边缘安全加速平台 EO

源站配置

产品文档

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

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

文档目录

源站配置
负载均衡
概述
快速创建负载均衡实例
健康检查策略介绍
查看源站健康状态
相关参考
负载均衡相关概念
请求重试策略介绍
源站组操作指引
回源配置
配置回源 HTTPS
Host Header 重写
回源请求参数设置
回源跟随重定向
HTTP/2 回源
分片回源
相关参考
旧版源站组兼容相关问题
VOD 源站相关说明
获取 EdgeOne 回源节点 IP

版权所有：腾讯云计算（北京）有限责任公司

源站配置
负载均衡
概述

最近更新时间：2024-05-29 10:33:37

EdgeOne 负载均衡适用于对源站可用性要求较高的场景，支持配置多级备源用于容灾切换，并且可以主动探测源站的健康情况，提前屏蔽故障源站，将业务流量调度至健康源站。

注意：

EdgeOne 负载均衡功能在内测中，如您需要使用请 联系我们。

适用场景

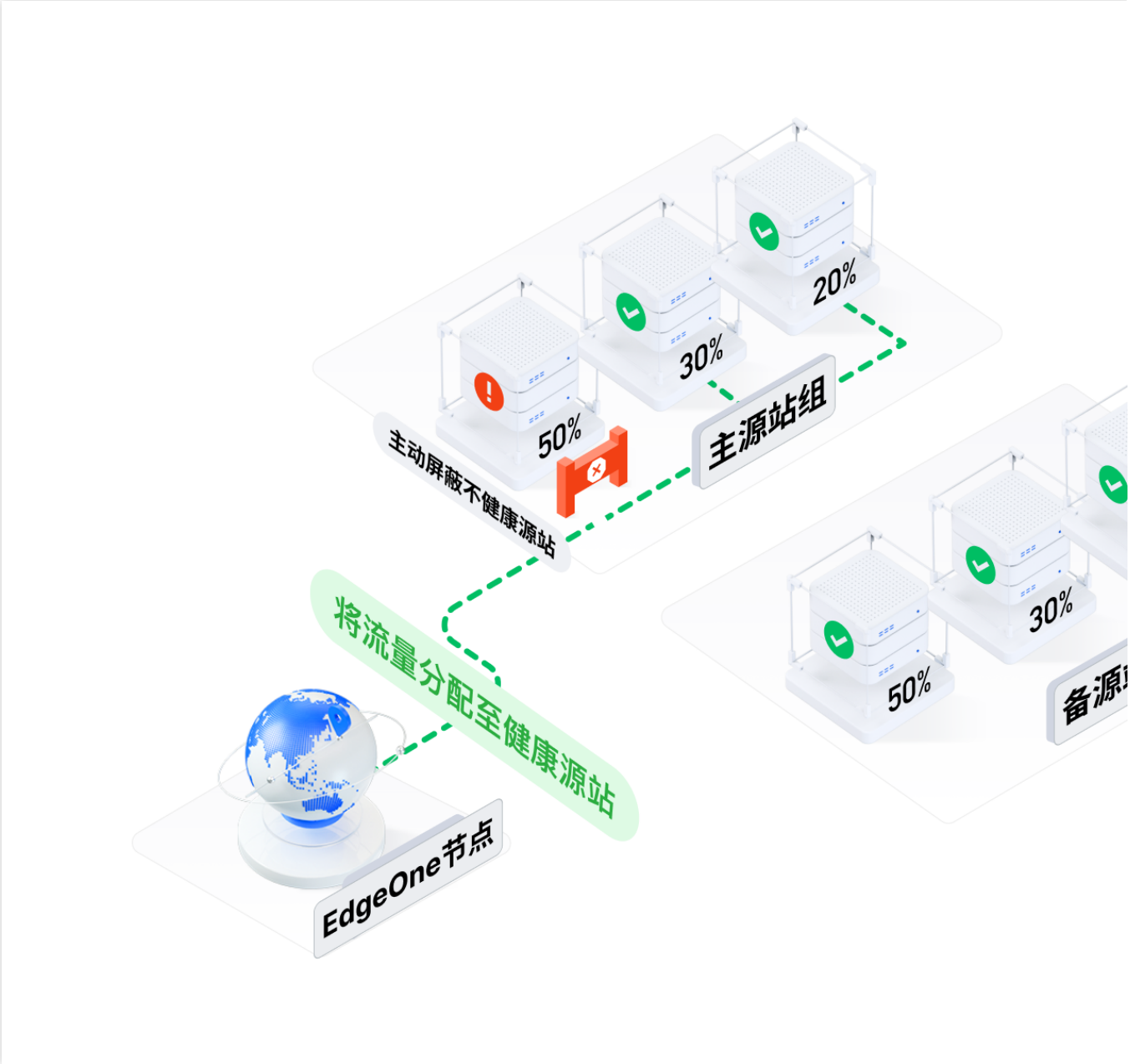
软硬件故障/网络故障/配置错误/安全攻击/自然灾害/人为错误等各种意外会影响源站可用性，对于金融/游戏/音视频/电商等要求高可用性的业务而言，即使是短时间的源站故障也会造成巨大损失，因此需要对源站做主备容灾和健康检查。

