPS 业务流量。

WAF 一个防护域名可以设置多少个回源 IP？

WAF 一个防护域名最多可以设置50个回源 IP。

WAF 是否支持健康检查？

WAF 默认启用健康检查。WAF 会对所有源站 IP 进行接入状态检测，如果某个源站 IP 没有响应，WAF 将不再将请求转发到该源站 IP ，直到接入状态恢复正常。

在 WAF 的控制台中，更改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。

SaaS 型和负载均衡型 WAF 是否支持 国密证书认证？

SaaS 型 WAF 暂不支持国密证书认证，负载均衡型 WAF 支持国密证书认证。

快速入门

WAF分为两种类型，SaaS 型 WAF 和负载均衡型 WAF，两种类型 WAF 域名接入方式不同，请根据实际情况完成接入。

SaaS型WAF接入配置

SaaS 型 WAF 通过为防护域名分配 CNAME，修改网站的 DNS 解析记录，将网站收到的 Web 请求转发给 WAF ，从而对网站进行安全防护。配合安全组使用，可以避免攻击者绕过 WAF 直接攻击网站源站。为了实现上述功能，您需要完成以下步骤：

步骤1：域名添加

为了使 Web 应用防火墙识别出需要防护的域名，需要先在 Web 应用防火墙中添加域名。下面以防护 waf.qcloudwaf.com 为例，说明配置步骤。

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择资产中心 > 接入管理，进入域名接入页面。
2. 在域名接入页面，单击添加域名，进入添加域名页面选择“SAAS型”。
3. 在添加域名页面，配置相关基础参数。



- 域名配置

1. 在域名输入框中添加需要防护的域名 waf.qcloudwaf.com 。
2. 协议和端口可按实际情况选择。例如：勾选 HTTP，选择80端口；勾选 HTTPS，选择443端口。
3. HTTPS 回源方式可选：HTTP 或 HTTPS。
4. 证书来源可选：托管证书，自有证书。
5. 在源站 IP 输入框内输入需要防护网站的真实 IP 源站地址，即源站的公网 IP 地址。

- 其他配置

1. 在 Web 应用防火墙前，是否接入了其他中间代理设备，若有，请选择【是】且支持自定义获取展示源IP的方式，若无，请选择【否】。
2. 单击【保存】，完成配置后，可在域名列表看到刚刚添加的域名和为站点分配的 CNAME地址。

Web 应用防火墙将会为每个添加到 Web 应用防火墙的域名(不区分一级域名和二级域名)分配一个唯一的 CNAME。

步骤2：本地测试

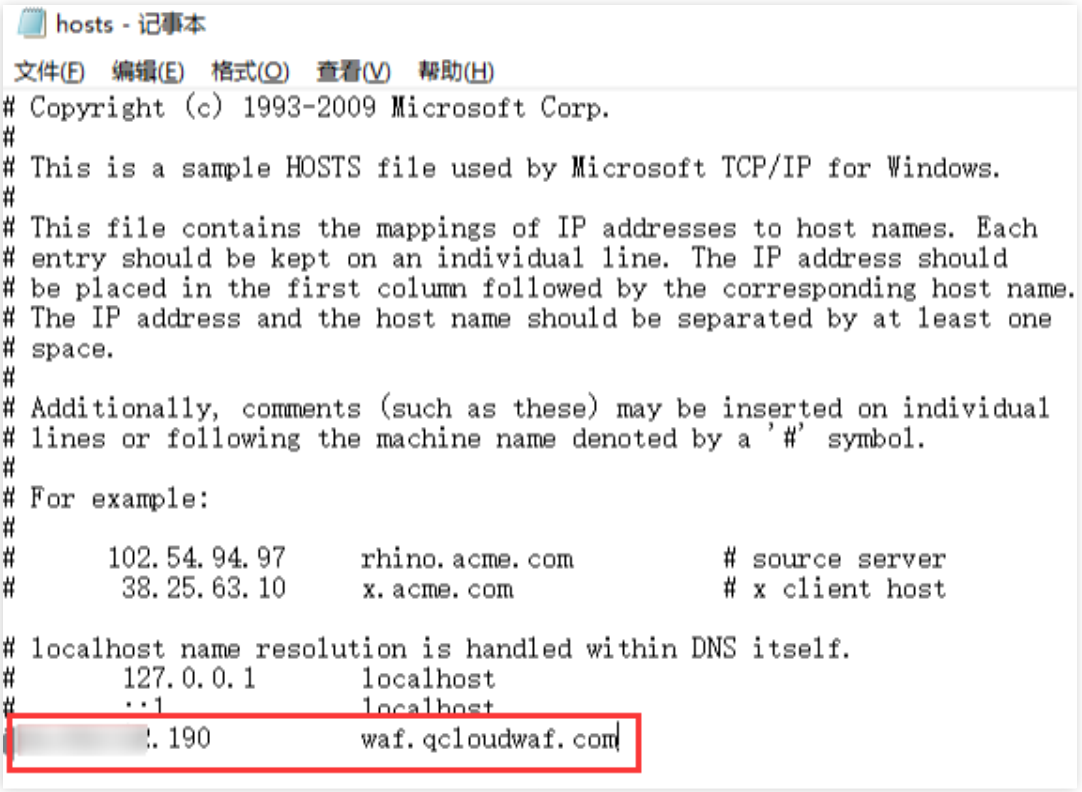
本地机器访问网站需要做 DNS 解析，在这之前会优先从本地 hosts 文件中获取目标域名对应的 IP 地址。所以可以用修改 hosts 文件的方式把本地的访问流量导向 Web 应用防火墙，从而测试经过 Web 应用防火墙访问 Web 站点的线路连通性，避免直接修改 DNS 解析记录，影响到公网用户对站点的访问。

1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择【Web 应用防火墙】>【防护设置】，在域名列表中查看 waf.qcloudwaf.com 的 VIP 地址。

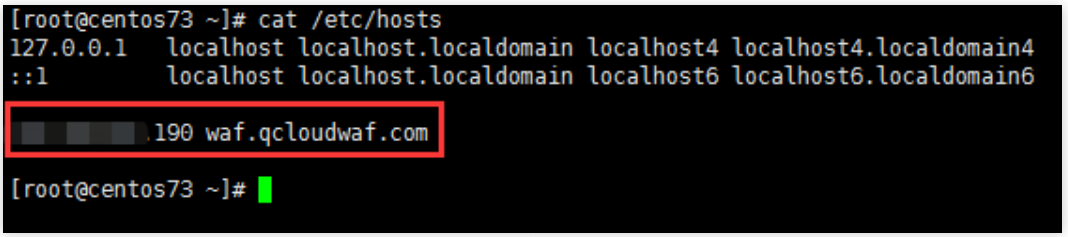


2. 修改 hosts 文件

- 在 Windows 下修改 C:\Windows\System32\drivers\etc\hosts ，增加条目。
  格式：VIP 地址+接入Web应用防火墙的域名。



- 在 Linux 下 修改 /etc/hosts ，增加条目。
  格式：VIP 地址+接入Web应用防火墙的域名。



3. 访问测试
   (1) 在本地电脑上访问 Web 站点，若站点能够正常打开，说明网站管家访问 Web 源站的线路连通性正常。
   (2) 在浏览器中输入下面的网址并访问。

   http://waf.qcloudwaf.com/?test=alert(123)

(3) 浏览器返回阻断页面，说明 Web 应用防火墙防护功能正常。

步骤3：修改 DNS 解析

当您想通过Web应用防火墙WAF防护公网用户访问网站的流量时，需要修改 DNS 的解析记录，相关DNS CNAME记录修改使用DNS标准修改流程即可。

步骤4：设置安全组

安全组是云平台提供的实例级别防火墙，可对任意云服务器进行入或出流量控制。在安全组中设置仅允许来自 Web 应用防火墙的流量访问网站，可避免攻击者绕过 Web 应用防火墙直接攻击网站源站。
下面以在安全组中放行 Web 应用防火墙的回源 IP 111.230.27.90 为例，说明配置过程。

1. 登录 云服务器控制台在左侧目录中，单击【安全组】。

2. 进入安全组页面，单击【新建】，根据要求填写信息，模板选择【自定义】，输入安全组的名称（例如 my-security-group），填写相关备注，填写完成后，单击【确定】。



3. 在安全组列表中，找到刚才新建的安全组，单击其 ID 进入详情页。

4. 在入站规则页面中，单击【添加规则】。



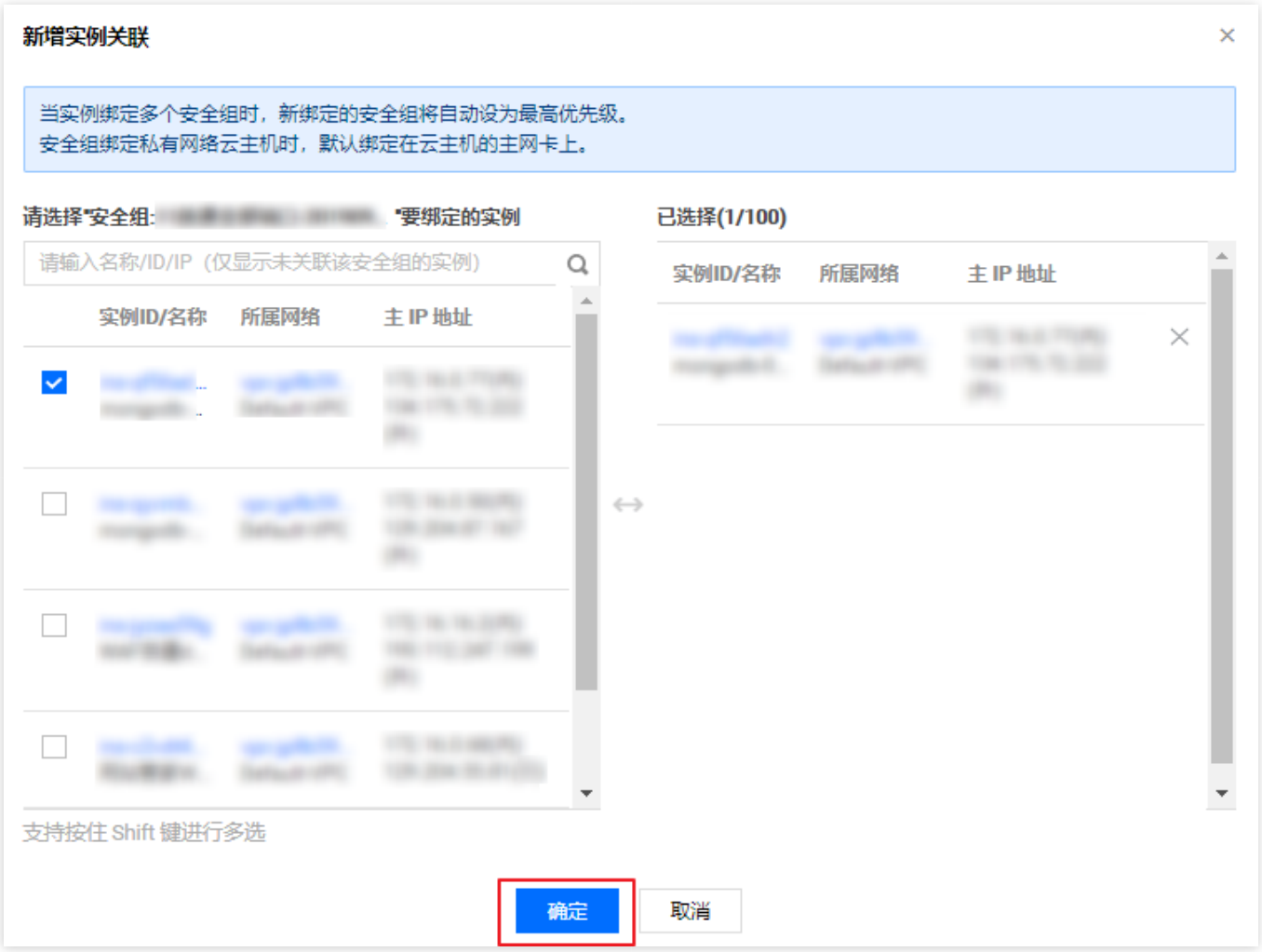
5. 在弹出框中填写相关信息，类型选择“HTTP（80）”，来源中填写需要放行的回源 IP，根据需求填写端口及策略，填写完毕后，单击【完成】。



6. 单击选项卡中的【关联实例】，在云服务器页面下，单击【新增关联】。



7. 在弹出框中选择需要绑定的云服务器，单击【确定】即可。



或者您还可以进入 云服务器列表页，查看或修改某云服务器已绑定的安全组，在列表页选择需要调整安全组的云服务器 ID，在右侧操作栏，选择【更多】>【安全组】>【配置安全组】，选择安全组进行绑定。



负载均衡型WAF

负载均衡型 WAF 通过配置域名和七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP 或 HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离。为了实现联动防护，您需要完成以下步骤：

步骤1：确认负载均衡配置

负载均衡型WAF通过添加域名和负载均衡监听器进行绑定，实现对经过负载均衡监听器的 HTTP 或 HTTPS 流量进行检测和拦截。在接入负载均衡型 WAF 前，请确保网站业务已经在云平台上，并且使用了负载均衡（原应用型负载均衡，网络类型为公网类型）。若您的网站业务不在云平台上，建议您使用 SaaS 型 WAF 接入防护。

为了使负载均衡型 WAF 能够识别出需要防护的域名，需要配置负载均衡并且在监听器配置相应域名，实现业务正常转发。详情请参见 配置 HTTP 监听器 和 配置 HTTPS 监听。

本文以防护wow.qcloudwaf.com为例，查看负载均衡监听器配置信息。

1. 登录云控制台，单击【云产品】>【云计算与网络】>【负载均衡】，进入负载均衡控制台。
2. 在“LB 实例列表”中，找到已创建的负载均衡实例，单击实例 ID，进入负载均衡详情页。



3. 在负载均衡详情页面，单击【监听器管理】，查看监听器域名配置信息。监听器的名称为 waftest，协议HTTP，端口80。



4. 创建转发规则，监听器转发规则监听的域名为 wow.qcloudwaf.com ，URL路径填“/”，选择是否进行监控检查，以及会话保持，点击【提交】，完成域名添加。此时域名防护状态为未启用。

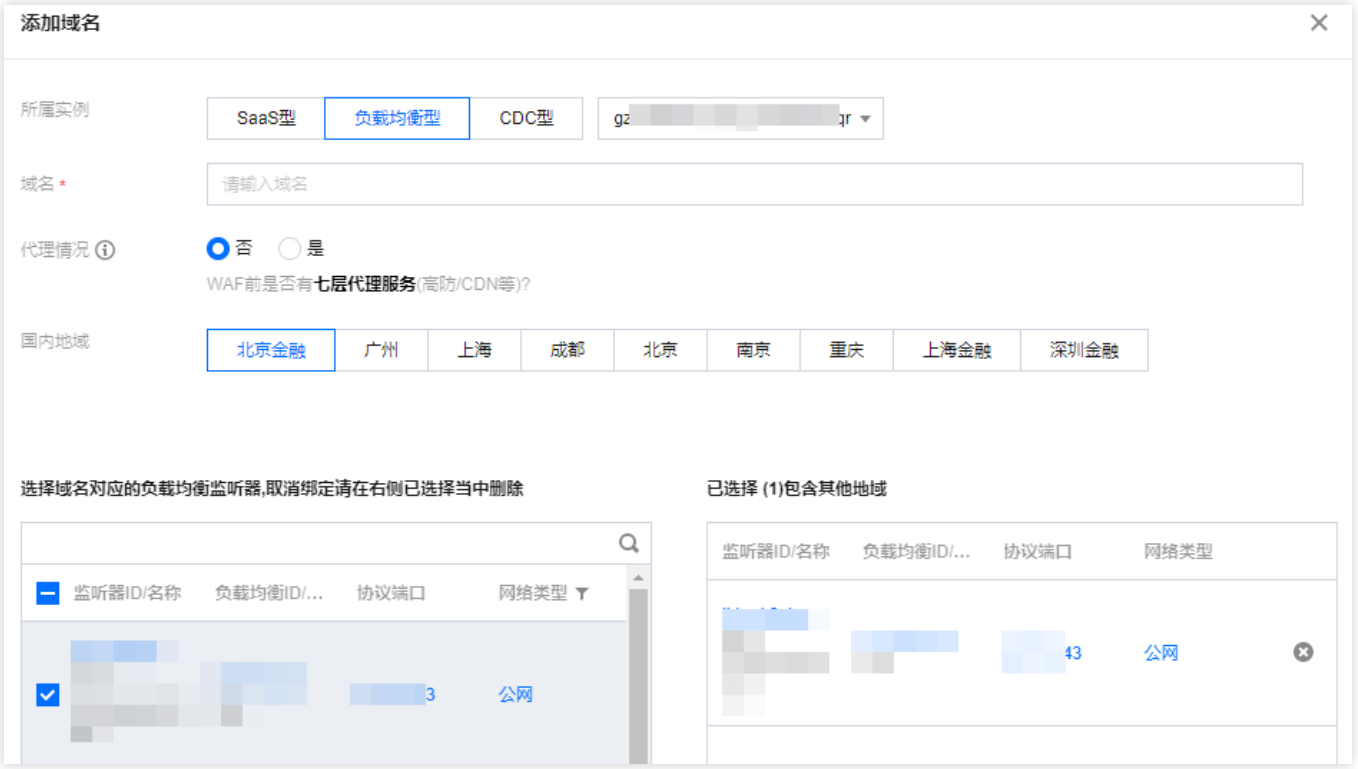




步骤2：域名添加绑定负载均衡

操作步骤

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择资产中心 > 接入管理，进入域名接入页面。
2. 在域名接入页面，单击添加域名，进入添加域名页面选择“负载均衡型”。
3. 在添加域名页面，填写需要防护域名，根据域名所在地域选择监听器信息，配置代理情况后确认完成接入。



> 注意：

> 填写的域名需要和负载均衡监听器中添加的域名保持一致。

步骤3：验证测试

1. 确保本地电脑可以正常访问 Web 站点。

2. 在浏览器中输入网址 http://wow.qcloudwaf.com/?test=alert(123) 并访问。

> 注意：
>
> wow.qcloudwaf.com 为本案例中域名，此处需要将域名替换为实际添加的域名。

3. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择【日志服务】>【攻击日志】，进入攻击日志查询页面，进行日志查询。

4. 选择添加防护的域名，单击【查询】。若看到攻击类型为 “XSS 攻击”，说明 WAF 配置已经生效。



> 说明：
>
> 如果域名未配置 DNS，可参见 SaaS 型 WAF 快速入门的步骤2：本地测试进行接入有效性验证。

操作指南
租户端功能清单

目录	页面	功能项
安全可视	概览	安全概览展示
		攻击总览展示
		基础安全分析展示
		业务运营分析展示
		域名Web攻击次数 TOP5(次)展示
		域名CC攻击次数 TOP5(次)展示
		攻击来源IP TOP5(次)展示
		攻击类型占比展示
		攻击来源区域分布(次)展示
日志服务	攻击日志	日志服务-原始数据展示
		日志检索
		日志下载
资产中心	接入管理	添加域名
		删除域名
		编辑域名
		域名列表展示
		WAF开关
	实例管理	新建实例
		删除实例
		管理域名
配置中心	基础安全	自定义返回拦截页面功能
		防护模式选择功能

		防护等级选择功能
		恶意文件检测
		IP封禁设置，包括Web攻击次数、检测时长、封禁时间
		tiga规则列表
		tiga规则检索功能
		单条tiga规则开关
		添加tiga规则白名单
		地域封禁功能
		访问控制规则功能
		CC防护功能
		网页防篡改功能
		信息防泄漏功能
	黑白名单	IP黑名单
		IP白名单
		精准白名单
		规则白名单
服务管理	web规则库	防护规则列表
	审计日志	在控制台调用waf接口日志列表

负载均衡WAF域名接入

负载均衡型 WAF 通过配置域名和七层负载均衡（监听器）集群进行联动，对经过负载均衡的 HTTP 或 HTTPS 流量进行旁路威胁检测和清洗，实现业务转发和安全防护分离。为了实现联动防护，您需要完成以下步骤：

步骤1：确认负载均衡配置

负载均衡型WAF通过添加域名和负载均衡监听器进行绑定，实现对经过负载均衡监听器的 HTTP 或 HTTPS 流量进行检测和拦截。在接入负载均衡型 WAF 前，请确保网站业务已经在该租户的VPC中，并且使用负载均衡（原应用型负载均衡，网络类型为公网类型）。
若您的网站业务未使用负载均衡，建议您使用 SaaS 型 WAF 提供防护。

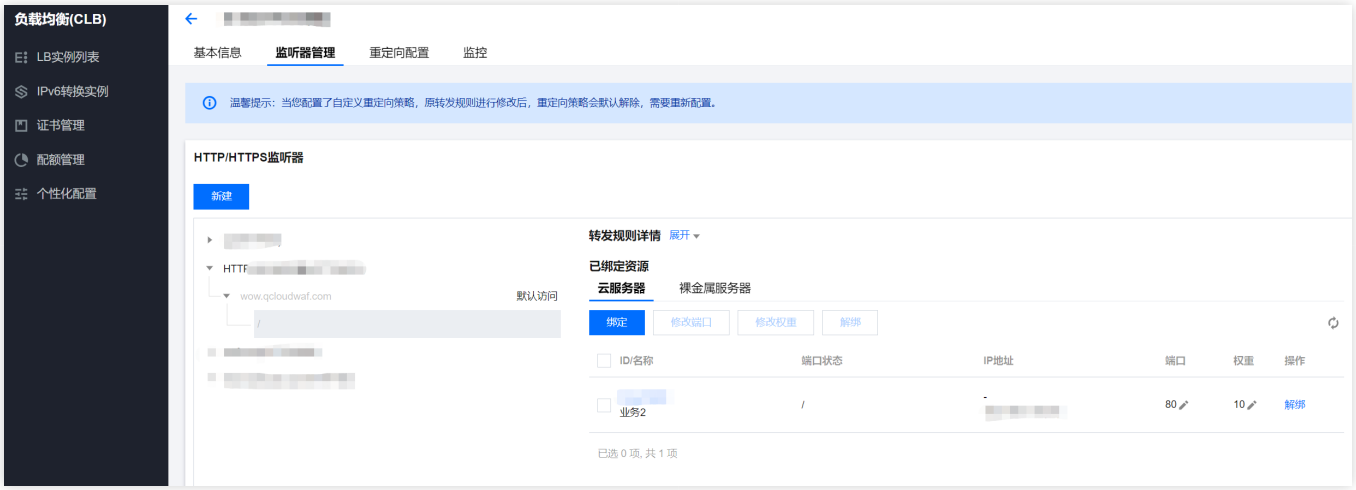
为了使负载均衡型 WAF 能够识别出需要防护的域名，需要配置负载均衡并且在监听器配置相应域名，实现业务正常转发。详情请参见 配置 HTTP 监听器 和 配置 HTTPS 监听。
本文以防护wow.qcloudwaf.com为例，查看负载均衡监听器配置信息。

1. 登录云租户控制台，单击【云产品】>【云计算与网络】>【负载均衡】，进入负载均衡控制台。
2. 在“LB 实例列表”中，找到已创建的负载均衡实例 clb-test，单击实例 ID，进入负载均衡详情页。
3. 在负载均衡详情页面，单击【监听器管理】，查看监听器域名配置信息。监听器的名称为 waftest，协议HTTP，端口80。



4. 创建转发规则，监听器转发规则监听的域名为 wow.qcloudwaf.com ，URL路径填“/”，选择是否进行监控检查，以及会话保持，点击【提交】，完成域名添加。此时域名防护状态为未启用。


创建HTTP/HTTPS转发规则
1 基本配置
2 健康检查
3 会话保持
域名
wow.qcloudwaf.com
默认域名
当客户端请求没有匹配本监听器的任何域名时，CLB会将请求转发给默认域名（Default Server），每个监听器只能配置且必须配置一个默认域名，详情
URL路径
/
均衡方式
按权重轮询
当后端CVM的权重都设置为同一个值时，权重属性将不生效，将按照简单的轮询策略分发请求
获取客户端IP
已启用
Gzip压缩
已启用
下一步：健康检查
取消

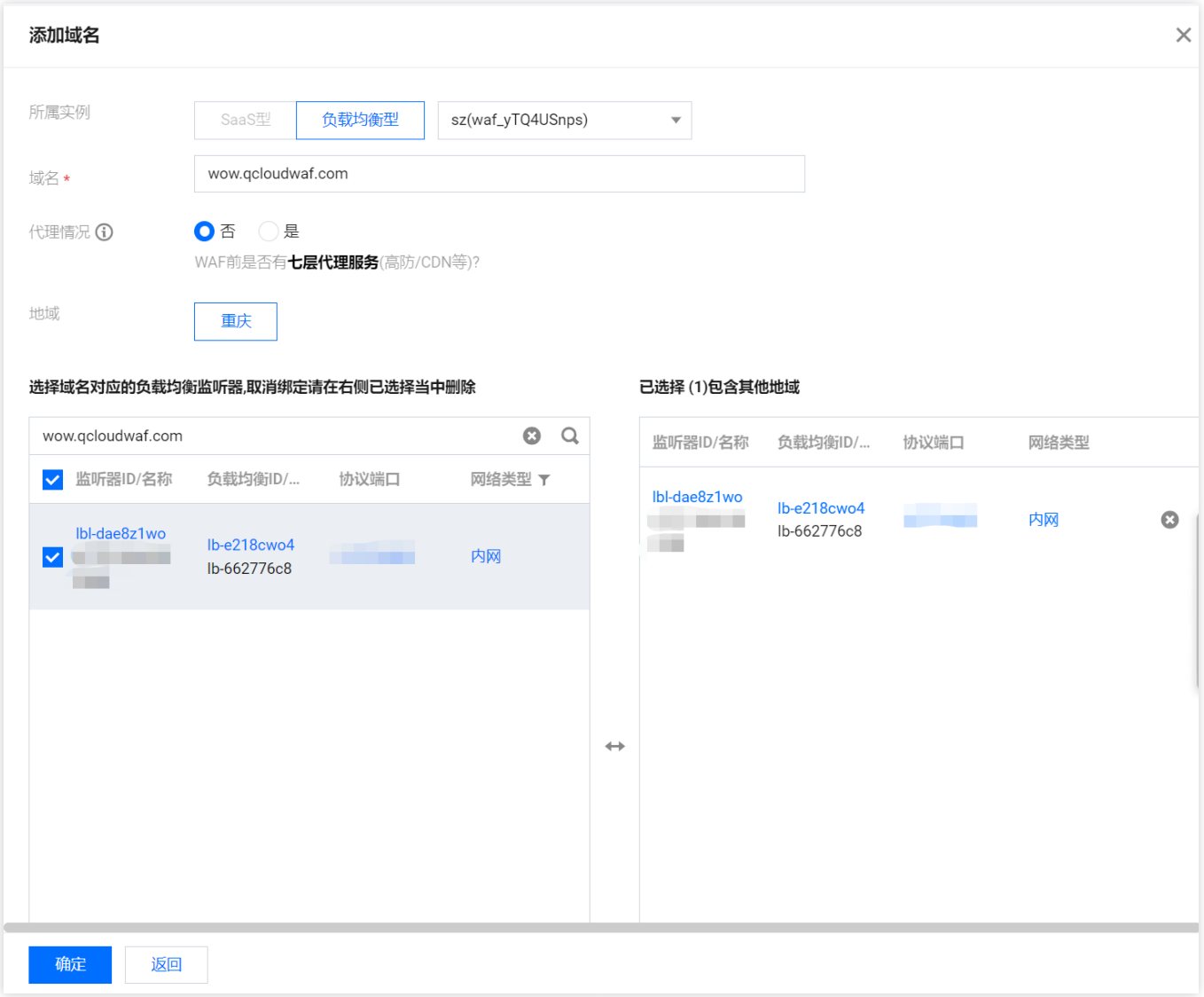

负载均衡(CLB)
LB实例列表
IPv6转换实例
证书管理
配额管理
个性化配置
基本信息
监听器管理
重定向配置
监控
温馨提示：当您配置了自定义重定向策略，原转发规则进行修改后，重定向策略会默认解除，需要重新配置。
HTTP/HTTPS监听器
新建
转发规则详情 展开
已绑定资源
云服务器
裸金属服务器
绑定
修改端口
修改权重
解绑
ID/名称
端口状态
IP地址
端口
权重
操作
业务2
80
10
解绑
已选 0 项, 共 1 项

步骤2：域名添加绑定负载均衡

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择资产中心 > 接入管理，进入域名接入页面。

2. 在域名接入页面，单击添加域名，进入添加域名页面选择“负载均衡型”。

3. 在添加域名页面，填写需要防护域名，根据域名所在地域选择监听器信息，配置代理情况后确认完成接入。



> 注意：
>
> 填写的域名需要和负载均衡监听器中添加的域名保持一致。

4. 绑定完成后，在页面下方，单击【完成】即可返回域名列表。在域名列表可以查看到防护域名wow.qcloudwaf.com和负载均衡的负载均衡 ID、名称、VIP 和监听器信息等。



步骤3：验证测试

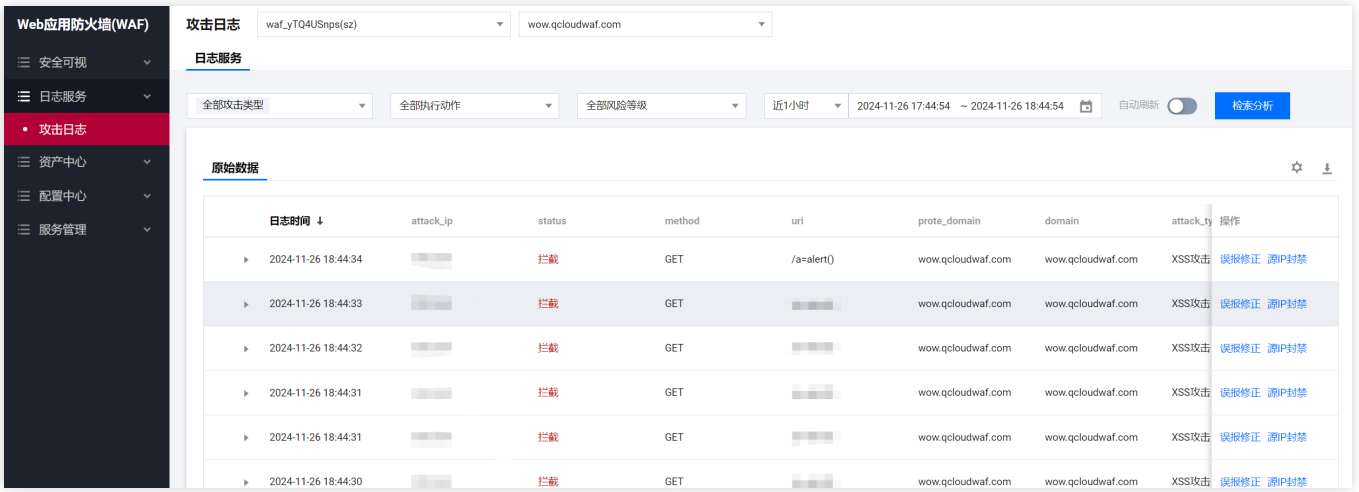
1. 确保本地电脑可以正常访问 Web 站点。

2. 在浏览器中输入网址 http://wow.qcloudwaf.com/?test=alert(123) 并访问。

> 注意：
>
> wow.qcloudwaf.com 为本案例中域名，此处需要将域名替换为实际添加的域名。

3. 登录Web 应用防火墙控制台，在左侧导航栏中，选择【日志服务】>【攻击日志】，进入攻击日志查询页面，进行日志查询。

4. 选择添加防护的域名，单击【查询】。若看到攻击类型为 “XSS 攻击”，说明 WAF 配置已经生效。



> 说明：
>
> 如果域名未配置 DNS，可参见 SaaS 型 WAF 快速入门的步骤2：本地测试进行接入有效性验证。

规则引擎

本文档将为您介绍如何通过 Web 应用防火墙（WAF）进行规则防护设置，以防护 Web 攻击。

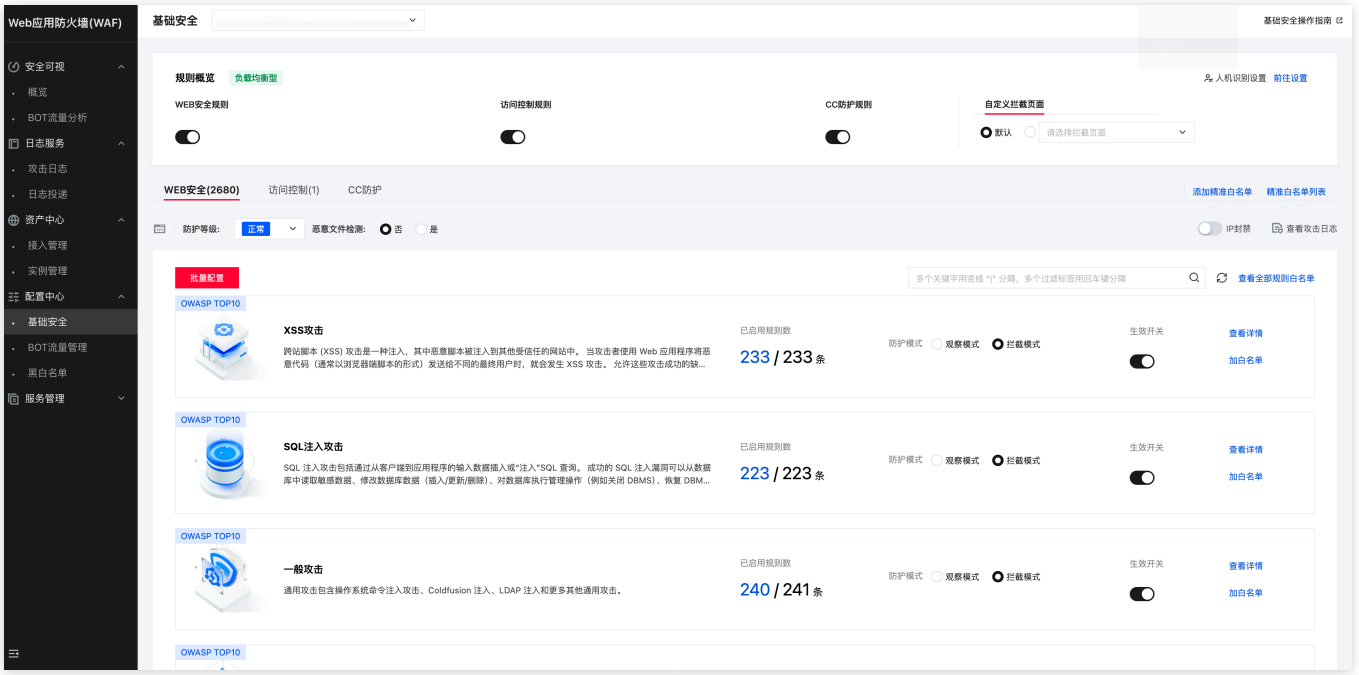
背景信息

Web 应用防火墙（WAF）使用基于正则的规则防护引擎和基于机器学习的 AI 防护引擎，进行 Web 漏洞和未知威胁防护。
WAF 规则防护引擎，提供基于安全 Web 威胁和情报积累的专家规则集，自动防护 OWASP TOP10 攻击。目前防护 Web 攻击包括： SQL 注入、XSS 攻击、恶意扫描、命令注入攻击、Web 应用漏洞、Webshell 上传、不合规协议、木马后门等12类通用的 Web 攻击。
WAF 规则防护引擎，支持规则等级划分，用户可根据实际业务需要进行规则防护等级设置，并支持对规则集规则或单条规则进行开关设置，可以对 WAF 预设的规则进行禁用操作，同时提供基于指定域名 URL 和规则 ID 白名单处置策略，进行误报处理。

操作步骤

域名规则防护引擎设置

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择【配置中心】>【基础安全】>【WEB安全】。
2. 在防护设置页面，对 Web 基础防护中的防护模式、防护等级、以及恶意文件检测方式进行配置，同时支持开启防扫描功能，并设置 IP 封禁规则。



字段说明：

- 规则引擎开关：默认开启。开关关闭后，经过 WAF 的域名请求将不进行规则引擎威胁处理。
- 防护模式：规则引擎工作模式，默认为拦截。
- 观察：不阻断攻击请求，进行预警，产生观察日志。
- 拦截：直接阻断 Web 攻击请求，产生拦截日志。
- 防护等级：规则引擎防护等级，默认为正常。
  - 正常：检测常见 Web 应用攻击。用户发现默认等级下存在较多误拦截，或者业务存在较多不可控的用户输入时（含有富文本编辑器的网站），建议您选择该模式。
  - 严格：严格检测 SQL 注入、XSS 攻击、命令执行等 Web 应用攻击，默认模式。
- 规则管理：通过规则管理，用户可查看规则引擎信息并对规则引擎进行设置，包括查看攻击分类、查看规则等级包含的规则内容、规则集更新动态，同时可对单条规则进行开关设置，添加基于域名 URL 和规则 ID 的白名单。
- 支持的解码类型：当前规则引擎默认支持以下解码类型，暂不支持手动设置。
- URL 解码（多重解码）、javascript Unicode 解码、注释处理、空格压缩、UTF-7 解码、HTML 实体解码、Multipart 解析、JSON 解析、XML 解析、Form 解析。
- 批量配置：支持对多个威胁类型进行统一的默认设置。



查看规则分类

1. 进入规则引擎设置页面。

- 方式1：登录 Web 应用防火墙控制台，在左侧导航栏中，选择【资产中心】>【接入管理】，进入域名列表管理页面，选择任意域名，点击操作列的【防护配置】按钮，进入域名的Web安全防护配置页面，查看规则详情。
- 方式2：
- a.登录 Web 应用防火墙控制台，在左侧导航栏中，选择【配置中心】>【基础安全】。
- b.在域名列表中，单击需要防护的域名，进入【Web安全】设置页面，进入规则引擎页面。

2. 进入规则库管理页面
登录 Web 应用防火墙控制台，在左侧导航栏中，选择【服务管理】>【Web规则库】，可查看当前 WAF 支持防护的攻击分类描述和规则更新动态信息。



当前 WAF 支持防护的攻击分类如下：

攻击分类	攻击描述
XSS 攻击	跨站脚本（XSS）攻击是一种注入，其中恶意脚本被注入到其他受信任的网站中。 当攻击者使用 Web 应用程序将恶意代码（通常以浏览器端脚本的形式）发送给不同的最终用户时，就会发生 XSS 攻击。 允许这些攻击成功的缺陷非常普遍，并且发生在 Web 应用程序在其生成的输出中使用来自用户的输入而不对其进行验证或编码的任何地方。 攻击者可以使用 XSS 向毫无戒心的用户发送恶意脚本。 最终用户的浏览器无法知道该脚本不应受信任，并且会执行该脚本。 由于它认为脚本来自可信来源，因此恶意脚本可以访问浏览器保留并与该站点一起使用的任何 cookie、会话令牌或其他敏感信息。 这些脚本甚至可以重写 HTML 页面的内容。
XSS 攻击(扩展)	跨站脚本攻击的扩展规则集，相比于标准规则集检测范围更广，检测内容更宽，检测能力更强，但是需要容忍一定的规则误报。
SQL 注入攻击	SQL 注入攻击包括通过从客户端到应用程序的输入数据插入或"注入"SQL 查询。 成功的 SQL 注入漏洞可以从数据库中读取敏感数据、修改数据库数据（插入/更新/删除）、对数据库执行管理操作（例如关闭 DBMS）、恢复 DBMS 文件中存在的给定文件的内容，并在某些情况下向操作系统发出命令。 SQL 注入攻击是一种注入攻击，其中 SQL 命令被注入到数据平面输入中，以影响预定义 SQL 命令的执行。
SQL 注入攻击(扩展)	SQL 注入攻击的扩展规则集，相比于标准规则集检测范围更广，检测内容更宽，检测能力更强，但是需要容忍一定的规则误报。
一般攻击	通用攻击包含操作系统命令注入攻击、Coldfusion 注入、LDAP 注入和更多其他通用攻击。
一般攻击(扩展)	通用攻击的扩展规则集，相比于标准规则集检测范围更广，检测内容更宽，检测能力更强，但是需要容忍一定的规则误报。
已知弱点	已知弱点主要用来检测各种应用、Web服务器、中间件等出现的远程任意代码执行漏洞、远程任意命令执行漏洞、路径遍历漏洞、开放重定向漏洞、未授权访问漏洞等。

攻击分类	攻击描述
恶意机器人	恶意机器人检测主要用来检测 Web 扫描器，脚本批量获取工具等恶意工具。

规则管理

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择【配置中心】>【基础安全】，选择需要管理的域名后，进入WEB安全页面。
2. 在 WEB 安全管理页面，支持规则的开启、关闭、观察模式管理，并提供将规则添加至白名单的能力。
   备注：所有规则默认为开启拦截模式。



3. 用户可以通过“规则等级”、“攻击分类”、“CVEID”或输入“规则 ID”进行规则集搜索，查看特定规则并进行操作。

> 说明：
>
> 严格规则等级包含正常和严格规则。

CC防护设置

功能简介

CC 防护对网站特定的 URL 进行访问保护。

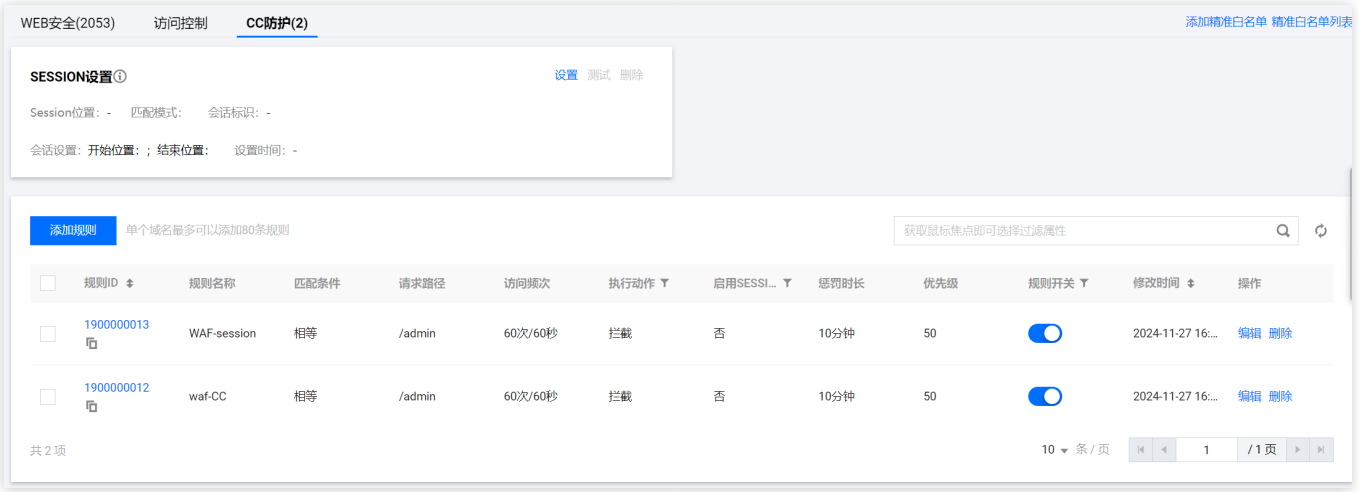
- 使用基于 SESSION 的 CC 防护策略，需要先进行 SESSION 设置，才能设置基于 SESSION 的 CC 防护策略。