主备容灾：当主源不可用时，自动切换至备源保障业务不中断。

主动检测源站健康状况：提前屏蔽故障源站，将业务流量分配至健康源站，避免源站发生故障时仍然有大量正常业务请求到故障源站。

支持的能力

1. 支持配置多级备源，实现多源容灾。
2. 支持配置 ICMP Ping、HTTP/HTTPS、TCP、UDP 等健康检查策略，提前屏蔽故障源站，将业务流量分配至健康源站。
3. 提供兜底重试策略，当真实的业务流量请求失败时重试至其他健康源站。



了解更多

快速创建负载均衡实例
负载均衡相关概念
健康检查策略

快速创建负载均衡实例

最近更新时间：2024-06-20 16:56:24

本文将为您介绍如何创建负载均衡实例。

注意：

EdgeOne 负载均衡功能在内测中，如您需要使用请 联系我们。

示例场景

例如当前您有一个加速域名 `www.example.com`，三个源站 `1.2.3.4`、`2.3.4.5` 和 `3.4.5.6`，正常情况下将 `1.2.3.4` 和 `2.3.4.5` 同时作为主源回源，当前已参考 源站组操作指引 配置为源站组 primary_origins。仅在主源站故障的情况下将 `3.4.5.6` 作为备源回源，配置为源站组 backup_origins 当真实业务请求失败时，重试同组内其他健康源站。同时需要定期主动探测，主动屏蔽不健康的源站。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**源站配置 > 负载均衡**。
3. 在负载均衡页面，单击**新建实例**。

4. 在第一步选择源站中，需要填写实例名称，选择实例类型，并添加源站组。
以该场景为例，添加源站组 primary_origins 为优先级1的源站组，添加源站组 backup_origins 为优先级2的源站组，单击**下一步**。

参数	说明
实例名称	限制 1-200 个字符长度，允许字符为 a-z，A-Z，0-9，_，-。
实例类型	HTTP 专用型：支持添加 HTTP 专用型和通用型源站组，仅支持被站点加速相关服务引用（如域名服务和规则引擎）。 通用型：仅支持添加通用型源站组，能被站点加速服务（如域名服务和规则引擎）和四层代理引用。
添加源站组	负载均衡实例中源站的最小配置维度是源站组，您需要将源站配置成源站组添加在此处。详情请参见 源站组操作指引。 您可以为添加的源站组设置优先级，在高优先级源站组中的存在健康源站的情况下，流量不会分配至低优先级源站组中的源站，最多支持配置 10 个源站组，优先级数字越小，优先级越高。

5. 进入第二步健康检查策略，支持 ICMP Ping、HTTPS/HTTP、TCP、UDP 四种探测方式，EdgeOne 将向您的源站主动发送探测请求，来检测您源站的时延和健康情况，您可以根据源站的负载情况选择合适的探测频率。这里根据诉求探测策略选择 ICMP Ping。 详细探测策略配置介绍请参见 健康检查策略介绍。配置完成后，单击**下一步**。

说明：

如果您不希望 EdgeOne 的节点对源站发起任何探测请求，可以选择**不启用**，此时负载均衡实例默认按照第一步源站组的优先级顺序进行流量调度，当 60s 内请求某一源站失败 5 次时会将相应源站按照默认策略屏蔽 10 分钟。

使用该策略将**无法提前屏蔽故障源站，**在**源站恢复正常后也不能自动快速恢复流量调度**，从而导致您在源站故障期间，相较于启用主动探测可能出现更多请求失败的情况。因此如果您希望业务可用性更高，建议您开启主动探测。

6. 在第三步流量调度策略，当前流量调度策略默认根据主动探测的结果按照优先级顺序进行故障转移，当实际业务请求回源时出现请求失败时，支持请求重试，请求重试策略提供以下两种，详情请参见 请求重试策略介绍。

策略一：当真实业务请求访问某个源站失败时，直接重试到下一优先级源站组中的源站。适用于源站组 1 和源站组 2 性能相近场景。

策略二：当真实业务请求访问某个源站失败时，直接重试到当前优先级源站组中的其他源站。适用于源站组 1 性能远大于源站组 2 场景。

7. 以该示例场景为例，可选择策略二，单击**完成**，即可完成实例的创建。

健康检查策略介绍

最近更新时间：2024-05-29 10:33:37

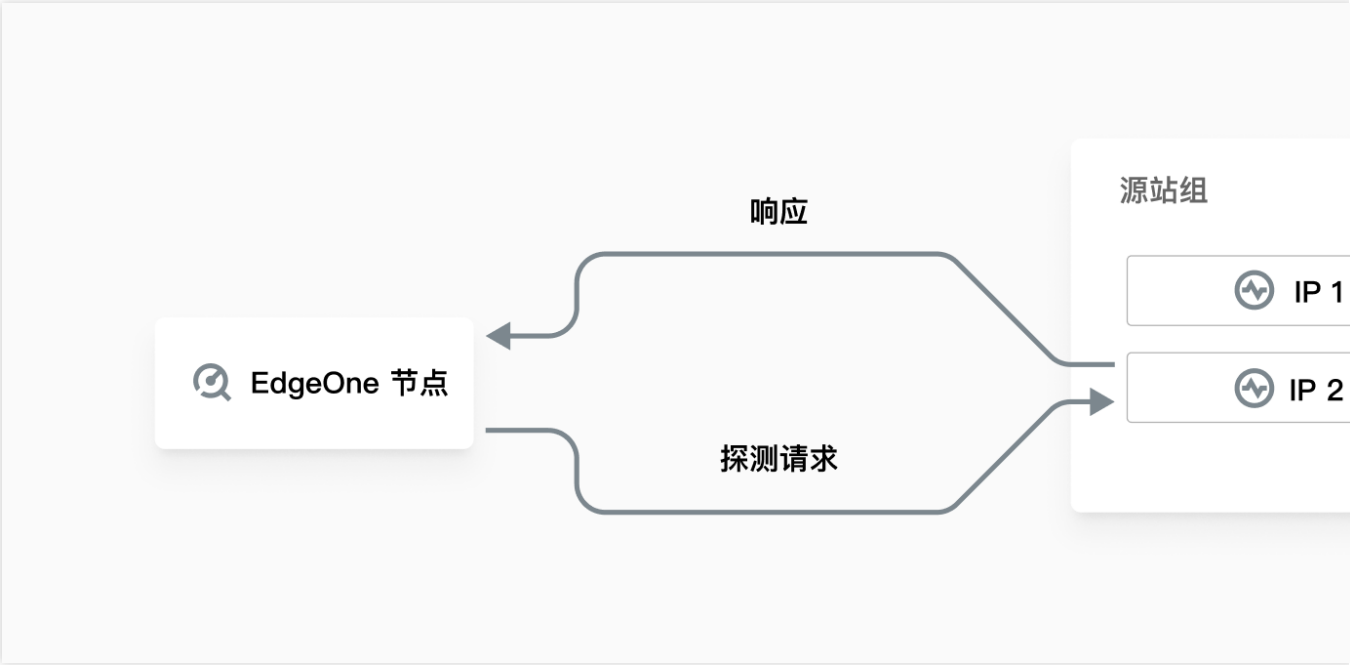
本文将为您介绍健康检查中的探测方式及其原理、源站健康判定条件以及计算方式。

注意：

EdgeOne 负载均衡功能在内测中，如您需要使用请 联系我们。

健康检查原理

配置了健康检查策略后，EdgeOne 不同地区的探测节点会向您的源站发送探测请求，并根据响应结果来判定源站的健康状态。健康检查策略由探测方式和源站健康判定条件组成，探测方式决定探测请求的类型，源站健康判定条件决定响应结果的处理方式。