配置步骤

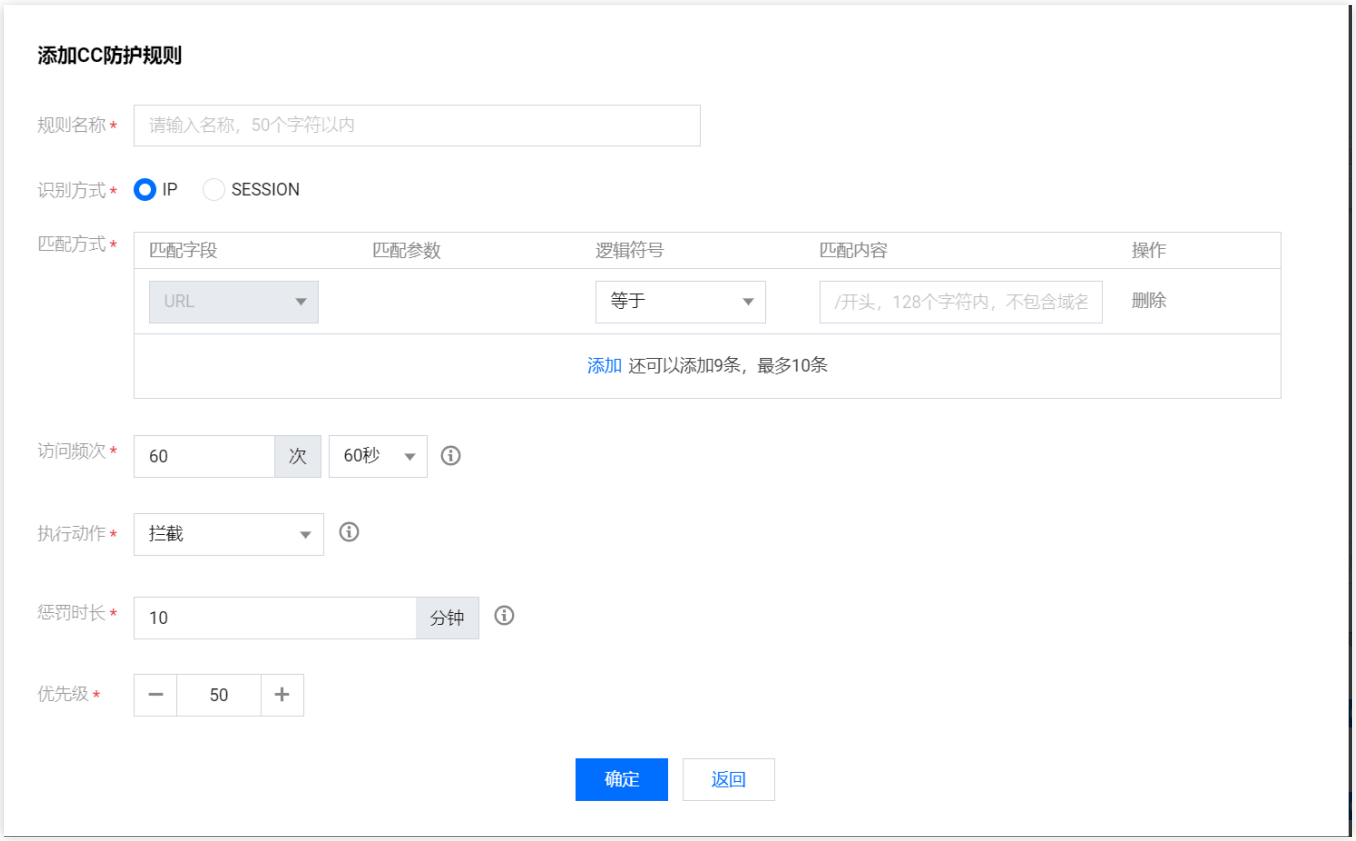
示例一： 基于访问源 IP 的 CC 防护设置

基于 IP 的 CC 防护策略，不需要对 SESSION 维度进行设置，直接配置即可。

1. 登录Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名，单击选择【CC防护】进入配置页面。



2. 点击【添加规则】支持用户自定义添加 CC 防护规则页面，填写相应信息。



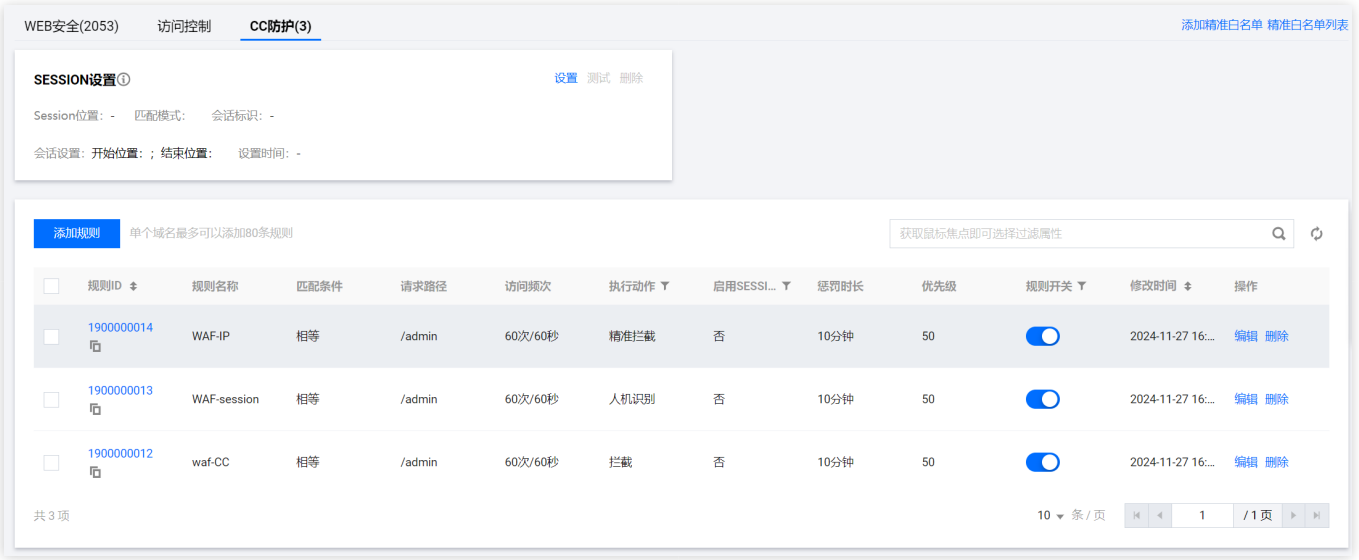
配置项说明：

- 识别模式： IP、SESSION。
- 匹配条件： 包括相等、前缀匹配和包含。

高级匹配：

- **匹配方式：**参考自定义规则的全部匹配字段设置。
- **访问频次：**根据业务情况设置访问频次。建议输入正常访问速度的3 - 10倍，例如网站平均访问20次/分钟，可配置为60 - 200/分钟，可依据被攻击严重程度调整。
- **执行动作：**观察、人机识别和阻断。
- **惩罚时长：**最短为1分钟，最长为一周。
- **优先级：**请输入1 - 100的整数，数字越小，代表这条规则的执行优先级越高，相同优先级下，创建时间越晚，优先级越高。

1. 规则操作，选择已经创建的规则，可以对规则进行关闭、修改和删除。

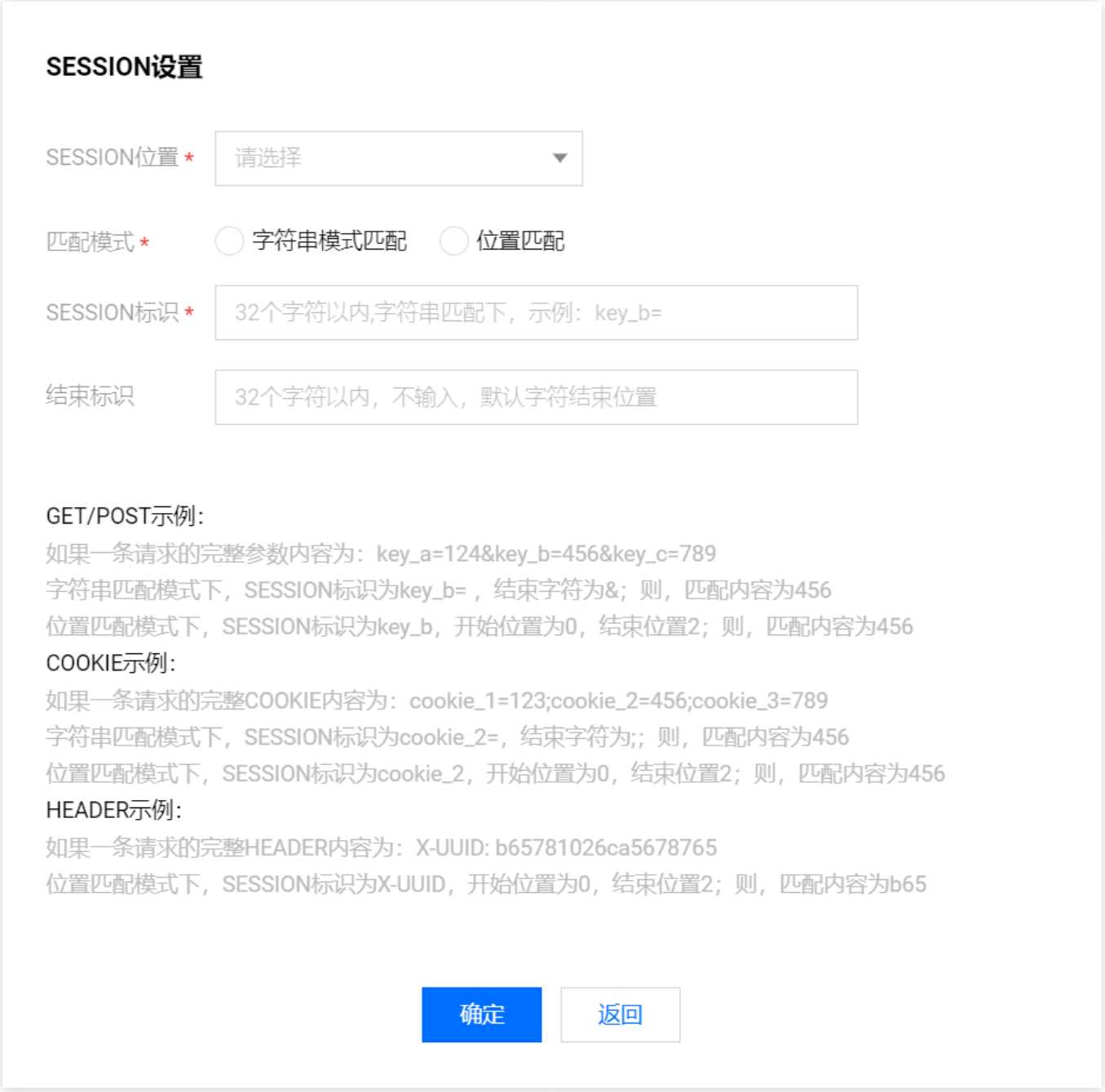


2. 根据规则设置，触发 CC 攻击行为，看到WAF返回的拦截页面。
3. 查看 IP 实时阻断信息。在左侧导航栏，选择【IP 管理】>【IP 封堵状态】，可以查看实时阻断的 IP 信息，并对 IP 进行加白或者加黑处理。

示例二： 基于 SESSION 的 CC 防护设置

基于 SESSION 访问速率的 CC 防护，能够有效解决在办公网、商超和公共 WIFI 场合，用户因使用相同 IP 出口而导致的误拦截问题。

1. 进入 Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名，单击选择【CC防护】进入配置页面。
2. 单击CC 防护设置中【新增】，支持自定义SESSION字段设置。



3. 进入 SESSION 设置页面，此示例选择 COOKIE 作为测试内容，标识为 security，开始位置为0，结束位置为9，配置完成后单击【设置】。

配置项说明：

- **SESSION 位置 ：**可选择 COOKIE、GET 或 POST，其中 GET 或 POST 是指 HTTP 请求内容参数，非 HTTP 头部信息。
- **匹配说明 ：**位置匹配或者字符串匹配。
- **SESSION 标识 ：**取值标识。
- **开始位置：**字符串或者位置匹配的开始位置。
- **结束位置：**字符串或位置匹配的结束位置。

GET/POST 示例 ：
如果一条请求的完整参数内容为：key_a = 124&key_b = 456&key_c = 789。

- 字符串匹配模式下，SESSION 标识为 key_b = ，结束字符为&，则匹配内容为456。
- 位置匹配模式下，SESSION 标识为 key_b，开始位置为0，结束位置2，则匹配内容为456。

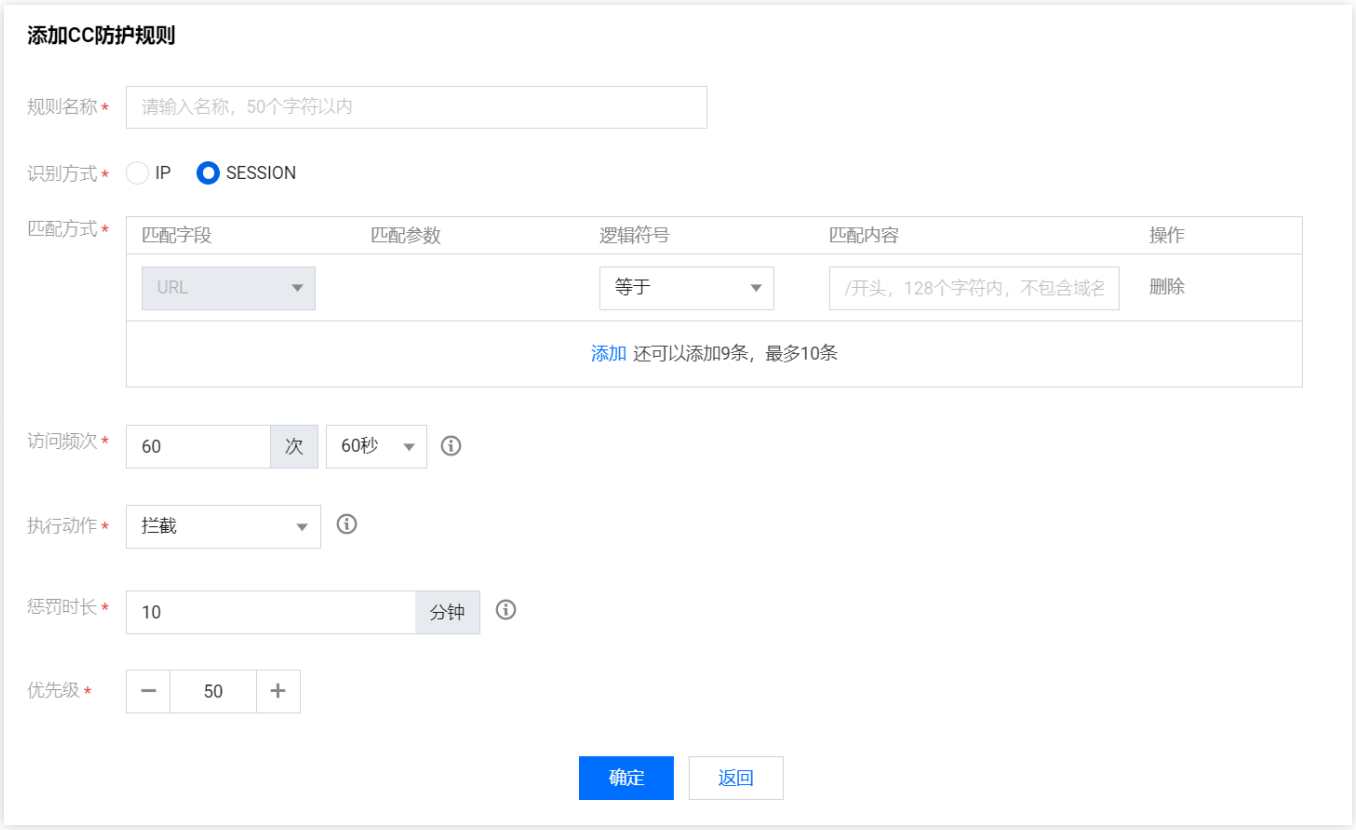
COOKIE 示例 ：
如果一条请求的完整 COOKIE 内容为：cookie_1 = 123;cookie_2 = 456;cookie_3 = 789。

- 字符串匹配模式下，SESSION 标识为 cookie_2 = ，结束字符为";"，则匹配内容为456。
- 位置匹配模式下，SESSION 标识为 cookie_2，开始位置为0，结束位置2，则匹配内容为456。

1. SESSION 维度信息测试。添加完成后，单击【测试】将填写内容进行测试。



2. 设置基于 SESSION 的 CC 防护策略，配置过程和示例一保持一致，识别模式选择 SESSION 即可。



3. 配置完成，基于 SESSION 的 CC 防护策略生效。

   使用基于 SESSION 的 CC 防护机制，无法在 IP 封堵状态中查看封堵信息。

自定义策略

功能简介

自定义策略支持从 HTTP 报文的请求路径、GET 参数、 POST 参数、 Referer 和 User-Agent 等多个特征进行组合，通过特征匹配来对公网用户的访问进行管控。面对来自互联网上的各种攻击行为，用户可以利用自定义策略灵活应对，组合出有针对性的规则来阻断各类攻击行为。

- 每个自定义策略最多可以设置5个条件进行特征控制。
- 每个自定义策略中的多个条件之间是"与"的关系，即所有条件全部匹配，策略才可生效。
- 每个自定义策略匹配之后可以配置两种处理动作：阻断和放行。
- 生效方式：支持立即生效、定制生效、周粒度周期生效、月粒度周期生效共四种不同的生效方式配置。
- 优先级：优先级数值越小则优先级越高，即1优先级最高，100优先级最低。

配置案例

案例一：禁止特定 IP 地址访问指定站点

当网站管理员需要禁止特定 IP 地址访问指定站点时，可以通过以下方法进行配置：

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【访问控制】进入配置页面。



2. 在添加规则页面内，输入规则名称（如001），在匹配字段中选择一个字段（如来源 IP），逻辑符号选择匹配，匹配内容填入需要禁止访问的来源 IP（如 192.168.1.1 ），选择执行动作（如阻断），填写完成后，单击 【添加】 保存规则。



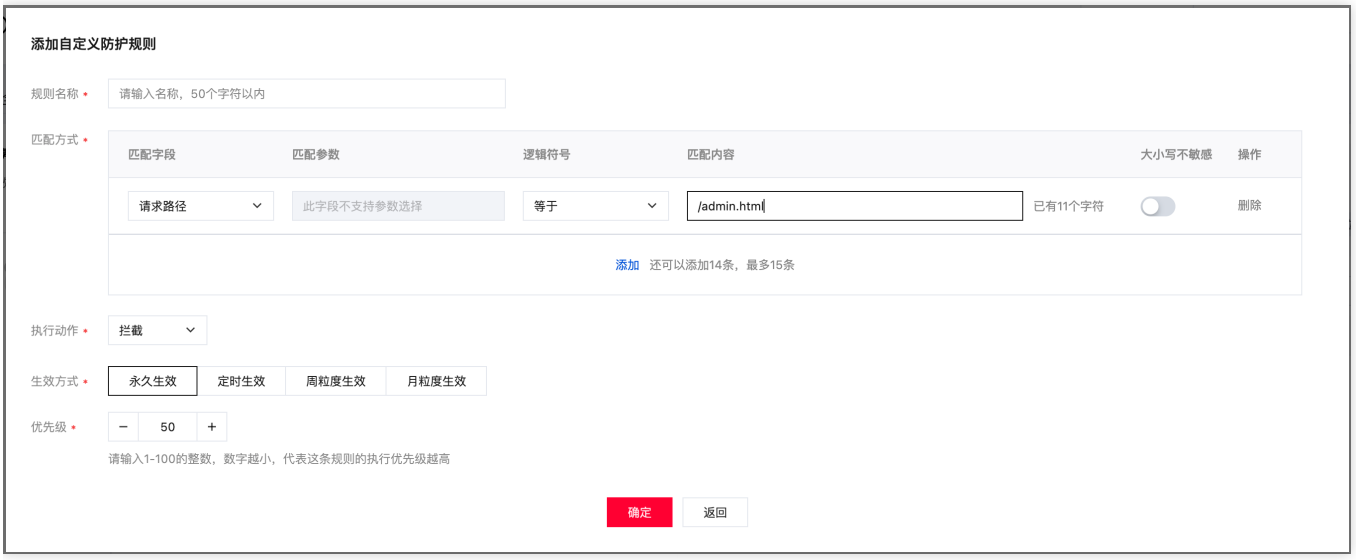
Web 应用防火墙的自定义策略支持使用掩码来控制某一网段的源 IP 的访问请求。我们可以在匹配内容中输入特定网段（如 10.10.10.10/24 ）。

3. 此时规则将会生效，来自特定源 IP 的 HTTP 访问请求将会全部阻断。



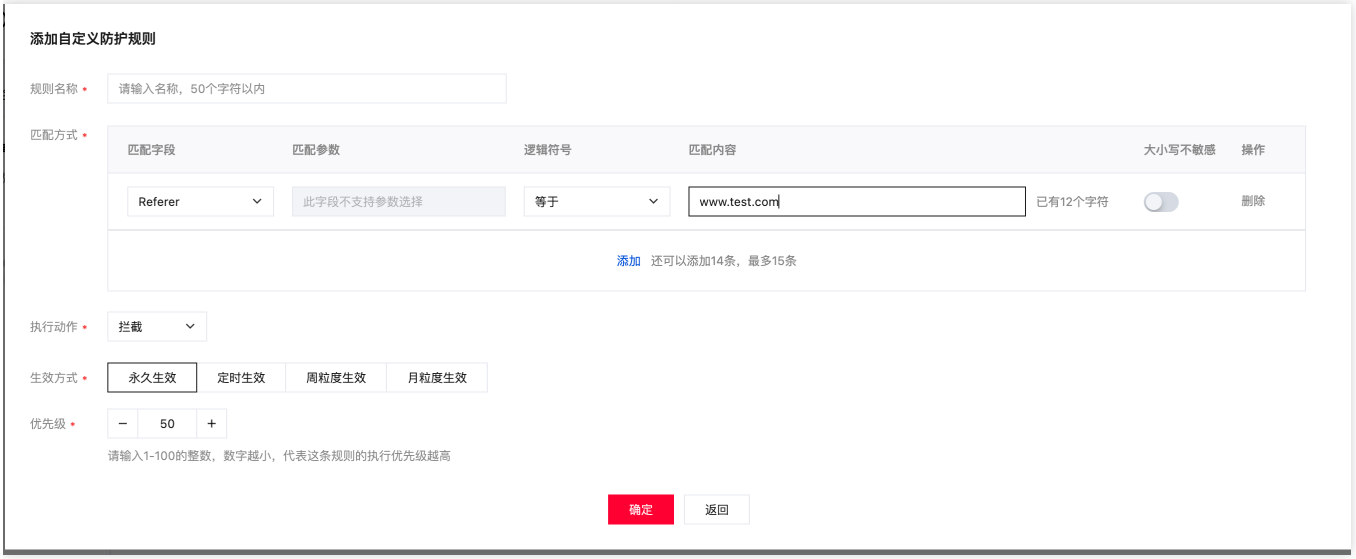
案例二：禁止公网用户访问特定的 Web 资源

当网站管理员不希望公网用户访问某些特定的 Web 资源时（如管理后台 /admin.html ），可以进行以下配置：匹配字段选择“请求路径”，逻辑符号选择“等于”，匹配内容输入“ /admin.html ”，执行动作选择“阻断”，配置完成后单击【添加】即可。



案例三：禁止某个外部站点盗链获取资源

当网站管理员需要阻断外部站点（如 www.test.com ）的盗链行为时，可以利用自定义策略对盗链请求的 Referer 特征进行捕获和阻断，配置如下：匹配字段选择 “Referer” ，逻辑符号选择“包含”，匹配内容输入“ www.test.com ”，执行动作选择“阻断”，配置完成后单击【添加】即可。



网页防篡改

功能简介

防篡改功能可用于防止发生指定页面被篡改而显示异常的问题。
指定页面仅限于 .html 、 .shtml 、 .txt 、 .js 、 .css 、 .jpg 、 .png 等静态资源。

> 说明：
>
> 负载均衡型 WAF 实例暂不支持此功能。

前提条件

使用云平台 SAAS 型 WAF 实例，且域名已接入SAAS型WAF 实例。

配置示例

保护网站主页不被篡改

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【防篡改】进入配置页面。



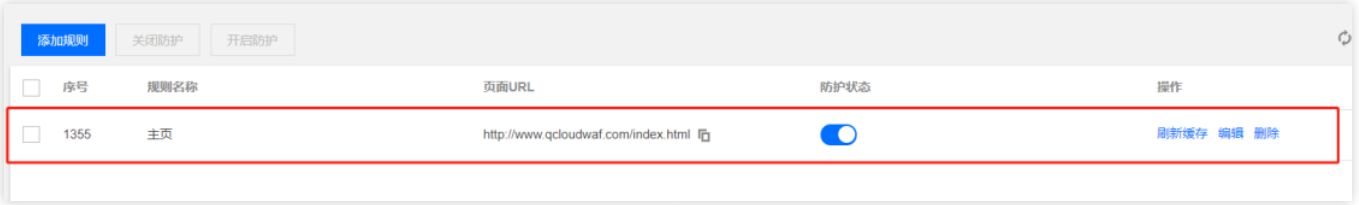
2. 进入防护设置页面，如果有需要可以在上方更换需要防护的站点域名，单击【防篡改】，进入防篡改配置界面，单击【添加规则】。



3. 在添加防篡改规则弹窗内，输入规则名称（如主页），输入规则（如主页）完整的 URL 路径（如 http://www.qcloudwaf.com/index.html ），输入完成后单击【添加】，保存规则。



4. 此时规则将会生效，如果规则更新，在右侧操作栏，单击【刷新缓存】，可更新缓存内容。



防信息泄露

功能简介

防信息泄露功能支持将您网页中返回的敏感信息进行替换，如手机号码、身份证号等。

> 说明：
>
> 负载均衡型 WAF 实例暂不支持此功能。

前提条件

使用云平台 SAAS 型 WAF 实例，且域名已接入 SAAS 型 WAF 实例。

配置示例

1. 登录Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【防信息泄漏】进入配置页面。选择【防信息泄露】>【添加规则】 。

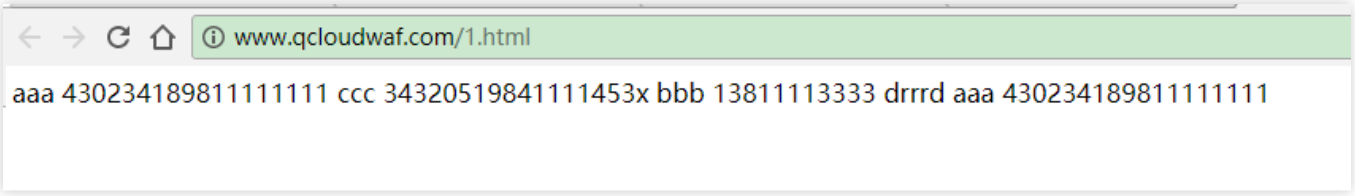


在添加规则页面，输入规则名称、选择匹配条件（匹配字段为敏感信息，匹配条件为包含，匹配内容为身份证或手机号）和执行动作（替换或观察），设置完成后，单击 【确定】 保存。



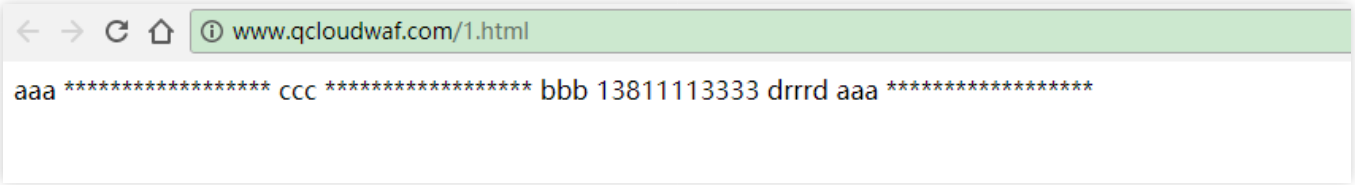
2. 规则生效，会对您网页中返回的敏感信息进行防护，防护效果如下（敏感内容为虚构）：

- 开启防护前：



开启防护前

- 开启防护后：

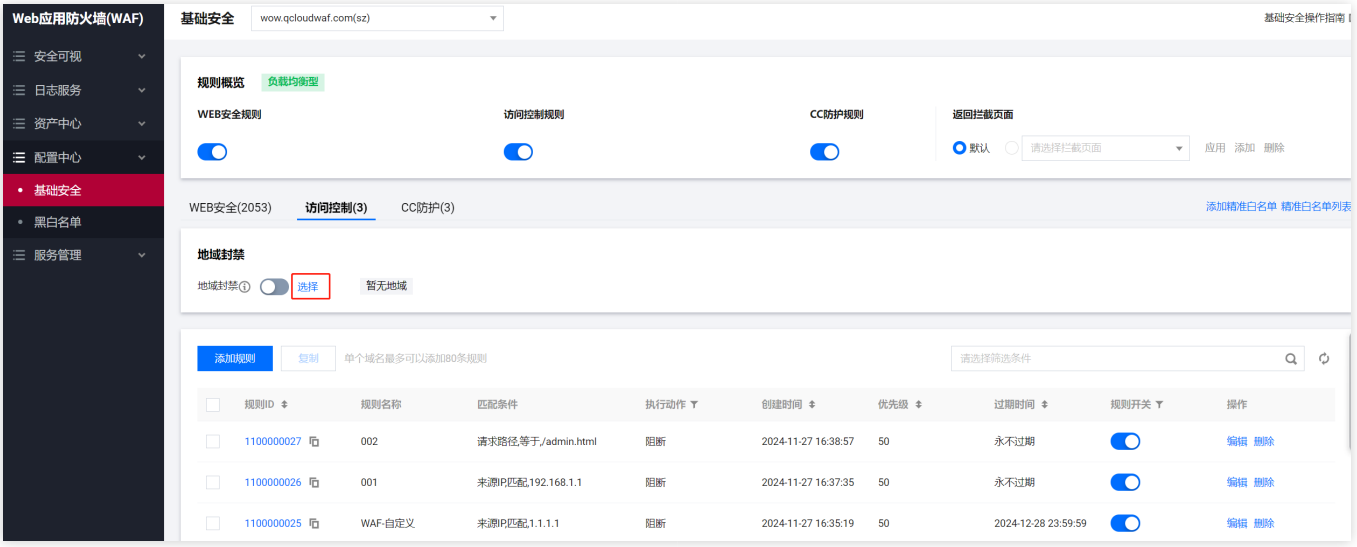


开启防护后

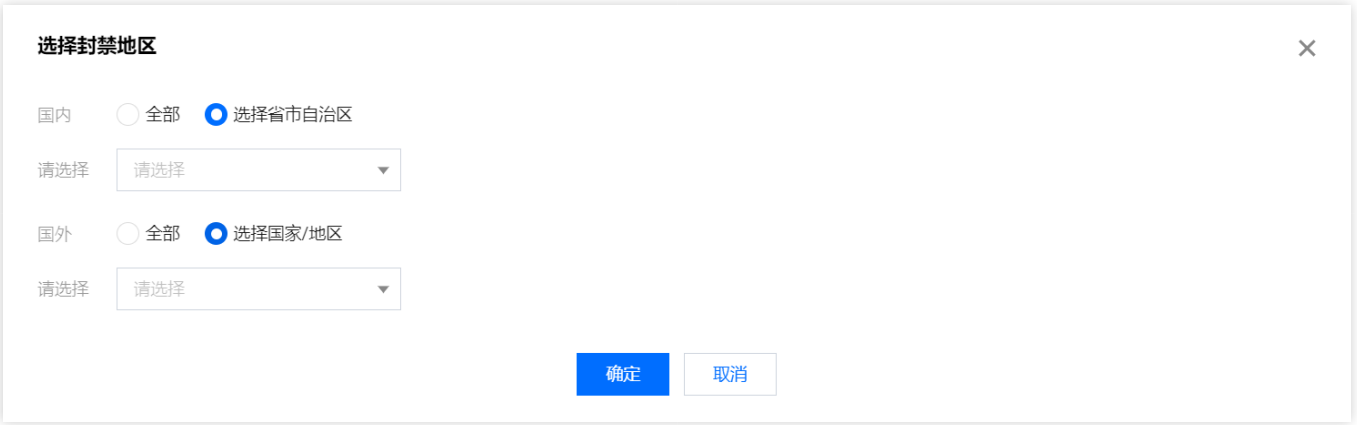
地域封禁

配置说明

1. 登录 Web 应用防火墙控制台，在左侧导航栏，选择【Web 应用防火墙】>【配置中心】>【基础安全】，选择防护的域名（如 www.qcloudwaf.com ），单击选择【访问控制】进入配置页面，选择地域封禁配置。



2. 在访问控制设置页面，单击【选择】地域封禁配置，进入地域封禁配置页面。



3. 在封禁地域设置页面，勾选需要封禁的国内地区，国外地区支持搜索或单击下拉列表进行选择，选择完成后单击【确定】。



4. 编辑完成后，开启地域封禁状态。

5. 此时您选择封禁的地区，将无法访问您的网站。本文将国外全部地区列入封禁地域后，使用境外 IP 地址访问防护网站，Web 应用防火墙会提示您已被拦截。

黑白名单管理
功能介绍

Web 应用防火墙的黑白名单功能，指的是对经过 Web 应用防火墙防护域名的访问源 IP 进行黑白名单设置，以及对多个 HTTP 特征进行精准白名单设置，主要功能包括： IP 黑白名单设置、精准白名单设置、以及规则白名单设置。

- IP 黑白名单设置，支持设置基于域名或全局的 IP 黑白名单规则，支持网段设置。
- 精准白名单设置，支持从 HTTP 报文的请求路径、GET 参数、 POST 参数、 Referer 和 User-Agent 等多个特征进行组合，通过特征匹配来对特定公网用户的访问进行加白。
- 规则白名单设置，支持通过规则类型、规则id，以及HTTP 报文的请求路径、GET 参数、 POST 参数、Referer 和 User-Agent 等多个特征进行组合，通过组合特征，规则id或规则类型组合放行流量。
  同时，可以添加基于域名的黑白名单或基于全局的黑白名单，生效优先级说明如下所示：
- 黑白名单的优先级仅低于 Web 应用防火墙精准白名单策略，高于其他检测逻辑。
- 黑白名单优先级从高到低顺序：全局白名单 > 域名白名单 >规则白名单->精准白名单策略 > 域名黑名单 >其他防护模块。

IP白名单

添加 IP 白名单

手动添加

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击配置中心 > 黑白名单，进入黑白名单页面。
2. 在黑白名单页面，左上角选择需要防护的域名，单击 IP 白名单，进入 IP 白名单页面。



3. 在 IP 白名单页面，单击添加地址，进入添加白名单页面。
4. 在添加白名单页面，配置相关参数，单击确定。



参数说明

- **IP 地址：**支持任意 IP 地址，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。

  > 说明
  >
  > - 选择域名为全局时，添加的 IP 地址或 IP 段为全局的白名单。

- 生效方式：永久生效、定时生效、月粒度周期生效，以及周粒度周期生效。

- **备注：**自定义，50个字符以内。

导入数据

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 白名单，进入 IP 白名单页面。
2. 在 IP 白名单页面，单击导入数据 > 导入，解析成功后，单击确认导入即可。



">

编辑 IP 白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 白名单，进入 IP 白名单页面。
2. 在 IP 白名单页面，选择所需 IP 地址，单击操作列的编辑，修改截止时间和备注，单击确定保存。



删除 IP 白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 白名单，进入 IP 白名单页面。
2. 在 IP 白名单页面，支持删除单个、部分、全部地址，具体操作如下：
   - 单个：选择单个 IP 地址，单击删除地址或操作列的删除，弹出“确认删除”弹窗。

     > 说明
     >
     > 删除后将无法恢复，重新添加才能生效。



- 部分：选择多个 IP 地址，单击删除地址，弹出“确认删除”弹窗。

> 说明
>
> 删除后将无法恢复，重新添加才能生效。



- 全部：单击全部删除，弹出“确认删除”弹窗。

> 注意
>
> 此操作将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

3. 在“确认删除”弹窗中，单击确定，即可删除地址。

导出全部筛选结果

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 白名单，进入 IP 白名单页面。
2. 在 IP 白名单页面，单击搜索框通过 IP 地址对 IP 进行筛选，或单击来源根据来源分类对 IP 进行筛选。



3. 筛选完所需 IP 后，单击导出全部筛选结果，即可导出所需的 IP 筛选结果。



精准白名单管理

当网站管理员需要根据用户的访问请求特征来放行公网用户访问指定站点时，可以通过添加精准白名单的方法进行配置。

添加精准白名单

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击配置中心 > 黑白名单，进入黑白名单页面。

2. 在黑白名单页面，左上角选择需要防护的域名，单击精准白名单，进入精准白名单页面。



3. 在精准白名单页面，单击添加规则，弹出添加精准白名单弹窗。

4. 在添加精准白名单弹窗中，配置相关参数，单击确定。



> 说明：
>
> Web 应用防火墙的精准白名单支持使用掩码来放行某一网段的源 IP 的访问请求。我们可以在匹配内容中输入特定网段（如10.10.10.0/24）。

5. 此时规则将会生效，来自特定源 IP 的 HTTP 访问请求将会全部放行。



编辑精准白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 精准白名单，进入精准白名单页面。
2. 在精准白名单页面，选择所需规则，单击编辑，弹出编辑精准白名单弹窗。



3. 在编辑精准白名单弹窗中，修改相关参数，单击确定保存。

删除精准白名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 精准白名单，进入精准白名单页面。
2. 在精准白名单页面，选择所需规则，单击删除，弹出确认删除弹窗。



3. 在确认删除弹窗中，单击确定，即可删除该规则。

> 说明：
>
> 删除后将无法恢复，重新添加才能生效。

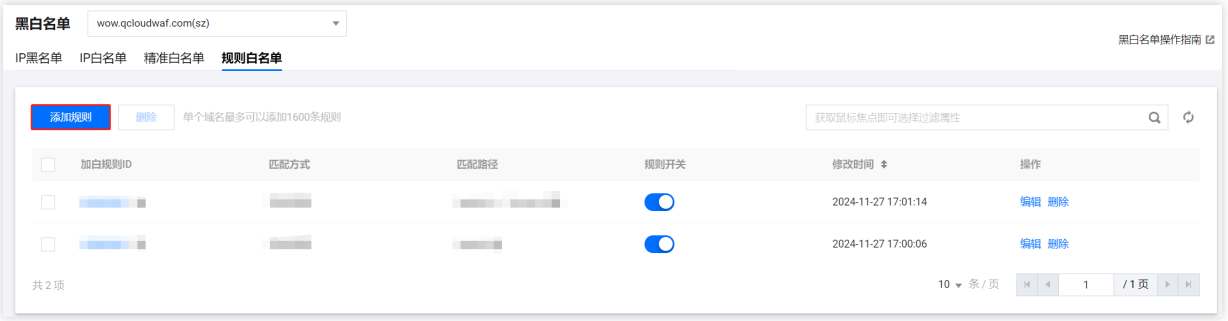
规则白名单

操作场景

在生产环境中如出现正常访问流量被 WAF 规则引擎拦截时，可以通过黑白名单中的规则白名单进行加白相应规则，加白该规则后就不会被拦截。

操作步骤

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，单击配置中心 > 黑白名单。
2. 在黑白名单页面，左上角选择需要防护的域名，单击规则白名单。
3. 在规则白名单页面，单击添加规则，弹出添加白名单弹窗。



4. 在添加规则弹窗中，配置相关参数，单击确定。

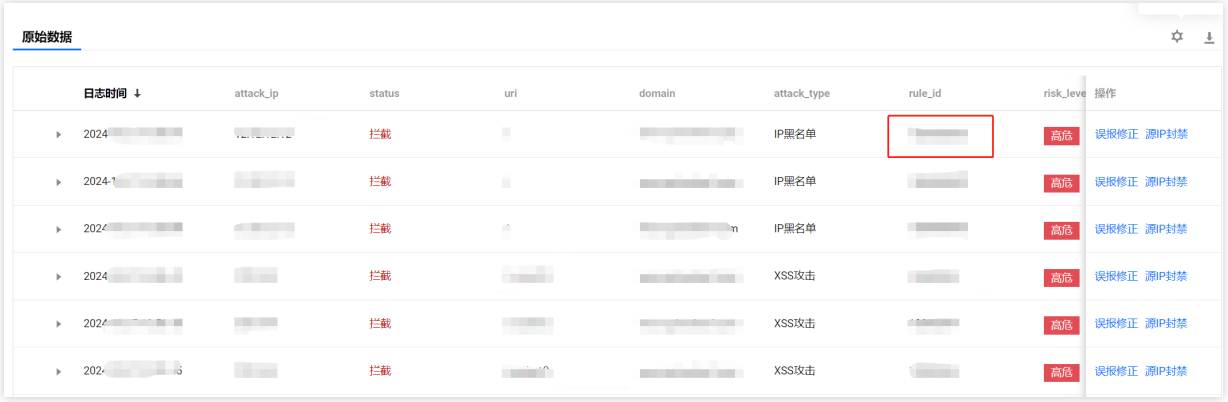


字段说明：

- 加白规则 ID：填写需要加白的规则 ID，一条策略可添加最多10个规则 ID。获取方法如下所示：
  - 在 基础安全页面，选择所需规则 ID，单击 复制。



- 在 日志服务页面，选择所需数据，复制该数据的 rule_id。



  - 匹配方式：加白 URL 路径的匹配方式，支持完全匹配（默认）、前缀匹配和后缀匹配。
  - URL 路径：需要加白的 URL 路径，同一个域名下 URL 不可重复添加。

IP黑名单

添加 IP 黑名单

手动添加

1. 登录 Web 应用防火墙控制台，在左侧导航栏中，选择【配置中心】 > 【黑白名单】。
2. 在黑白名单页面，左上角选择需要防护的域名，单击 IP 黑名单。



3. 在 IP 黑名单页面，单击添加地址，进入添加黑名单页面。
4. 在添加黑名单页面，配置相关参数，单击确定。



字段说明：

- **IP 地址：**支持任意 IP 地址或IP地址段，例如10.0.0.10或 FF05::B5；支持 CIDR 格式地址，例如10.0.0.0/16或FF05:B5::/60，使用换行符进行分隔，一次最多添加20个。

  > 说明：
  >
  > - 选择域名为全局时，添加的 IP 地址或 IP 段为全局的黑白名单。

- **生效方式：**永久生效、定时生效、月粒度周期生效，以及周粒度周期生效。

- **备注：**自定义，50个字符以内。

导入数据

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 黑名单。
2. 在 IP 黑名单页面，单击导入数据 > 导入，解析成功后，单击确认导入即可。



编辑 IP 黑名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 黑名单。
2. 在 IP 黑名单页面，选择所需 IP 地址，单击操作列的编辑，修改截止时间和备注，单击确定保存。



删除 IP 黑名单

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 黑名单。

2. 在 IP 黑名单页面，支持删除单个、部分、全部地址，具体操作如下：

   - 单个：选择单个 IP 地址，单击删除地址或操作列的删除，弹出“确认删除”弹窗。

     > 说明

> 删除后将无法恢复，重新添加才能生效。



- 部分：选择多个 IP 地址，单击删除地址，弹出“确认删除”弹窗。

> 说明
>
> 删除后将无法恢复，重新添加才能生效。



- 全部：单击全部删除，弹出“确认删除”弹窗。

> 注意
>
> 此操作将清除当前域名下所有的 IP 黑白名单信息，请谨慎操作！删除后将无法恢复，重新添加才能生效。

3. 在“确认删除”弹窗中，单击确定，即可删除地址。

导出全部筛选结果

1. 在 黑白名单页面，左上角选择需要防护的域名，单击 IP 黑名单。
2. 在 IP 黑名单页面，单击搜索框通过 IP 地址对 IP 进行筛选，或单击来源根据来源分类对 IP 进行筛选。
3. 筛选完所需 IP 后，单击导出全部筛选结果，即可导出所需的 IP 筛选结果。

攻击日志

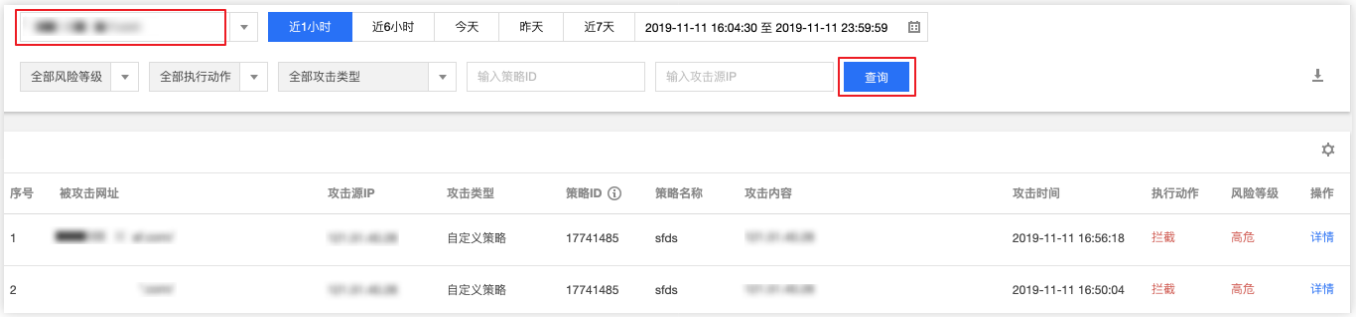
功能简介

Web 应用防火墙默认记录 Web 攻击日志信息，包括攻击产生的时间、攻击源 IP、攻击类型、攻击详情等信息。您可以根据需要按照过滤条件进行日志查询，并下载查询结果。