探测方式

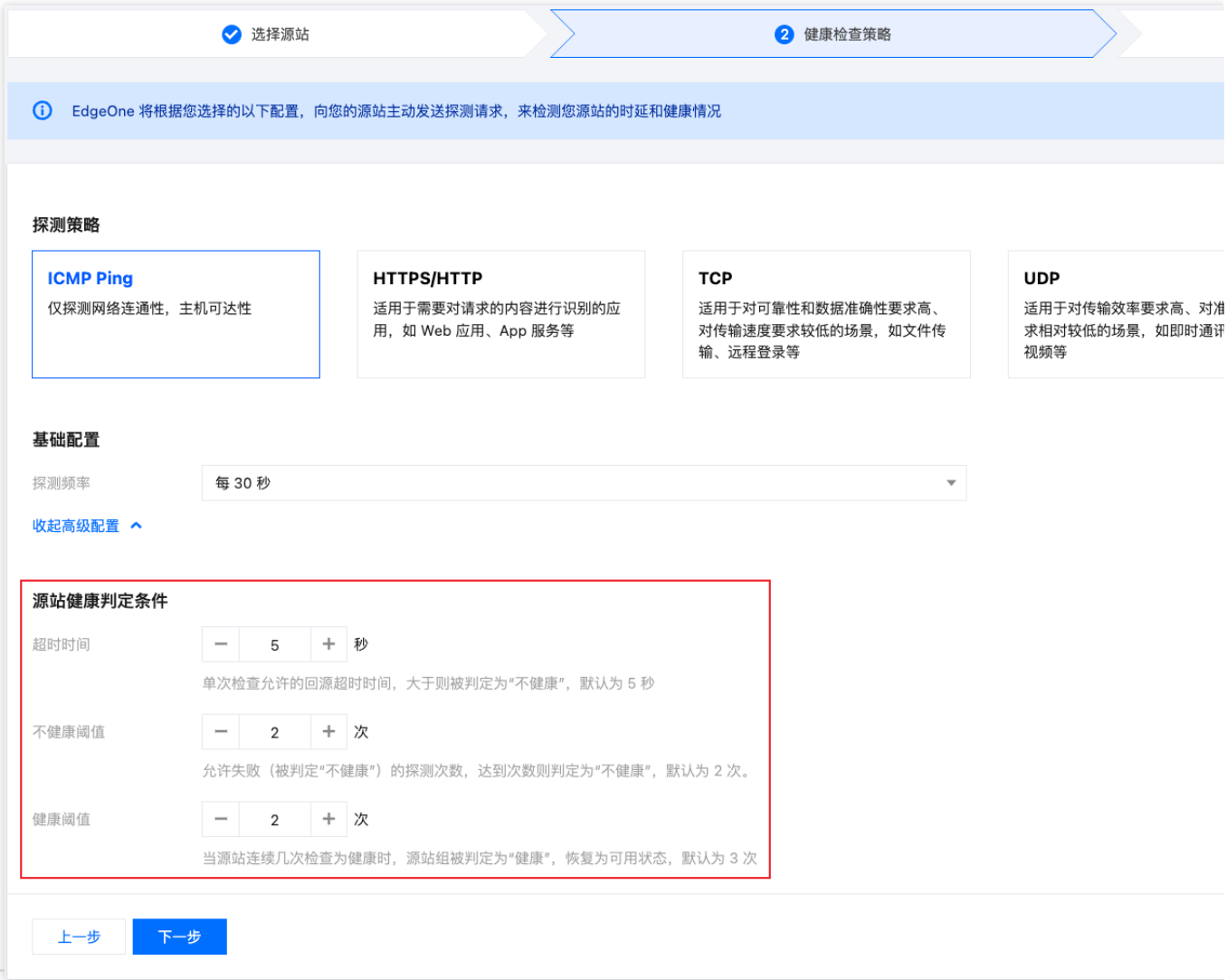
当前支持 ICMP Ping、HTTP/HTTPS、TCP 和 UDP 这四种探测方式，详情请参见 探测方式的原理介绍。以下为对应的配置项说明：

探测方式	适用场景	配置项	说明
ICMP Ping	仅探测网络连通性，主机可达性。	探测频率	必填，可选每 30 秒、每 60 秒、每 3 分钟、每 5 分钟、每 10 分钟。

HTTP/HTTPS	适用于需要对请求的内容进行识别的应用，如 Web 应用、App 服务等。	探测频率	必填，可选每 30 秒、每 60 秒、每 3 分钟、每 5 分钟、每 10 分钟。
		URL	必填，健康检查的请求完整 URL，例如：`www.example.com/test` 。
		探测端口	必填，默认为 80 端口。除需要指定特定端口以外，其余情况建议不修改。
		HTTP Method	必填，健康检查的 HTTP 请求方式，默认为 HEAD，可选：GET 或 HEAD。 若使用 HEAD 方法，服务器仅返回 HTTP 头部信息，可降低后端开销，提升请求效率，对应的源站服务需支持 HEAD。 若使用 GET 方法，则源站服务支持 GET 即可。
		HTTP 状态码	必填，当状态码为所选状态码时，即认为源站健康。默认包含 2XX，可选：1XX、2XX、3XX、4XX、5XX。
		遵循重定向	默认关闭。开启后，探测节点将根据源站响应的 301/302 重定向地址再次发起探测，以最后一次跳转响应的状态码作为健康状态码的判定结果，最多支持跳转3次。
		自定义请求头	选填，发起健康检查时，可以配置携带自定义请求头回源，至多可配置 8 个，例如：`host: www.example.com` 。
TCP	适用于对可靠性和数据准确性要求高、对传输速度要求较低的场景，如文件传输、远程登录等。	探测频率	必填，可选每 30 秒、每 60 秒、每 3 分钟、每 5 分钟、每 10 分钟。
		探测端口	必填，默认为 80 端口。除需要指定特定端口以外，其余情况建议不修改。
UDP	适用于对传输效率要求高、对准确性要求相对较低的场景，如即时通讯、在线视频等。	探测频率	必填，可选每 30 秒、每 60 秒、每 3 分钟、每 5 分钟、每 10 分钟。
		探测端口	必填，默认为 80 端口。除需要指定特定端口以外，其余情况建议不修改。
		探测请求	必填，自定义健康检查请求的内容，可填写 500 个长度以内的字符。
		探测返回结果	必填，自定义健康检查返回结果的内容，可填写 500 个长度以内的字符。