使用说明

查询攻击日志

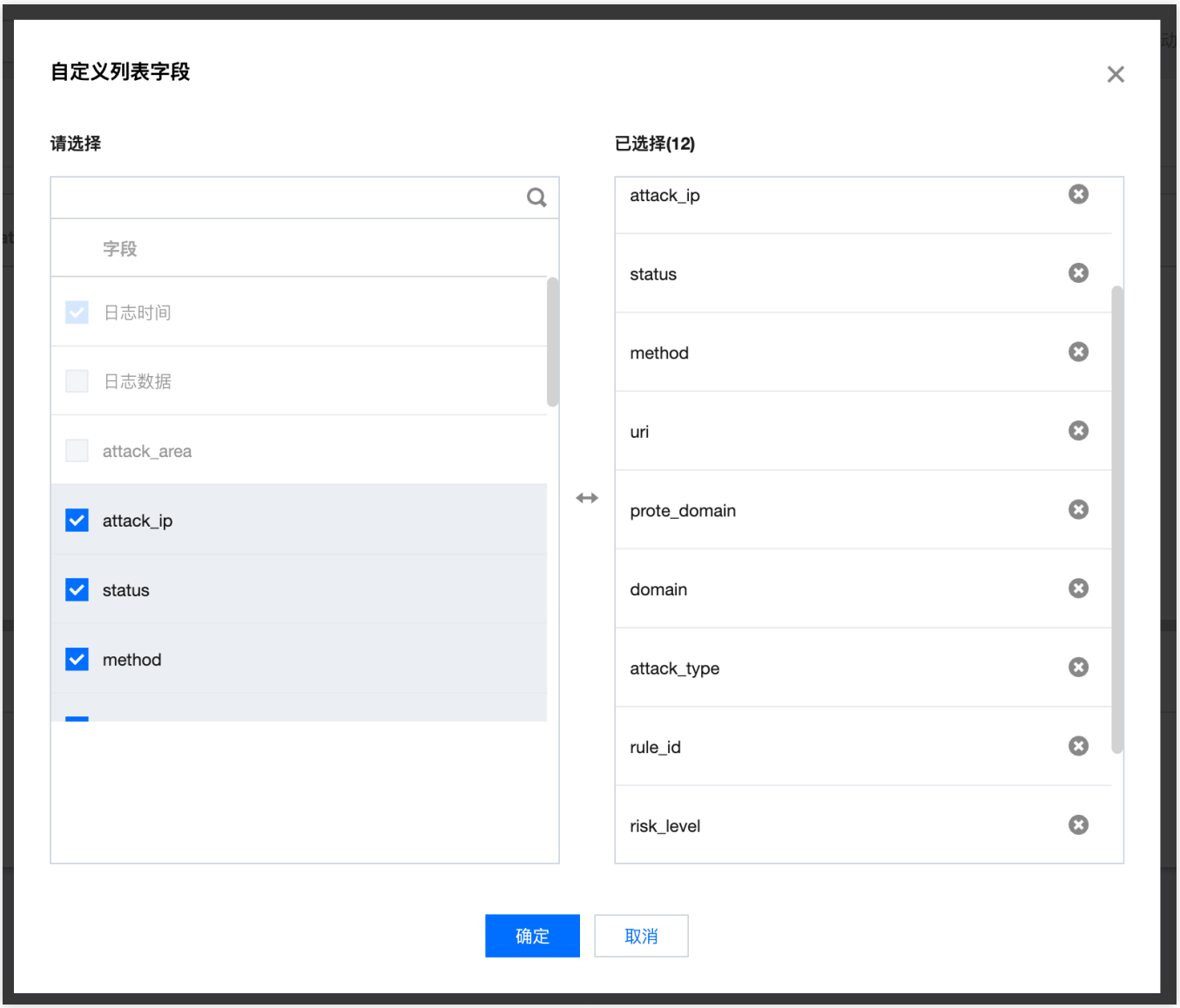
1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择【日志服务】>【攻击日志】。进入攻击日志查询页面，单击【日志查询】，在上方下拉搜索列表中选择域名，根据需要设置查询条件，单击【查询】，查看对应的攻击日志信息。



查询条件说明：

- 域名：在域名下拉搜索列表中，选择需要查询的域名。
- 时间条件：默认为1个小时，最长可查询30天的攻击日志信息。
- 风险等级：默认为全部，可选择高危、中危、低危。
- 执行动作：默认为全部，可选观察和拦截。
- 策略 ID：输入您需要查询的策略 ID（策略 ID 可以在日志条目中查看）。
- 攻击源 IP：输入您要查询的攻击源 IP，进行查询。

2. 单击攻击日志右上角的设置按钮 ，在弹出的"自定义列表字段"弹窗中，选择需要显示的列表详细信息。如下图所示：



3. 查看攻击详情。选择您需要查看日志条目，在右侧操作栏，单击【详情】，查看攻击详情信息。

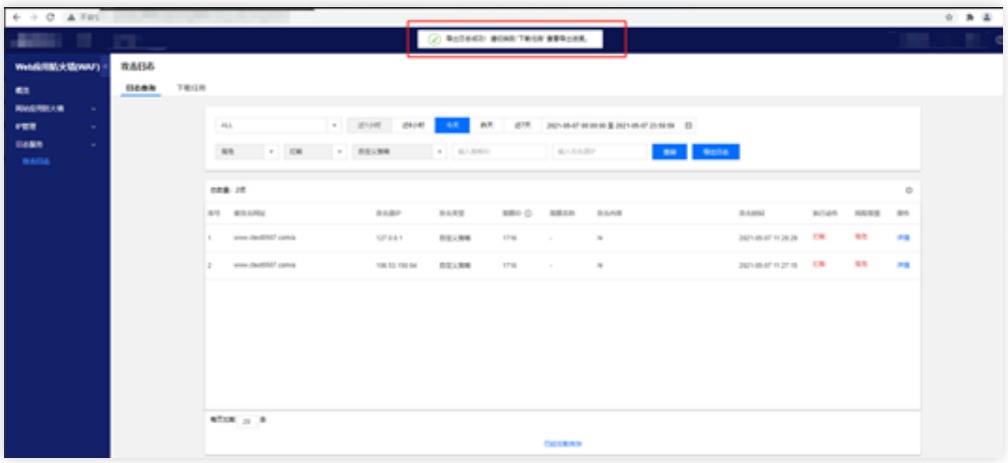


4. 进入日志详情页面，查看对应字段。



导出攻击日志

1. 登录Web 应用防火墙控制台，在左侧导航栏中，选择【日志服务】>【攻击日志】。进入攻击日志查询页面，单击【日志查询】，在上方下拉搜索列表中选择域名，根据需要设置查询条件，单击【查询】，查看对应的攻击日志信息。单击【导出日志】，导出对应的攻击日志信息。



导出条件说明：

- 域名：在域名下拉搜索列表中，选择需要查询的域名。
- 时间条件：默认为1个小时，最长可查询30天的攻击日志信息。
- 风险等级：默认为全部，可选择高危、中危、低危。
- 执行动作：默认为全部，可选观察和拦截。
- 策略 ID：输入您需要查询的策略 ID（策略 ID 可以在日志条目中查看）。
- 攻击源 IP：输入您要查询的攻击源 IP，进行查询。
- 日志表格内容不可为空。

2. 选择【日志服务】>【攻击日志】>【下载任务】。进入下载任务查询页面。如下图所示：



3. 单击【下载】，提示"日志文件下地址复制成功，请新建浏览器窗口打开"将链接复制到浏览器中打开，成功下载出日志压缩包。



日志详情字段说明：

- 基础信息

字段名称	字段说明
域名	客户端访问的域名
攻击类型	当前 Web 应用防火墙支持的攻击类型信息，默认为全部。
聚合攻击次数	相同攻击源 IP 和攻击类型，汇总每10秒产生的攻击次数。
攻击源 IP	客户端攻击的源 IP。
命中规则 ID	触发防护策略的规则 ID，其中 AI 引擎检出的攻击，规则 ID 为0。
命中规则名称	触发防护策略的策略名称，其中规则引擎和 AI 引擎的策略名称为空。
请求方法	客户端攻击请求方法。
风险等级	客户端攻击触发的风险等级。
攻击时间	客户端攻击触发的时间。
匹配来源	客户端攻击匹配来源信息，如来源 IP。

字段名称	字段说明
执行动作	客户端攻击触发的动作。
请求 URI	请求 URI 的内容。
攻击内容	客户端触发攻击的内容。

- 攻击 IP 详情

字段名称	字段说明
地区	使用源 IP 国家英文缩写。
IP 所有者	使用源 IP 所有者信息。
国家	攻击源 IP 所属的国家名称。
省份	攻击源 IP 所属的省份信息。
城市	攻击源 IP 所属的城市信息。
运营商	攻击源 IP 所属的运营商信息。
经度	攻击源 IP 的经度信息。
纬度	攻击源 IP 的纬度信息。

- 详情信息

字段名称	字段说明
协议版本	攻击源 IP 的 HTTP 协议版本信息。
User-Agent	攻击源 IP 向服务器用来表明自己的浏览器类型和操作系统标识等信息。

IP管理

功能简介

Web 应用防火墙 IP 管理功能，对经过 Web 应用防火墙防护域名的访问源 IP 进行状态查询和黑白名单设置，主要功能包括：IP 查询，IP 黑白名单设置和 IP 封堵状态查询。

- IP 查询，查询输入 IP 在防御域名中状态信息，包括是否在黑白名单中，是否处于封堵状态。
- IP 黑白名单设置，支持设置基于域名或全局的 IP 黑白名单规则。
- IP 封堵状态，实时查看 CC 攻击、自定义策略人机识别等源 IP 封堵状态信息。

配置步骤

示例一 IP 查询

1. 进入 Web 应用防火墙控制台，选择【IP 管理】>【IP 查询】输入需要查询的 IP 地址查看该 IP 状态。



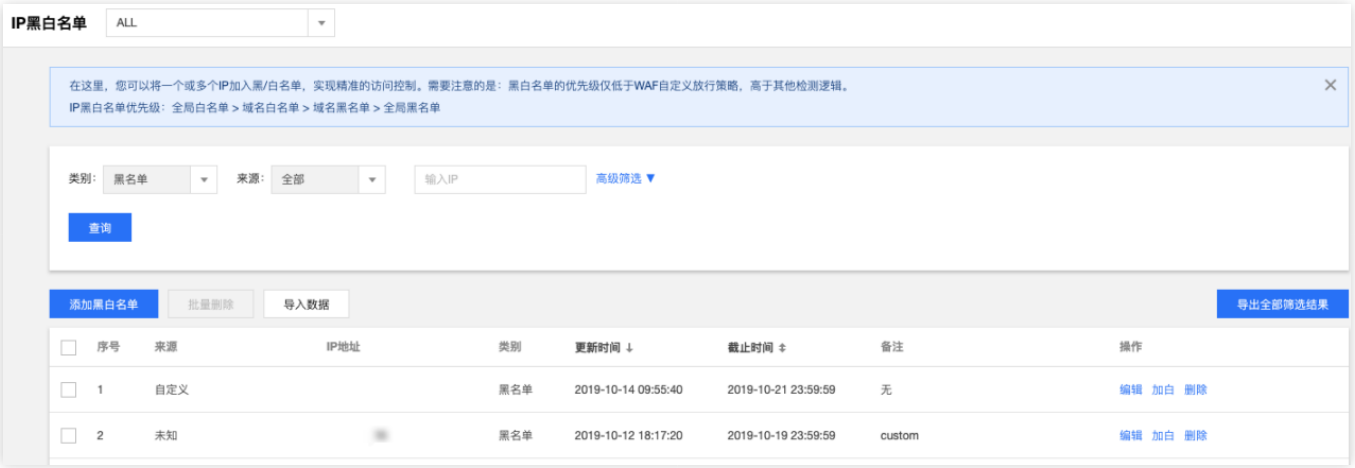
2. 查询出的 IP 地址，可手动添加黑白名单。



示例二 添加 IP 黑名单

1. 进入 Web 应用防火墙控制台，选择【IP 管理】>【IP 黑白名单】进入配置页面。
   IP 黑名单名单模块，可以添加基于域名的黑白名单或基于全局的黑白名单，生效优先级说明说如下：

- 黑白名单的优先级仅低于 Web 应用防火墙自定义放行策略，高于其他检测逻辑。
- IP黑白名单优先级从高到低顺序：全局白名单>域名白名单>域名黑名单>全局黑名单。



配置项说明：

- 类别：黑名单、白名单。
- 来源：CC 防护、自定义规则。

- 高级筛选：利用创建时间和有效截止时间进行 IP 信息筛选。

2. 添加黑白名单。左上角选择需要添加防护的域名，单击【添加黑白名单】，选择黑名单添加需要加黑的 IP 地址。



选择域名为 ALL 时，添加的 IP 黑白名单为全局的黑白名单。

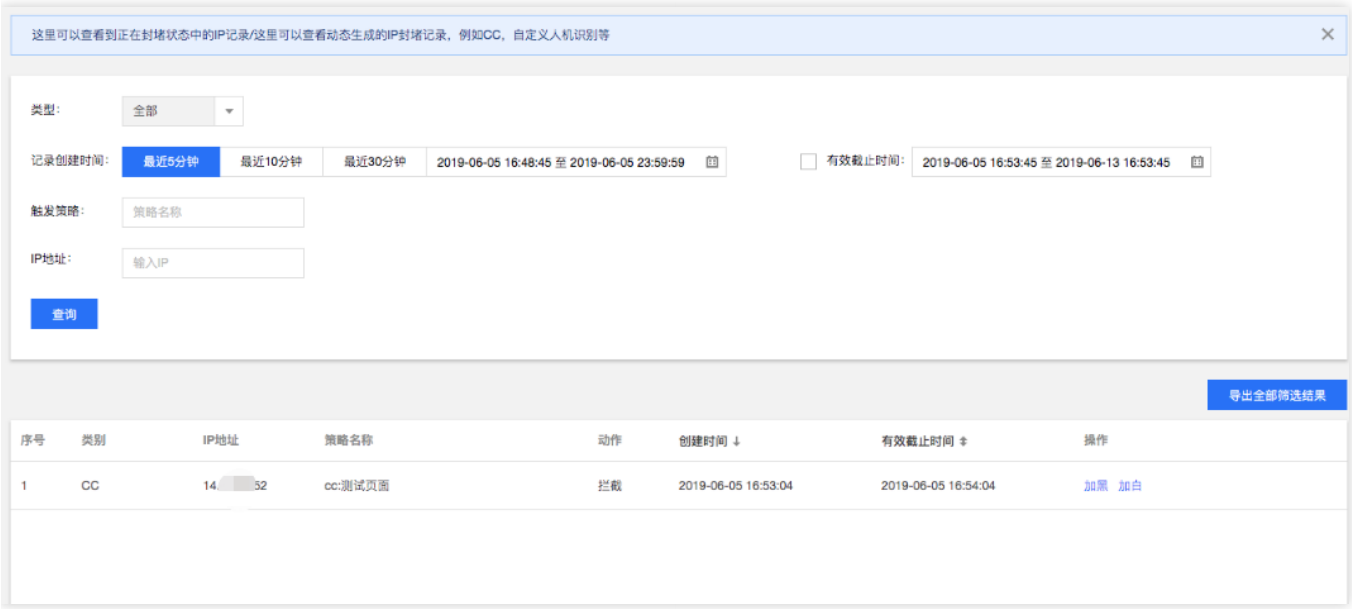
3. 黑白名单支持导入和筛选结果导出，导入 IP 信息时，请参考导出格式。



4. 添加完成后，可以在 IP 查询中输入添加的源 IP，查询状态信息。

示例三 IP 封堵状态查询

进入Web 应用防火墙控制台，选择【IP 管理】>【IP 封堵状态】进入查询页面，可以查询自定义规则、CC 防护模块拦截的 IP 信息。可对查询结果进行导出，对单个 IP 进行加黑加白操作。



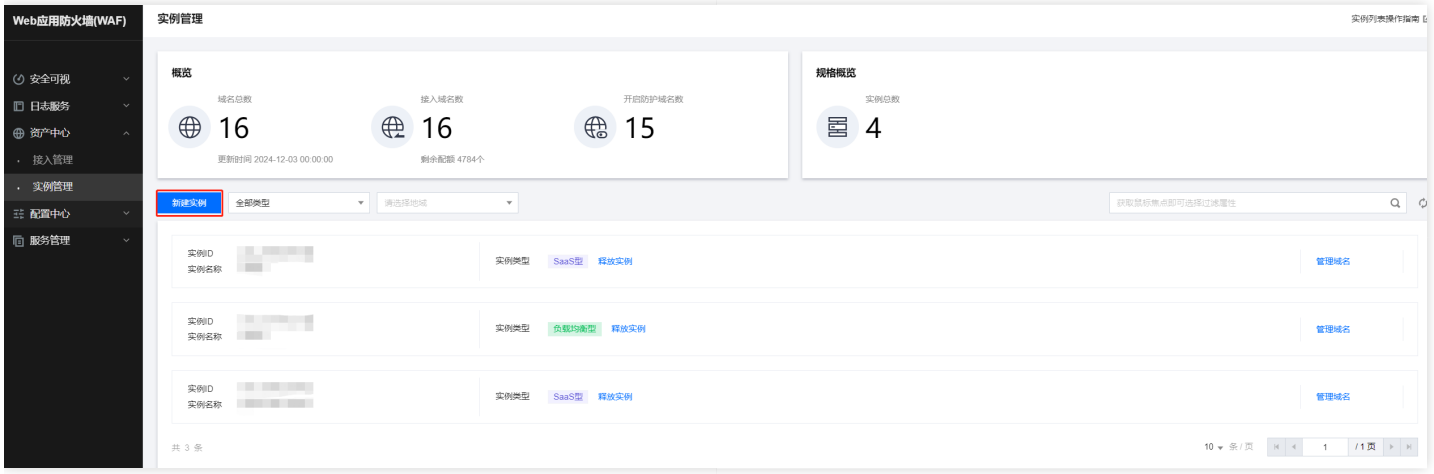
常见操作

场景1：创建实例

实例是WAF计量的最小单位，支持创建多个实例；1个实例支持管理20个域名。
以下操作以cloud为例，创建实例。

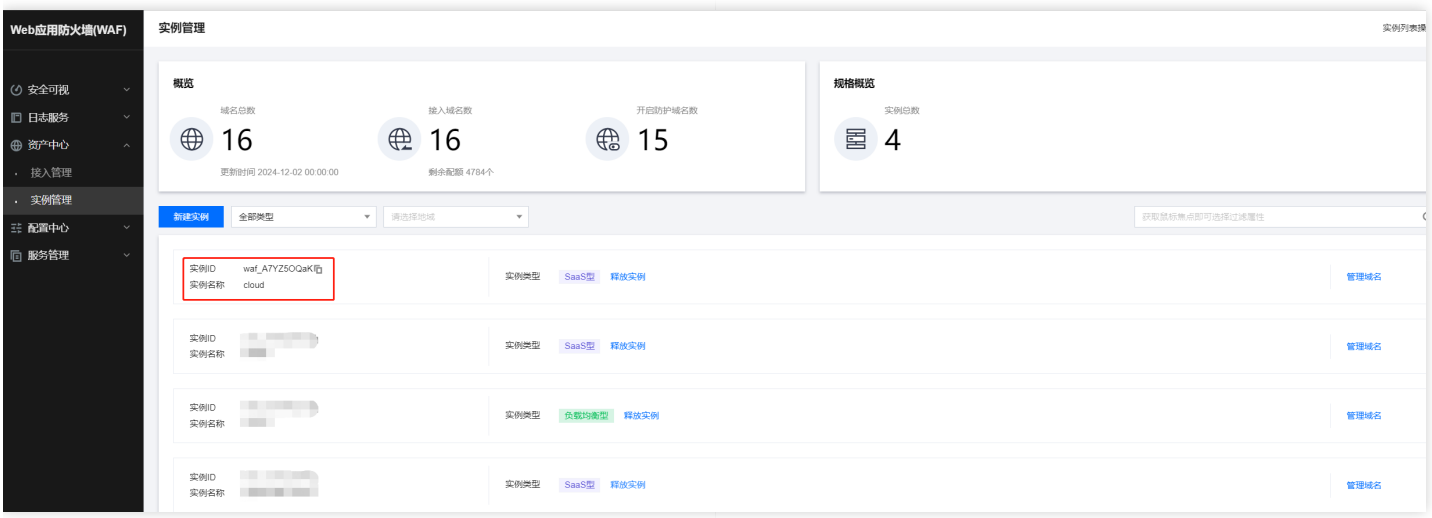
创建SaaS型实例

1.登录租户端WAF-资产中心-实例管理页面，点击新建实例；



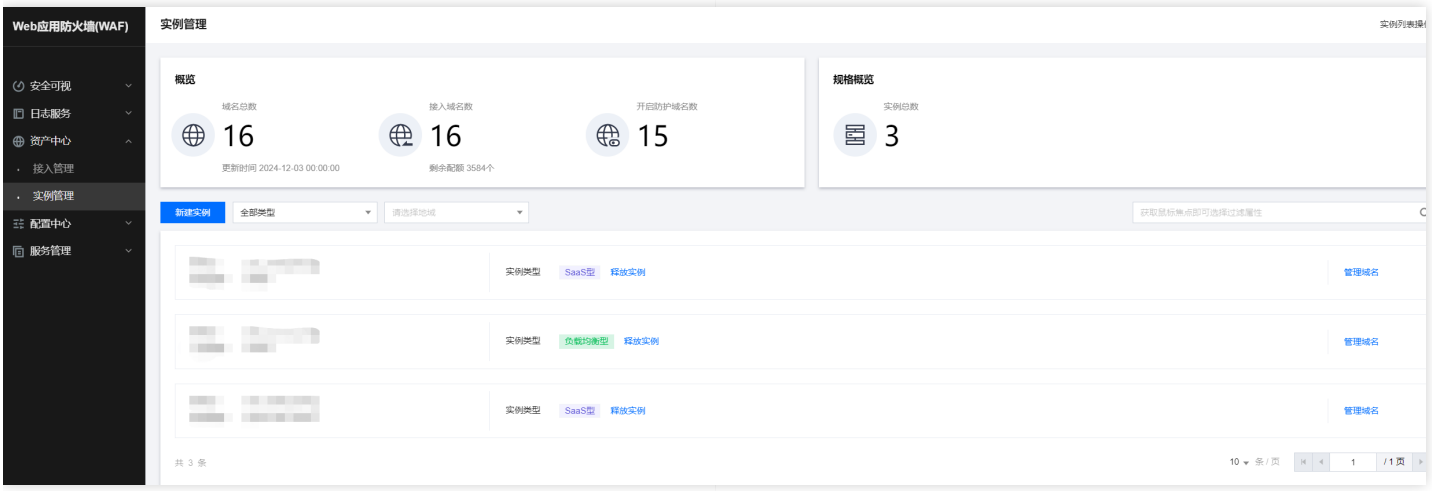
2.在购买页，实例类型选择“SaaS型”，实例名称填“cloud”，最后点击“立即购买”；



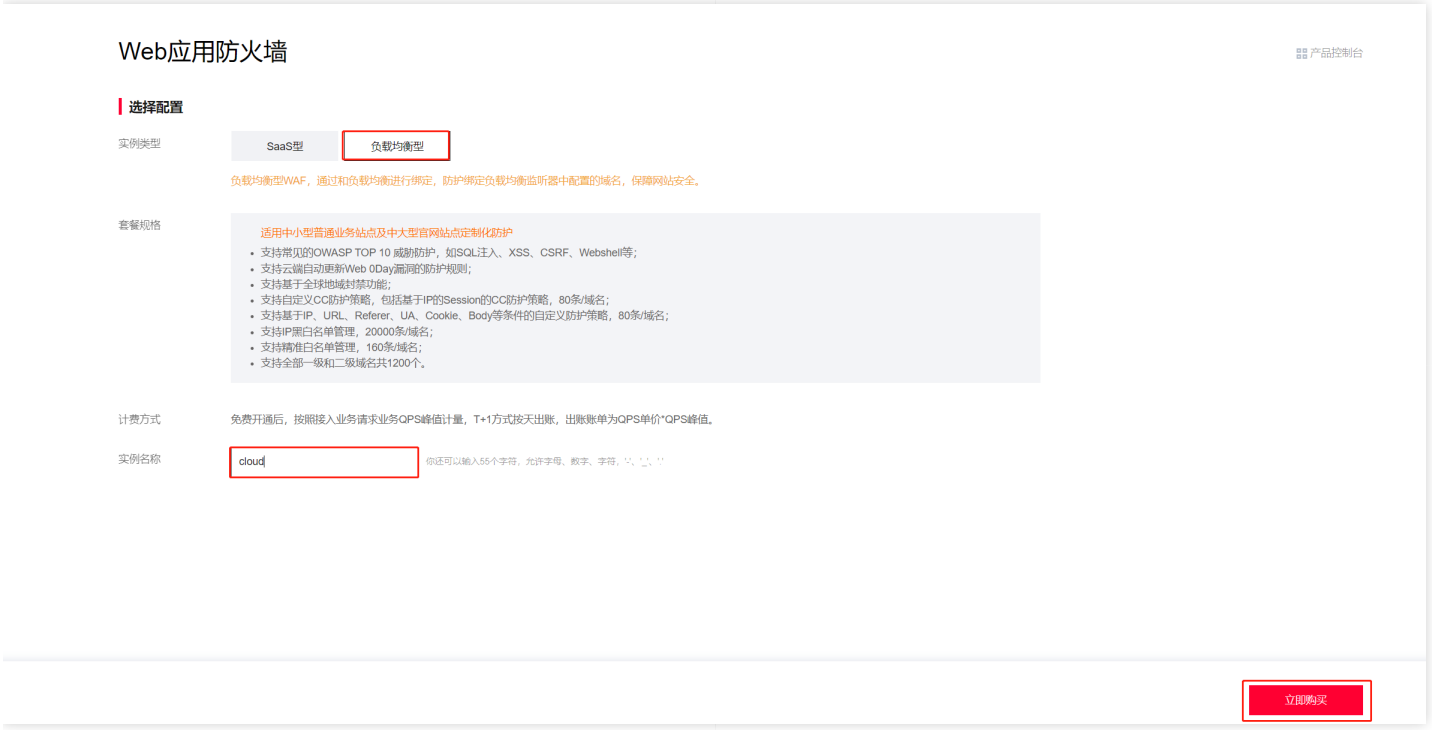


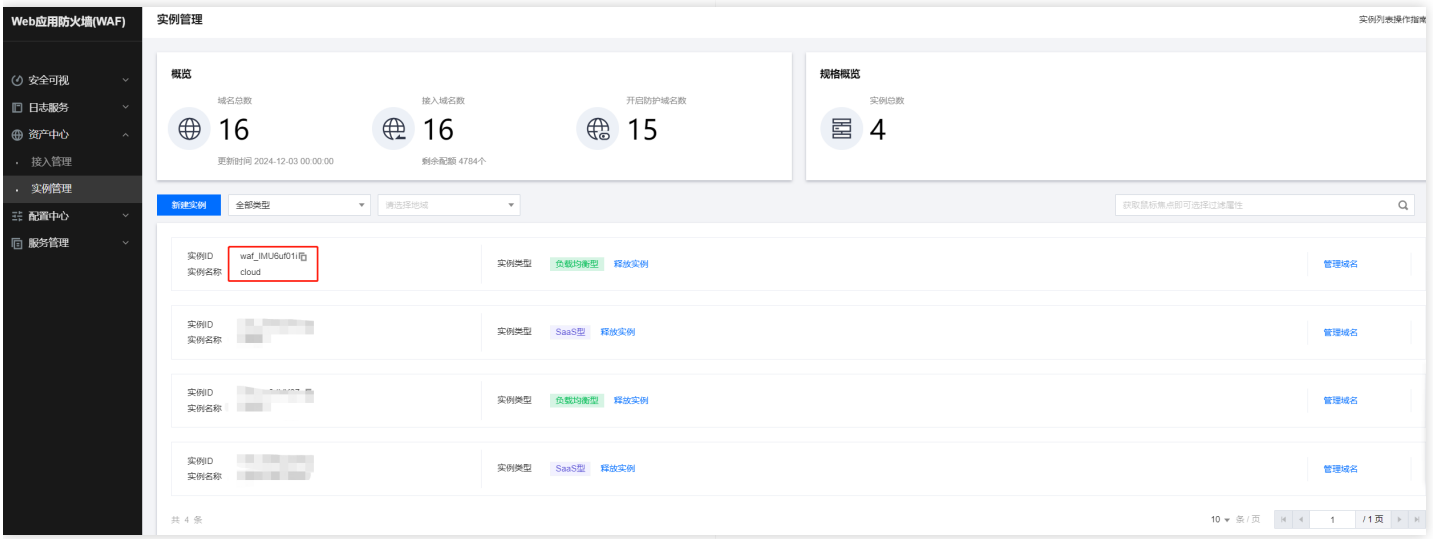
创建负载均衡型实例

1.登录租户端WAF-资产中心-实例管理页面，点击新建实例；



2.在购买页，实例类型选择“负载均衡型实例”，实例名称填“cloud”，最后点击“立即购买”；

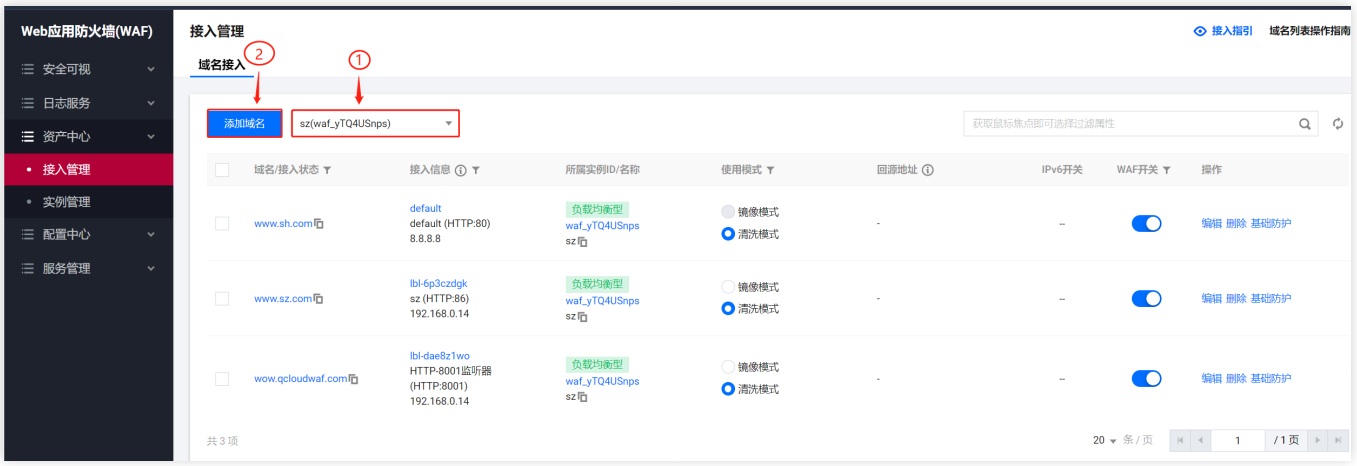



Web应用防火墙(WAF)
实例管理
实例列表操作指南
安全可视
日志服务
资产中心
接入管理
实例管理
配置中心
服务管理
概览
域名总数
16
更新时间 2024-12-03 00:00:00
接入域名数
16
剩余配额 4784个
开启防护域名数
15
规格概览
实例总数
4
新建实例
全部类型
请选择地域
获取鼠标焦点即可选择过滤属性
实例ID
实例名称
waf_IMU6uf01i
cloud
实例类型
负载均衡型
释放实例
管理域名
实例ID
实例名称
实例类型
SaaS型
释放实例
管理域名
实例ID
实例名称
实例类型
负载均衡型
释放实例
管理域名
实例ID
实例名称
实例类型
SaaS型
释放实例
管理域名
共 4 条
10 条 / 页
1
/ 1 页

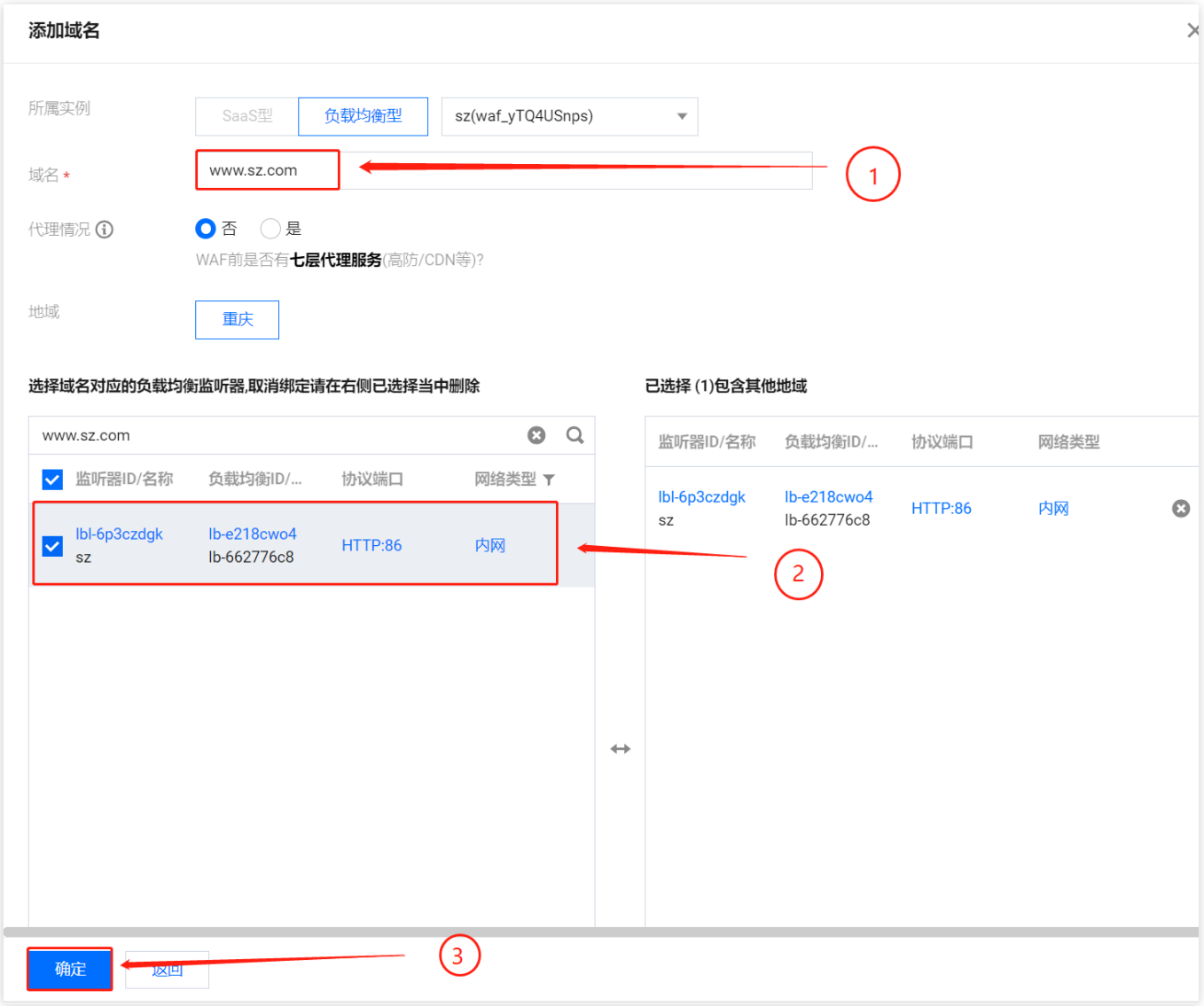
场景2：添加clb-waf型防护域名

如下操作是以“www.sz.com”为例，“www.sz.com”域名绑定在该租户的CLB中。

1. 登录租户端WAF-资产中心-接入管理页面，先选择实例，然后点击添加域名。



2. 进入添加域名界面，先输入域名，勾选域名对应的负载均衡监听器，最后点击确定。





3. 进入接入管理界面，核实域名防护状态。

- 检查域名/接入状态，确认添加的域名为预期域名；
- 检查接入信息中的ip为clb实例中的vip；
- 检查所属实例ID/名称为预期创建的实例ID；
- 检查使用模式为清洗模式：清洗模式可检测流量、可拦截恶意流量，镜像模式不能拦截流量、可检测流量；
- 检查WAF开关为蓝色开启状态。


添加域名
请选择实例
获取鼠标焦点即可选择过滤属性
1
2
3
4
5
域名/接入状态
接入信息
所属实例ID/名称
使用模式
回源地址
IPv6开关
WAF开关
操作
www.sz.com
lbl-6p3czdgk
sz (HTTP:86)
192.168.0.14
负载均衡型
waf_yTQ4USnps
sz
镜像模式
清洗模式
-
--
编辑 删除 基础防护

场景3：添加saas-waf型防护域名

如下操作是以“www.cloud.com”为例。

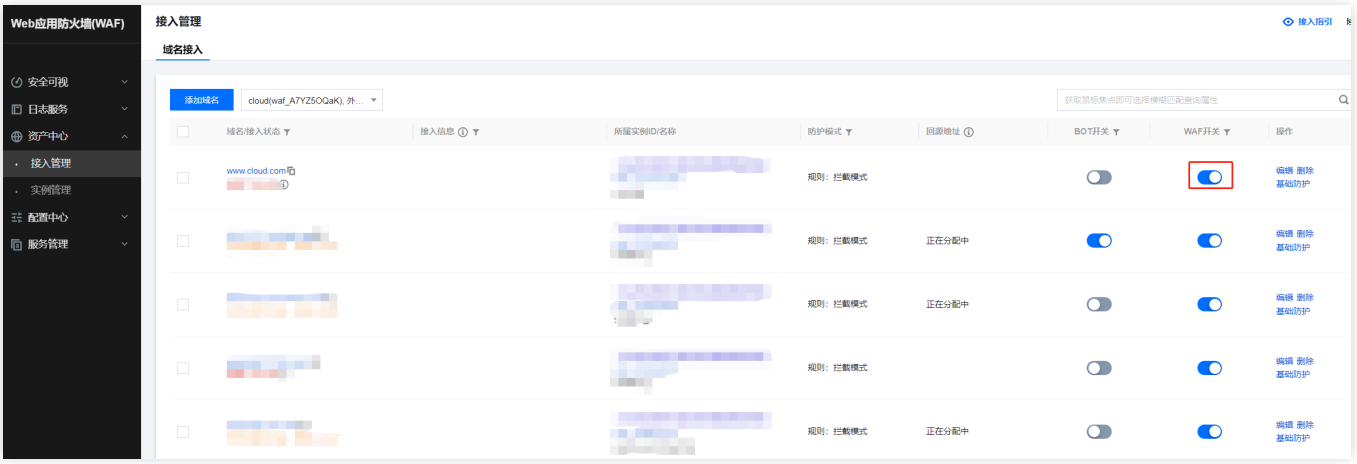
1. 在租户端WAF-资产中心-接入管理页面，选择"cloud"实例，点击“添加域名”按钮；



2. 在添加域名界面，选择Saas型，确认实例为预期的实例，填写实例域名，选择实际的站点端口，写入实际的源站地址，最后点击“确定”按钮；



3. 域名接入成功后，在租户端WAF-资产中心-接入管理页面，检查域名接入状态正常，检查WAF开关正常开启。


Web应用防火墙(WAF)
接入管理
域名接入
接入指引
安全可视
日志服务
资产中心
接入管理
实例管理
配置中心
服务管理
添加域名
域名/接入状态
接入信息
所属实例ID/名称
防护模式
回源地址
BOT开关
WAF开关
操作
www.cloud.com
规则：拦截模式
正在分配中
编辑 删除
基础防护

场景4：删除防护域名

如下操作是以“www.sz.com”为例

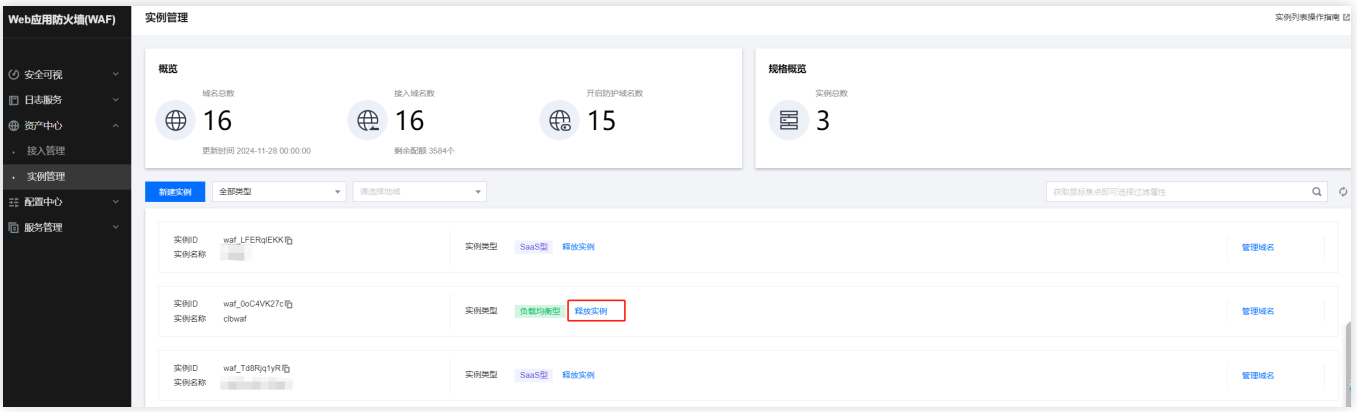
1. 登录租户端WAF-资产中心-接入管理，找到对应域名，删除对应域名。



场景5：删除实例

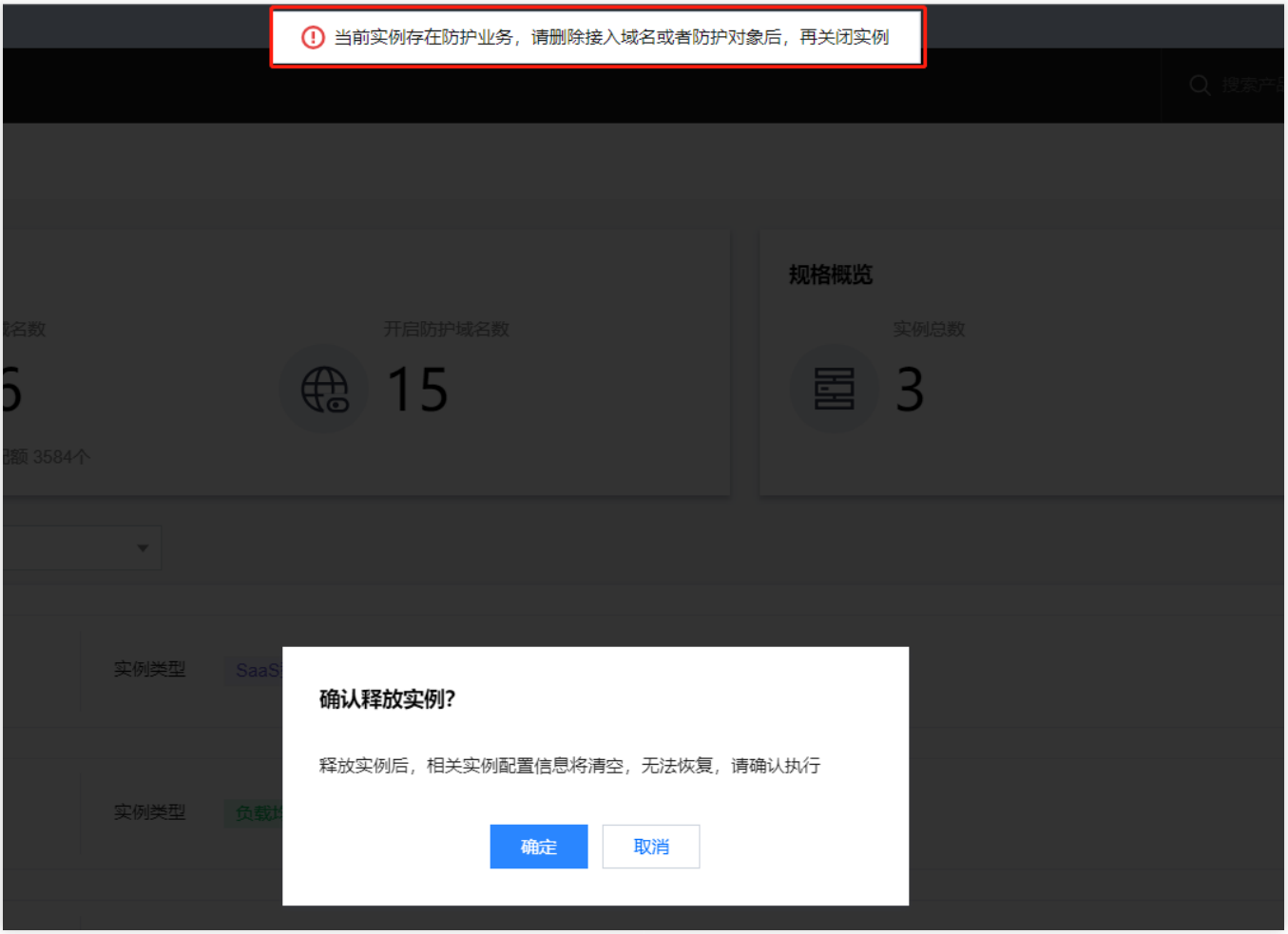
如下操作是以“clbwaf”为例，前提条件是实例内无域名：

1. 登录租户端WAF-资产中心-实例管理，找到对应实例，点击释放实例按钮，然后点击确定。



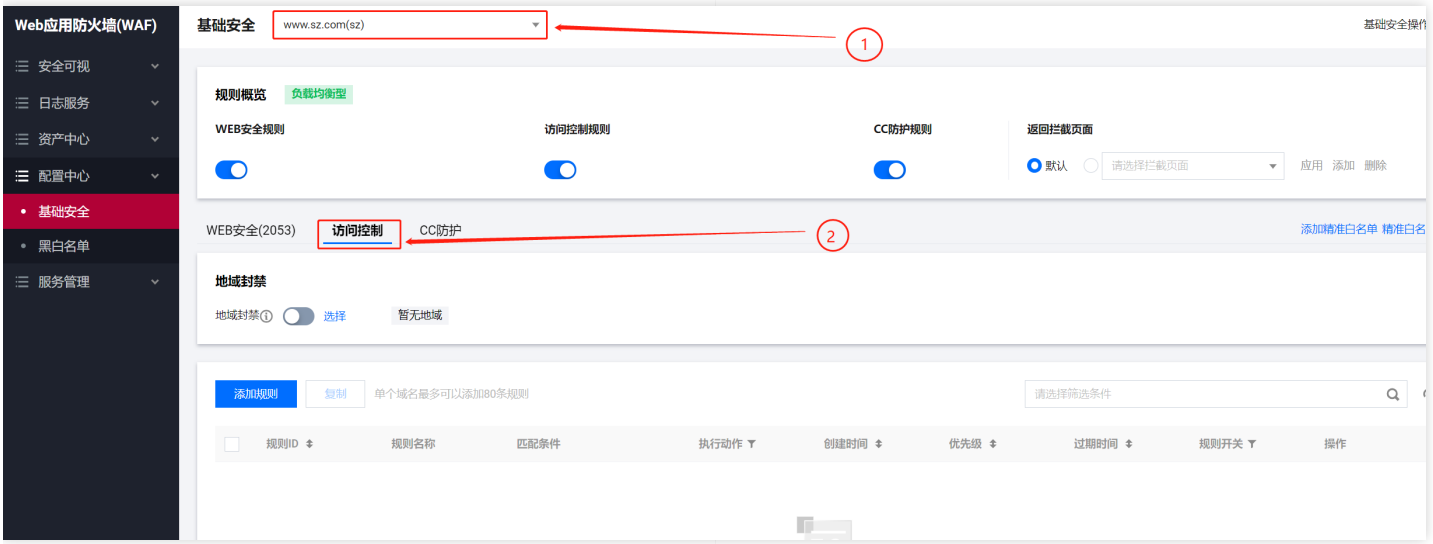


2. 如果实例中存在域名，则会释放实例失败。

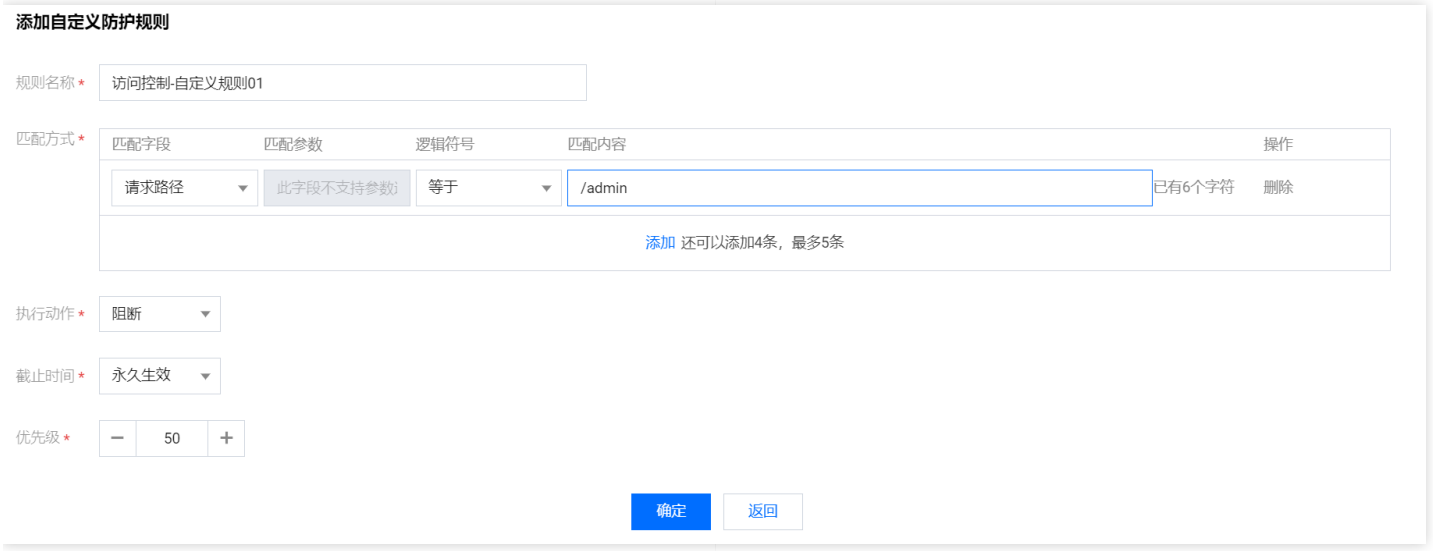

当前实例存在防护业务，请删除接入域名或者防护对象后，再关闭实例
规格概览
开启防护域名数
15
实例总数
3
实例类型
实例类型
确认释放实例?
释放实例后，相关实例配置信息将清空，无法恢复，请确认执行
确定
取消

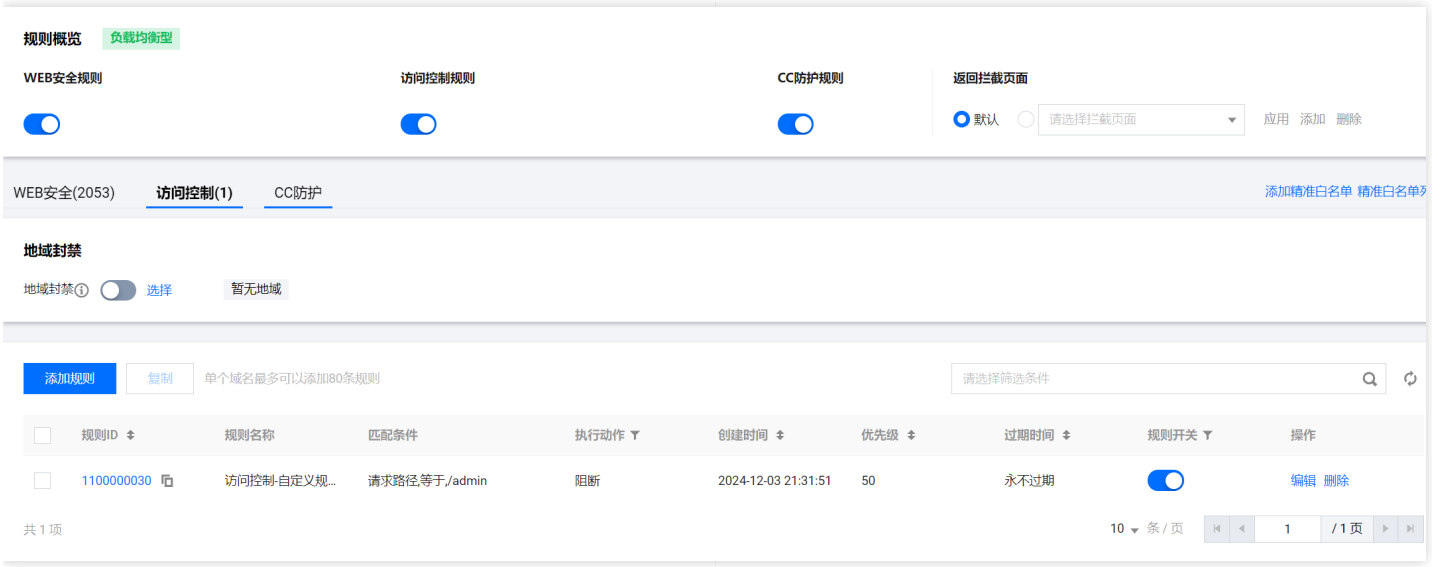
场景6：添加自定义规则

1.登录租户端WAF控制台-基础安全界面，选择需要的域名，点击“访问控制”。



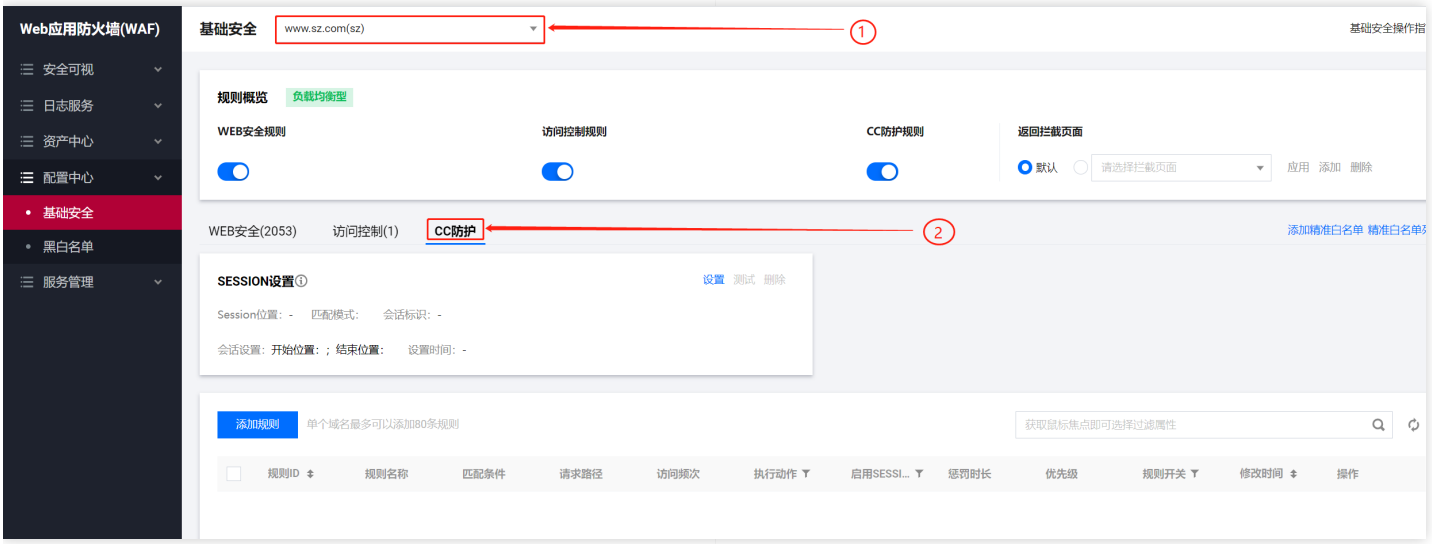
2.点击添加规则，添加一条自定义策略，匹配字段为‘请求路径’，逻辑符号选择‘包含’匹配内容为‘/admin’,执行阻断操作,最后点击确定。



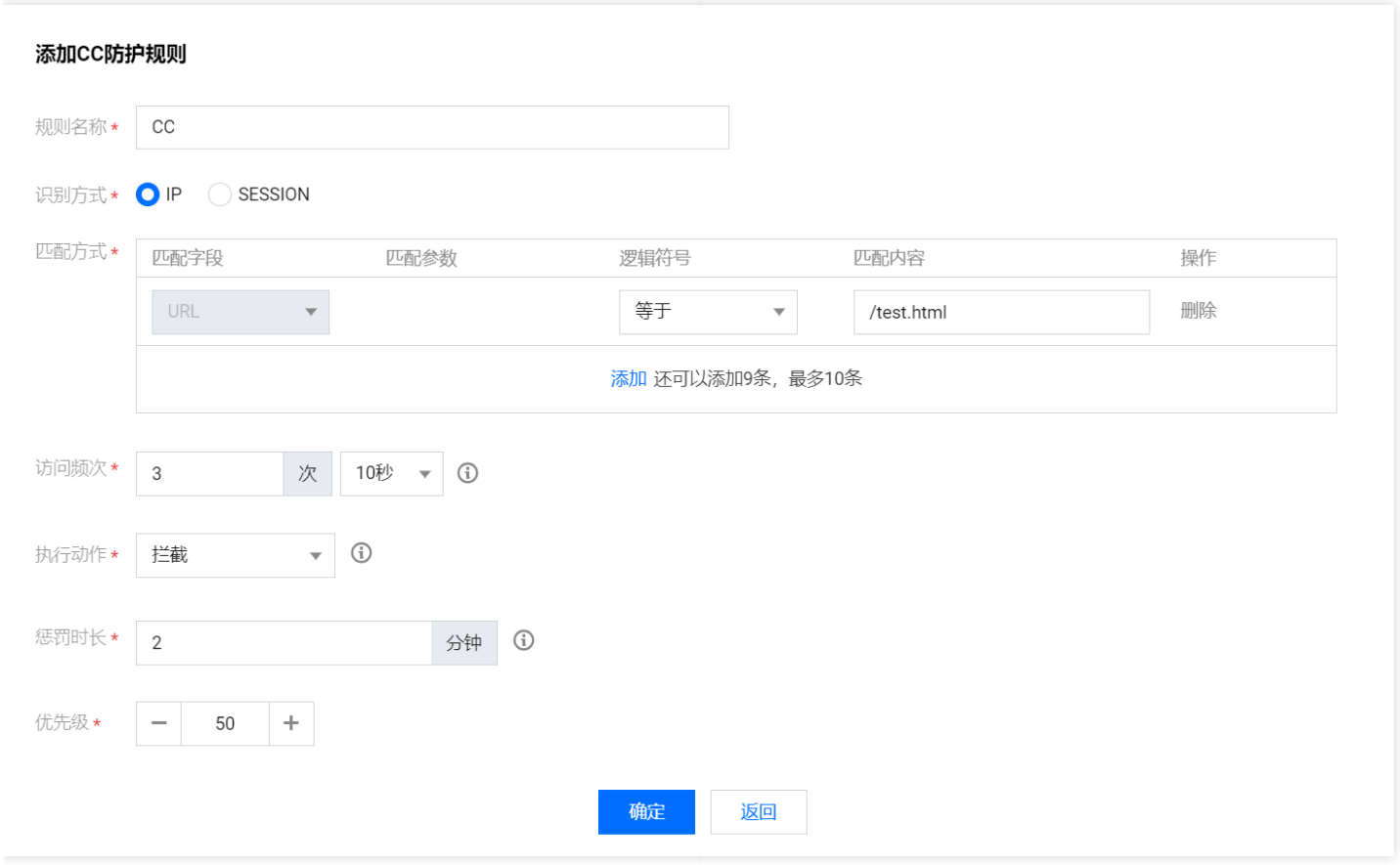

规则概览
负载均衡型
WEB安全规则
访问控制规则
CC防护规则
返回拦截页面
默认
请选择拦截页面
应用 添加 删除
WEB安全(2053)
访问控制(1)
CC防护
添加精准白名单 精准白名单列
地域封禁
地域封禁
选择
暂无地域
添加规则
复制
单个域名最多可以添加80条规则
请选择筛选条件
规则ID
规则名称
匹配条件
执行动作
创建时间
优先级
过期时间
规则开关
操作
1100000030
访问控制-自定义规...
请求路径等于/admin
阻断
2024-12-03 21:31:51
50
永不过期
编辑 删除
共 1 项
10 条 / 页
1
/ 1 页

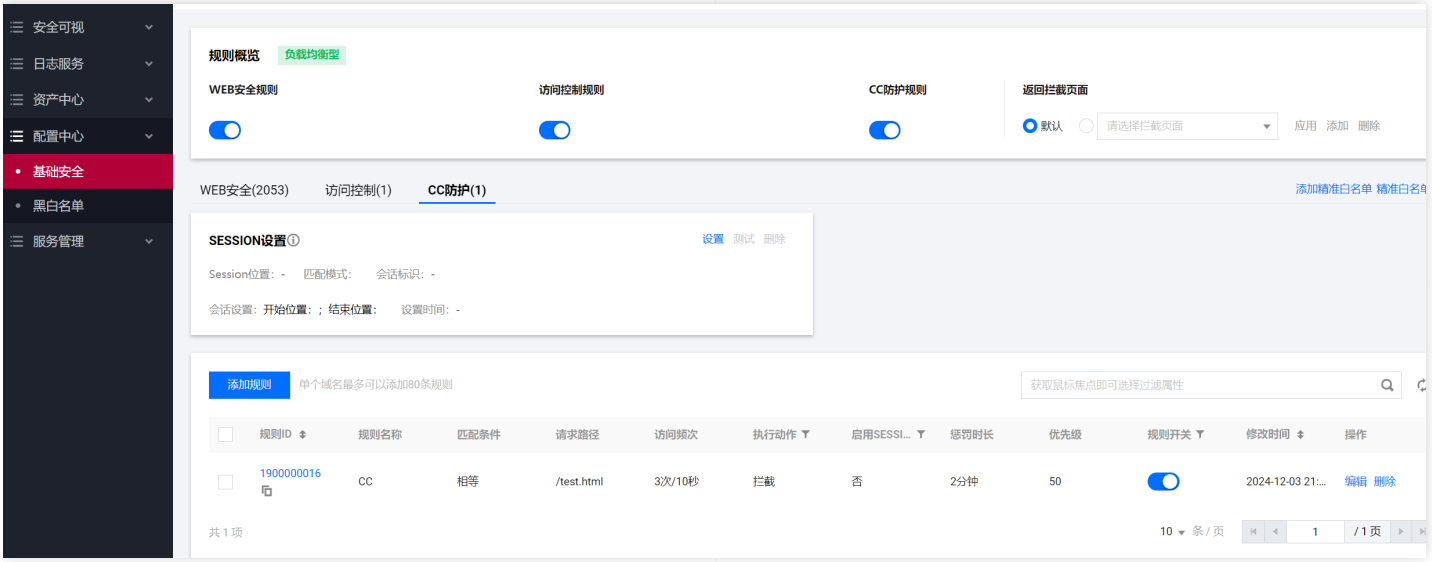
场景7：添加CC防护规则

1.登录租户端WAF控制台-基础安全界面，选择需要的域名，点击“CC防护”。



2.点击添加规则，添加一条CC防护设置，输入规则名称，URL输入为‘/test.html’,访问频次为3次/10秒，执行‘拦截’动作，惩罚时间设为2分钟,最后点击确定。




安全可视
日志服务
资产中心
配置中心
基础安全
黑白名单
服务管理
规则概览
负载均衡型
WEB安全规则
访问控制规则
CC防护规则
返回拦截页面
默认
请选择拦截页面
应用 添加 删除
WEB安全(2053)
访问控制(1)
CC防护(1)
添加精准白名单 精准白名单
SESSION设置
设置 测试 删除
Session位置：- 匹配模式： 会话标识：-
会话设置：开始位置：；结束位置： 设置时间：-
添加规则
单个域名最多可以添加80条规则
获取鼠标焦点即可选择过滤属性
规则ID
规则名称
匹配条件
请求路径
访问频次
执行动作
启用SESSI...
惩罚时长
优先级
规则开关
修改时间
操作
1900000016
CC
相等
/test.html
3次/10秒
拦截
否
2分钟
50
2024-12-03 21:...
编辑 删除
共 1 项
10 条 / 页
1
/ 1 页

场景8：检查域名是否处于被防护状态

租户端域名是否开启防护的巡检方案

操作人：租户端运维人员

步骤一：查看WAF配置防护的域名数量和具体域名

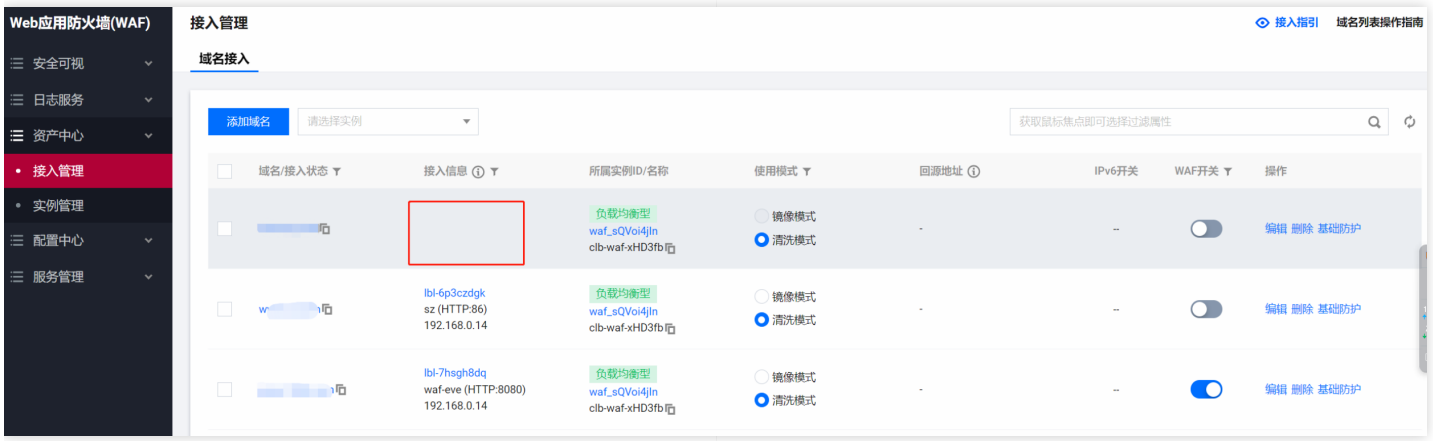
登录租户端WAF-资产中心-接入管理界面，查看WAF防护域名的数量和具体域名。



步骤二：查看域名防护状态，如下4种场景域名防护状态为关闭状态

监听器为空白或者“defalut”

登录租户端WAF-资产中心-接入管理界面查看域名接入信息，如果接入信息为空白或者default,即域名防护不正常；





域名防护开关为“关闭”

登录租户端WAF-资产中心-接入管理界面查看WAF开关，如果WAF开关为“灰色”，则流量不会转给WAF，既域名防护不生效；

备注：WAF开关 开启为 “蓝色”；WAF开关关闭为“灰色”。



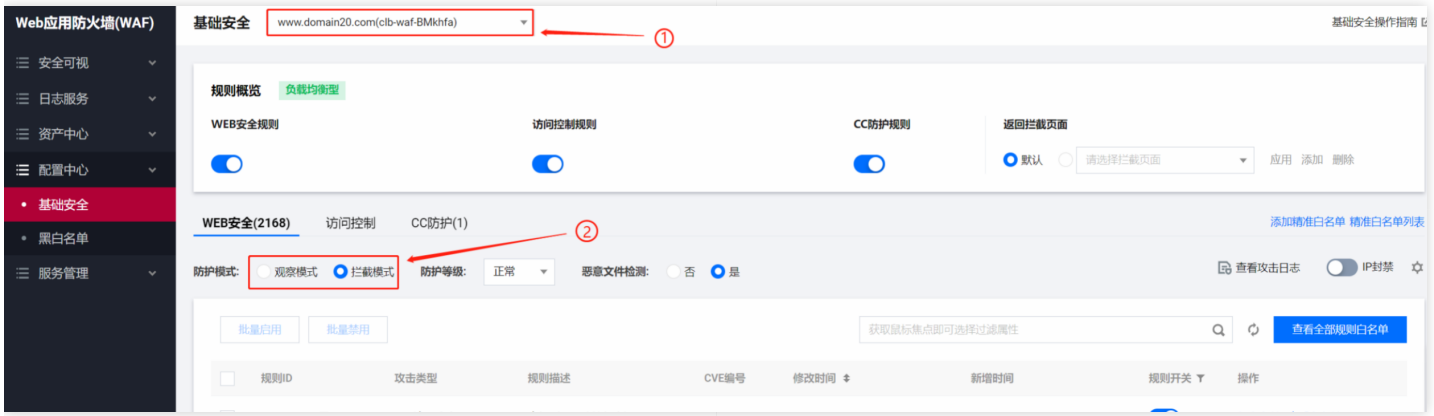
域名流量模式为“镜像模式”

登录租户端WAF-资产中心-接入管理界面查看域名使用模式，如果是镜像模式，只记录攻击日志不拦截，即域名防护拦截不生效；



域名规则模式为“观察模式”

登录租户端WAF-配置中心-基础安全界面，选择域名，查看域名防护模式，如果是观察模式，则域名规则拦截功能不生效。



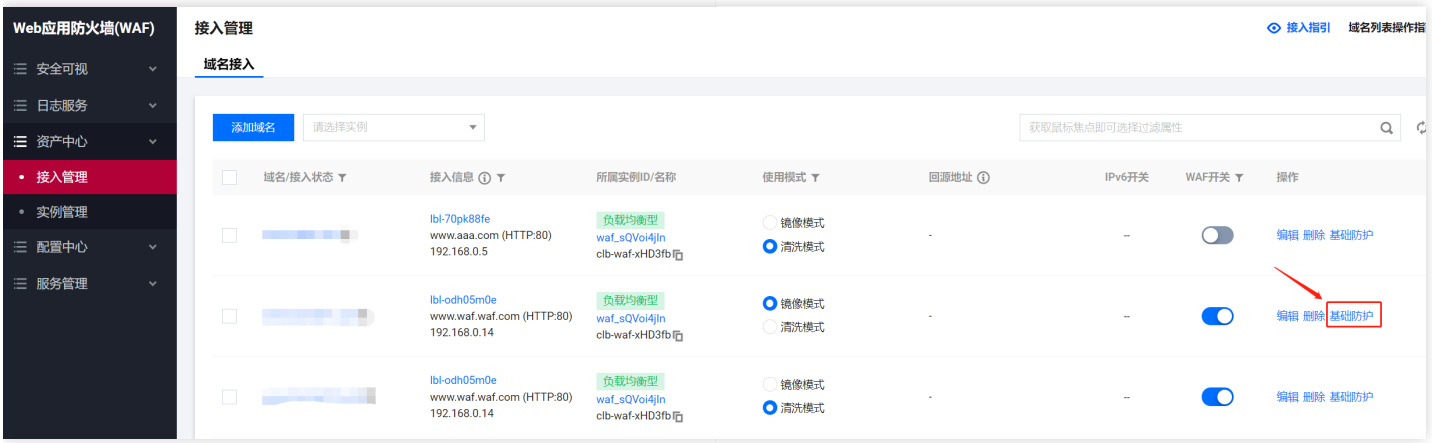
场景9：应急预案

防护域名出现误拦截客户业务应急预案

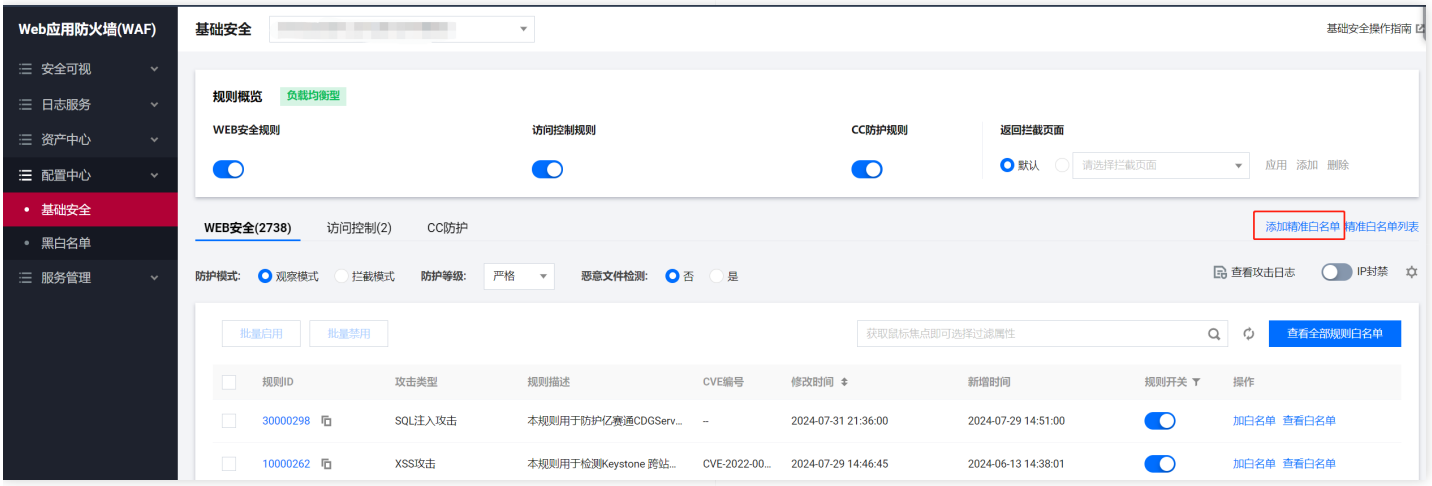
防护域名接入waf后，部分url出现正常访问被拦截情况，按照业务的影响面评估，推荐依次使用手段三 -> 手段二 -> 手段一。

应急手段一：添加白名单(特定白名单放行，其他访问命中规则则拦截)

在控制台页面上添加放行的规则；



选择 "精准白名单"



根据告警的路径配置规则；



如果上述配置后不符合预期，则执行手段二；

应急手段二：将流量模式改为镜像模式(只告警不拦截)

在控制台页面上将waf工作模式改为镜像模式。
点击-接入管理-配置镜像模式；



如果配置后仍然不符合预期，执行手段三。

应急手段三：关闭域名的防护能力(不告警也不拦截)

在控制台页面上关闭waf开关,此时整个域名不拦截任何攻击；


Web应用防火墙(WAF)
安全可视
日志服务
资产中心
接入管理
实例管理
配置中心
服务管理
接入管理
接入指引
域名列表操作指南
域名接入
添加域名
请选择实例
获取鼠标焦点即可选择过滤属性
域名/接入状态
接入信息
所属实例ID/名称
使用模式
回源地址
IPv6开关
WAF开关
操作
www.domain1.com
lbl-odh05m0e
www.waf.waf.com (HTTP:80)
192.168.0.14
负载均衡型
waf_sQVoi4jIn
clb-waf-xHD3fb
镜像模式
清洗模式
-
--
编辑 删除 基础防护
www.domain12.com
lbl-odh05m0e
www.waf.waf.com (HTTP:80)
192.168.0.14
负载均衡型
waf_sQVoi4jIn
clb-waf-xHD3fb
镜像模式
清洗模式
-
--
编辑 删除 基础防护
abc.testwaf.com
lbl-odh05m0e
www.waf.waf.com (HTTP:80)
192.168.0.14
负载均衡型
waf_sQVoi4jIn
clb-waf-xHD3fb
镜像模式
清洗模式
-
--
编辑 删除 基础防护

最佳实践
搭建负载均衡型WAF测试环境

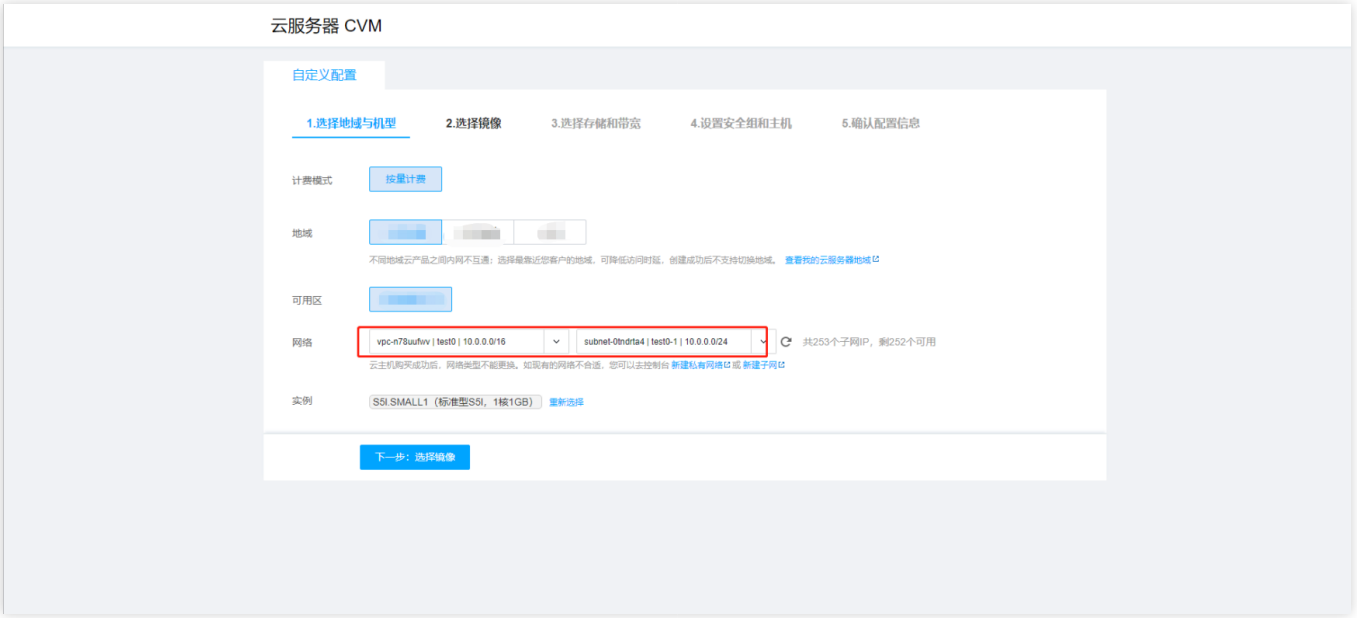
搭建负载均衡型WAF测试环境

创建 CVM

1. 登录租户端，进入到CVM页面，选择对应的地域，点击【新建】；



2. 所选网络需要与CLB网络一致，其余选项按照实际情况选择，点击【下一步：选择镜像】；



3. 按照实际情况选择镜像后，点击【下一步：选择存储和带宽】；



4. 按照实际情况选择存储和带宽后，点击【下一步：设置安全组和主机】；



5. 按照实际情况选择安全组合主机后，输入主机密码，点击【下一步：确认配置信息】；





6. 查看到刚才所选的信息，确认无误后，点击【开通】；



申请弹性公网ip地址，绑定CVM

1. CVM菜单下，点击【弹性公网IP】，选择与CVM相同的地域后，点击【申请】，按照实际情况选择各项；



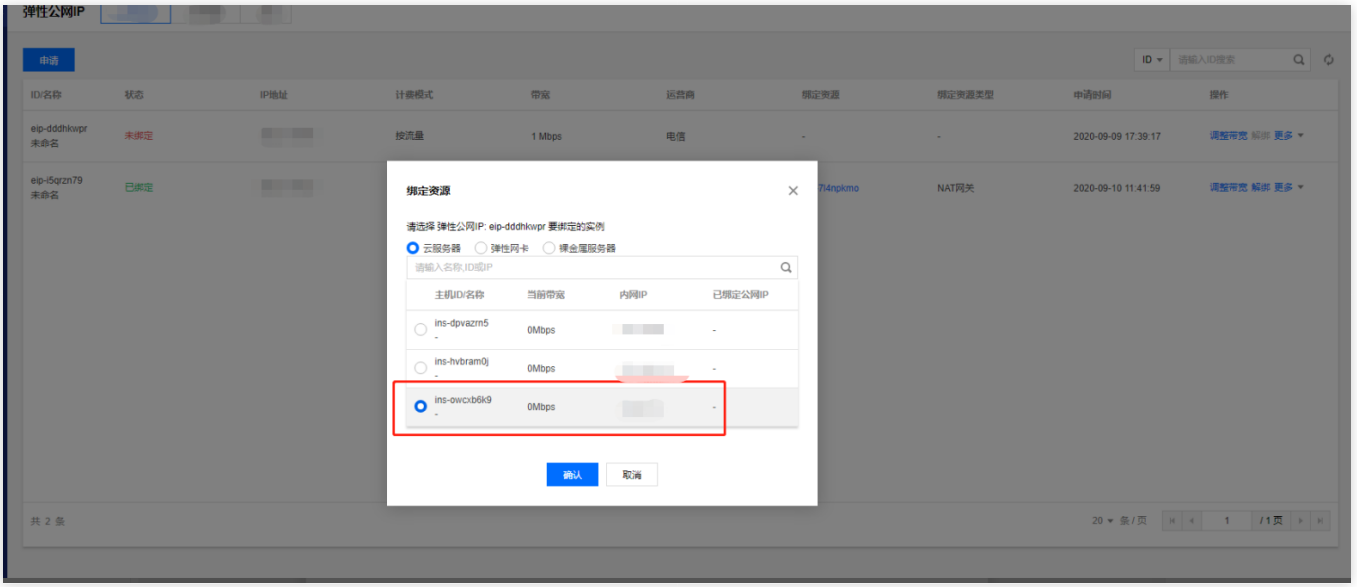
2. 点击【确认】，返回到弹性公网IP列表页面，可以查看到新建的弹性公网IP显示未绑定状态；



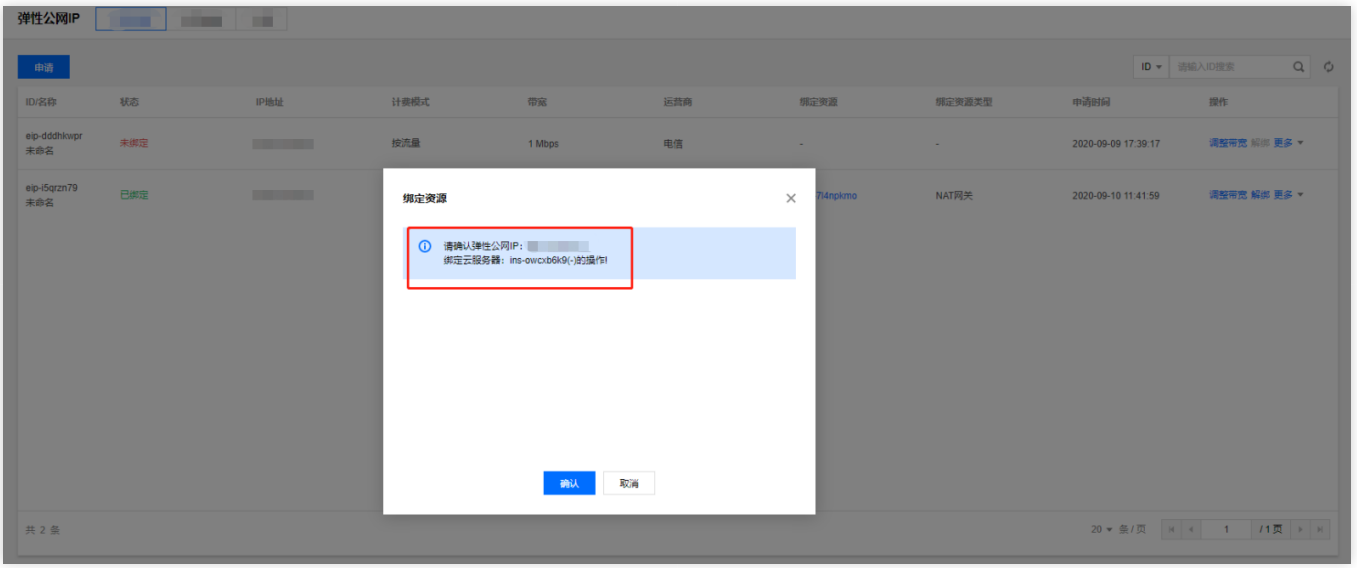
3. 点击弹性公网IP的“操作”栏，点击【更多】，选择【绑定】；



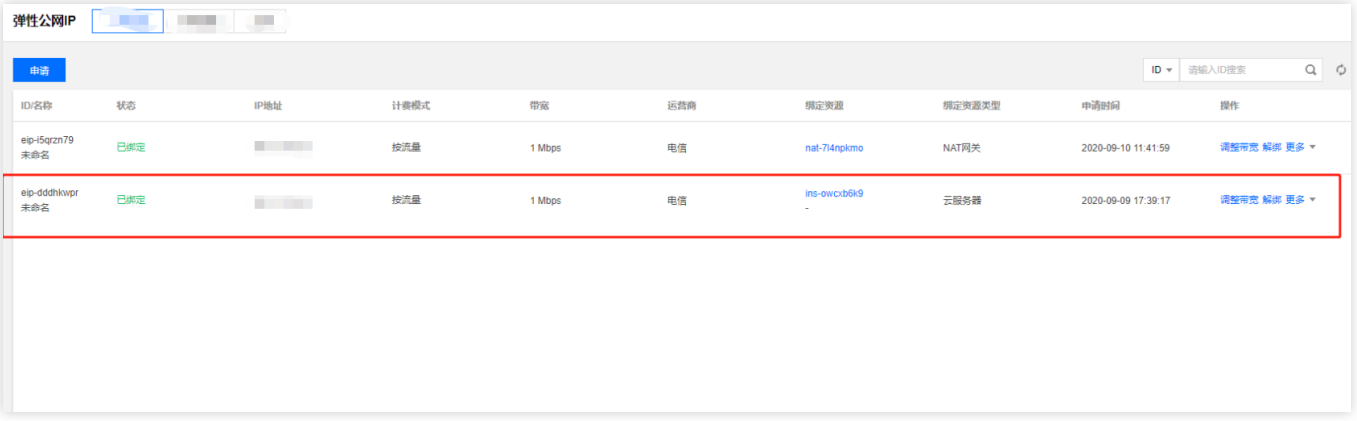
4. 选择要绑定的CVM，点击【确认】；



5. 查看需要确认的信息，确认无误后点击【确认】；

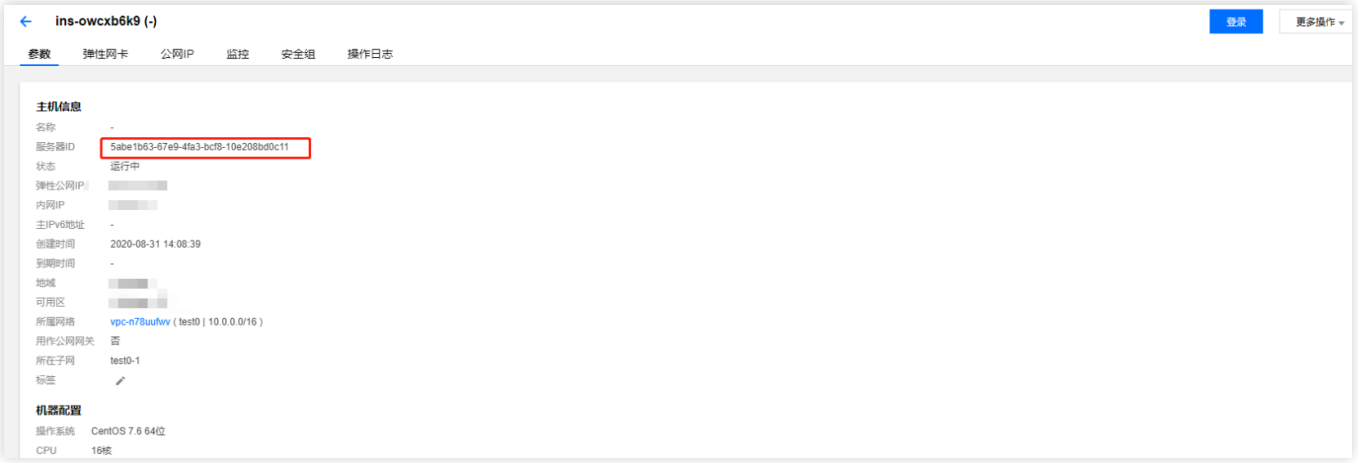


6. 返回到弹性公网IP列表页面，显示“已绑定”状态；

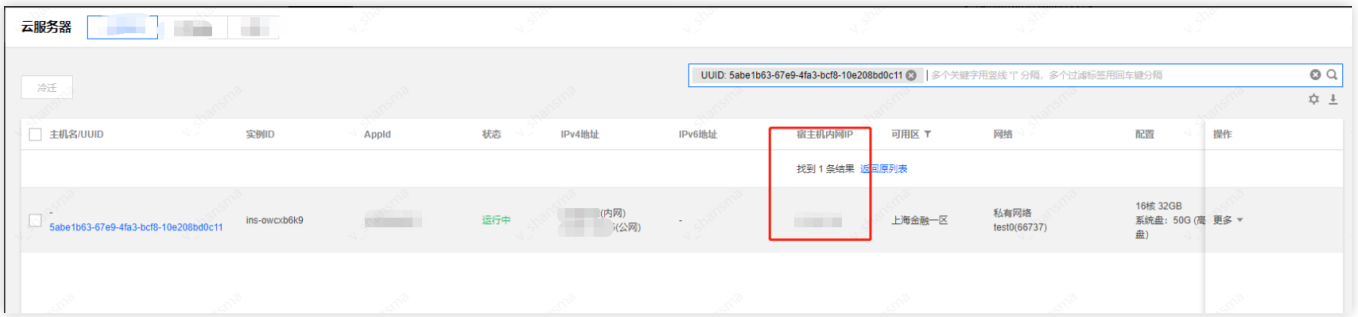


安装nginx，启用80端口

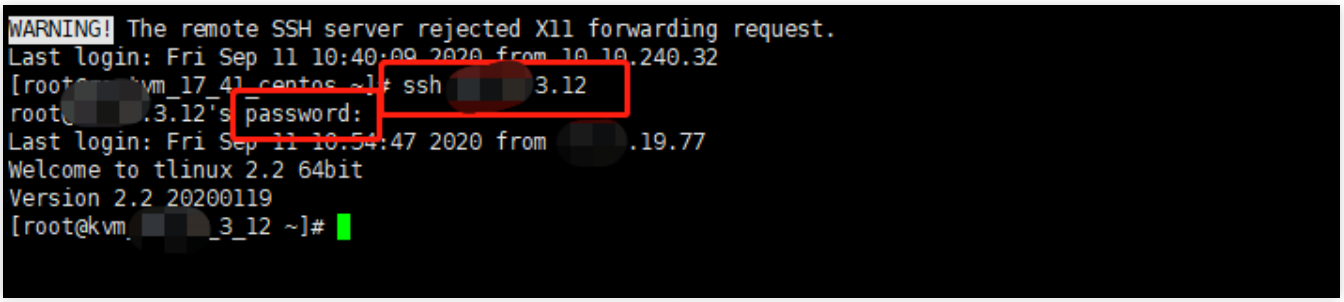
1. 点击CVM的ID，进入到CVM参数页面，复制CVM的服务器ID；



2. 在运营端中CVM-云主机（租户资源）下，搜索框中选择UUID，粘贴刚才复制的服务器ID，可以查询到宿主机内网IP；

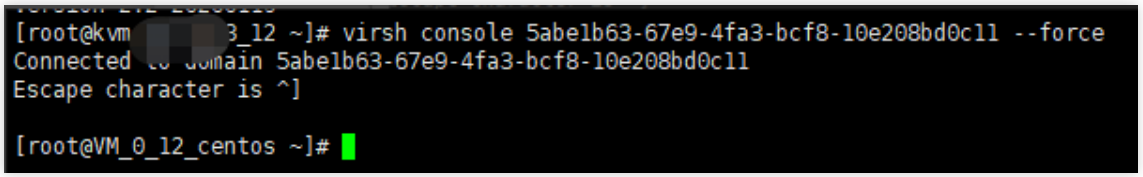


3. 登录到宿主机内网IP，输入命令：ssh 宿主机内网IP，密码为开通CVM时填入的密码；

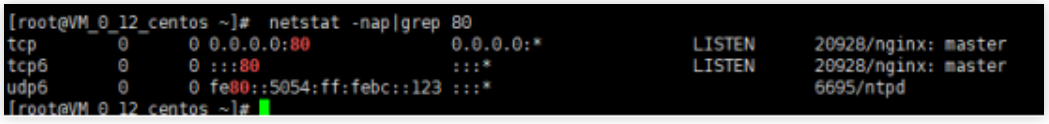




4. 输入命令 virsh console UUID --force ，如virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force，进入到CVM中；