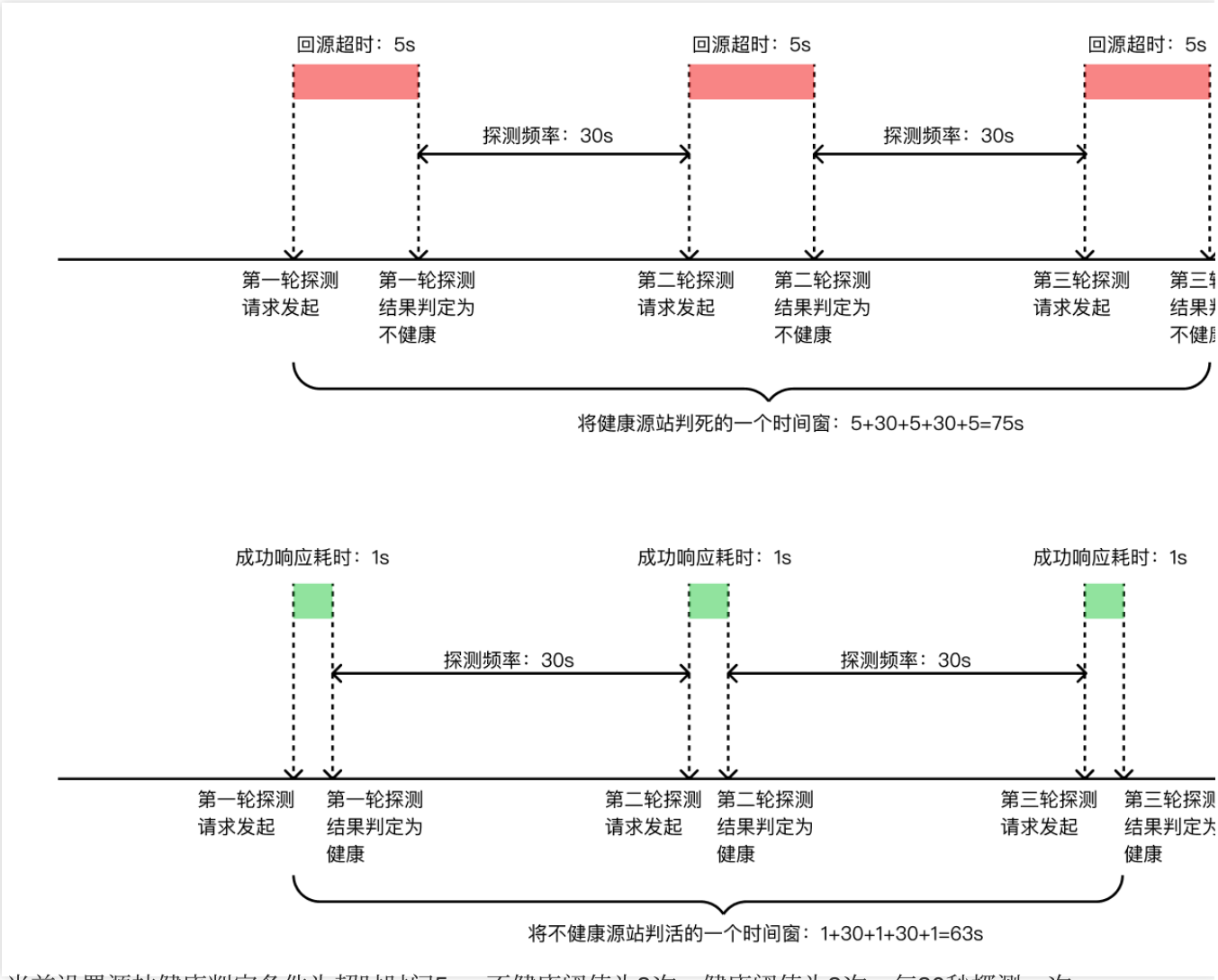
源站健康判定条件

选择 ICMP Ping、HTTP/HTTPS、TCP 和 UDP 任一探测策略，单击**展开高级配置**即可配置源站健康判定条件。以下为各配置项说明：



配置项	说明
超时时间	单次探测请求允许的回源超时时间，大于该时长未响应则被判定为“不健康”，默认为 5 秒，可配置区间为 [1, 30]。
不健康阈值	判断源站“不健康”所需要的探测次数，达到指定的次数则判定为“不健康”，默认为 2 次，可配置区间为 [1, 5]。例如：将该值设置为 2，当某个源站处于“健康”状态时，连续两次探测结果都是“不健康”，那么该源站就会被判定为“不健康”。
健康阈值	恢复源站为“健康”所需要的探测次数，达到指定的次数则判定为“健康”，恢复为可用状态，默认为3次，可配置区间为 [1, 5]。例如：将该值设置为 3，当某个源站处于“不健康”状态时，连续三次探测结果都是“健康”，那么该源站就会被判定为“健康”。