5. 进入后输入以下命令进行安装；
   安装： yum install -y nginx
   启动Nginx服务： service nginx start
   查看80端口是否启用： netstat -nap|grep 80



由于有些客户公网ip地址禁止对外开放端口80和443，需要通过natgw把cvm的80端口转到其他端口，例如788，并在路由表中关联此网关（如不涉及此项请忽略）；

1. 私有网络菜单下选择NAT网关，选择对应的地域后，点击【新建】，新建NAT网关；



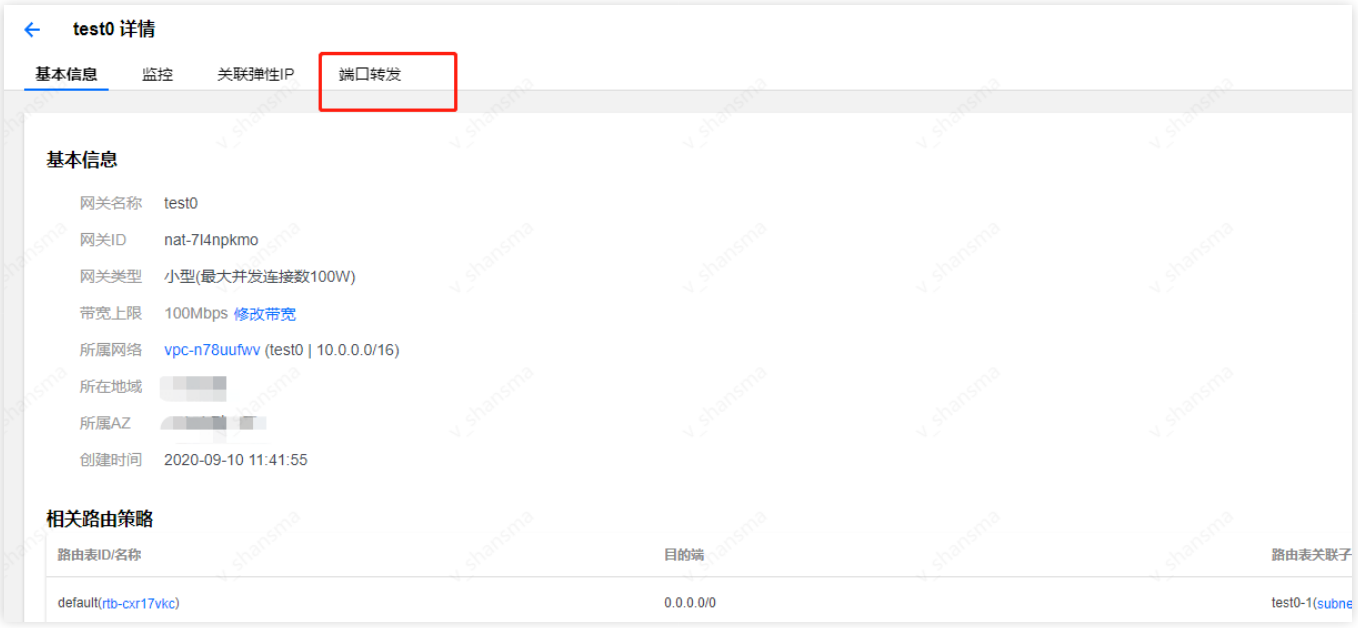
2. 按照实际情况输入各项，点击【创建】，返回到NAT网关列表页面；



3. 在新建的NAT网关中点击网关ID；



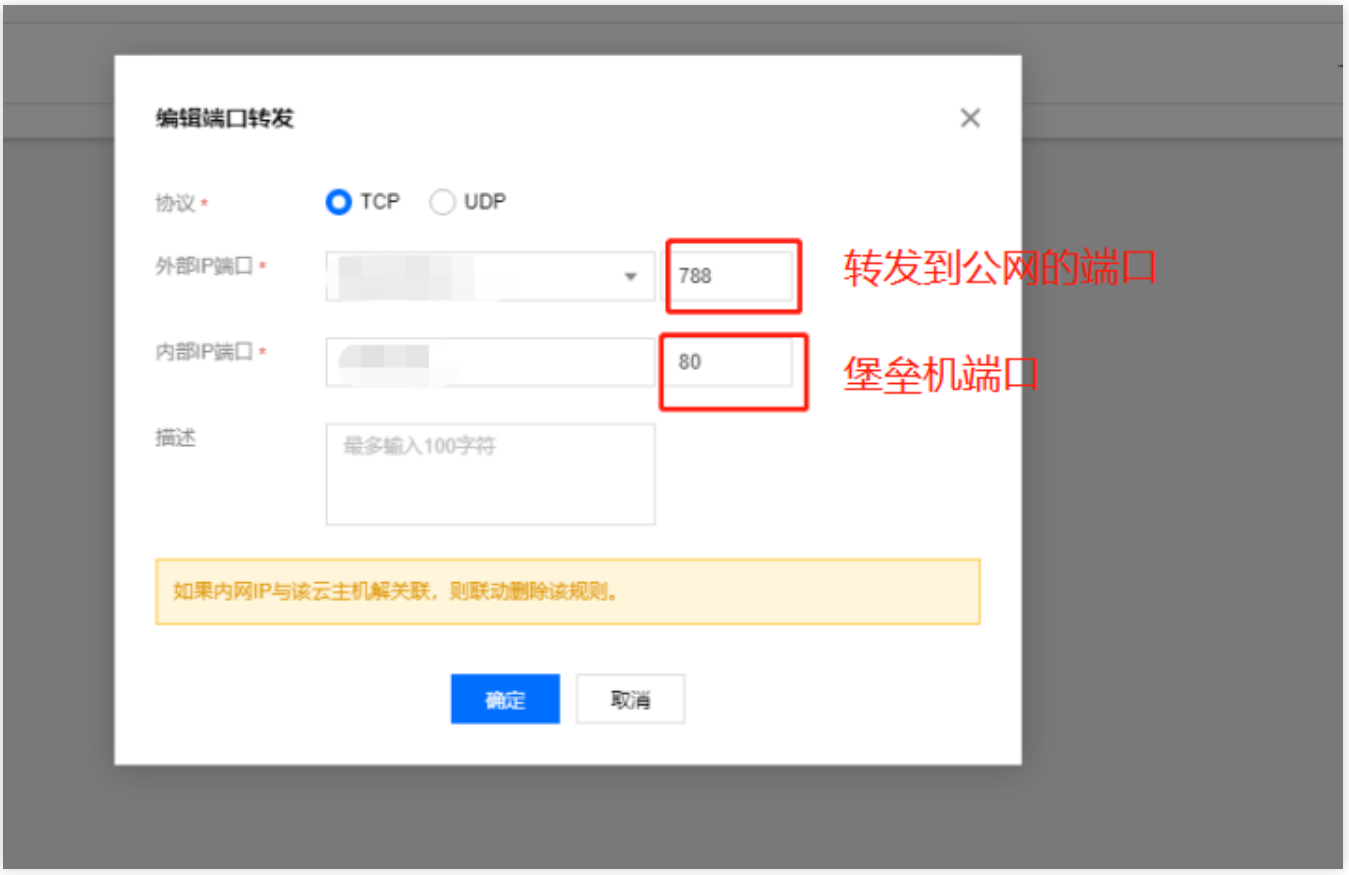
4. 点击端口转发；



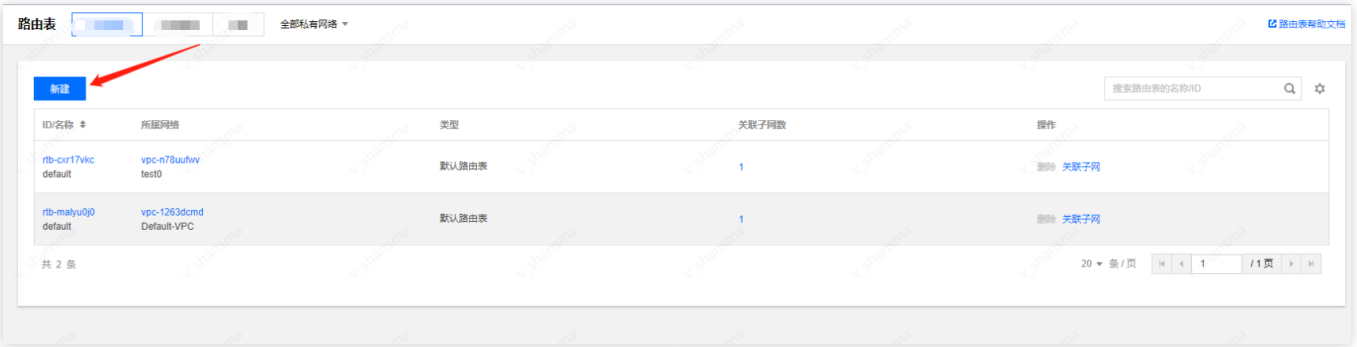
5. 点击【新建】；



6. 添加转发端口；



7. 在私有网络下，选择路由表，在相应的地域下，点击【新建】，新建路由表；

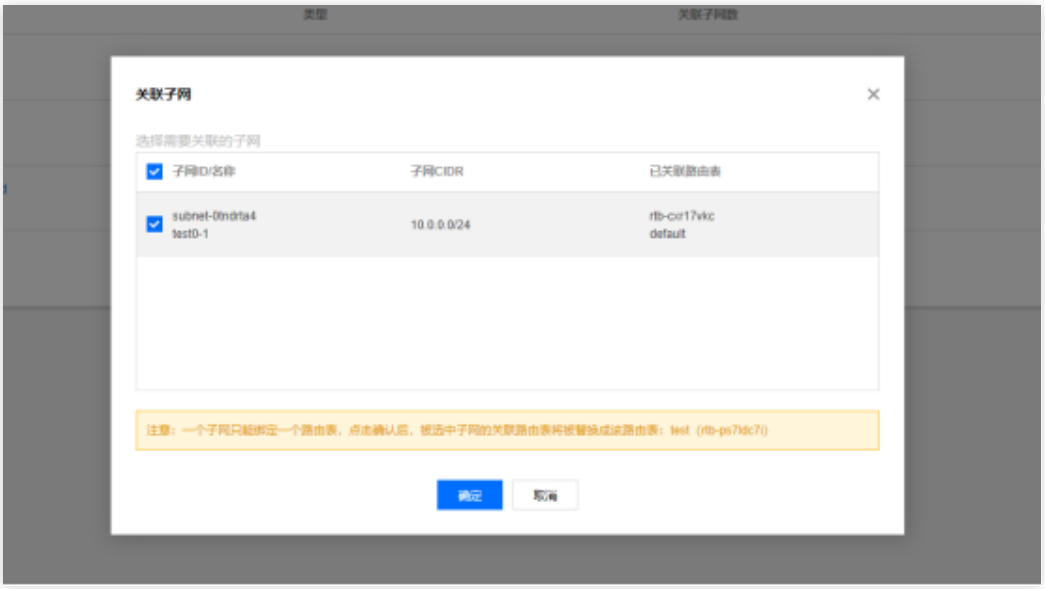




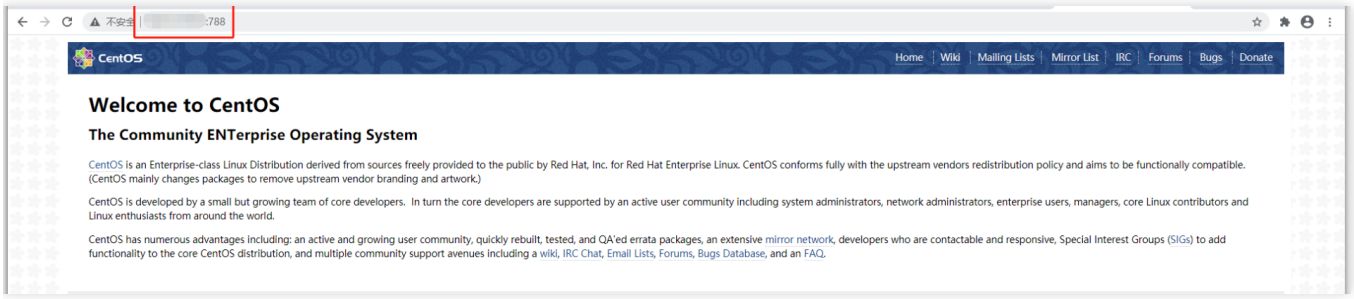
8. 输入各项后点击【创建】，策略选择已经添加的NAT网关；



9. 提示需要关联子网，选择关联的子网后，点击【确定】，返回到路由表列表页面；



访问http://公网ip:788/ 验证web网站是否正常

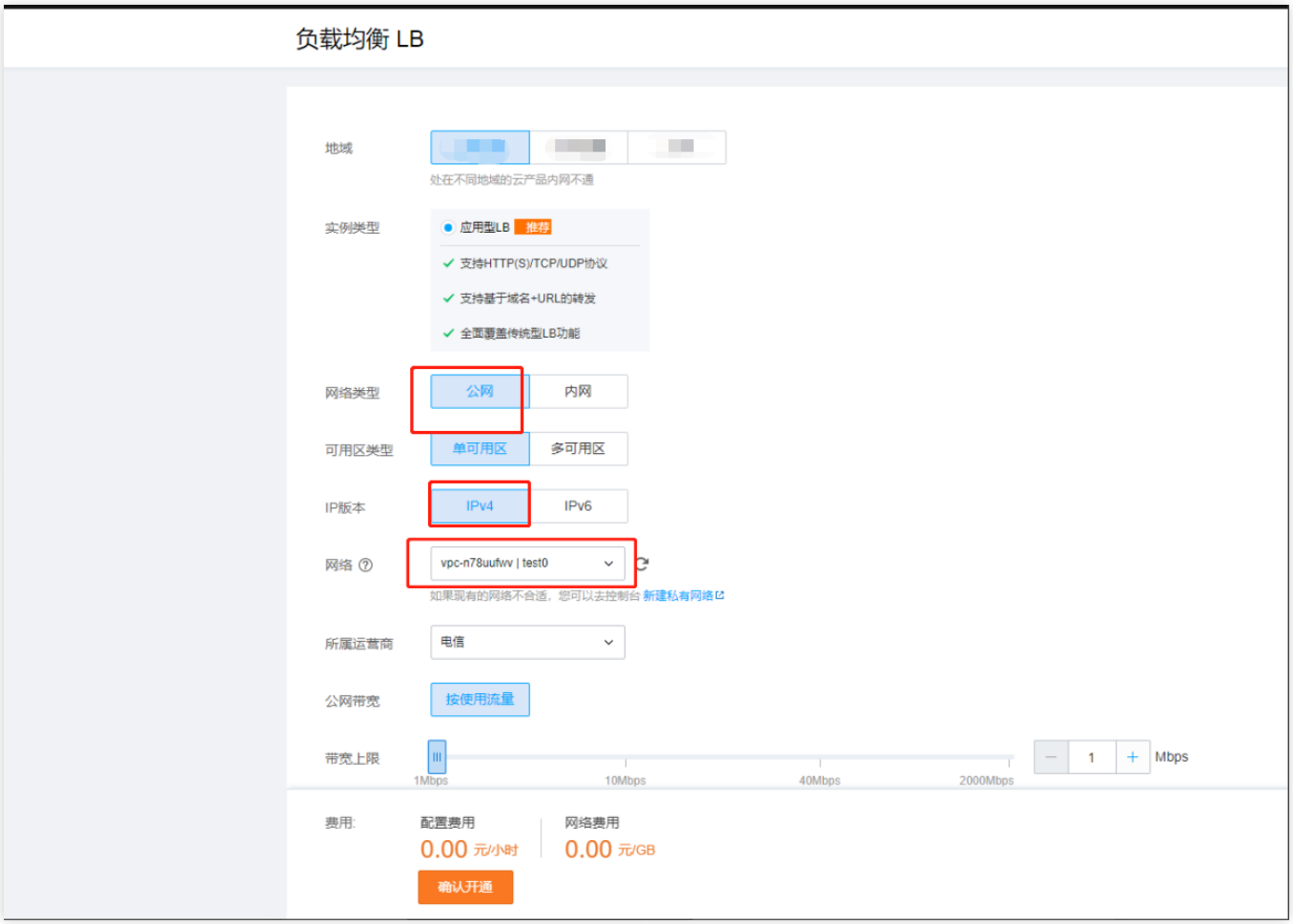


新增CLB实例及监听器；

1. 点击【负载均衡】，在LB实例列表页点击【新建】；



2. 按照实际情况输入各项，负载均衡需要与CVM网络一致。点击【确认开通】；



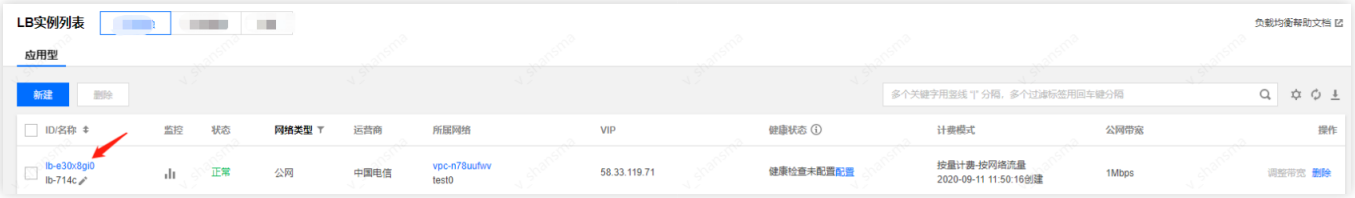
3. 在确认提示页点击【确认】；



4. 点击【完成】；



5. 在LB实例列表页可以查看到刚创建的实例，点击实例ID；



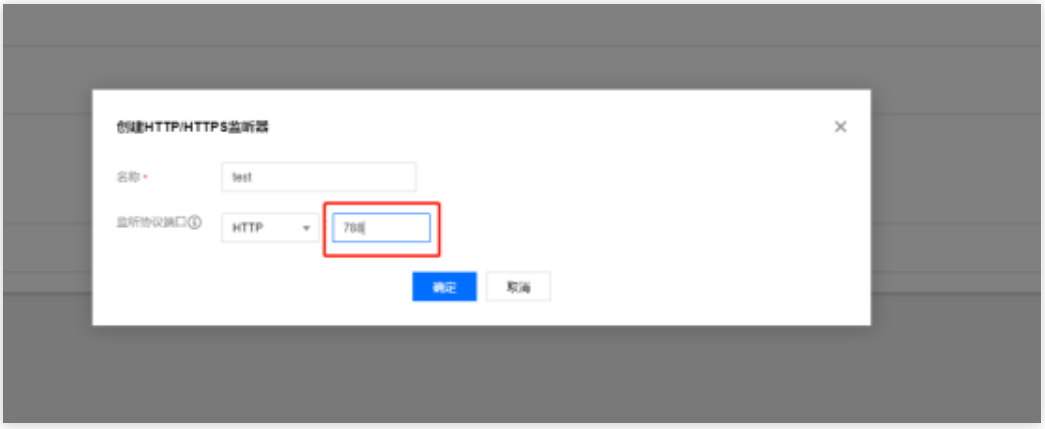
6. 点击监听器管理；



7. 点击【新建】或者【开始创建】，创建监听器；



8. 输入名称、协议和端口号，端口号输入NAT网关转发的端口号，如788，点击【确定】；



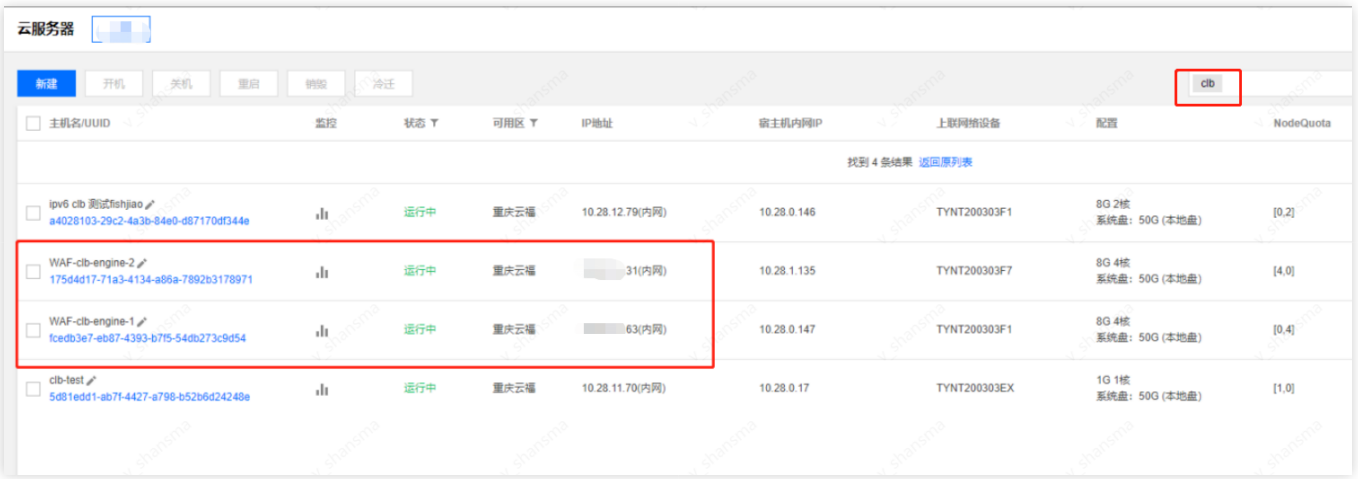
9. 点击监听器下的“开始创建”，输入要配置的域名，后续步骤参照“功能测试用例（负载均衡型）租户端”文档中“在负载均衡实例中绑定HTTP类型监听器”步骤操作即可；


lb-714c详情
基本信息
监听器管理
重定向配置
监控
温馨提示：当您配置了自定义重定向策略，原转发规则进行修改后，重定向策略会默认解除，需要重新配置。
HTTP/HTTPS监听器
新建
test(HTTP:788)
您还未创建转发规则，点击开始创建
监听器详情
名称 test
ID lbl-qgw9pkui
协议端口 HTTP:788
创建时间 2020-09-11 11:52:23
TCP/UDP监听器
新建
您还未创建监听器，点击开始创建

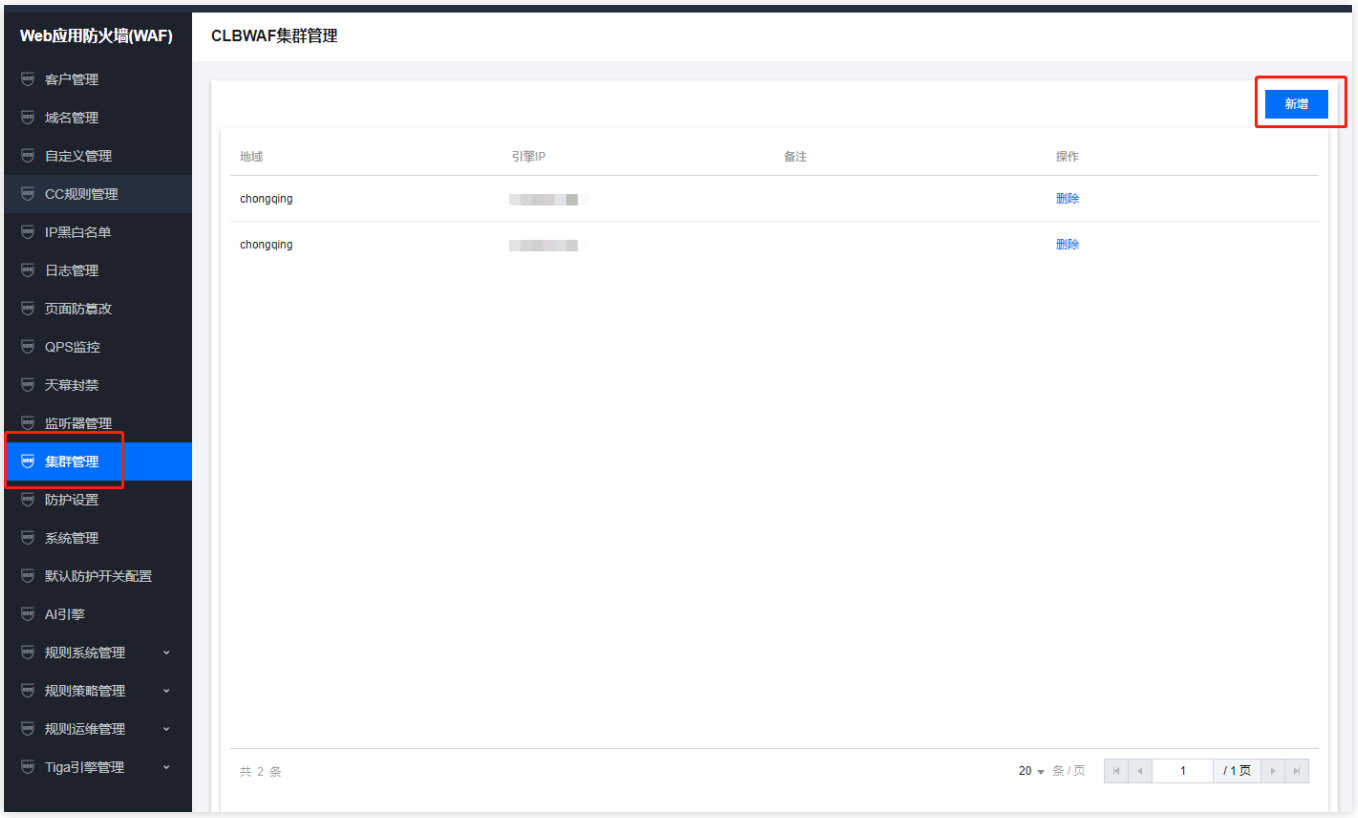

lb-714c详情
基本信息
监听器管理
重定向配置
监控
温馨提示：当您配置了自定义重定向策略，原转发规则进行修改后，重定向策略会默认解除，需要重新配置。
HTTP/HTTPS监听器
新建
test(HTTP:788)
您还未创建转发规则，点击开始创建
TCP/UDP监听器
新建
您还未创建监听器，点击开始创建
创建HTTP/HTTPS转发规则
1 基本配置
2 健康检查
3 会话保持
域名
URL路径
均衡方式
按权重轮询
当后端CVM的权重都设置为同一个值时，权重属性将不生效，将按照简单的轮询策略分发请求
获取客户端IP 已启用
Gzip压缩 已启用
下一步：健康检查
取消

添加负载均衡型WAF的引擎节点：

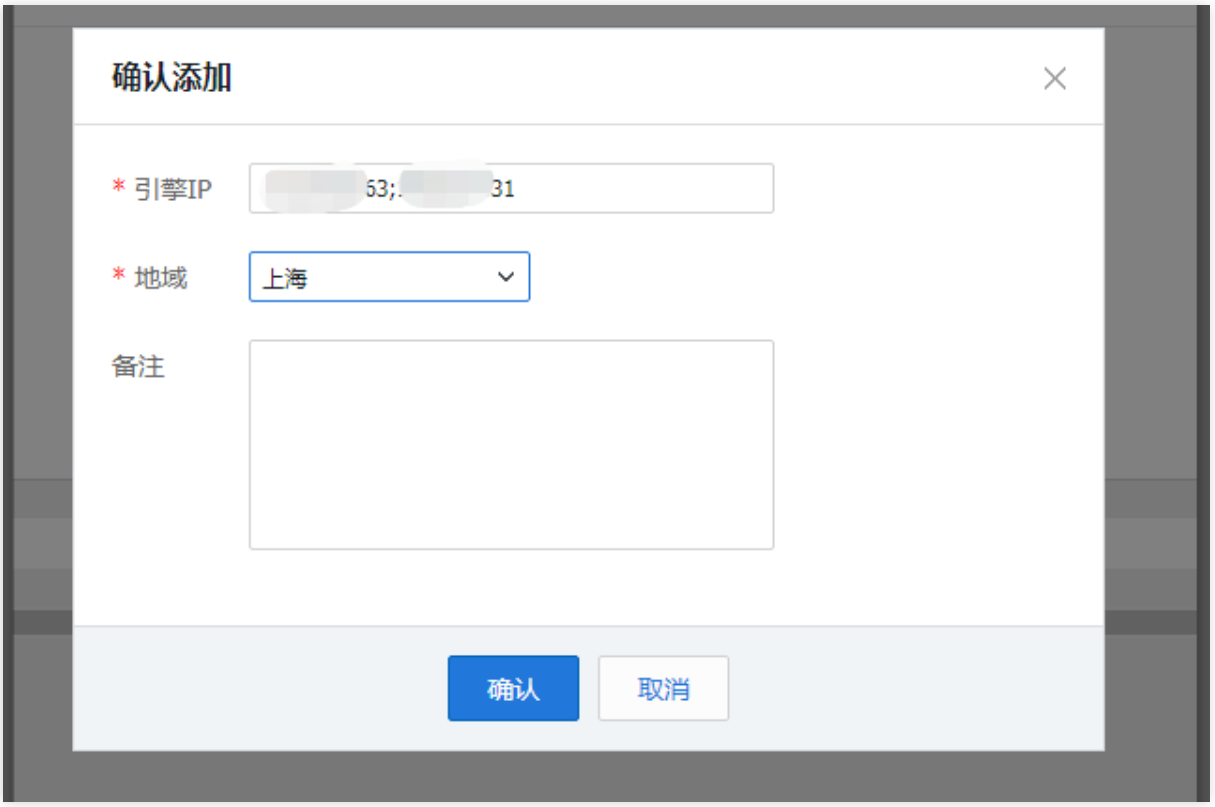
1. 登录运营端，云服务器中的虚拟机管理-运营端资源，找环境管理员申请后，分配引擎节点IP；



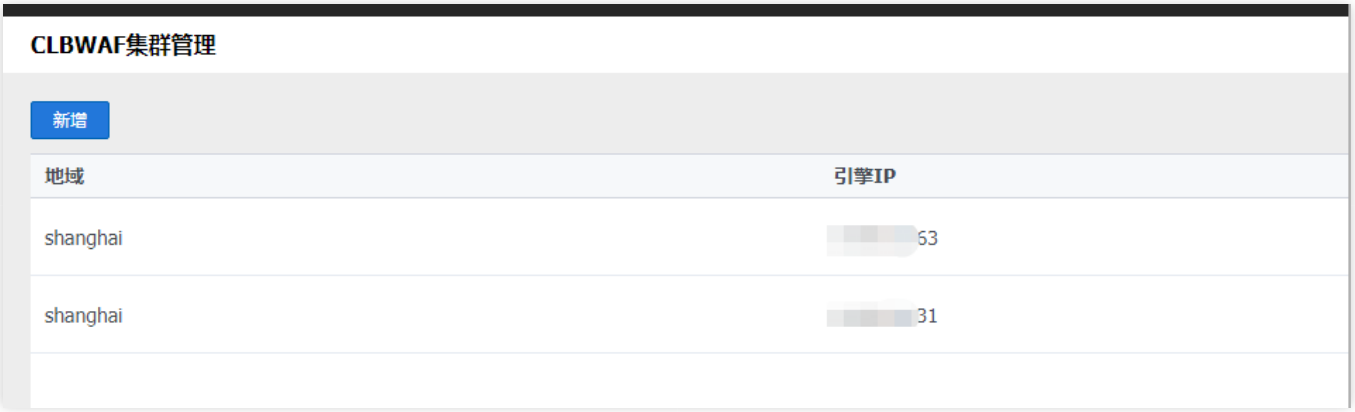
2. 登录WAF运营端，在集群管理中，点击【新增】；



3. 输入引擎IP，多个用";"隔开，点击【确认】；


确认添加
* 引擎IP
63;
31
* 地域
上海
备注
确认
取消

4. 新增成功；


CLBWAF集群管理
新增
地域
引擎IP
shanghai
63
shanghai
31

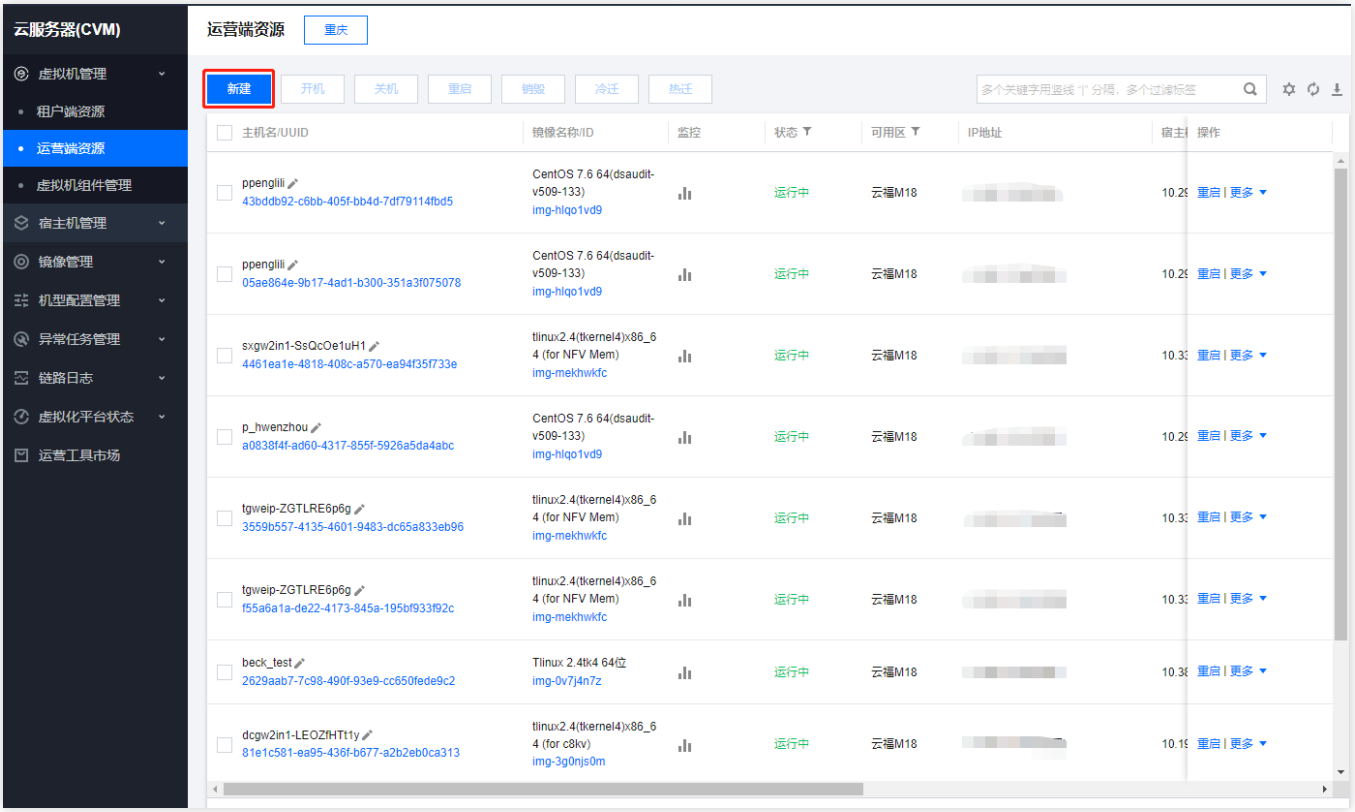
搭建SaaS型WAF源站

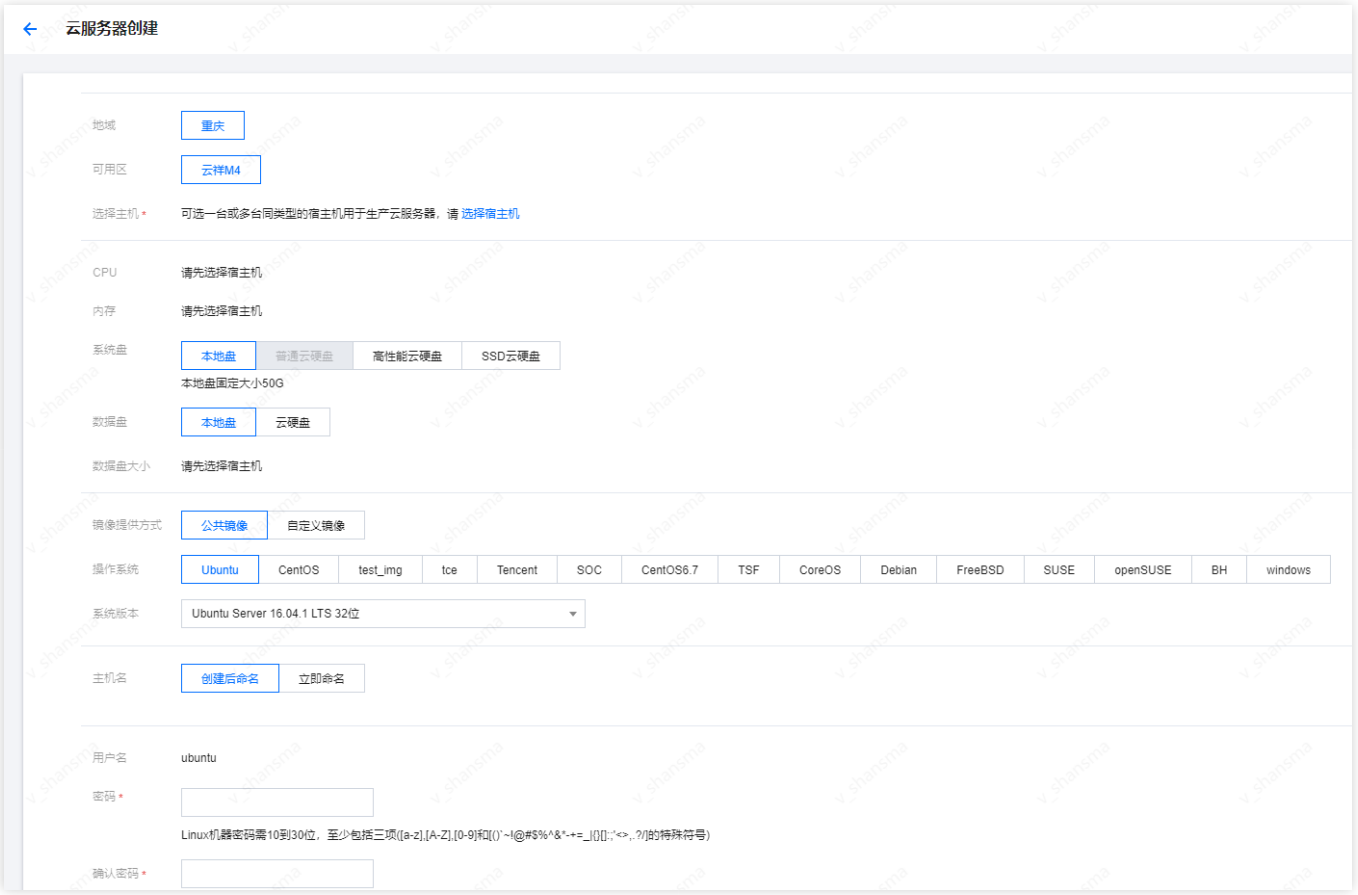
搭建SaaS型WAF源站

在新建SaaS型WAF域名时需要输入源站地址，源站地址只要与SaaS型WAF的引擎连通即可，源站IP可以使用内网IP，也可以使用外网IP。下面分别创建内网IP类型源站和外网IP类型源站。

1. 内网IP类型源站

1. 登录运营端选择云服务器创建CVM，点击运营端资源，点击【新建】；

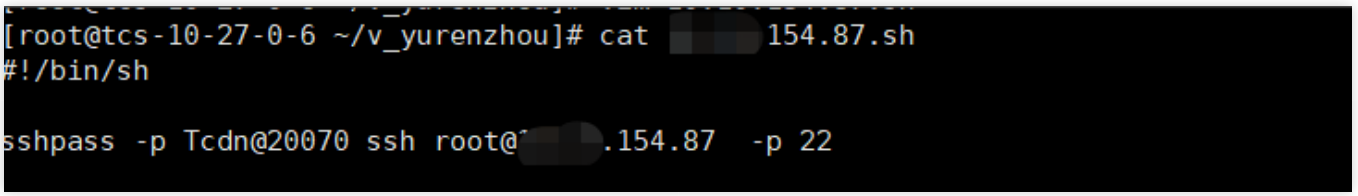




2. 在新建页面输入各项后，可以查看到新增的CVM;



3. 进入到新增的CVM中;



```
[root@tcs-10-27-0-6 ~/v_yurenzhou]# .  154.87.sh
Warning: Permanently added '  154.87' (ECDSA) to the list of known hosts.
[root@VM_154_87_linux ~]# ll
总用量 4
-rw-r--r-- 1 root root 90 1月   6 23:01 test
[root@VM_154_87_linux ~]# find / -name nginx
```

4. 在CVM中安装Nginx，输入命令 yum install -y nginx ;

```
[root@VM_154_87_linux ~]# yum -y install nginx
已加载插件：fastestmirror, langpacks
epel                                                     | 4.7 kB  00:00:00
extras                                                   | 2.9 kB  00:00:00
os                                                       | 3.6 kB  00:00:00
updates                                                  | 2.9 kB  00:00:00
(1/7): epel/7/x86_64/group_gz                            |  95 kB  00:00:00
(2/7): extras/7/x86_64/primary_db                        | 206 kB  00:00:00
(3/7): os/7/x86_64/group_gz                              | 153 kB  00:00:00
(4/7): epel/7/x86_64/updateinfo                          | 1.0 MB  00:00:00
(5/7): os/7/x86_64/primary_db                            | 6.1 MB  00:00:00
(6/7): updates/7/x86_64/primary_db                       | 3.8 MB  00:00:00
(7/7): epel/7/x86_64/primary_db                          | 6.9 MB  00:00:00
Determining fastest mirrors
```

启动Nginx服务： service nginx start

查看80端口是否启用： netstat -nap|grep nginx

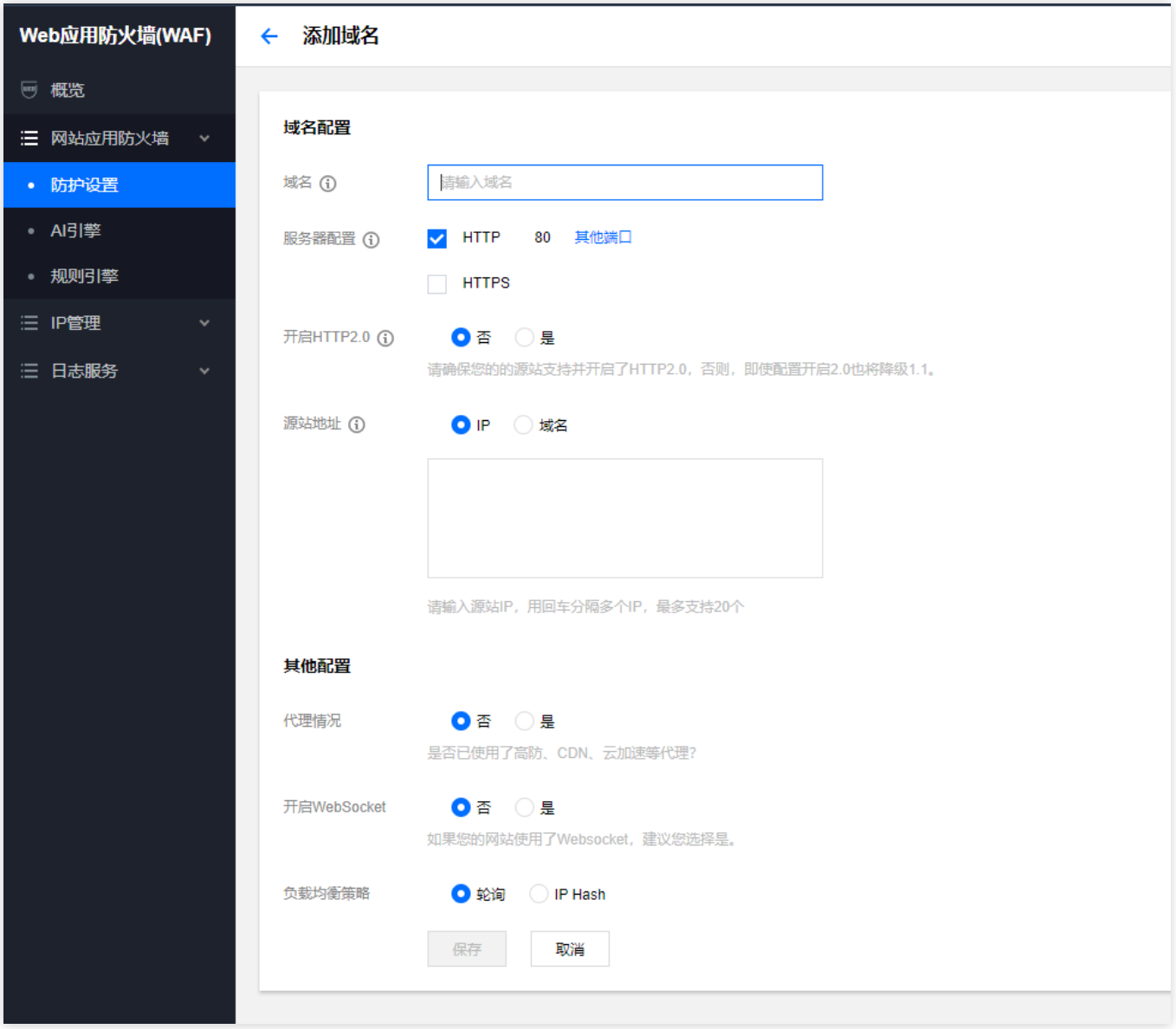
```
[root@VM_154_87_linux ~]# service nginx start
Redirecting to /bin/systemctl start nginx.service
[root@VM_154_87_linux ~]# netstat -nap |grep nginx
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      27979/nginx: master
tcp6       0      0 :::80                   :::*                    LISTEN      27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103293   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103296   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103295   27979/nginx: master
unix  3      [ ]         STREAM     CONNECTED     103294   27979/nginx: master
```