主动探测源站为不健康或恢复为健康所需时间周期



例如：当前设置源站健康判定条件为超时时间5s，不健康阈值为3次，健康阈值为3次，每30秒探测一次。

则判断该源站为不健康所需耗时为：5+30+5+30+5=75秒。

恢复该源站为健康状态所需耗时为（假定主动探测收到成功响应耗时需1秒）：1+30+1+30+1=63秒。

了解更多

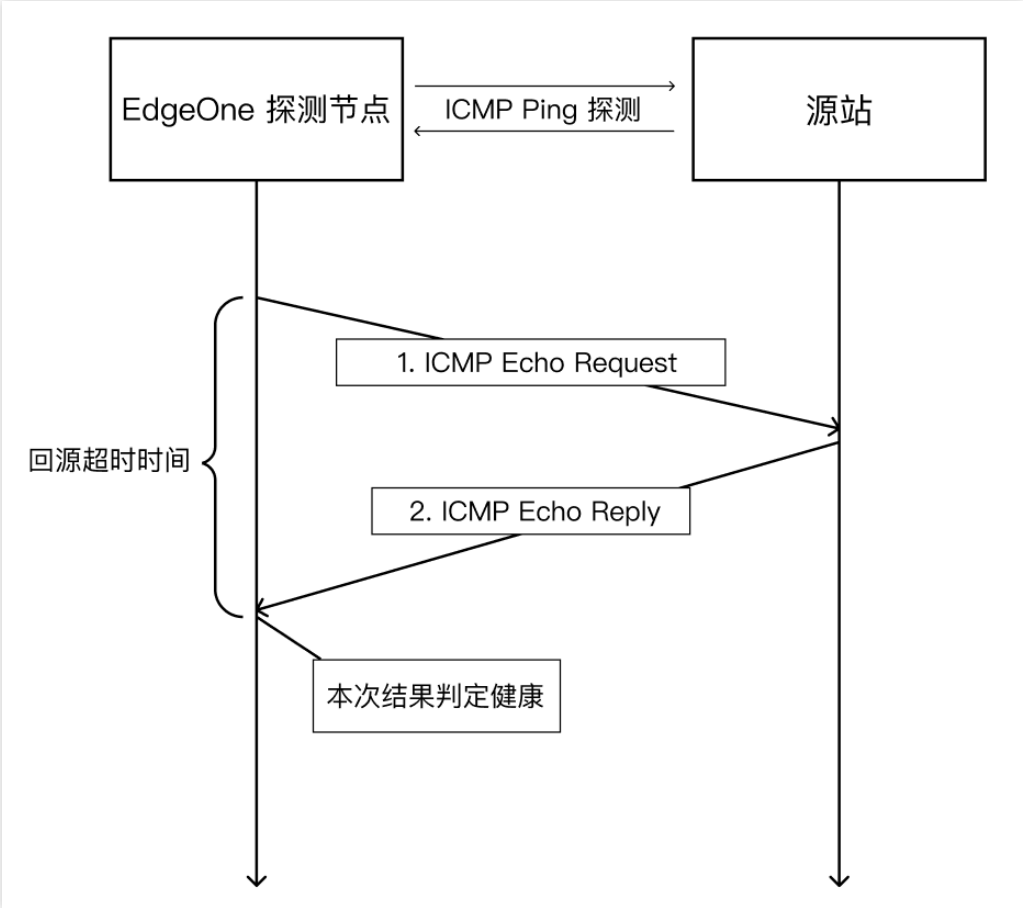
探测方式的原理介绍

ICMP Ping

HTTP/HTTPS

TCP

UDP



ICMP Ping 健康检查机制如下：