5. 在Saas引擎中ping和telnet cvm的IP地址及端口查看是否连通;

```
[root@VM_12_7_centos ~]# ping  .154.87
PING 10.10.154.87 (10.10.154.87) 56(84) bytes of data.
64 bytes from  .154.87: icmp_seq=1 ttl=53 time=0.823 ms
64 bytes from  .154.87: icmp_seq=2 ttl=53 time=0.832 ms
^C
--- .154.87 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.823/0.827/0.832/0.029 ms
```

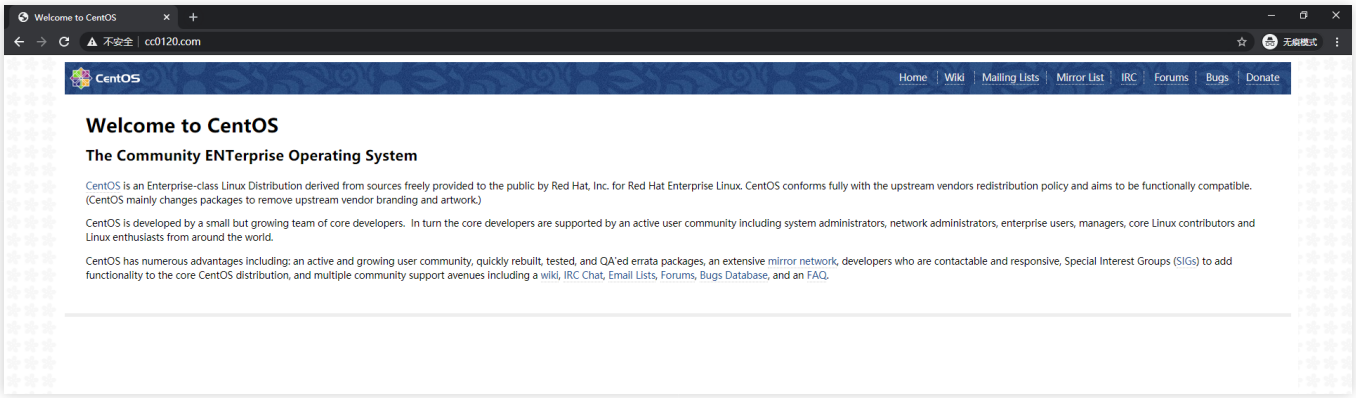
```
[root@VM_12_7_centos ~]# telnet  .154.87 80
Trying .154.87...
Connected to .154.87.
Escape character is '^]'.
^]
telnet>
```

6. 在saas型WAF中新增域名,源站IP输入已申请CVM的IP地址;



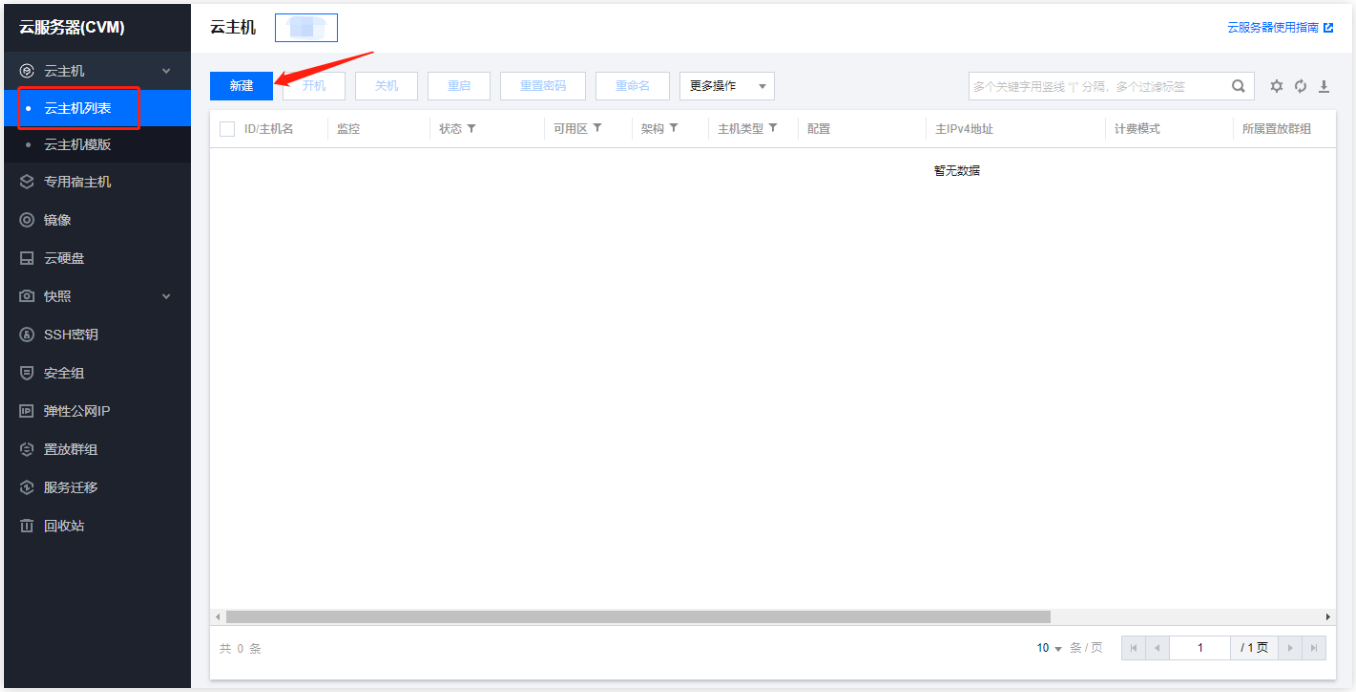


7. 配置host，访问新增域名，可以访问到内网IP类型的源站;

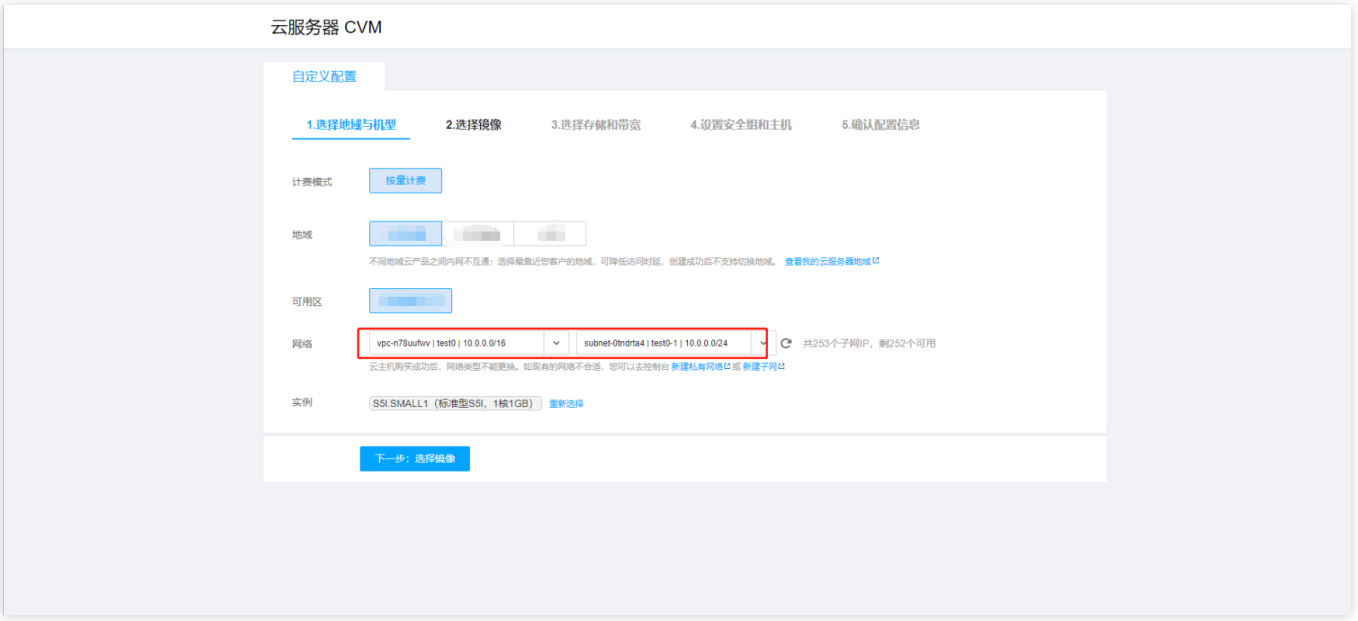


2. 外网IP类型源站

1. 登录租户端，进入到CVM页面，选择对应的地域，点击【新建】；



2. 所选网络需要与CLB网络一致，其余选项按照实际情况选择，点击【下一步：选择镜像】；



3. 按照实际情况选择镜像后，点击【下一步：选择存储和带宽】；



4. 按照实际情况选择存储和带宽后，点击【下一步：设置安全组和主机】；



5. 按照实际情况选择安全组和主机后，输入主机密码，点击【下一步：确认配置信息】；

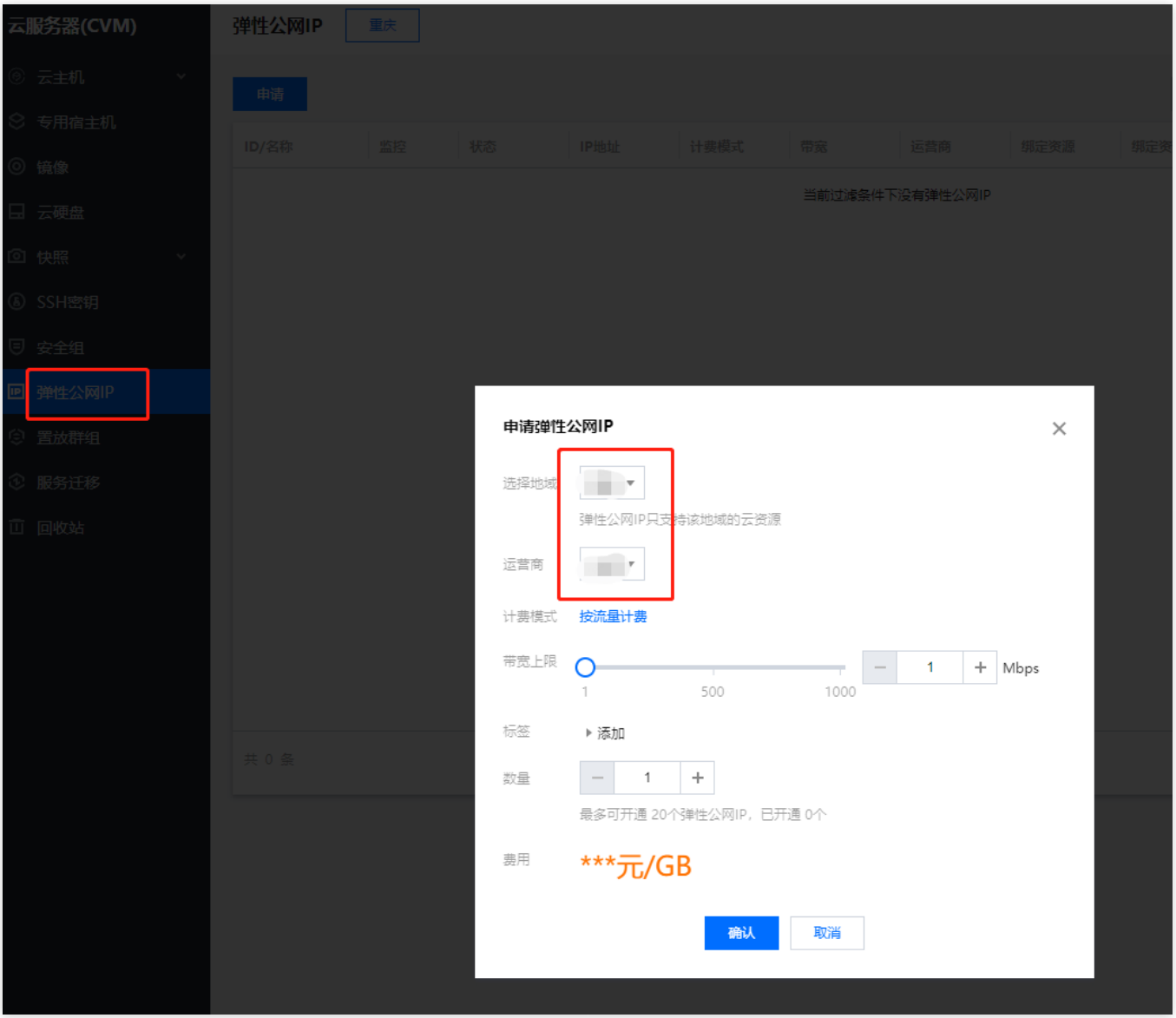




6. 查看到刚才所选的信息，确认无误后，点击【开通】；



7. 申请弹性公网IP地址，绑定CVM，CVM菜单下，点击【弹性公网IP】，选择与CVM相同的地域后，点击【申请】，按照实际情况选择各项；



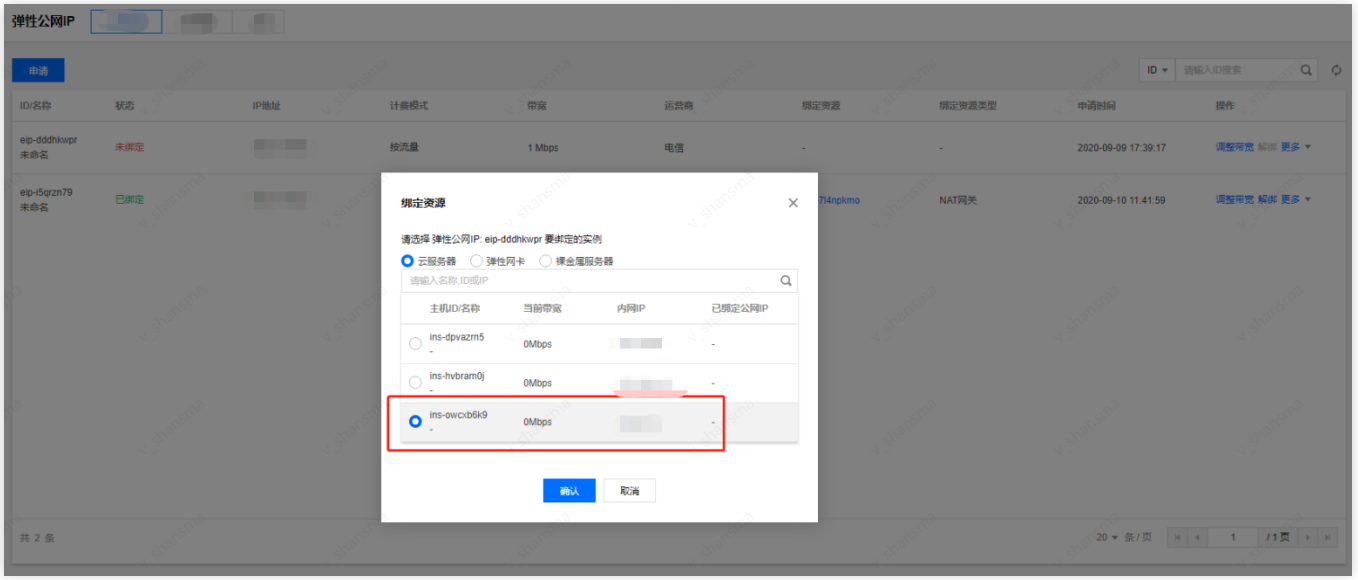
8. 点击【确认】，返回到弹性公网IP列表页面，可以查看到新建的弹性公网IP显示未绑定状态；



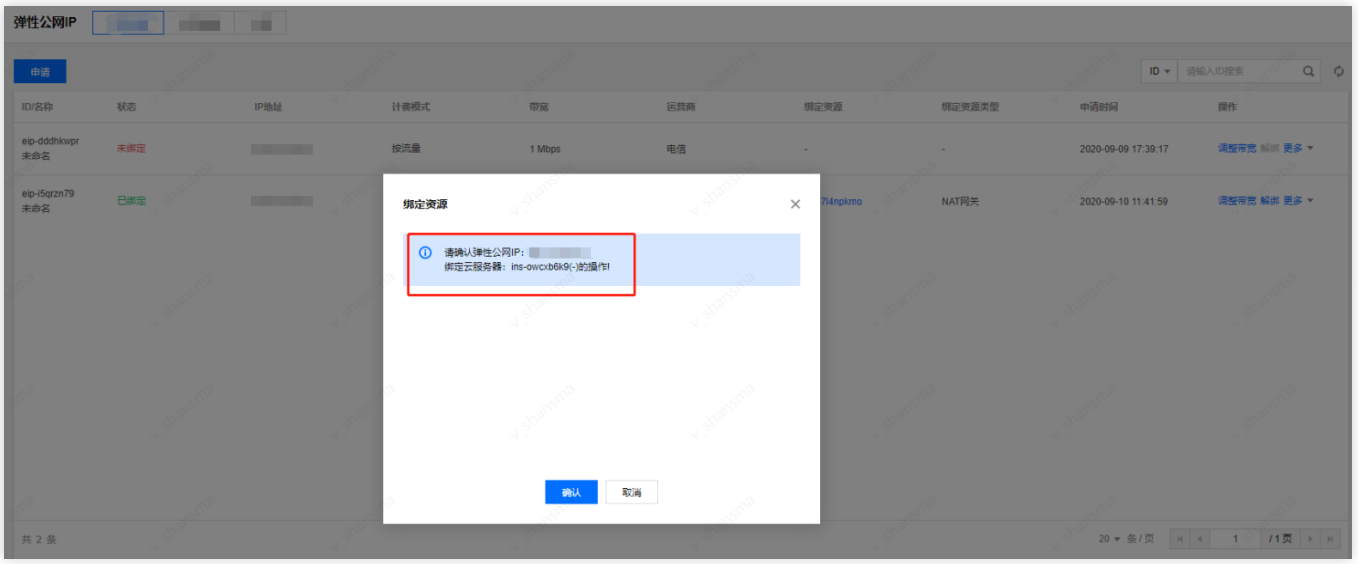
9. 点击弹性公网IP的"操作"栏，点击【更多】，选择【绑定】；



10. 选择要绑定的CVM，点击【确认】；



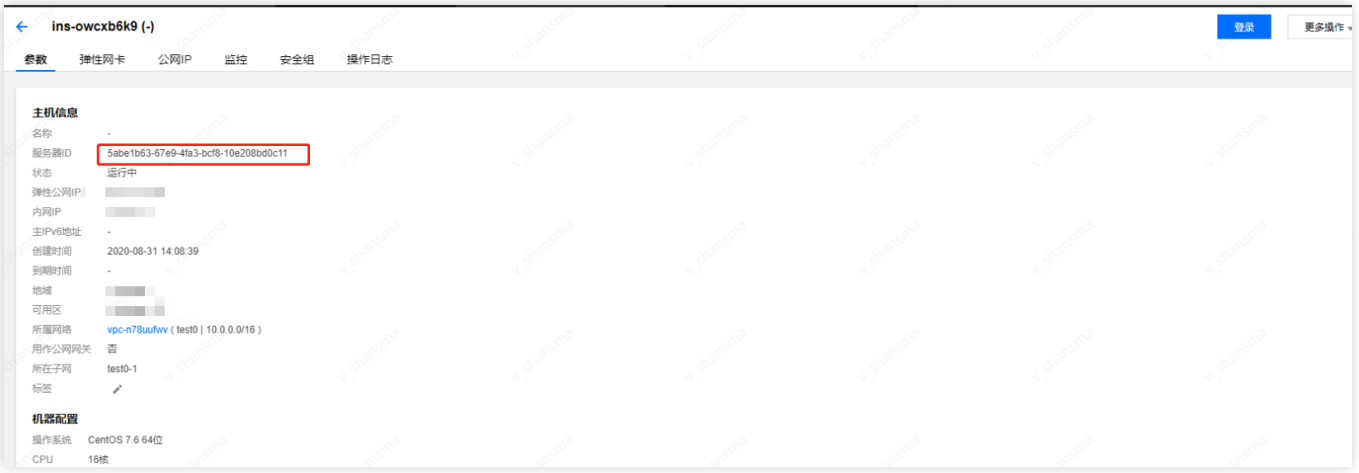
11. 查看需要确认的信息，确认无误后点击【确认】；



12. 返回到弹性公网IP列表页面，显示“已绑定”状态；



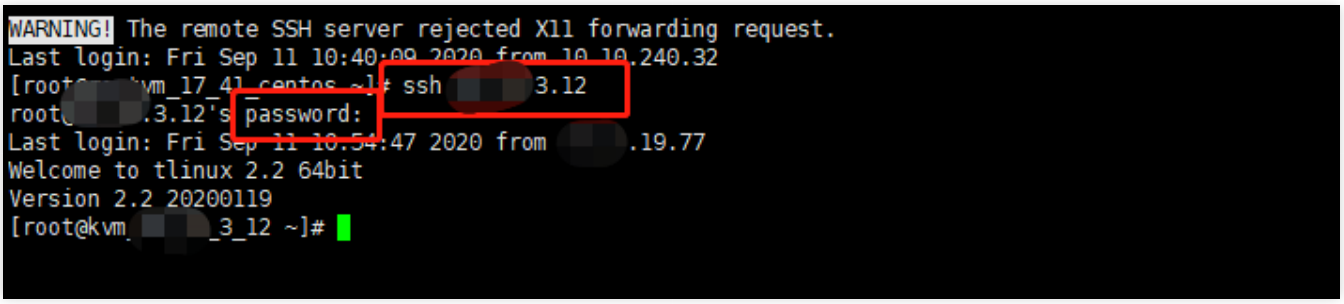
13. 安装Nginx，启用80端口，点击CVM的ID，进入到CVM参数页面，复制CVM的服务器ID；

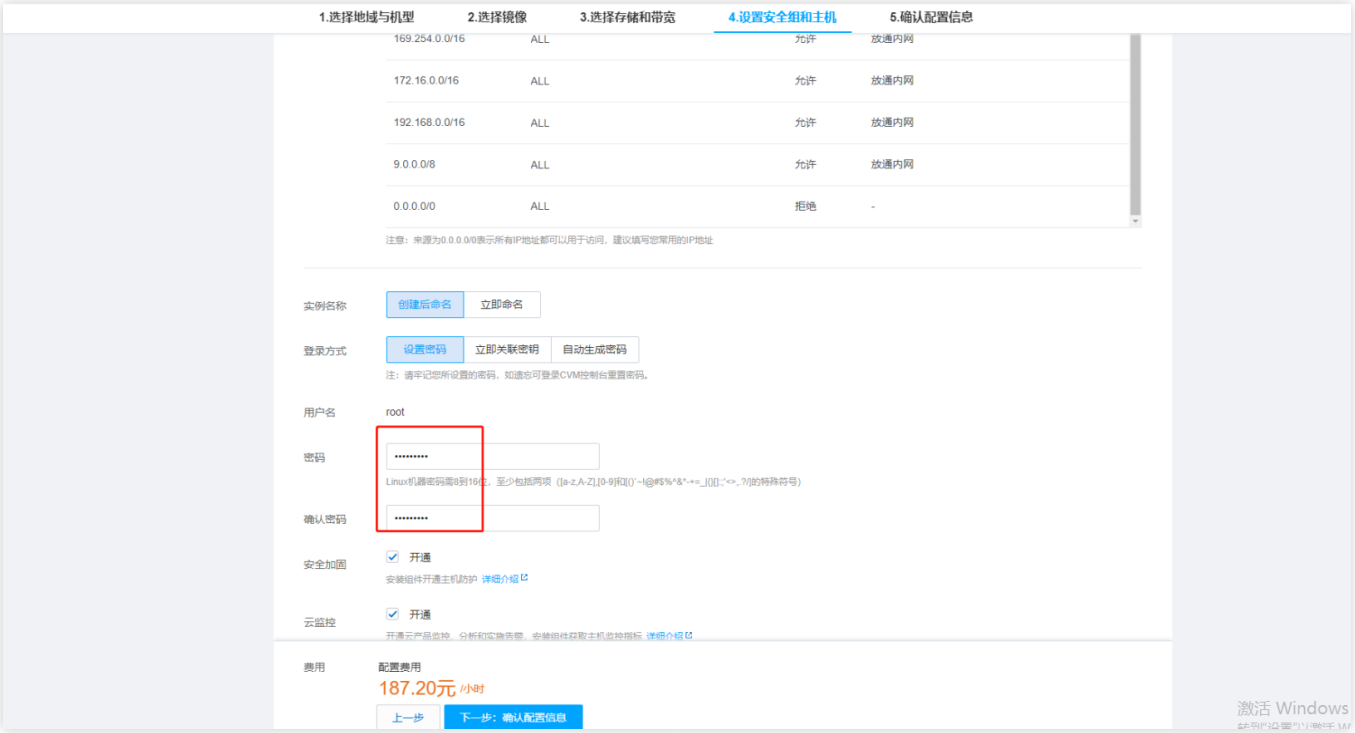


14. 在运营端中CVM-租户端资源下，搜索框中选择UUID，粘贴刚才复制的服务器ID，可以查询到宿主机内网IP；

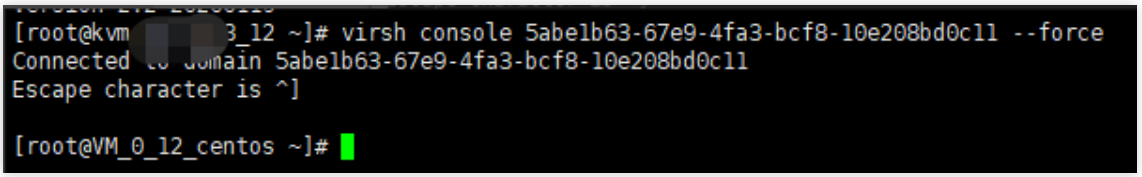


15. 登录到宿主机内网IP，输入命令：ssh 宿主机内网IP，密码为开通CVM时填入的密码；





16. 输入命令 virsh console UUID --force ，如virsh console 5abe1b63-67e9-4fa3-bcf8-10e208bd0c11 --force，进入到CVM中；



17. 进入后输入以下命令进行安装；

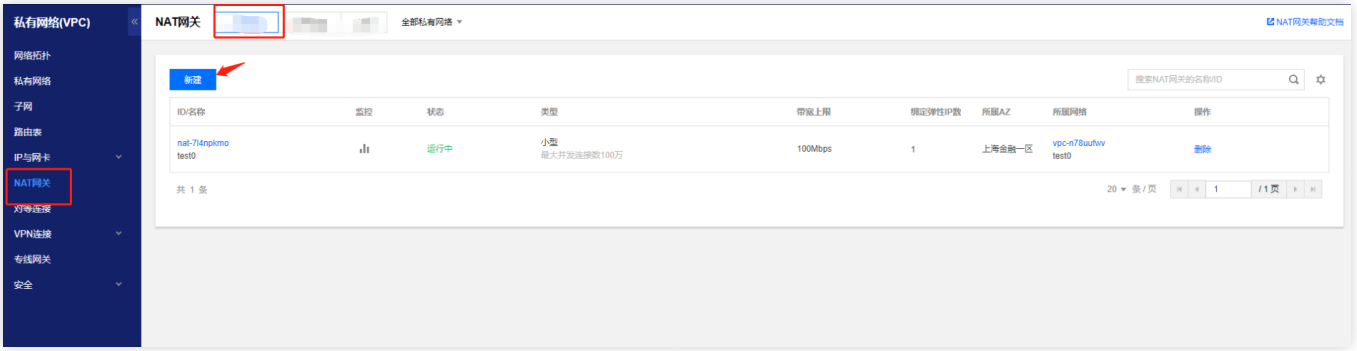
    安装： yum install -y nginx

    启动Nginx服务： service nginx start

    查看80端口是否启用： netstat -nap|grep 80

```
[root@VM_0_12_centos ~]#  netstat -nap|grep 80
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      20928/nginx: master
tcp6       0      0 :::80                   :::*                    LISTEN      20928/nginx: master
udp6       0      0 fe80::5054:ff:febc::123 :::*                                6695/ntpd
[root@VM_0_12_centos ~]#
```

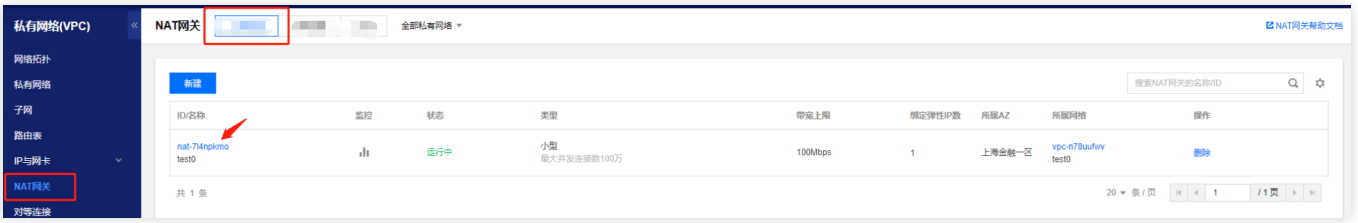
18. 由于有些客户公网ip地址禁止对外开放端口80和443，需要通过natgw把cvm的80端口转到其他端口，例如788，并在路由表中关联此网关（如不涉及此项请忽略步骤2.18-2.26）；私有网络菜单下选择NAT网关，选择对应的地域后，点击【新建】，新建NAT网关；



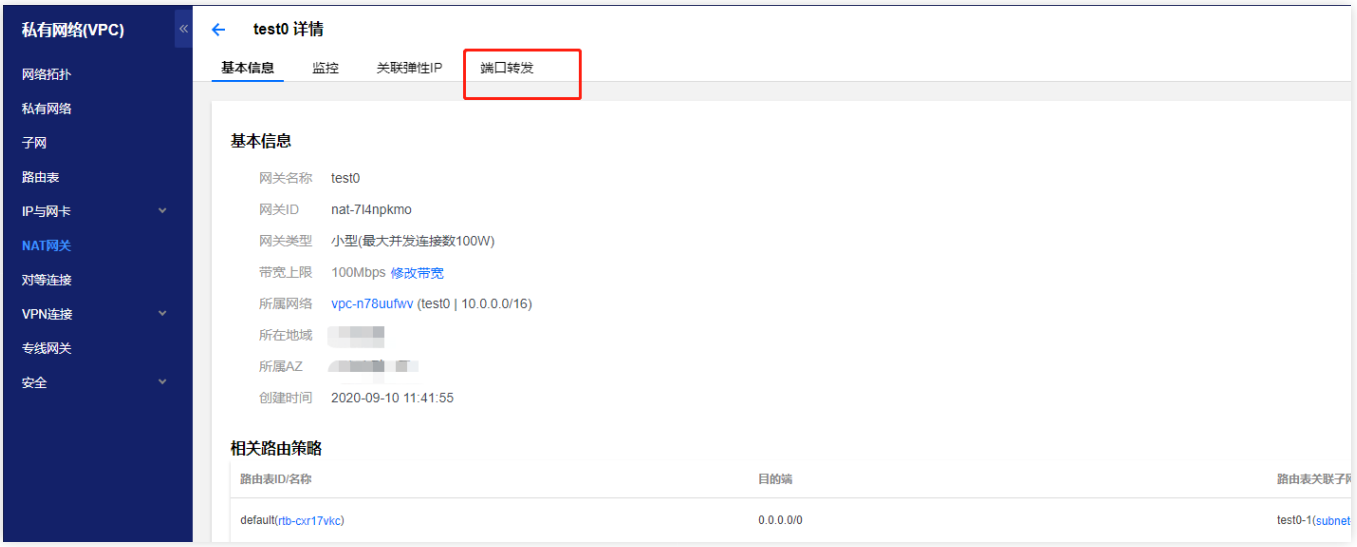
19. 按照实际情况输入各项，点击【创建】，返回到NAT网关列表页面；



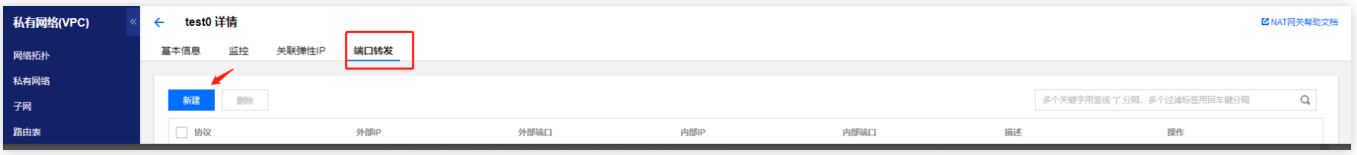
20. 在新建的NAT网关中点击网关ID；



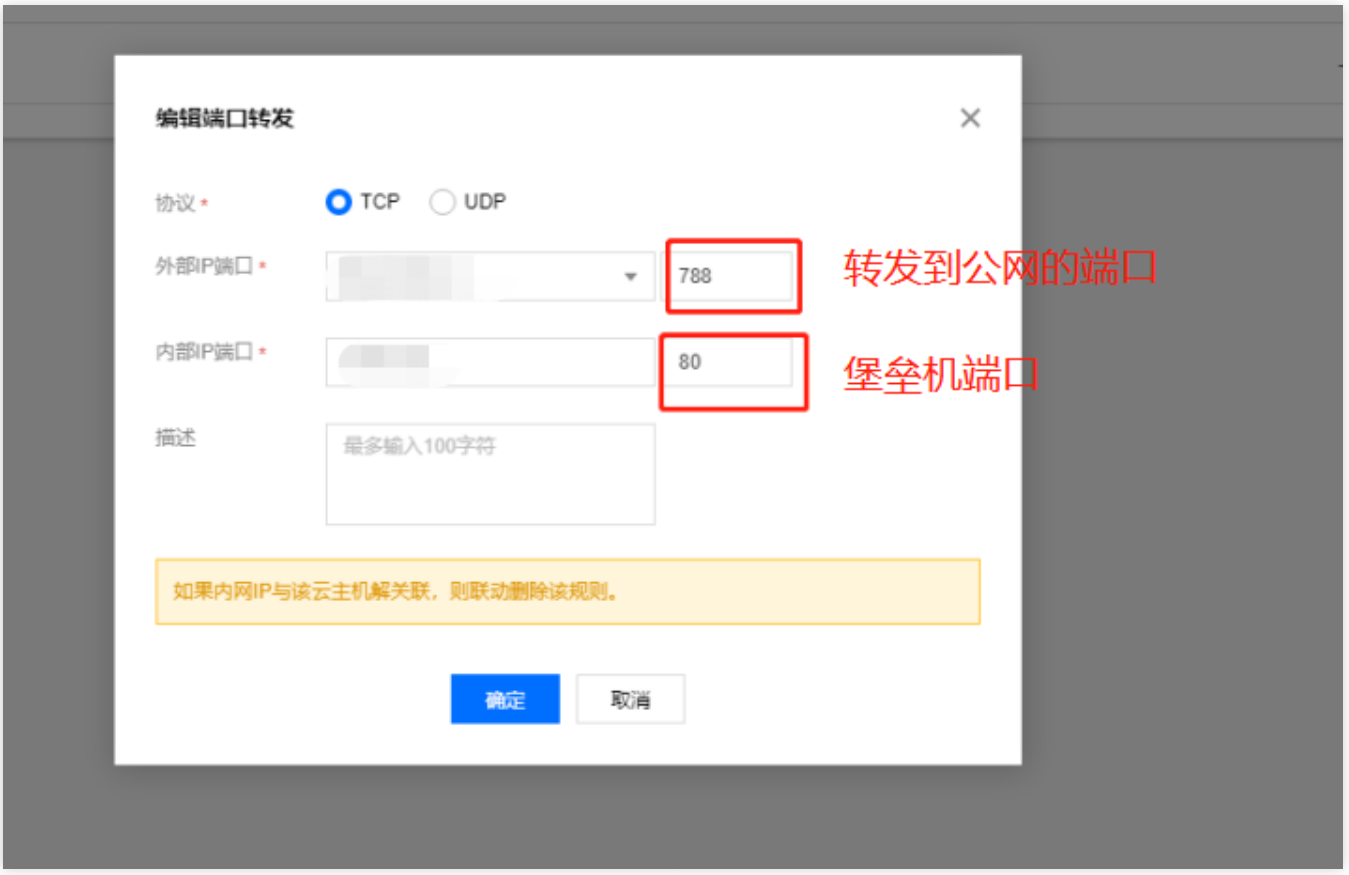
21. 点击端口转发；



22. 点击【新建】；



23. 添加转发端口；



24. 在私有网络下，选择路由表，在相应的地域下，点击【新建】，新建路由表；

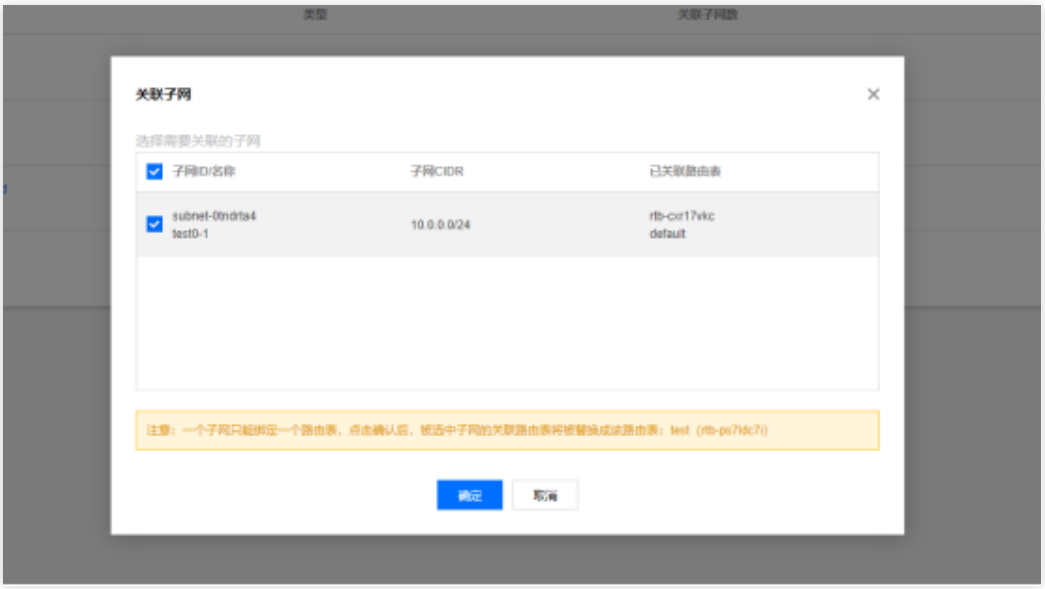


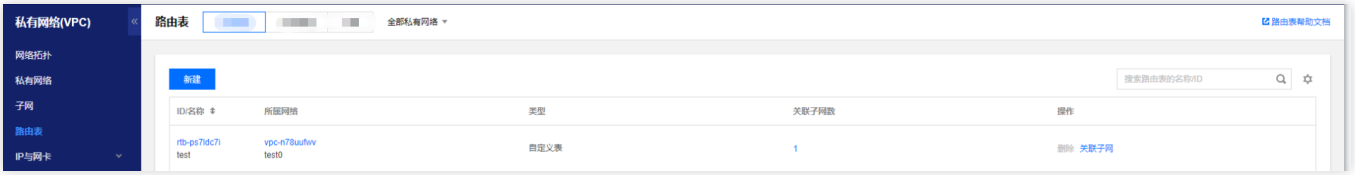


25. 输入各项后点击【创建】，策略选择已经添加的NAT网关；

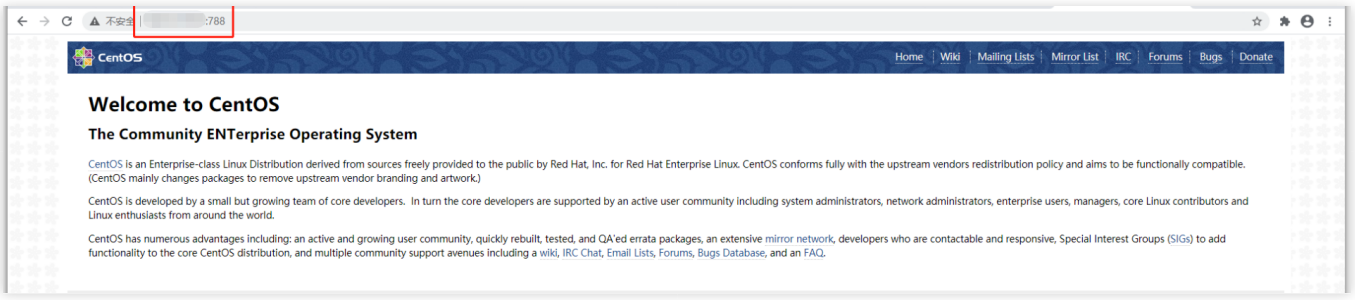


26. 提示需要关联子网，选择关联的子网后，点击【确定】，返回到路由表列表页面；





27. 访问http://公网ip:788/ 验证web网站是否正常



28. 在SaaS型WAF中新增域名,源站IP输入弹性IP的地址;


域名配置
域名
testsaaswaf0118.com
服务器配置
HTTP
80
其他端口
HTTPS
开启HTTP2.0
否
是
请确保您的的源站支持并开启了HTTP2.0，否则，即使配置开启2.0也将降级1.1。
源站地址
IP
域名
请输入源站IP，用回车分隔多个IP，最多支持20个
其他配置
代理情况
否
是
是否已使用了高防、CDN、云加速等代理?
开启WebSocket
否
是
如果您的网站使用了Websocket，建议您选择是。
负载均衡策略
轮询
IP Hash
保存
取消


Web应用防火墙(WAF)
概览
网站应用防火墙
防护设置
AI引擎
IP管理
日志服务
SaaS型
负载均衡型
防护设置
域名列表
添加域名
删除
域名
VIP地址
使用模式
回源IP地址
WAF开关
操作
testsaaswaf0118.com
109.244.100.200
规则：拦截模式
109.244.100.240
删除 编辑 防护配置

常见问题
常见问题

非云内的服务器能否使用 Web 应用防火墙？

Web 应用防火墙支持云外机房用户接入，可以保护任何公网的服务器，包括但不限于云平台，包括其他厂商的云，IDC 等。

> 注意：
>
> 在部分地区接入的域名必须按照工信部要求进行 ICP 备案。

Web 应用防火墙是否支持 HTTPS 防护？

Web 应用防火墙全面支持 HTTPS 业务。用户只需根据提示将 SSL 证书及私钥上传，Web 应用防火墙即可防护 HTTPS 业务流量。

Web 应用防火墙的源站 IP 可以填写内网 IP 吗？

Web 应用防火墙添加域名时，填写的源站地址必须是公网 IP 或者域名。内网IP需要和管理员确认。

Web 应用防火墙一个防护域名可以设置多少个回源 IP？

Web 应用防火墙一个防护域名最多可以设置20个回源 IP。

Web 应用防火墙配置多个源站时如何实现负载均衡？

如果配置了多个回源 IP，Web 应用防火墙采用轮询的方式对访问请求进行负载均衡。

Web 应用防火墙是否支持健康检查？

Web 应用防火墙默认启用健康检查。Web 应用防火墙会对所有源站 IP 进行接入状态检测，如果某个源站 IP 没有响应，Web 应用防火墙将不再将请求转发到该源站 IP ，直到接入状态恢复正常。

Web 应用防火墙是否支持会话保持？

Web 应用防火墙支持会话保持，默认开启。

在 Web 应用防火墙的控制台中，更改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。

Web 应用防火墙是否会自动将回源 IP 段加入安全组？

不会自动将回源 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。

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 Web 应用防火墙不会被拦截，如果使用 Web 应用防火墙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，Web 应用防火墙不支持防护。

Web应用防火墙支持哪些非标端口？

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、8060、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、9999、10000、10001、10080、10083、12601、20080、20083、25060、28080、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

API文档
网站管家（waf）
版本（2018-01-25）
API 概览

API版本

V3

其他接口

接口名称	接口功能
AddCustomRule	增加自定义规则
DescribeApiVersion	获取系统版本
DescribeRuleVersion	获取规则版本
DescribeWhiteByKey	waf获取白名单列表
WafCreateResourceAfterPay	购买WAF
WafGetDomainEngineType	WafGetDomainEngineType

日志服务相关接口

接口名称	接口功能
CreateAttackDownloadTask	创建攻击日志下载任务
DeleteDownloadRecord	删除下载记录

防护设置相关接口

接口名称	接口功能
AddUserWhiteRule	增加规则引擎白名单
CheckUserWhiteRuleName	查询用户白名单名字重复
DeleteSession	Waf 会话定义 Delete接口
DeleteUserWhiteRule	删除全局白名单
DescribeCustomRules	获取自定义策略列表
DescribeMainClass	获取主类及子类信息
DescribeRuleUpdateLog	获取特征规则更新动态
DescribeUserEngineType	获取用户规则引擎类型
DescribeUserLevel	获取用户防护规则等级
DescribeUserSignatureRule	获取用户特征规则列表
DescribeUserWhiteRule	获取全局白名单
DescribeWebshellEnable	获得webshell切换状态
ModifyCustomRuleStatus	切换自定义规则的开关
ModifyUserLevel	修改用户防护规则等级
ModifyUserSignatureRule	修改用户防护规则
ModifyUserWhiteRule	变更全局白名单
ModifyWebshellEnable	切换webshell切换状态

调用方式
接口签名v1

TCloudFinanceZone API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。
签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。
安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录TCloudFinanceZone管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. 生成签名串

有了安全凭证SecretId 和 SecretKey后，就可以生成签名串了。以下是生成签名串的详细过程：

假设用户的 SecretId 和 SecretKey 分别是：

- SecretId: AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
- SecretKey: Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

注意：这里只是示例，请根据用户实际申请的 SecretId 和 SecretKey 进行后续操作！

以云服务器查看实例列表(DescribeInstances)请求为例，当用户调用这一接口时，其请求参数可能如下:

参数名称	中文	参数值

参数名称	中文	参数值
Action	方法名	DescribeInstances
SecretId	密钥Id	AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE
Timestamp	当前时间戳	1465185768
Nonce	随机正整数	11886
Region	实例所在区域	shjr
InstanceIds.0	待查询的实例ID	ins-09dx96dg
Offset	偏移量	0
Limit	最大允许输出	20
Version	接口版本号	2017-03-12

2.1. 对参数排序

首先对所有请求参数按参数名的字典序（ ASCII 码）升序排序。注意：1）只按参数名进行排序，参数值保持对应即可，不参与比大小；2）按 ASCII 码比大小，如 InstanceIds.2 要排在 InstanceIds.12 后面，不是按字母表，也不是按数值。用户可以借助编程语言中的相关排序函数来实现这一功能，如 php 中的 ksort 函数。上述示例参数的排序结果如下:

```
{
    'Action' : 'DescribeInstances',
    'InstanceIds.0' : 'ins-09dx96dg',
    'Limit' : 20,
    'Nonce' : 11886,
    'Offset' : 0,
    'Region' : 'shjr',
    'SecretId' : 'AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE',
    'Timestamp' : 1465185768,
    'Version': '2017-03-12',
}
```

使用其它程序设计语言开发时，可对上面示例中的参数进行排序，得到的结果一致即可。

2.2. 拼接请求字符串

此步骤生成请求字符串。
将把上一步排序好的请求参数格式化成“参数名称”=“参数值”的形式，如对 Action 参数，其参数名称为 "Action" ，参数值为 "DescribeInstances" ，因此格式化后就为 Action=DescribeInstances 。
注意：“参数值”为原始值而非url编码后的值。

然后将格式化后的各个参数用"&"拼接在一起，最终生成的请求字符串为:

```
Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.3. 拼接签名原文字符串

此步骤生成签名原文字符串。
签名原文字符串由以下几个参数构成:

1. 请求方法: 支持 POST 和 GET 方式，这里使用 GET 请求，注意方法为全大写。
2. 请求主机:查看实例列表(DescribeInstances)的请求域名为：cvm.finance.cloud.tencent.com。实际的请求域名根据接口所属模块的不同而不同，详见各接口说明。
3. 请求路径: 当前版本云API的请求路径固定为 / 。
4. 请求字符串: 即上一步生成的请求字符串。

签名原文串的拼接规则为: 请求方法 + 请求主机 +请求路径 + ？ + 请求字符串

示例的拼接结果为：

```
GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12
```

2.4. 生成签名串

此步骤生成签名串。
首先使用 HMAC-SHA1 算法对上一步中获得的签名原文字符串进行签名，然后将生成的签名串使用 Base64 进行编码，即可获得最终的签名串。

具体代码如下，以 PHP 语言为例:

```
$secretKey = 'Gu5t9xGARNpq86cd98joQYCN3EXAMPLE';
$srcStr = 'GETcvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Timestamp=1465185768&Version=2017-03-12';
$signStr = base64_encode(hash_hmac('sha1', $srcStr, $secretKey, true));
echo $signStr;
```

最终得到的签名串为:

```
EliP9YW3pW28FpsEdkXt/+WcGeI=
```

使用其它程序设计语言开发时，可用上面示例中的原文进行签名验证，得到的签名串与例子中的一致即可。

3. 签名串编码

生成的签名串并不能直接作为请求参数，需要对其进行 URL 编码。

如上一步生成的签名串为 EliP9YW3pW28FpsEdkXt/+WcGeI= ，最终得到的签名串请求参数（Signature）为：EliP9YW3pW28FpsEdkXt%2f%2bWcGeI%3d，它将用于生成最终的请求 URL。

注意：如果用户的请求方法是 GET，或者请求方法为 POST 同时 Content-Type 为 application/x-www-form-urlencoded，则发送请求时所有请求参数的值均需要做 URL 编码，参数键和=符号不需要编码。非 ASCII 字符在 URL 编码前需要先以 UTF-8 进行编码。

注意：有些编程语言的 http 库会自动为所有参数进行 urlencode，在这种情况下，就不需要对签名串进行 URL 编码了，否则两次 URL 编码会导致签名失败。

注意：其他参数值也需要进行编码，编码采用 RFC 3986。使用 %XY 对特殊字符例如汉字进行百分比编码，其中“X”和“Y”为十六进制字符（0-9 和大写字母 A-F），使用小写将引发错误。

4. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

5. 签名演示

在实际调用 API 3.0 时，推荐使用配套的TCloudFinanceZone SDK 3.0 ，SDK 封装了签名的过程，开发时只关注产品提供的具体接口即可。详细信息参见 SDK 中心。当前支持的编程语言有：

- Python
- Java

- PHP
- Go
- Node

为了更清楚的解释签名过程，下面以实际编程语言为例，将上述的签名过程具体实现。请求的域名、调用的接口和参数的取值都以上述签名过程为准，代码只为解释签名过程，并不具备通用性，实际开发请尽量使用 SDK 。

最终输出的 url 可能为： https://cvm.finance.cloud.tencent.com/?Action=DescribeInstances&InstanceIds.0=ins-09dx96dg&Limit=20&Nonce=11886&Offset=0&Region=shjr&SecretId=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE&Signature=EliP9YW3pW28FpsEdkXt%2F%2BWcGeI%3D&Timestamp=1465185768&Version=2017-03-12

注意：由于示例中的密钥是虚构的，时间戳也不是系统当前时间，因此如果将此 url 在浏览器中打开或者用 curl 等命令调用时会返回鉴权错误：签名过期。为了得到一个可以正常返回的 url ，需要修改示例中的 SecretId 和 SecretKey 为真实的密钥，并使用系统当前时间戳作为 Timestamp 。

注意：在下面的示例中，不同编程语言，甚至同一语言每次执行得到的 url 可能都有所不同，表现为参数的顺序不同，但这并不影响正确性。只要所有参数都在，且签名计算正确即可。

注意：以下代码仅适用于 API 3.0，不能直接用于其他的签名流程，即使是旧版的 API ，由于存在细节差异也会导致签名计算错误，请以对应的实际文档为准。

Java

```
import java.io.UnsupportedEncodingException;
import java.net.URLEncoder;
import java.util.Random;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.xml.bind.DatatypeConverter;

public class CloudAPIDemo {
    private final static String CHARSET = "UTF-8";

    public static String sign(String s, String key, String method) throws Exception {
        Mac mac = Mac.getInstance(method);
        SecretKeySpec secretKeySpec = new SecretKeySpec(key.getBytes(CHARSET), mac.getAlgorithm());
        mac.init(secretKeySpec);
        byte[] hash = mac.doFinal(s.getBytes(CHARSET));
        return DatatypeConverter.printBase64Binary(hash);
    }

    public static String getStringToSign(TreeMap<String, Object> params) {
        StringBuilder s2s = new StringBuilder("GETcvm.finance.cloud.tencent.com/?");
```

```
        // 签名时要求对参数进行字典排序，此处用TreeMap保证顺序
        for (String k : params.keySet()) {
            s2s.append(k).append("=").append(params.get(k).toString()).append("&");
        }
        return s2s.toString().substring(0, s2s.length() - 1);
    }

    public static String getUrl(TreeMap<String, Object> params) throws UnsupportedEncodingException
{
        StringBuilder url = new StringBuilder("https://cvm.finance.cloud.tencent.com/?");
        // 实际请求的url中对参数顺序没有要求
        for (String k : params.keySet()) {
            // 需要对请求串进行urlencode，由于key都是英文字母，故此处仅对其value进行urlencode
            url.append(k).append("=").append(URLEncoder.encode(params.get(k).toString(), CHARSET)).app
end("&");
        }
        return url.toString().substring(0, url.length() - 1);
    }

    public static void main(String[] args) throws Exception {
        TreeMap<String, Object> params = new TreeMap<String, Object>(); // TreeMap可以自动排序
        // 实际调用时应当使用随机数，例如：params.put("Nonce", new Random().nextInt(java.lang.Intege
r.MAX_VALUE));
        params.put("Nonce", 11886); // 公共参数
        // 实际调用时应当使用系统当前时间，例如：  params.put("Timestamp", System.currentTimeMillis() /
1000);
        params.put("Timestamp", 1465185768); // 公共参数
        params.put("SecretId", "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"); // 公共参数
        params.put("Action", "DescribeInstances"); // 公共参数
        params.put("Version", "2017-03-12"); // 公共参数
        params.put("Region", "shjr"); // 公共参数
        params.put("Limit", 20); // 业务参数
        params.put("Offset", 0); // 业务参数
        params.put("InstanceIds.0", "ins-09dx96dg"); // 业务参数
        params.put("Signature", sign(getStringToSign(params), "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE
", "HmacSHA1")); // 公共参数
        System.out.println(getUrl(params));
    }
}
```

Python

注意：如果是在 Python 2 环境中运行，需要先安装 requests 依赖包： pip install requests 。

```
# -*- coding: utf8 -*-
import base64
```

```
import hashlib
import hmac
import time

import requests

secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

def get_string_to_sign(method, endpoint, params):
    s = method + endpoint + "/?"
    query_str = "&".join("%s=%s" % (k, params[k]) for k in sorted(params))
    return s + query_str

def sign_str(key, s, method):
    hmac_str = hmac.new(key.encode("utf8"), s.encode("utf8"), method).digest()
    return base64.b64encode(hmac_str)

if __name__ == '__main__':
    endpoint = "cvm.finance.cloud.tencent.com"
    data = {
        'Action' : 'DescribeInstances',
        'InstanceIds.0' : 'ins-09dx96dg',
        'Limit' : 20,
        'Nonce' : 11886,
        'Offset' : 0,
        'Region' : 'shjr',
        'SecretId' : secret_id,
        'Timestamp' : 1465185768, # int(time.time())
        'Version': '2017-03-12'
    }
    s = get_string_to_sign("GET", endpoint, data)
    data["Signature"] = sign_str(secret_key, s, hashlib.sha1)
    print(data["Signature"])
    # 此处会实际调用，成功后可能产生计费
    # resp = requests.get("https://" + endpoint, params=data)
    # print(resp.url)
```

接口签名v3

TCloudFinanceZone API 会对每个访问请求进行身份验证，即每个请求都需要在公共请求参数中包含签名信息（Signature）以验证请求者身份。
签名信息由安全凭证生成，安全凭证包括 SecretId 和 SecretKey；若用户还没有安全凭证，请前往云API密钥页面申请，否则无法调用云API接口。

1. 申请安全凭证

在第一次使用云API之前，请前往云API密钥页面申请安全凭证。
安全凭证包括 SecretId 和 SecretKey：

- SecretId 用于标识 API 调用者身份
- SecretKey 用于加密签名字符串和服务器端验证签名字符串的密钥。
- 用户必须严格保管安全凭证，避免泄露。

申请安全凭证的具体步骤如下：

1. 登录TCloudFinanceZone管理中心控制台。
2. 前往云API密钥的控制台页面
3. 在云API密钥页面，点击【新建】即可以创建一对SecretId/SecretKey

注意：开发商帐号最多可以拥有两对 SecretId / SecretKey。

2. TC3-HMAC-SHA256 签名方法

注意：对于GET方法，只支持 Content-Type: application/x-www-form-urlencoded 协议格式。对于POST方法，目前支持 Content-Type: application/json 以及 Content-Type: multipart/form-data 两种协议格式，json 格式默认所有业务接口均支持，multipart 格式只有特定业务接口支持，此时该接口不能使用 json 格式调用，参考具体业务接口文档说明。

下面以云服务器查询广州区实例列表作为例子，分步骤介绍签名的计算过程。我们仅用到了查询实例列表的两个参数：Limit 和 Offset，使用 GET 方法调用。

假设用户的 SecretId 和 SecretKey 分别是：AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE 和 Gu5t9xGARNpq86cd98joQYCN3EXAMPLE

2.1. 拼接规范请求串

按如下格式拼接规范请求串（CanonicalRequest）：

```
CanonicalRequest =
    HTTPRequestMethod + '\n' +
    CanonicalURI + '\n' +
    CanonicalQueryString + '\n' +
    CanonicalHeaders + '\n' +
    SignedHeaders + '\n' +
    HashedRequestPayload
```

- HTTPRequestMethod：HTTP 请求方法（GET、POST ），本示例中为 GET；
- CanonicalURI：URI 参数，API 3.0 固定为正斜杠（/）；
- CanonicalQueryString：发起 HTTP 请求 URL 中的查询字符串，对于 POST 请求，固定为空字符串，对于 GET 请求，则为 URL 中问号（?）后面的字符串内容，本示例取值为：Limit=10&Offset=0。注意：CanonicalQueryString 需要经过 URL 编码。
- CanonicalHeaders：参与签名的头部信息，至少包含 host 和 content-type 两个头部，也可加入自定义的头部参与签名以提高自身请求的唯一性和安全性。拼接规则：1）头部 key 和 value 统一转成小写，并去掉首尾空格，按照 key:value\n 格式拼接；2）多个头部，按照头部 key（小写）的字典排序进行拼接。此例中为： content-type:application/x-www-form-urlencoded\nhost:cvm.finance.cloud.tencent.com\n
- SignedHeaders：参与签名的头部信息，说明此次请求有哪些头部参与了签名，和 CanonicalHeaders 包含的头部内容是一一对应的。content-type 和 host 为必选头部。拼接规则：1）头部 key 统一转成小写；2）多个头部 key（小写）按照字典排序进行拼接，并且以分号（;）分隔。此例中为： content-type;host
- HashedRequestPayload：请求正文的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(RequestPayload)))，对 HTTP 请求整个正文 payload 做 SHA256 哈希，然后十六进制编码，最后编码串转换成小写字母。注意：对于 GET 请求，RequestPayload 固定为空字符串，对于 POST 请求，RequestPayload 即为 HTTP 请求正文 payload。

根据以上规则，示例中得到的规范请求串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
GET
/
Limit=10&Offset=0
content-type:application/x-www-form-urlencoded
host:cvm.finance.cloud.tencent.com

content-type;host
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

2.2. 拼接待签名字符串

按如下格式拼接待签名字符串：

```
StringToSign =
    Algorithm + \n +
```

```
RequestTimestamp + \n +
CredentialScope + \n +
HashedCanonicalRequest
```

- Algorithm：签名算法，目前固定为 TC3-HMAC-SHA256；
- RequestTimestamp：请求时间戳，即请求头部的 X-TC-Timestamp 取值，如上示例请求为 1539084154；
- CredentialScope：凭证范围，格式为 Date/service/tc3_request，包含日期、所请求的服务和终止字符串（tc3_request）。Date 为 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service 为产品名，必须与调用的产品域名一致，例如 cvm。如上示例请求，取值为 2018-10-09/cvm/tc3_request；
- HashedCanonicalRequest：前述步骤拼接所得规范请求串的哈希值，计算方法为 Lowercase(HexEncode(Hash.SHA256(CanonicalRequest)))。

注意：

> 1. Date 必须从时间戳 X-TC-Timestamp 计算得到，且时区为 UTC+0。如果加入系统本地时区信息，例如东八区，将导致白天和晚上调用成功，但是凌晨时调用必定失败。假设时间戳为 1551113065，在东八区的时间是 2019-02-26 00:44:25，但是计算得到的 Date 取 UTC+0 的日期应为 2019-02-25，而不是 2019-02-26。
> 2. Timestamp 必须是当前系统时间，且需确保系统时间和标准时间是同步的，如果相差超过五分钟则必定失败。如果长时间不和标准时间同步，可能导致运行一段时间后，请求必定失败（返回签名过期错误）。

根据以上规则，示例中得到的待签名字符串如下（为了展示清晰，\n 换行符通过另起打印新的一行替代）：

```
TC3-HMAC-SHA256
1539084154
2018-10-09/cvm/tc3_request
91c9c192c14460df6c1ffc69e34e6c5e90708de2a6d282cccf957dbf1aa7f3a7
```

2.3. 计算签名

1）计算派生签名密钥，伪代码如下

```
SecretKey = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"
SecretDate = HMAC_SHA256("TC3" + SecretKey, Date)
SecretService = HMAC_SHA256(SecretDate, Service)
SecretSigning = HMAC_SHA256(SecretService, "tc3_request")
```

- SecretKey：原始的 SecretKey；
- Date：即 Credential 中的 Date 字段信息，如上示例，为2018-10-09；
- Service：即 Credential 中的 Service 字段信息，如上示例，为 cvm；

2）计算签名，伪代码如下

```
Signature = HexEncode(HMAC_SHA256(SecretSigning, StringToSign))
```

- SecretSigning：即以上计算得到的派生签名密钥；
- StringToSign：即步骤2计算得到的待签名字符串；

2.4. 拼接 Authorization

按如下格式拼接 Authorization：

```
Authorization =
    Algorithm + ' ' +
    'Credential=' + SecretId + '/' + CredentialScope + ', ' +
    'SignedHeaders=' + SignedHeaders + ', '
    'Signature=' + Signature
```

- Algorithm：签名方法，固定为 TC3-HMAC-SHA256；
- SecretId：密钥对中的 SecretId；
- CredentialScope：见上文，凭证范围；
- SignedHeaders：见上文，参与签名的头部信息；
- Signature：签名值

根据以上规则，示例中得到的值为：

```
TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
```

最终完整的调用信息如下：

```
https://cvm.finance.cloud.tencent.com/?Limit=10&Offset=0

Authorization: TC3-HMAC-SHA256 Credential=AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE/2018-10-09/cvm/tc3_request, SignedHeaders=content-type;host, Signature=5da7a33f6993f0614b047e5df4582db9e9bf4672ba50567dba16c6ccf174c474
Content-Type: application/x-www-form-urlencoded
Host: cvm.finance.cloud.tencent.com
X-TC-Action: DescribeInstances
X-TC-Version: 2017-03-12
X-TC-Timestamp: 1539084154
X-TC-Region: shjr
```

3. 签名失败

根据实际情况，存在以下签名失败的错误码，请根据实际情况处理

错误代码	错误描述
AuthFailure.SignatureExpire	签名过期
AuthFailure.SecretIdNotFound	密钥不存在
AuthFailure.SignatureFailure	签名错误
AuthFailure.TokenFailure	token 错误
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）

4. 签名演示

Java

```
import java.io.BufferedReader;
import java.io.InputStream;
import java.io.InputStreamReader;
import java.net.URL;
import java.text.SimpleDateFormat;
import java.util.Date;
import java.util.Map;
import java.util.TimeZone;
import java.util.TreeMap;
import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;
import javax.net.ssl.HttpsURLConnection;
import javax.xml.bind.DatatypeConverter;

import org.apache.commons.codec.digest.DigestUtils;

public class CloudAPITC3Demo {
    private final static String CHARSET = "UTF-8";
    private final static String ENDPOINT = "cvm.finance.cloud.tencent.com";
    private final static String PATH = "/";
    private final static String SECRET_ID = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE";
    private final static String SECRET_KEY = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE";
    private final static String CT_X_WWW_FORM_URLENCODED = "application/x-www-form-urlencode
d";
    private final static String CT_JSON = "application/json";
```

```
    private final static String CT_FORM_DATA = "multipart/form-data";

    public static byte[] sign256(byte[] key, String msg) throws Exception {
        Mac mac = Mac.getInstance("HmacSHA256");
        SecretKeySpec secretKeySpec = new SecretKeySpec(key, mac.getAlgorithm());
        mac.init(secretKeySpec);
        return mac.doFinal(msg.getBytes(CHARSET));
    }

    public static void main(String[] args) throws Exception {
        String service = "cvm";
        String host = "cvm.finance.cloud.tencent.com";
        String region = "shjr";
        String action = "DescribeInstances";
        String version = "2017-03-12";
        String algorithm = "TC3-HMAC-SHA256";
        String timestamp = "1539084154";
        //String timestamp = String.valueOf(System.currentTimeMillis() / 1000);
        SimpleDateFormat sdf = new SimpleDateFormat("yyyy-MM-dd");
        // 注意时区，否则容易出错
        sdf.setTimeZone(TimeZone.getTimeZone("UTC"));
        String date = sdf.format(new Date(Long.valueOf(timestamp + "000")));

        // ************* 步骤 1：拼接规范请求串 *************
        String httpRequestMethod = "GET";
        String canonicalUri = "/";
        String canonicalQueryString = "Limit=10&Offset=0";
        String canonicalHeaders = "content-type:application/x-www-form-urlencoded\n" + "host:" + host
+ "\n";
        String signedHeaders = "content-type;host";
        String hashedRequestPayload = DigestUtils.sha256Hex("");
        String canonicalRequest = httpRequestMethod + "\n" + canonicalUri + "\n" + canonicalQueryStri
ng + "\n"
                + canonicalHeaders + "\n" + signedHeaders + "\n" + hashedRequestPayload;
        System.out.println(canonicalRequest);

        // ************* 步骤 2：拼接待签名字符串 *************
        String credentialScope = date + "/" + service + "/" + "tc3_request";
        String hashedCanonicalRequest = DigestUtils.sha256Hex(canonicalRequest.getBytes(CHARSET));
        String stringToSign = algorithm + "\n" + timestamp + "\n" + credentialScope + "\n" + hashedCan
onicalRequest;
        System.out.println(stringToSign);

        // ************* 步骤 3：计算签名 *************
        byte[] secretDate = sign256(("TC3" + SECRET_KEY).getBytes(CHARSET), date);
        byte[] secretService = sign256(secretDate, service);
        byte[] secretSigning = sign256(secretService, "tc3_request");
```

```
        String signature = DatatypeConverter.printHexBinary(sign256(secretSigning, stringToSign)).toLow
erCase();
        System.out.println(signature);

        // ************* 步骤 4：拼接 Authorization *************
        String authorization = algorithm + " " + "Credential=" + SECRET_ID + "/" + credentialScope + ", "
                + "SignedHeaders=" + signedHeaders + ", " + "Signature=" + signature;
        System.out.println(authorization);

        TreeMap<String, String> headers = new TreeMap<String, String>();
        headers.put("Authorization", authorization);
        headers.put("Host", host);
        headers.put("Content-Type", CT_X_WWW_FORM_URLENCODED);
        headers.put("X-TC-Action", action);
        headers.put("X-TC-Timestamp", timestamp);
        headers.put("X-TC-Version", version);
        headers.put("X-TC-Region", region);
    }
}
```

Python

```
# -*- coding: utf-8 -*-
import hashlib, hmac, json, os, sys, time
from datetime import datetime

# 密钥参数
secret_id = "AKIDz8krbsJ5yKBZQpn74WFkmLPx3EXAMPLE"
secret_key = "Gu5t9xGARNpq86cd98joQYCN3EXAMPLE"

service = "cvm"
host = "cvm.finance.cloud.tencent.com"
endpoint = "https://" + host
region = "shjr"
action = "DescribeInstances"
version = "2017-03-12"
algorithm = "TC3-HMAC-SHA256"
timestamp = 1539084154
date = datetime.utcfromtimestamp(timestamp).strftime("%Y-%m-%d")
params = {"Limit": 10, "Offset": 0}

# ************* 步骤 1：拼接规范请求串 *************
http_request_method = "GET"
canonical_uri = "/"
canonical_querystring = "Limit=10&Offset=0"
ct = "x-www-form-urlencoded"
```

```
payload = ""
if http_request_method == "POST":
    canonical_querystring = ""
    ct = "json"
    payload = json.dumps(params)
canonical_headers = "content-type:application/%s\nhost:%s\n" % (ct, host)
signed_headers = "content-type;host"
hashed_request_payload = hashlib.sha256(payload.encode("utf-8")).hexdigest()
canonical_request = (http_request_method + "\n" +
                     canonical_uri + "\n" +
                     canonical_querystring + "\n" +
                     canonical_headers + "\n" +
                     signed_headers + "\n" +
                     hashed_request_payload)
print(canonical_request)

# ************* 步骤 2：拼接待签名字符串 *************
credential_scope = date + "/" + service + "/" + "tc3_request"
hashed_canonical_request = hashlib.sha256(canonical_request.encode("utf-8")).hexdigest()
string_to_sign = (algorithm + "\n" +
                  str(timestamp) + "\n" +
                  credential_scope + "\n" +
                  hashed_canonical_request)
print(string_to_sign)

# ************* 步骤 3：计算签名 *************
# 计算签名摘要函数
def sign(key, msg):
    return hmac.new(key, msg.encode("utf-8"), hashlib.sha256).digest()
secret_date = sign(("TC3" + secret_key).encode("utf-8"), date)
secret_service = sign(secret_date, service)
secret_signing = sign(secret_service, "tc3_request")
signature = hmac.new(secret_signing, string_to_sign.encode("utf-8"), hashlib.sha256).hexdigest()
print(signature)

# ************* 步骤 4：拼接 Authorization *************
authorization = (algorithm + " " +
                 "Credential=" + secret_id + "/" + credential_scope + ", " +
                 "SignedHeaders=" + signed_headers + ", " +
                 "Signature=" + signature)
print(authorization)

# 公共参数添加到请求头部
headers = {
    "Authorization": authorization,
    "Host": host,
    "Content-Type": "application/%s" % ct,
```

```
    "X-TC-Action": action,
    "X-TC-Timestamp": str(timestamp),
    "X-TC-Version": version,
    "X-TC-Region": region,
}
```

请求结构

1. 服务地址

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 查询地域列表 查看完成的地域列表。

2. 通信协议

TCloudFinanceZone API 的所有接口均通过 HTTPS 进行通信，提供高安全性的通信通道。

3. 请求方法

支持的 HTTP 请求方法:

- POST（推荐）
- GET

POST 请求支持的 Content-Type 类型：

- application/json（推荐），必须使用 TC3-HMAC-SHA256 签名方法。
- application/x-www-form-urlencoded，必须使用 HmacSHA1 或 HmacSHA256 签名方法。
- multipart/form-data（仅部分接口支持），必须使用 TC3-HMAC-SHA256 签名方法。

GET 请求的请求包大小不得超过 32 KB。POST 请求使用签名方法为 HmacSHA1、HmacSHA256 时不得超过 1 MB。POST 请求使用签名方法为 TC3-HMAC-SHA256 时支持 10 MB。

4. 字符编码

均使用UTF-8编码。

返回结果

正确返回结果

以云服务器的接口查看实例状态列表 (DescribeInstancesStatus) 2017-03-12 版本为例，若调用成功，其可能的返回如下为：

```
{
    "Response": {
        "TotalCount": 0,
        "InstanceStatusSet": [],
        "RequestId": "b5b41468-520d-4192-b42f-595cc34b6c1c"
    }
}
```

- Response 及其内部的 RequestId 是固定的字段，无论请求成功与否，只要 API 处理了，则必定会返回。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。
- 除了固定的字段外，其余均为具体接口定义的字段，不同的接口所返回的字段参见接口文档中的定义。此例中的 TotalCount 和 InstanceStatusSet 均为 DescribeInstancesStatus 接口定义的字段，由于调用请求的用户暂时还没有云服务器实例，因此 TotalCount 在此情况下的返回值为 0， InstanceStatusSet 列表为空。

错误返回结果

若调用失败，其返回值示例如下为：

```
{
    "Response": {
        "Error": {
            "Code": "AuthFailure.SignatureFailure",
            "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
        },
        "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
    }
}
```

- Error 的出现代表着该请求调用失败。Error 字段连同其内部的 Code 和 Message 字段在调用失败时是必定返回的。
- Code 表示具体出错的错误码，当请求出错时可以先根据该错误码在公共错误码和当前接口对应的错误码列表里面查找对应原因和解决方案。

- Message 显示出了这个错误发生的具体原因，随着业务发展或体验优化，此文本可能会经常保持变更或更新，用户不应依赖这个返回值。
- RequestId 用于一个 API 请求的唯一标识，如果 API 出现异常，可以联系我们，并提供该 ID 来解决问题。

公共错误码

返回结果中如果存在 Error 字段，则表示调用 API 接口失败。 Error 中的 Code 字段表示错误码，所有业务都可能出现的错误码为公共错误码，下表列出了公共错误码。

错误码	错误描述
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。
AuthFailure.SignatureExpire	签名过期。
AuthFailure.SignatureFailure	签名错误。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。

错误码	错误描述
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

公共参数

公共参数是用于标识用户和接口鉴权目的的参数，如非必要，在每个接口单独的接口文档中不再对这些参数进行说明，但每次请求均需要携带这些参数，才能正常发起请求。

签名方法 v3

使用 TC3-HMAC-SHA256 签名方法时，公共参数需要统一放到 HTTP Header 请求头部中，如下：

参数名称	类型	必选	描述
X-TC-Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
X-TC-Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。
X-TC-Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如 1529223702。注意：如果与服务器时间相差超过5分钟，会引起签名过期错误。
X-TC-Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
Authorization	String	是	HTTP 标准身份认证头部字段，例如： TC3-HMAC-SHA256 Credential=AKIDEXAMPLE/Date/service/tc3_request, SignedHeaders=content-type;host, Signature=fe5f80f77d5fa3beca038a248ff027d0445342fe2855ddc963176630326f1024 其中， - TC3-HMAC-SHA256：签名方法，目前固定取该值； - Credential：签名凭证，AKIDEXAMPLE 是 SecretId；Date 是 UTC 标准时间的日期，取值需要和公共参数 X-TC-Timestamp 换算的 UTC 标准时间日期一致；service为产品名，必须与调用的产品域名一致，例如cvm； - SignedHeaders：参与签名计算的头部信息，content-type 和 host 为必选头部； - Signature：签名摘要。
X-TC-Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token。

签名方法 v1

使用 HmacSHA1 和 HmacSHA256 签名方法时，公共参数需要统一放到请求串中，如下

参数名称	类型	必选	描述
Action	String	是	操作的接口名称。取值参考接口文档中输入参数公共参数 Action 的说明。例如云服务器的查询实例列表接口，取值为 DescribeInstances。
Region	String	是	地域参数，用来标识希望操作哪个地域的数据。接口接受的地域取值参考接口文档中输入参数公共参数 Region 的说明。注意：某些接口不需要传递该参数，接口文档中会对此特别说明，此时即使传递该参数也不会生效。

参数名称	类型	必选	描述
Timestamp	Integer	是	当前 UNIX 时间戳，可记录发起 API 请求的时间。例如1529223702，如果与当前时间相差过大，会引起签名过期错误。
Nonce	Integer	是	随机正整数，与 Timestamp 联合起来，用于防止重放攻击。
SecretId	String	是	在云API密钥上申请的标识身份的 SecretId，一个 SecretId 对应唯一的 SecretKey ，而 SecretKey 会用来生成请求签名 Signature。
Signature	String	是	请求签名，用来验证此次请求的合法性，需要用户根据实际的输入参数计算得出。具体计算方法参见接口鉴权文档。
Version	String	是	操作的 API 的版本。取值参考接口文档中入参公共参数 Version 的说明。例如云服务器的版本 2017-03-12。
SignatureMethod	String	否	签名方式，目前支持 HmacSHA256 和 HmacSHA1。只有指定此参数为 HmacSHA256 时，才使用 HmacSHA256 算法验证签名，其他情况均使用 HmacSHA1 验证签名。
Token	String	否	临时证书所用的 Token ，需要结合临时密钥一起使用。临时密钥和 Token 需要到访问管理服务调用接口获取。长期密钥不需要 Token 。

地域列表

地域（Region）是指物理的数据中心的地理区域。TCloudFinanceZone交付验证不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您选择最靠近您客户的地域。

您可以通过 API接口 查询地域列表 查看完成的地域列表。

其他接口
增加自定义规则

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

增加自定义规则

默认接口请求频率限制：20次/秒。

接口更新时间：2020-03-18 16:51:56。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddCustomRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Name	是	否	String	规则名称 示例值：
SortId	是	否	String	优先级 示例值：
Redirect	否	否	String	如果动作是重定向，则表示重定向的地址；其他情况可以为空 示例值：
ExpireTime	是	否	String	过期时间 示例值：
Strategies	是	否	Array of Strategy	策略详情 示例值：查看

参数名称	必选	允许NULL	类型	描述
Domain	是	否	String	需要添加策略的域名 示例值：
ActionType	是	否	String	动作类型 示例值：
Edition	否	否	String	"clb-waf"或者"sparta-waf" 示例值：
Bypass	否	否	String	放行的详情 示例值：

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取系统版本

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取系统版本

默认接口请求频率限制：20次/秒。

接口更新时间：2020-09-17 15:41:10。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeApiVersion
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。

3. 输出参数

参数名称	类型	描述
VersionData	String	系统版本 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
ResourceInsufficient	资源不足。
UnauthorizedOperation	未授权操作。
FailedOperation	操作失败。
InvalidParameterValue	参数取值错误。
ResourceInUse	资源被占用。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
ResourcesSoldOut	资源售罄。
UnknownParameter	未知参数错误。

获取规则版本

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取规则版本

默认接口请求频率限制：20次/秒。

接口更新时间：2020-09-18 15:13:19。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRuleVersion
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Page	是	否	Uint64	分页 示例值：
Rows	是	否	Uint64	分页 示例值：

3. 输出参数

参数名称	类型	描述
RuleVersionData	Array of RuleVersionData	出参 示例值：查看
RuleCount	Uint64	分页 示例值：

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。
InvalidParameter	参数错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
ResourceInsufficient	资源不足。
UnauthorizedOperation	未授权操作。
FailedOperation	操作失败。
InvalidParameterValue	参数取值错误。
ResourceInUse	资源被占用。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
ResourcesSoldOut	资源售罄。
UnknownParameter	未知参数错误。

waf获取白名单列表

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

waf获取白名单列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-09-16 10:28:08。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWhiteByKey
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Keys	是	否	String	参数 示例值：

3. 输出参数

参数名称	类型	描述
Data	String	白名单列表 示例值：
ErrData	String	错误信息 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
UnauthorizedOperation	未授权操作。
FailedOperation	操作失败。
InvalidParameter	参数错误。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceInUse	资源被占用。
ResourceUnavailable	资源不可用。
ResourcesSoldOut	资源售罄。
UnknownParameter	未知参数错误。
InternalError	内部错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。

购买WAF

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

用于购买waf服务

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-07 17:27:26。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：WafCreateResourceAfterPay
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RegionId	否	否	String	区域 示例值：
PayMode	否	否	String	购买模式 示例值：
Pid	否	否	String	pid 示例值：
InterfaceName	否	否	String	接口名 示例值：
Type	否	否	String	类型 示例值：
ProjectId	否	否	String	项目id 示例值：

参数名称	必选	允许NULL	类型	描述
GoodsNum	否	否	String	goodsnum 示例值：

3. 输出参数

参数名称	类型	描述
Code	Uint64	状态码 示例值：
CodeDesc	String	状态码解释 示例值：
Data	String	返回数据 示例值：
Message	String	消息 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound	资源不存在。
UnauthorizedOperation	未授权操作。
FailedOperation	操作失败。
InvalidParameterValue	参数取值错误。
MissingParameter	缺少参数错误。
ResourceInsufficient	资源不足。
UnknownParameter	未知参数错误。
InternalError	内部错误。

错误码	描述
InvalidParameter	参数错误。
ResourcesSoldOut	资源售罄。
LimitExceeded	超过配额限制。
ResourceUnavailable	资源不可用。

WafGetDomainEngineType

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取域名使用的规则引擎类型

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 18:01:16。

接口只验签名不鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：WafGetDomainEngineType
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domains	是	否	Array of String	域名数组 示例值：

3. 输出参数

参数名称	类型	描述
CodeDesc	String	返回码信息 示例值：
Message	String	返回信息 示例值：
Data	Array of WafGetDomainEngineTypeData	引擎数据 示例值：查看

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

日志服务相关接口
创建攻击日志下载任务

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

创建攻击日志下载任务

默认接口请求频率限制：20次/秒。

接口更新时间：2020-02-17 16:54:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CreateAttackDownloadTask
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名，所有域名填写all 示例值：
FromTime	是	否	Datetime	查询起始时间 示例值：
ToTime	是	否	Datetime	查询结束时间 示例值：
Name	是	否	String	下载任务名字 示例值：
RiskLevel	否	否	Uint64	风险等级 示例值：
Status	否	否	Uint64	拦截状态 示例值：

参数名称	必选	允许NULL	类型	描述
RuleId	否	否	Uint64	自定义策略ID 示例值：
AttackIp	否	否	String	攻击者IP 示例值：
AttackType	否	否	String	攻击类型 示例值：

3. 输出参数

参数名称	类型	描述
Flow	String	任务ID 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

删除下载记录

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

删除下载记录

默认接口请求频率限制：20次/秒。

接口更新时间：2020-03-20 17:24:26。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteDownloadRecord
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Flow	是	否	String	记录id 示例值：

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述

错误码	描述
InternalError	内部错误。

防护设置相关接口
增加规则引擎白名单

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

增加规则引擎白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 16:16:18。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：AddUserWhiteRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RuleId	否	否	Uint64	规则序号 示例值：
Domain	是	否	String	域名 示例值：
SignatureId	是	否	String	规则Id 示例值：
Status	是	否	Uint64	规则状态 示例值：
Rules	是	否	Array of GlobalWhiteCond	匹配规则项列表 示例值：查看

参数名称	必选	允许NULL	类型	描述
Name	否	否	String	规则名称 示例值：

3. 输出参数

参数名称	类型	描述
RuleId	Uint64	规则总数 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

查询用户白名单名字重复

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

查询用户白名单名字重复

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 16:16:43。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：CheckUserWhiteRuleName
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Name	是	否	String	名字 示例值：
Domain	是	否	String	域名 示例值：

3. 输出参数

参数名称	类型	描述
Duplicate	Int64	是否重复 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

Waf 会话定义 Delete接口

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

Waf 会话定义 Delete接口

默认接口请求频率限制：20次/秒。

接口更新时间：2020-03-20 15:29:57。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteSession
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
Edition	否	否	String	clb-waf 或者 sprta-waf 示例值：

3. 输出参数

参数名称	类型	描述
Data	String	结果 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

删除全局白名单

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

删除全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 16:15:23。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DeleteUserWhiteRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
Ids	是	否	Array of Uint64	ID列表 示例值：

3. 输出参数

参数名称	类型	描述
FailIds	Array of Uint64	失败id列表 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取自定义策略列表

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取自定义策略列表

默认接口请求频率限制：20次/秒。

接口更新时间：2020-03-18 16:51:37。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeCustomRules
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
Edition	否	否	String	clb-waf或者sparta-waf 示例值：
Paging	是	否	DescribeCustomRulesPagingInfo	分页参数 示例值：查看
ActionType	否	否	String	过滤参数：动作类型：0放行，1阻断，2人机识别，3观察，4重定向 示例值：
Search	否	否	String	过滤参数：规则名称过滤条件 示例值：

3. 输出参数

参数名称	类型	描述
RuleList	Array of DescribeCustomRulesRspRuleListItem	规则详情 示例值：查看
TotalCount	String	规则条数 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

获取主类及子类信息

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取主类及子类信息

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-13 11:20:08。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeMainClass
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Offset	是	否	Uint64	分页 示例值：
Limit	是	否	Uint64	每页容量 示例值：
Filters	否	否	Array of FiltersItemNew	筛选条件，支持 MainClassID 示例值：查看

3. 输出参数

参数名称	类型	描述
Total	Uint64	主类的总数 示例值：

参数名称	类型	描述
MainClass	Array of MainClassItem	主类的详细信息 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取特征规则更新动态

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取特征规则更新动态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-12-07 15:46:18。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeRuleUpdateLog
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Order	否	否	String	排序方式 示例值：
Offset	否	否	Uint64	偏移量 示例值：
Limit	否	否	Uint64	分页 示例值：

3. 输出参数

参数名称	类型	描述
Total	Uint64	总数 示例值：

参数名称	类型	描述
List	Array of RuleUpdateLog	日志详细 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取用户规则引擎类型

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取用户规则引擎类型Tiga

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 16:14:43。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUserEngineType
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	否	否	String	域名 示例值：

3. 输出参数

参数名称	类型	描述
Type	Uint64	0：menshen 1: Tiga 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取用户防护规则等级

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取用户防护规则等级

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-13 10:58:58。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUserLevel
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：

3. 输出参数

参数名称	类型	描述
Level	Uint64	300:正常 400:严格 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取用户特征规则列表

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取用户特征规则列表Tiga

默认接口请求频率限制：20次/秒。

接口更新时间：2022-10-17 17:50:25。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUserSignatureRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	需要查询的域名 示例值：
By	否	否	String	排序字段，支持 signature_id, modify_time 示例值：
Order	否	否	String	排序方式 示例值：
Offset	是	否	Uint64	分页 示例值：
Limit	是	否	Uint64	每页容量 示例值：
Filters	否	否	Array of FiltersItemNew	筛选条件，支持 MainClassName，SubClassID ,CveID, Status, ID；ID为规则id 示例值：查看

3. 输出参数

参数名称	类型	描述
Total	Uint64	规则总数 示例值：
Rules	Array of UserSignatureRule	规则列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获取全局白名单

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获取全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 16:15:51。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeUserWhiteRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
Offset	否	否	Uint64	分页偏移 示例值：
Limit	是	否	Uint64	分页 示例值：
By	否	否	String	排序 示例值：
Order	否	否	String	升序/降序 示例值：
Filters	否	否	Array of FiltersItemNew	过滤条件，支持SignatureId，Status，Target，TargetValue 示例值：查看

3. 输出参数

参数名称	类型	描述
Total	Uint64	总数 示例值：
List	Array of UserWhiteRule	全局规则列表 示例值：查看
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

获得webshell切换状态

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

获得webshell切换状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-04-06 10:57:30。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：DescribeWebshellEnable
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	否	否	String	域名 示例值：

3. 输出参数

参数名称	类型	描述
Code	Uint64	返回状态 示例值：
Data	Uint64	状态 示例值：
Msg	String	返回信息 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
ResourceNotFound	资源不存在。
UnauthorizedOperation	未授权操作。
FailedOperation	操作失败。
InvalidParameterValue	参数取值错误。
MissingParameter	缺少参数错误。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourcesSoldOut	资源售罄。
UnknownParameter	未知参数错误。
ResourceUnavailable	资源不可用。
InvalidParameter	参数错误。
LimitExceeded	超过配额限制。
InternalError	内部错误。

切换自定义规则的开关

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

切换自定义规则的开关

默认接口请求频率限制：20次/秒。

接口更新时间：2020-02-24 11:15:08。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyCustomRuleStatus
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
RuleId	是	否	Uint64	规则ID 示例值：
Status	是	否	Uint64	开关的状态，1是开启、0是关闭 示例值：
Edition	否	否	String	WAF的版本，clb-waf代表负载均衡WAF、sparta-waf代表SaaS WAF，默认是sparta-waf。 示例值：

3. 输出参数

参数名称	类型	描述

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

以下仅列出了接口业务逻辑相关的错误码，其他错误码详见公共错误码。

错误码	描述
InternalError	内部错误。

修改用户防护规则等级

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

修改用户防护规则等级

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-13 11:02:03。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyUserLevel
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
Level	是	否	Uint64	防护规则等级 300=standard，400=extended 示例值：

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

修改用户防护规则

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

修改用户防护规则

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-13 11:11:37。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyUserSignatureRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	是	否	String	域名 示例值：
MainClassID	否	否	String	主类id 示例值：
Status	否	否	Int64	主类开关0=关闭，1=开启，2=只告警 示例值：
RuleID	否	否	Array of ReqUserRule	下发修改的规则列表 示例值：查看

3. 输出参数

参数名称	类型	描述
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

变更全局白名单

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

变更全局白名单

默认接口请求频率限制：20次/秒。

接口更新时间：2023-01-04 16:17:11。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyUserWhiteRule
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
RuleId	是	否	Uint64	全局规则ID 示例值：
Name	否	否	String	规则名称 示例值：
Domain	是	否	String	域名 示例值：
SignatureId	是	否	String	规则id 示例值：
Status	否	否	Uint64	规则状态 示例值：
Rules	是	否	Array of GlobalWhiteCond	规则详细信息 示例值：查看

3. 输出参数

参数名称	类型	描述
RuleId	Uint64	全局规则id 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

切换webshell切换状态

1. 接口描述

接口请求域名： waf.api3.finance.cloud.tencent.com。

切换webshell切换状态

默认接口请求频率限制：20次/秒。

接口更新时间：2022-04-06 10:57:11。

接口既验签名又鉴权。

2. 输入参数

以下请求参数列表仅列出了接口请求参数和部分公共参数，完整公共参数列表见公共请求参数。

参数名称	必选	允许NULL	类型	描述
Action	是	否	String	公共参数，本接口取值：ModifyWebshellEnable
Version	是	否	String	公共参数，本接口取值：2018-01-25
Region	是	否	String	公共参数，地域信息本接口不需要传递此参数。
Domain	否	否	String	域名 示例值：
Status	否	否	Uint64	状态 示例值：

3. 输出参数

参数名称	类型	描述
Code	Uint64	返回码 示例值：
Msg	String	消息 示例值：
RequestId	String	唯一请求 ID，每次请求都会返回。定位问题时需要提供该次请求的 RequestId。

4. 错误码

该接口暂无业务逻辑相关的错误码，其他错误码详见公共错误码。

数据结构

ActionedIpItem

ip查询参数

被如下接口引用：DescribeActionedIp

名称	必选	允许NULL	类型	描述
Action	是	否	Uint64	动作 示例值：
Category	是	否	String	类别 示例值：
Ip	是	否	String	ip 示例值：
Name	是	否	String	策略名称 示例值：
Note	是	否	String	备注 示例值：
TsVersion	是	否	Uint64	更新时间戳 示例值：
ValidTs	是	否	Uint64	有效时间戳 示例值：

DescribeAntiInfoLeakRulesRuleItem

DescribeAntiInfoLeakRules返回的规则列表元素

被如下接口引用：DescribeAntiInfoLeakRules

名称	必选	允许NULL	类型	描述
RuleId	是	否	String	规则ID 示例值：
Name	是	否	String	规则名称 示例值：

名称	必选	允许NULL	类型	描述
Status	是	否	String	规则状态 示例值：
ActionType	是	否	String	规则动作类型 示例值：
CreateTime	是	否	String	规则创建时间 示例值：
Strategies	是	否	Array of DescribeAntiInfoLeakRulesStrategyItem	详细的规则 示例值：查看

MonitorDomainItem

云监控域名字段

被如下接口引用：DescribeMonitorDomains

名称	必选	允许NULL	类型	描述
Domain	是	否	String	域名 示例值：
Appid	是	否	Uint64	用户自己的Appid 示例值：
Edition	是	否	Int64	域名对应的版本信息，0代表saas，1代表clb 示例值：
DomainId	是	否	String	域名ID 示例值：

PageInfoForInt

分页参数复杂结构体

被如下接口引用：DescribeDNSDetectDomainList

名称	必选	允许NULL	类型	描述
PageNumber	是	否	Uint64	页码 示例值：
PageSize	是	否	Uint64	每页个数 示例值：

SearchLogsSimpleRsp

SearchLogsSimple的返回值

被如下接口引用：DescribeAccessLogs

名称	必选	允许NULL	类型	描述
Code	是	否	Int64	是否成功执行，0表示成功执行 示例值：
Count	是	否	Int64	日志的数目 示例值：
Context	是	否	String	日志的内容，可以用作游标 示例值：
Data	是	否	Array of String	具体的日志内容 示例值：

StatisticType

攻击类型统计

被如下接口引用：DescribeStatisticTypes

名称	必选	允许NULL	类型	描述
Type	是	否	String	攻击类型 示例值：
Count	是	否	Int64	攻击类型数目 示例值：

SearchItem

接入列表查询复杂条件

被如下接口引用：DescribeHosts

名称	必选	允许NULL	类型	描述
ClsStatus	否	否	String	日志开关 示例值：

名称	必选	允许NULL	类型	描述
Status	否	否	String	waf开关 示例值：
FlowMode	否	否	String	流量模式 示例值：

DescribeAntiInfoLeakRulesStrategyItem

DescribeAntiInfoLeakRules返回的规则元素中的具体的规则元素

被如下接口引用：DescribeAntiInfoLeakRules

名称	必选	允许NULL	类型	描述
Field	是	否	String	字段 示例值：
CompareFunc	是	否	String	条件 示例值：
Content	是	否	String	内容 示例值：

DomainPackage

clb-waf 域名扩展套餐

被如下接口引用：DescribeUserInfo

名称	必选	允许NULL	类型	描述
ResourceIds	是	否	String	资源ID 示例值：
ValidTime	是	否	String	过期时间 示例值：
AutoRenew	是	否	Uint64	是否自动续费，1：自动续费，0：不自动续费 示例值：
Count	是	否	Uint64	套餐购买个数 示例值：
Region	是	否	String	套餐购买地域，clb-waf暂时没有用到 示例值：

DescribePieChartRsp

DescribePieChart的返回值

被如下接口引用：DescribePieChart

名称	必选	允许NULL	类型	描述
Piechart	是	是	Array of String	详细的内容 示例值：

DescribeBotUCBFeatureRuleRsp

DescribeBotUCBFeatureRule的返回参数

被如下接口引用：DescribeBotUCBFeatureRule

名称	必选	允许NULL	类型	描述
TotalCount	是	否	Int64	规则数目 示例值：
Res	是	否	Array of String	详细的规则 示例值：

PortItem

防护域名端口配置信息

被如下接口引用：AddSpartaProtection、DescribeSpartaProtectionInfo、DescribeSpartaProtectionList

名称	必选	允许NULL	类型	描述
Port	是	否	String	监听端口配置 示例值：
Protocol	是	否	String	与Port一一对应，表示端口对应的协议 示例值：
UpstreamPort	是	否	String	与Port一一对应，表示回源端口 示例值：
UpstreamProtocol	是	否	String	与Port一一对应，表示回源协议 示例值：

名称	必选	允许NULL	类型	描述
NginxServerId	是	否	String	Nginx的服务器ID 示例值：

WebshellStatus

域名的webshell开启状态

被如下接口引用：ModifyWebshellStatus

名称	必选	允许NULL	类型	描述
Domain	是	否	String	域名 示例值：
Status	是	否	Uint64	webshell开关，1：开。0：关。2：观察 示例值：

MenshenDomainRule

门神域名规则列表

被如下接口引用：DescribeDomainRules

名称	必选	允许NULL	类型	描述
Id	是	是	Uint64	Id 示例值：
Type	是	是	String	规则类型 示例值：
Level	是	是	String	等级 示例值：
Description	是	是	String	描述 示例值：
CVE	是	是	String	CVE 示例值：
Status	是	是	String	状态 示例值：
ModifyTime	是	是	Datetime	修改时间 示例值：

名称	必选	允许NULL	类型	描述
TypeEn	是	是	String	规则类型英文 示例值：
LevelEn	是	是	String	等级英文 示例值：
DescriptionEn	是	是	String	描述英文 示例值：

FiltersItemNew

实例入参过滤器

被如下接口引用：DescribeMainClass、DescribeUserSignatureRule、DescribeUserWhiteRule

名称	必选	允许NULL	类型	描述
Name	是	否	String	字段名 示例值：
Values	是	否	Array of String	过滤值 示例值：
ExactMatch	是	否	Bool	是否精确查找 示例值：

HostStatus

设置WAF状态的结构体

被如下接口引用：ModifyHostStatus

名称	必选	允许NULL	类型	描述
Domain	是	否	String	域名 示例值：
DomainId	是	否	String	域名ID 示例值：
Status	是	否	Uint64	WAF的开关，1：开，0：关 示例值：

Protection

域名配置信息

被如下接口引用：DescribeSpartaProtectionList

名称	必选	允许NULL	类型	描述
Domain	是	否	String	域名 示例值：
DomainId	是	否	String	域名Id 示例值：
Cname	是	否	String	cname地址 示例值：
Status	是	否	String	waf开关 0表示关闭, 1表示开启 示例值：
State	是	否	String	防护状况：0 正常防护　1 未检测到流量　2 即将到期　3 已到期 示例值：
CreateTime	是	否	String	域名创建时间 示例值：
Mode	是	否	String	防御模式 示例值：
Engine	是	否	String	AI防御模式 示例值：
Vip	是	否	Array of String	接入IP列表 示例值：
IsGray	是	否	String	灰度标识，1灰度0不灰度 示例值：
GrayAreas	是	否	Array of String	灰度区域，不灰传no 示例值：
CertType	是	否	String	证书类型，1表示自有证书，2表示腾讯云托管证书 示例值：
Cert	是	否	String	证书内容 示例值：
PrivateKey	是	否	String	证书私钥 示例值：

名称	必选	允许NULL	类型	描述
SSLId	是	否	String	腾讯云托管证书id，当certType=2时有效 示例值：
IsCdn	是	否	String	1有cdn，0无cdn 示例值：
IsHttp2	是	否	String	1开启http2，0不开启 示例值：
IsWebsocket	是	否	String	1开启websocket，0不开启 示例值：
HttpsRewrite	是	否	String	是否http强制跳转https，"1" 是、"0" 否 示例值：
HttpsUpstreamPort	是	否	String	https回源端口 示例值：
UpstreamType	是	否	String	回源方式，"0"为ip回源，"1"为域名回源 示例值：
UpstreamDomain	是	否	String	回源域名 示例值：
UpstreamScheme	是	否	String	回源协议 示例值：
Cls	是	否	String	日志包 示例值：
CCList	是	否	Array of String	CC列表 示例值：
LoadBalance	是	否	String	负载均衡算法，0表示轮询，1表示ip hash，默认为0 示例值：
Ports	是	否	Array of PortItem	服务端口配置 示例值：查看
RsList	是	否	Array of String	回源ip 示例值：
SrcList	是	否	Array of String	ip列表 示例值：

CacheUrlItem

防篡改url元素

被如下接口引用：DescribeAntiFakeUrl

名称	必选	允许NULL	类型	描述
Id	是	否	String	Id 示例值：
Name	是	否	String	名称 示例值：
Domain	是	否	String	域名 示例值：
Uri	是	否	String	uri 示例值：
Protocol	是	否	String	协议 示例值：
Status	是	否	String	状态 示例值：

DownloadRecordItem

下载记录

被如下接口引用：DescribeAttackDownloadRecords

名称	必选	允许NULL	类型	描述
Name	是	否	String	任务名 示例值：
Flow	是	否	String	任务ID 示例值：
Host	是	否	String	任务对应域名 示例值：
CreateTime	是	否	Datetime	任务创建时间 示例值：
ExpireTime	是	否	Datetime	任务过期时间 示例值：
Count	是	否	Uint64	任务涉及的记录条数 示例值：

名称	必选	允许NULL	类型	描述
Status	是	否	Uint64	任务运行状态，0运行中，1完成，2失败 示例值：
Url	是	否	String	任务结果的下载地址 示例值：
Id	是	否	Uint64	数据库自增ID 示例值：

ResponseCode

响应体的返回码

被如下接口引用：DeleteHost、DescribeHostLimit、ModifyHostFlowMode、ModifyHostMode、ModifyHostStatus、ModifyPackageRenew、ModifyWebshellStatus

名称	必选	允许NULL	类型	描述
Code	是	否	String	如果成功则返回Success，失败则返回yunapi定义的错误码 示例值：
Message	是	否	String	如果成功则返回Success，失败则返回WAF定义的二级错误码 示例值：

SpartaProtectionPort

waf斯巴达-编辑防护域名中的端口结构

被如下接口引用：ModifySpartaProtection

名称	必选	允许NULL	类型	描述
NginxServerId	是	否	Uint64	nginx Id 示例值：
Port	是	否	String	端口 示例值：
Protocol	是	否	String	协议 示例值：
UpstreamPort	是	否	String	后端端口 示例值：

名称	必选	允许NULL	类型	描述
UpstreamProtocol	是	否	String	后端协议 示例值：

IpAccessControlData

数据封装

被如下接口引用：DescribeIpAccessControl

名称	必选	允许NULL	类型	描述
Res	是	是	Array of IpAccessControlItem	ip黑白名单 示例值：查看
TotalCount	是	否	Uint64	计数 示例值：

PageInfo

公共翻页参数

被如下接口引用：DescribeAntiFakeUrl、DescribeAntiInfoLeakRules、DescribeCachePath、DescribeDNSDetectHijackData

名称	必选	允许NULL	类型	描述
PageNumber	是	否	String	页码 示例值：
PageSize	是	否	String	页条目数量 示例值：

IpHitItem

ip封堵状态数据

被如下接口引用：DescribeIpHitItems

名称	必选	允许NULL	类型	描述
Action	是	否	Uint64	动作 示例值：

名称	必选	允许NULL	类型	描述
Category	是	否	String	类别 示例值：
Ip	是	否	String	ip 示例值：
Name	是	否	String	规则名称 示例值：
TsVersion	是	否	Uint64	时间戳 示例值：
ValidTs	是	否	Uint64	有效截止时间戳 示例值：

BotTcbRuleData

封装使用

被如下接口引用：DescribeBotTCBRule

名称	必选	允许NULL	类型	描述
Res	是	否	Array of String	tcb规则 示例值：

BotUCBPreinstallRuleData

BotUCBPreinstallRule封装

被如下接口引用：DescribeBotUCBPreinstallRule

名称	必选	允许NULL	类型	描述
Res	是	否	Array of BotUCBPreinstallRule	参数封装 示例值：查看

CopyBotsUCBFeatureRuleRsp

CopyBotsUCBFeatureRule的返回值

被如下接口引用：CopyBotUCBFeatureRules

名称	必选	允许NULL	类型	描述
Code	是	否	Int64	0表示成功，其他表示失败 示例值：
ErrMsg	是	否	String	错误信息 示例值：
SuccessNum	是	否	Int64	成功的数目 示例值：
FailedNum	是	否	Int64	失败的数目 示例值：
T	是	否	Array of String	成功的域名列表 示例值：

LoadBalancer

负载均衡的监听器

被如下接口引用：CreateHost、DescribeHost、DescribeHosts、DescribeWafInfo、ModifyHost

名称	必选	允许NULL	类型	描述
LoadBalancerId	是	否	String	负载均衡LD的ID 示例值：
LoadBalancerName	是	否	String	负载均衡LD的名称 示例值：
ListenerId	是	否	String	负载均衡监听器的ID 示例值：
ListenerName	是	否	String	负载均衡监听器的名称 示例值：
Vip	是	否	String	负载均衡实例的IP 示例值：
Vport	是	否	Uint64	负载均衡实例的端口 示例值：
Region	是	否	String	负载均衡LD的地域 示例值：
Protocol	是	否	String	监听器协议，http、https 示例值：

名称	必选	允许NULL	类型	描述
Zone	是	否	String	负载均衡监听器所在的zone 示例值：
NumericalVpcId	是	是	Int64	网络 示例值：
LoadBalancerType	是	是	String	网络类型 示例值：

ClsPackage

clb-waf 日志套餐

被如下接口引用：DescribeSpartUserInfo、DescribeUserInfo

名称	必选	允许NULL	类型	描述
ResourceIds	是	否	String	资源ID 示例值：
ValidTime	是	否	String	过期时间 示例值：
AutoRenew	是	否	Int64	是否自动续费，1：自动续费，0：不自动续费 示例值：
Count	是	否	Int64	套餐个数 示例值：
Region	是	否	String	地域，目前在clb-waf中没有用到 示例值：

RuleUpdateLog

tiga引擎规则更新动态日志

被如下接口引用：DescribeRuleUpdateLog

名称	必选	允许NULL	类型	描述
Id	否	否	Uint64	id值 示例值：
CreateTime	否	否	Datetime_iso	创建时间 示例值：

名称	必选	允许NULL	类型	描述
ModifyTime	否	否	Datetime_iso	修改时间 示例值：
Detail	否	否	String	详细修改动态 示例值：
Language	否	否	String	en/cn 描述信息语言 示例值：
LogVersion	否	否	String	版本信息 示例值：

CCRuleData

数据封装

被如下接口引用：DescirbeCCRule

名称	必选	允许NULL	类型	描述
Res	是	否	Array of CCRuleItem	cc规则 示例值：查看
TotalCount	是	否	Int64	规则数目 示例值：

AttackDetail

攻击详情数据类型

被如下接口引用：DescribeAttackDetail

名称	必选	允许NULL	类型	描述
ArgsName	是	否	String	攻击命中位置 示例值：
AttackContent	是	否	String	攻击命中的内容 示例值：
AttackIp	是	否	String	攻击者IP 示例值：
AttackTime	是	否	String	攻击时间 示例值：

名称	必选	允许NULL	类型	描述
AttackType	是	否	String	攻击类型 示例值：
Count	是	否	Uint64	攻击聚合次数 示例值：
Domain	是	否	String	被攻击的域名 示例值：
HttpLog	是	否	String	原始请求字符串 示例值：
IpinfoCity	是	是	String	攻击者城市 示例值：
IpinfoDetail	是	否	String	攻击者运营商 示例值：
IpinfoDimensionality	是	是	Float	经度 示例值：
IpinfoLongitude	是	是	Float	纬度 示例值：
IpinfoIsp	是	否	String	线路 示例值：
IpinfoNation	是	否	String	国家 示例值：
IpinfoProvince	是	否	String	省份 示例值：
IpinfoState	是	否	String	国家简称 示例值：
Method	是	否	String	HTTP方法 示例值：
RiskLevel	是	否	Uint64	风险等级 示例值：
RuleId	是	否	Uint64	规则ID 示例值：
Status	是	否	Uint64	拦截状态，0是观察，1是放行 示例值：

名称	必选	允许NULL	类型	描述
Uri	是	否	String	攻击的Uri 示例值：
UserAgent	是	否	String	攻击者浏览器User Agent 示例值：
Uuid	是	否	String	请求ID 示例值：
RuleName	是	否	String	如果是自定义规则，则显示规则的名字，如果不是则为- 示例值：

MenshenDomainWhiteRule

门神-白名单规则列表

被如下接口引用：DescribeDomainWhiteRules

名称	必选	允许NULL	类型	描述
Id	是	是	Uint64	Id 示例值：
Rules	是	是	Array of Uint64	规则id列表 示例值：
Url	是	是	String	地址 示例值：
Function	是	是	String	比较方法 示例值：
Status	是	是	Uint64	状态 示例值：
Time	是	是	Datetime	时间 示例值：

BotListStat

bot列表的stat数据

被如下接口引用：DescribeBotTCBRecords、DescribeBotUBRecords、DescribeBotUCBRecords

名称	必选	允许NULL	类型	描述
AvgSpeed	是	否	Float	平均速度 示例值：

HostRecord

clb-waf防护域名

被如下接口引用：CreateHost、DescribeHost、DescribeHosts、ModifyHost

名称	必选	允许NULL	类型	描述
Domain	是	否	String	域名 示例值：
DomainId	是	否	String	域名ID 示例值：
MainDomain	是	否	String	主域名，入参时为空 示例值：
Mode	是	否	Uint64	waf模式，同saas waf保持一致 示例值：
Status	是	否	Uint64	waf和LD的绑定，0：没有绑定，1：绑定 示例值：
State	是	否	Uint64	域名状态，0：正常，1：未检测到流量，2：即将过期，3：过期 示例值：
Engine	是	否	Uint64	使用的规则，同saas waf保持一致 示例值：
IsCdn	是	否	Uint64	是否开启代理，0：不开启，1：开启 示例值：
LoadBalancerSet	是	否	Array of LoadBalancer	绑定的LB列表 示例值：查看
Region	是	否	String	域名绑定的LB的地域，以,分割多个地域 示例值：
Edition	是	否	String	产品分类，取值为：sparta-waf、clb-waf、cdn-waf 示例值：

名称	必选	允许NULL	类型	描述
FlowMode	是	否	Uint64	WAF的流量模式，1：清洗模式，0：镜像模式 示例值：
ClsStatus	是	否	Uint64	是否开启访问日志，1：开启，0：关闭 示例值：
NetworkType	是	否	String	网络类型 示例值：
Level	是	否	Uint64	门神防护等级 示例值：

BotListScore

拨通列表得分字段

被如下接口引用：DescribeBotTCBRecords、DescribeBotUBRecords、DescribeBotUCBRecords

名称	必选	允许NULL	类型	描述
Total	是	否	Int64	得分 示例值：

DomainBotStatusData

封装参数

被如下接口引用：DescribeBotStatus

名称	必选	允许NULL	类型	描述
Res	是	否	Array of DomainBotStatus	数据 示例值：查看

PeakPointsItem

PeakPoints数组项

被如下接口引用：DescribePeakPoints

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
Time	是	否	Uint64	秒级别时间戳 示例值：
Access	是	否	Uint64	QPS 示例值：
Up	是	否	Uint64	上行带宽峰值，单位B 示例值：
Down	是	否	Uint64	下行带宽峰值，单位B 示例值：
Attack	是	否	Uint64	Web攻击次数 示例值：
Cc	是	否	Uint64	CC攻击次数 示例值：

PiechartItem

饼图数据类型

被如下接口引用：DescribeAttackType

名称	必选	允许NULL	类型	描述
Type	是	否	String	类型 示例值：
Count	是	否	Uint64	数量 示例值：

SessionItem

session定义

被如下接口引用：DescribeSession

名称	必选	允许NULL	类型	描述
Category	是	否	String	匹配类型 示例值：
KeyOrStartMat	是	否	String	起始模式 示例值：

名称	必选	允许NULL	类型	描述
EndMat	是	否	String	结束模式 示例值：
StartOffset	是	否	String	起始偏移 示例值：
EndOffset	是	否	String	结束偏移 示例值：
Source	是	否	String	数据源 示例值：
TsVersion	是	否	String	更新时间戳 示例值：

UserSignatureRule

用户特征规则描述

被如下接口引用：DescribeUserSignatureRule

名称	必选	允许NULL	类型	描述
ID	否	否	String	特征ID 示例值：
Status	否	否	Int64	规则开关 示例值：
MainClassID	否	否	String	主类ID 示例值：
SubClassID	否	否	String	子类ID 示例值：
CveID	否	否	String	CVE ID 示例值：
CreateTime	否	否	Datetime_iso	创建时间 示例值：
ModifyTime	否	否	Datetime_iso	更新时间 示例值：
MainClassName	否	否	String	主类名字，根据Language字段输出中文/英文 示例值：

名称	必选	允许NULL	类型	描述
SubClassName	否	否	String	子类名字，根据Language字段输出中文/英文，若子类id为00000000，此字段为空 示例值：
Description	否	否	String	规则描述 示例值：

DescribeAreaBanAreasRsp

DescribeAreaBanAreas接口的回包

被如下接口引用：DescribeAreaBanAreas

名称	必选	允许NULL	类型	描述
Status	是	否	String	状态 "0"：未开启地域封禁 "1"：开启地域封禁 示例值：
Areas	是	否	Array of String	字符串数据，配置的地域列表 示例值：

InstancePriceItem

商品价格询价结果

被如下接口引用：InquiryPriceWafInstance

名称	必选	允许NULL	类型	描述
Pid	是	否	Int64	商品的编码 示例值：
RealTotalCost	是	否	Int64	折扣后的价格 示例值：
TotalCost	是	否	Int64	折扣前的价格 示例值：

SubClassItem

子类信息

被如下接口引用：DescribeMainClass

名称	必选	允许NULL	类型	描述
SubClassID	否	否	String	子类id 示例值：
SubClassName	否	否	String	子类名字 示例值：
Description	否	否	String	描述 示例值：

BotItemsListItem

bot列表元素

被如下接口引用：DescribeBotTCBRecords、DescribeBotUBRecords、DescribeBotUCBRecords

名称	必选	允许NULL	类型	描述
Action	是	否	String	动作 示例值：
BotFeature	是	是	Array of String	bot特征 示例值：
Id	是	否	String	mongodb id 示例值：
Nums	是	否	Int64	数目 示例值：
RuleName	是	是	String	关联规则名称 示例值：
Score	是	否	BotListScore	得分 示例值：查看
SessionDuration	是	否	Float	持续时间 示例值：
SrcIp	是	否	String	源ip 示例值：
Stat	是	否	BotListStat	统计数据 示例值：查看
Timestamp	是	否	Uint64	时间戳 示例值：

名称	必选	允许NULL	类型	描述
TcbDetail	是	是	String	公开类型附加参数 示例值：

MenshenRuleType

门神-规则类型信息

被如下接口引用：DescribeRuleTypes

名称	必选	允许NULL	类型	描述
Id	是	是	Uint64	Id 示例值：
Name	是	是	String	规则类型名称 示例值：
Description	是	是	String	规则类型描述 示例值：
Count	是	是	Uint64	规则数量 示例值：
DescriptionEn	是	是	String	规则类型描述英文 示例值：
NameEn	是	是	String	规则类型名称英文 示例值：

BotsDomainAggStatStyledItem

GetBotsDomainAggStatStyled接口的返回数组的元素类型

被如下接口引用：DescribeBotAggregateDomainStat

名称	必选	允许NULL	类型	描述
Key	是	否	String	域名 示例值：
Value	是	否	Int64	攻击次数 示例值：

IpHitItemsData

封装参数

被如下接口引用：DescribeIpHitItems

名称	必选	允许NULL	类型	描述
Res	是	否	Array of IpHitItem	数组封装 示例值：查看
TotalCount	是	否	Uint64	总数目 示例值：

DNSDetectHijackData

DNS劫持检测的劫持记录结构体

被如下接口引用：DescribeDNSDetectHijackData

名称	必选	允许NULL	类型	描述
Domain	是	否	String	被劫持的域名 示例值：
HijackIP	是	否	String	被劫持后的IP 示例值：
Operator	是	否	String	被劫持后的IP的运营商 示例值：
HijackRegions	是	否	Uint64	被劫持的地域数 示例值：
HijackUsers	是	否	Uint64	被劫持的用户数 示例值：
AuthIP	是	否	String	权威记录 示例值：

BotRecordItem

Bot_V2 bot记录访问详情元素结构

被如下接口引用：DescribeBotRecordItems

名称	必选	允许NULL	类型	描述
Items	是	否	String	压缩的字符串 示例值：

DonwloadRecordItem

下载记录数据项

被如下接口引用：DescribeAccessDownloadRecords、DescribeAttackDownloadRecord

名称	必选	允许NULL	类型	描述
Name	是	否	String	下载任务名 示例值：
FlowId	是	否	String	任务ID 示例值：
Host	是	否	String	域名 示例值：
CreateTime	是	否	String	创建时间 示例值：
ExpireTime	是	否	String	过期时间 示例值：
Count	是	否	String	记录条数 示例值：
Status	是	否	String	下载状态 示例值：
Url	是	否	String	下载文件URL 示例值：
Id	是	否	String	记录ID 示例值：
Appid	是	否	String	产品ID 示例值：

GlobalWhiteCond

全局白名单规则项

被如下接口引用：AddUserWhiteRule、DescribeUserWhiteRule、ModifyUserWhiteRule

名称	必选	允许NULL	类型	描述
Target	是	否	String	匹配目标，HTTP-Method,Host,URI,FULL-URL,Parameter,Cookie,HTTP-Header,JSON-Elements 示例值：
Operation	是	否	String	匹配操作，String-Match 字符串匹配，支持通配符，例如/floder1/ */floder1//*index.htm；Regular-Expression-Match 正则表达式匹配， Include 包含（HTTP-Method），Exclude 不包含（HTTP-Method） 示例值：
HttpMethodList	否	否	Array of String	方法列表，"GET", "POST", "HEAD" 示例值：
Name	否	否	String	变量名称, 适用于Parameter,Cookie,HTTP-Header,JSON-Elements 示例值：
CheckValue	否	否	Uint64	是否检查变量值，0:disable, 1: enable。 适用于Parameter,Cookie,HTTP-Header,JSON-Elements 示例值：
Value	否	否	String	变量值，适用于Host,URI,FULL-URL,Parameter,Cookie,HTTP-Header,JSON-Elements 示例值：
Concatenate	否	否	String	条件之间的链接方式，可以为AND/OR。AND 表示与上一个条件与的关系，OR表示与上一个条件是或的关系。多个条件之间的链接关系如下： C1.AND C2.AND C3.OR C4.OR C5.AND C6.AND, 则组合的逻辑关系是： c1 and (c2 or c3 or c4) and c5 and c6 示例值：

BotUCBPreinstallRule

bot内置类型自定义策略

被如下接口引用：DescribeBotUCBPreinstallRule

名称	必选	允许NULL	类型	描述
Action	是	否	String	动作 示例值：

名称	必选	允许NULL	类型	描述
AdditionArg	是	否	String	附加参数 示例值：
Name	是	否	String	名称 示例值：
OnOff	是	否	String	开关 示例值：
Timestamp	是	否	Uint64	时间戳 示例值：
ValidTime	是	否	Uint64	有效时间 示例值：

MapItem

地图类型

被如下接口引用：DescribeAttackWorldMap

名称	必选	允许NULL	类型	描述
Country	是	否	String	城市 示例值：
Count	是	否	Uint64	数量 示例值：

AppIdDetail

clb-waf AppId对应的详情

被如下接口引用：DescribeUserInfo

名称	必选	允许NULL	类型	描述
Level	是	否	Uint64	套餐版本，跟saas保持一致 示例值：
AutoRenew	是	否	Uint64	是否自动续费，1：自动续费，0：不自动续费 示例值：
BeginTime	是	否	String	套餐的购买时间 示例值：

名称	必选	允许NULL	类型	描述
Cls	是	是	ClsPackage	购买的日志套餐 示例值：查看
ValidTime	是	否	String	过期时间 示例值：
DomainLimit	是	否	Uint64	套餐子域名限制个数 示例值：
DomainCount	是	否	Uint64	套餐子域名已经使用的个数 示例值：
MainDomainCount	是	否	Uint64	套餐主域名已经使用的个数 示例值：
MainDomainLimit	是	否	Uint64	套餐主域名限制个数 示例值：
RegionLimit	是	否	Uint64	套餐的地域限制个数 示例值：
LbLimit	是	否	Uint64	套餐的监听器限制个数 示例值：
QPS	是	是	QPSPackage	购买的QPS套餐 示例值：查看
MaxQPS	是	否	Uint64	当前的QPS峰值 示例值：
ResourceIds	是	否	String	资源ID 示例值：
Type	是	是	String	暂时未用到 示例值：
DomainPkg	是	是	DomainPackage	购买的域名套餐 示例值：查看
AllowRegions	是	是	String	账号开通了clbwaf的地域白名单，如果为空则表示开通了全部地域，否则则开通的地域以,串接。 示例值：
CCGuardRegions	是	是	String	账号开通了clbwaf的清洗模式的地域白名单，如果为空则表示没有地域开启了清洗模式，否则则开通的地域以,串接。 示例值：

ClbHostResult

CLB查询对应绑定的WAF状态的结果参数

被如下接口引用：DescribeWafInfo

名称	必选	允许NULL	类型	描述
LoadBalancer	是	否	LoadBalancer	WAF绑定的监听器实例 示例值：查看
Domain	是	否	String	WAF绑定的域名 示例值：
DomainId	是	否	String	WAF绑定的实例ID 示例值：
Status	是	否	Uint64	是否有绑定WAF，1：绑定了WAF，0：没有绑定WAF 示例值：
FlowMode	是	否	Uint64	绑定了WAF的情况下，WAF流量模式，1：清洗模式，0：镜像模式（默认） 示例值：

ClbHostsParams

CLB回调WAF接口（获取、删除）的参数

被如下接口引用：DescribeWafInfo

名称	必选	允许NULL	类型	描述
LoadBalancerId	是	否	String	负载均衡实例ID，如果不传次参数则默认认为操作的是整个AppId的监听器，如果此参数不为空则认为操作的是对应负载均衡实例。 示例值：
ListenerId	否	否	String	负载均衡监听器ID，，如果不传次参数则默认认为操作的是整个负载均衡实例，如果此参数不为空则认为操作的是对应负载均衡监听器。 示例值：
DomainId	否	否	String	WAF实例ID，，如果不传次参数则默认认为操作的是整个负载均衡监听器实例，如果此参数不为空则认为操作的是对应负载均衡监听器的某一个具体的域名。 示例值：

QPSPackage

clb-waf QPS套餐

被如下接口引用：DescribeSpartUserInfo、DescribeUserInfo

名称	必选	允许NULL	类型	描述
ResourceIds	是	否	String	资源ID 示例值：
ValidTime	是	否	String	过期时间 示例值：
AutoRenew	是	否	Int64	是否自动续费，1：自动续费，0：不自动续费 示例值：
Count	是	否	Int64	套餐购买个数 示例值：
Region	是	否	String	套餐购买地域，clb-waf暂时没有用到 示例值：

WafGetDomainEngineTypeData

WafGetDomainEngineType返回参数

被如下接口引用：WafGetDomainEngineType

名称	必选	允许NULL	类型	描述
EngineType	否	否	String	引擎类型 示例值：
Domain	否	否	String	域名 示例值：

BotsGeoStatStyledItem

GetBotsGeoStatStyled接口的返回数据的元素类型

被如下接口引用：DescribeBotRegionsStat

名称	必选	允许NULL	类型	描述
Key	是	否	String	地域

名称	必选	允许NULL	类型	描述
				示例值：
Value	是	否	Int64	值 示例值：

DescribeDNSDetectDomainListDomainListItem

DescribeDNSDetectDomainList返回值的元素

被如下接口引用：DescribeDNSDetectDomainList

名称	必选	允许NULL	类型	描述
Id	是	否	String	id 示例值：
Domain	是	否	String	域名 示例值：
HijackRecords	是	否	String	hijackRecords 示例值：
HijackRegions	是	否	String	hijackRegions 示例值：
CreateTime	是	否	String	创建时间 示例值：
AuthIP	是	否	Array of String	授权的IP 示例值：

RuleVersionData

数组

被如下接口引用：DescribeRuleVersion

名称	必选	允许NULL	类型	描述
Id	是	否	Int64	出参 示例值：
Appid	是	是	Int64	出参 示例值：

名称	必选	允许NULL	类型	描述
Version	是	是	String	出参 示例值：
Rules	是	是	Int64	出参 示例值：
Description	是	是	String	出参 示例值：
CreateTime	是	是	String	出参 示例值：
ModifyTime	是	是	String	出参 示例值：

DescribeDNSDetectDataMapRspItem

DescribeDNSDetectDataMap返回值的元素

被如下接口引用：DescribeDNSDetectDataMap

名称	必选	允许NULL	类型	描述
Key	是	否	String	地域 示例值：
Value	是	否	String	地域的劫持数量 示例值：

KVInt

Key-Value的形式，Value为Int

被如下接口引用：DescribeTopAttackDomain

名称	必选	允许NULL	类型	描述
Key	是	否	String	Key 示例值：
Value	是	否	Uint64	Value 示例值：

DescribeSpartaProtectionListItem

DescribeSpartaProtectionList的入参

被如下接口引用：DescribeSpartaProtectionList

名称	必选	允许NULL	类型	描述
IsCdn	否	否	String	是否是cdn 示例值：
Status	否	否	String	状态 示例值：
LogStatus	否	否	String	日志开关 示例值：
Mode	否	否	String	AI模式 示例值：
State	否	否	String	状态 示例值：

DomainBotStatus

DomainBotStatus

被如下接口引用：DescribeBotStatus

名称	必选	允许NULL	类型	描述
Category	是	否	String	类别 示例值：
Domain	是	否	String	域名 示例值：
Status	是	否	Uint64	状态 示例值：

UserWhiteRule

全局规则白名单

被如下接口引用：DescribeUserWhiteRule

名称	必选	允许NULL	类型	描述
Id	否	否	Uint64	序号 示例值：
Name	否	否	String	规则名称 示例值：
Domain	否	否	String	域名 示例值：
SignatureId	否	否	String	特征序号 示例值：
Status	否	否	Uint64	规则开关 示例值：
CreateTime	否	否	Datetime_iso	创建时间 示例值：
ModifyTime	否	否	Datetime_iso	修改时间 示例值：
Rules	否	否	Array of GlobalWhiteCond	规则详细 示例值：查看

IpAccessControlItem

ip黑白名单

被如下接口引用：DescribeIpAccessControl

名称	必选	允许NULL	类型	描述
ActionType	是	否	Uint64	动作 示例值：
Ip	是	否	String	ip 示例值：
Note	是	否	String	备注 示例值：
Source	是	否	String	来源 示例值：
TsVersion	是	是	Uint64	更新时间戳 示例值：

名称	必选	允许NULL	类型	描述
ValidTs	是	否	Uint64	有效截止时间戳 示例值：

CCRuleItem

cc规则

被如下接口引用：DescirbeCCRule

名称	必选	允许NULL	类型	描述
ActionType	是	否	Uint64	动作 示例值：
Advance	是	否	Uint64	高级模式 示例值：
Interval	是	否	Uint64	时间周期 示例值：
Limit	是	否	Uint64	限制次数 示例值：
MatchFunc	是	否	Uint64	匹配方法 示例值：
Name	是	否	String	名称 示例值：
Priority	是	否	Uint64	优先级 示例值：
Status	是	否	Int64	状态 示例值：
TsVersion	是	否	Uint64	更新时间戳 示例值：
Url	是	否	String	匹配url 示例值：
ValidTime	是	否	Uint64	策略动作有效时间 示例值：
OptionsArr	是	是	String	高级参数 示例值：

CopyBotTCBRuleRsp

CopyBotTCBRule函数的返回值

被如下接口引用：CopyBotTCBRule

名称	必选	允许NULL	类型	描述
Code	是	否	Int64	0表示成功，其他表示失败 示例值：
ErrMsg	是	否	String	错误信息 示例值：
SuccessNum	是	否	Int64	成功的数目 示例值：
FailedNum	是	否	Int64	失败的数目 示例值：
T	是	否	Array of String	成功的域名列表 示例值：

DescribeCustomRulesPagingInfo

DescribeCustomRules接口的翻页参数

被如下接口引用：DescribeCustomRules

名称	必选	允许NULL	类型	描述
Offset	是	否	Int64	当前页码 示例值：
Limit	是	否	Int64	当前页的最大数据条数 示例值：

ReqUserRule

用户规则更新输出规则子项

被如下接口引用：ModifyUserSignatureRule

名称	必选	允许NULL	类型	描述
Id	是	否	String	特征序号

名称	必选	允许NULL	类型	描述
				示例值：
Status	是	否	Int64	规则开关 0：关 1：开 2：只告警 示例值：
Reason	否	否	Int64	修改原因 0：无(兼容记录为空) 1：业务自身特性 示例值：

AttackExportJobInfo

攻击日志导出任务基本信息

被如下接口引用：DescribeExportAttackDetailJobs

名称	必选	允许NULL	类型	描述
Id	是	否	Uint64	ID 示例值：
CreateTime	是	否	Datetime	创建时间 示例值：
FileName	是	否	String	任务名称 示例值：
LogsCount	是	否	Uint64	日志总数量 示例值：
UploadCount	是	否	Uint64	日志已导出数量 示例值：
UploadProgress	是	否	String	日志导出进度 示例值：
DeleteFlag	是	否	Uint64	cos删除标志 0为未删除,1为已删除 示例值：
ExpiredDays	是	否	Uint64	过期天数 示例值：
ExpiredTime	是	否	Datetime	过期时间 示例值：
FileDownloadUrl	是	否	String	cos文件下载地址 示例值：

名称	必选	允许NULL	类型	描述
TaskType	是	否	Uint64	任务类型 0租户端 1运营端 示例值：
TaskStatus	是	否	Uint64	任务状态 0、进行中 1、完成 2、失败 示例值：
QueryParams	是	否	String	查询参数 示例值：
AppId	是	否	Uint64	Appid 示例值：
Uin	是	否	Uint64	账号 示例值：

SessionData

参数包装

被如下接口引用：DescribeSession

名称	必选	允许NULL	类型	描述
Res	是	否	Array of SessionItem	session定义 示例值：查看

CreateAccessDownloadRecordRsp

CreateAccessDownloadRecord接口的返回值

被如下接口引用：CreateAccessDownloadRecord

名称	必选	允许NULL	类型	描述
Code	是	否	Int64	是否成功，正常情况为0 示例值：
Flow	是	否	String	下载记录编号 示例值：

MainClassItem

主类信息

被如下接口引用：DescribeMainClass

名称	必选	允许NULL	类型	描述
MainClassID	否	否	String	主类id 示例值：
MainClassName	否	否	String	主类名字 示例值：
Description	否	否	String	描述 示例值：
SubClass	否	是	Array of SubClassItem	子类 示例值：查看
RuleCount	否	是	Uint64	当前主类的规则个数 示例值：

CopyBotsUCBPreinstallRuleRsp

CopyBotsUCBPreinstallRule接口的返回自

被如下接口引用：CopyBotUCBPreinstallRule

名称	必选	允许NULL	类型	描述
Code	是	否	Int64	0表示成功，其他表示失败 示例值：
ErrMsg	是	否	String	错误信息 示例值：
SuccessNum	是	否	Int64	成功的数目 示例值：
FailedNum	是	否	Int64	失败的数目 示例值：
T	是	否	Array of String	成功的域名列表 示例值：

DescribeCachePathRspListItem

DescribeCachePath返回值中的类型

被如下接口引用：DescribeCachePath

名称	必选	允许NULL	类型	描述
Id	是	否	String	ID 示例值：
Domain	是	否	String	域名 示例值：
Name	是	否	String	名称 示例值：
State	是	否	String	状态 示例值：
Path	是	否	String	路径 示例值：
CreateTime	是	否	String	创建时间 示例值：
ModifyTime	是	否	String	修改时间 示例值：

StrategyForAntiInfoLeak

防信息泄露的匹配条件结构体

被如下接口引用：AddAntiInfoLeakRules、ModifyAntiInfoLeakRules

名称	必选	允许NULL	类型	描述
Field	是	否	String	匹配字段 示例值：
CompareFunc	是	否	String	逻辑符号 示例值：
Content	是	否	String	匹配内容 示例值：

BotListData

bot列表数据封装

被如下接口引用：DescribeBotTCBRecords、DescribeBotUBRecords、DescribeBotUCBRecords

名称	必选	允许NULL	类型	描述
Res	是	是	Array of BotItemsListItem	bot列表 示例值：查看
TotalCount	是	否	Uint64	统计总数 示例值：

HostDel

CLB-WAF删除域名参数

被如下接口引用：DeleteHost

名称	必选	允许NULL	类型	描述
Domain	是	否	String	域名 示例值：
DomainId	是	否	String	域名ID 示例值：

PageForDescribeSpartaProtectionList

PageForDescribeSpartaProtectionList接口专用的翻页结构体

被如下接口引用：DescribeSpartaProtectionList

名称	必选	允许NULL	类型	描述
Count	是	否	Uint64	每页个数 示例值：
Index	是	否	Uint64	页码 示例值：

Strategy

自定义规则的匹配条件结构体

被如下接口引用：AddCustomRule、DescribeCustomRules、ModifyCustomRule

名称	必选	允许NULL	类型	描述

名称	必选	允许NULL	类型	描述
Field	是	否	String	匹配字段 示例值：
CompareFunc	是	否	String	逻辑符号 示例值：
Content	是	否	String	匹配内容 示例值：
Arg	是	否	String	匹配参数 示例值：

DescribeCustomRulesRspRuleListItem

DescribeCustomRules接口回包中的复杂类型

被如下接口引用：DescribeCustomRules

名称	必选	允许NULL	类型	描述
ActionType	是	否	String	动作类型 示例值：
Bypass	是	否	String	跳过的策略 示例值：
CreateTime	是	否	String	创建时间 示例值：
ExpireTime	是	否	String	过期时间 示例值：
Name	是	否	String	策略名称 示例值：
Redirect	是	否	String	重定向地址 示例值：
RuleId	是	否	String	策略ID 示例值：
SortId	是	否	String	优先级 示例值：
Status	是	否	String	状态 示例值：

名称	必选	允许NULL	类型	描述
Strategies	是	否	Array of Strategy	策略详情 示例值：查看

MenshenRulesInfo

门神-规则库描述信息

被如下接口引用：DescribeRulesInfo

名称	必选	允许NULL	类型	描述
Date	是	是	Date	日期 示例值：
Version	是	是	String	版本 示例值：
Memos	是	是	Array of String	描述信息 示例值：
MemosEng	是	是	Array of String	描述标题 示例值：

ActionedIpData

封装数据

被如下接口引用：DescribeActionedIp

名称	必选	允许NULL	类型	描述
Res	是	是	Array of ActionedIpItem	ip数据 示例值：查看
TotalCount	是	否	Uint64	计数 示例值：

错误码

功能说明

如果返回结果中存在 Error 字段，则表示调用 API 接口失败。例如：

```
{
  "Response": {
    "Error": {
      "Code": "AuthFailure.SignatureFailure",
      "Message": "The provided credentials could not be validated. Please check your signature is cor
rect."
    },
    "RequestId": "ed93f3cb-f35e-473f-b9f3-0d451b8b79c6"
  }
}
```

Error 中的 Code 表示错误码，Message 表示该错误的具体信息。

错误码列表

公共错误码

错误码	说明
AuthFailure.InvalidSecretId	密钥非法（不是云 API 密钥类型）。
AuthFailure.MFAFailure	MFA 错误。
AuthFailure.SecretIdNotFound	密钥不存在。 请在控制台检查密钥是否已被删除或者禁用，如状态正常，请检查密钥是否填写正确，注意前后不得有空格。
AuthFailure.SignatureExpire	签名过期。Timestamp 和服务器时间相差不得超过五分钟，请检查本地时间是否和标准时间同步。
AuthFailure.SignatureFailure	签名错误。 签名计算错误，请对照调用方式中的接口鉴权文档检查签名计算过程。
AuthFailure.TokenFailure	token 错误。
AuthFailure.UnauthorizedOperation	请求未 CAM 授权。
DryRunOperation	DryRun 操作，代表请求将会是成功的，只是多传了 DryRun 参数。

错误码	说明
FailedOperation	操作失败。
InternalError	内部错误。
InvalidAction	接口不存在。
InvalidParameter	参数错误。
InvalidParameterValue	参数取值错误。
LimitExceeded	超过配额限制。
MissingParameter	缺少参数错误。
NoSuchVersion	接口版本不存在。
RequestLimitExceeded	请求的次数超过了频率限制。
ResourceInUse	资源被占用。
ResourceInsufficient	资源不足。
ResourceNotFound	资源不存在。
ResourceUnavailable	资源不可用。
UnauthorizedOperation	未授权操作。
UnknownParameter	未知参数错误。
UnsupportedOperation	操作不支持。
UnsupportedProtocol	http(s)请求协议错误，只支持 GET 和 POST 请求。
UnsupportedRegion	接口不支持所传地域。

业务错误码

错误码	说明
MissingParameter	缺少参数错误。
InvalidParameter	参数错误。
ResourcesSoldOut	资源售罄。
ResourceUnavailable	资源不可用。

错误码	说明
UnauthorizedOperation	未授权操作。
InvalidParameterValue	参数取值错误。
ResourceInUse	资源被占用。
FailedOperation	操作失败。
ResourceNotFound	资源不存在。
ResourceInsufficient	资源不足。
UnknownParameter	未知参数错误。
LimitExceeded	超过配额限制。
InternalError	内部错误。