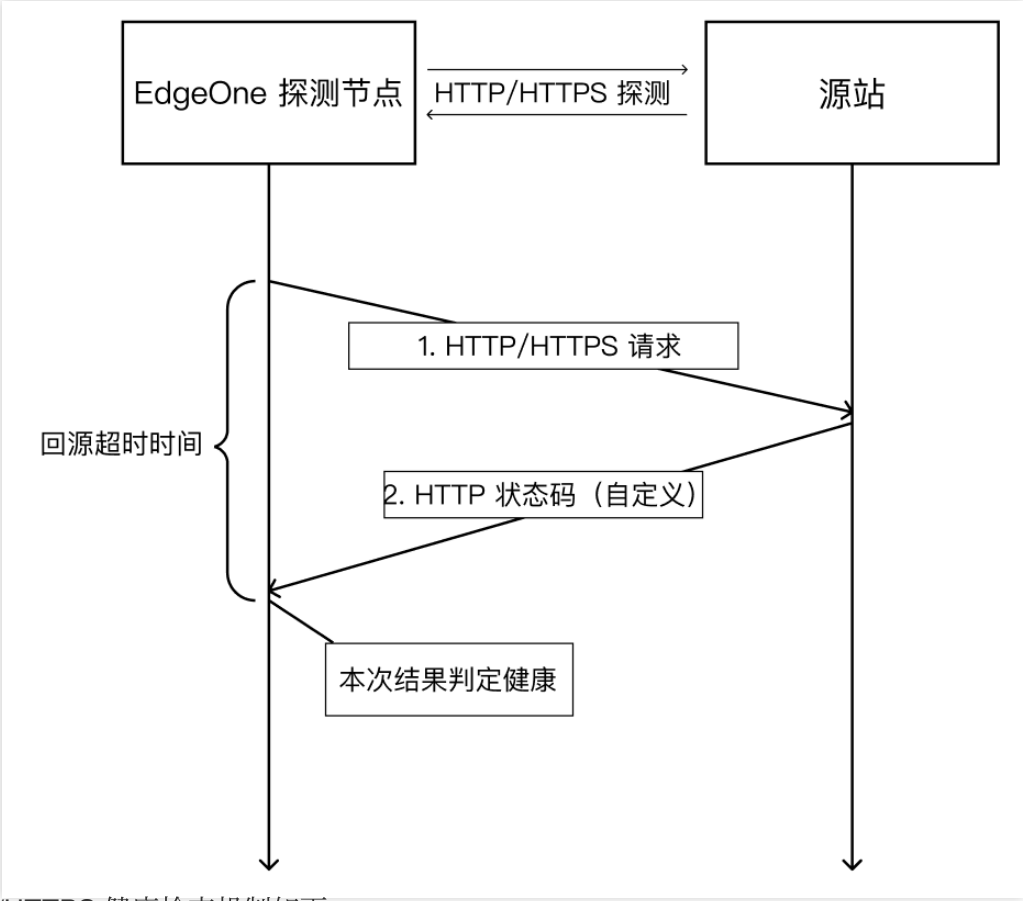
1. EdgeOne 探测节点向您的源站发送 Ping 命令。

2. 若 Ping 成功，且在回源超时时间内，源站收到 ICMP reply，则表示服务正常，本次结果判定为健康；

3. 若 Ping 失败，在回源超时时间内，探测节点未收到源站返回的 ICMP reply，则表示服务异常，本次结果判定为不健康。

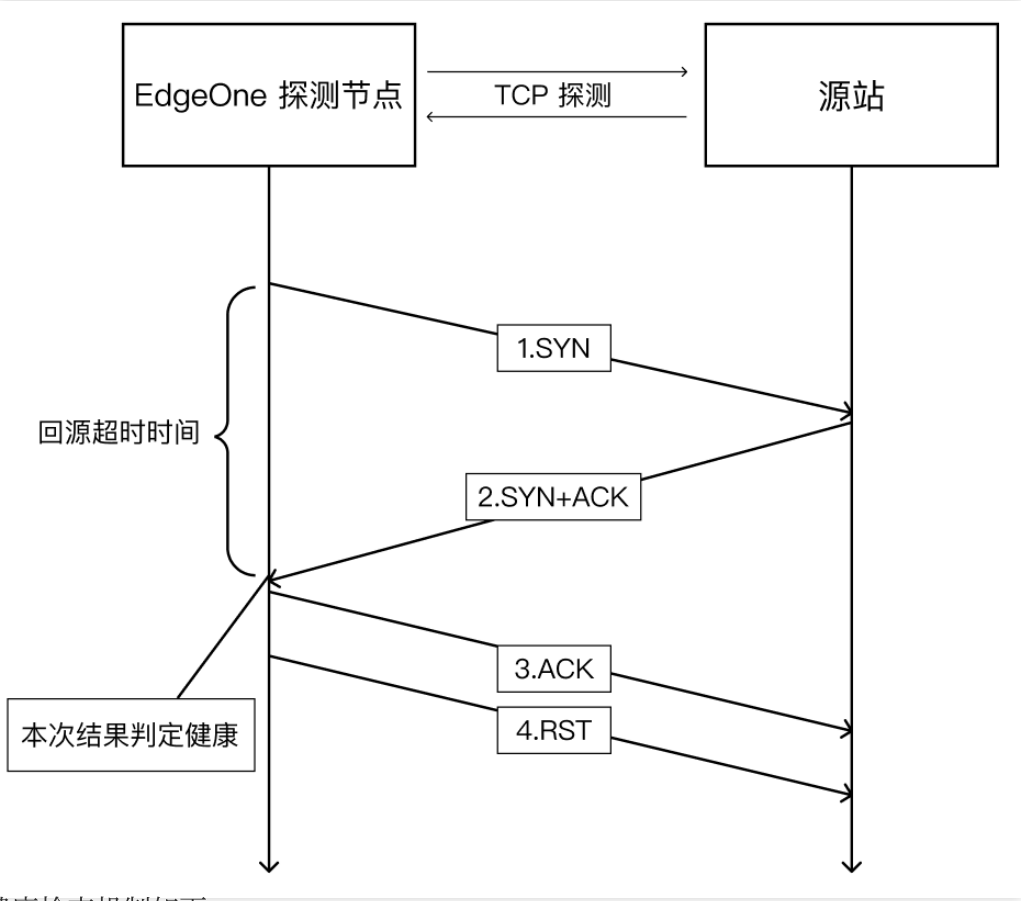
说明：

ICMP Ping 需要您的源站支持 Ping。



HTTP/HTTPS 健康检查机制如下：

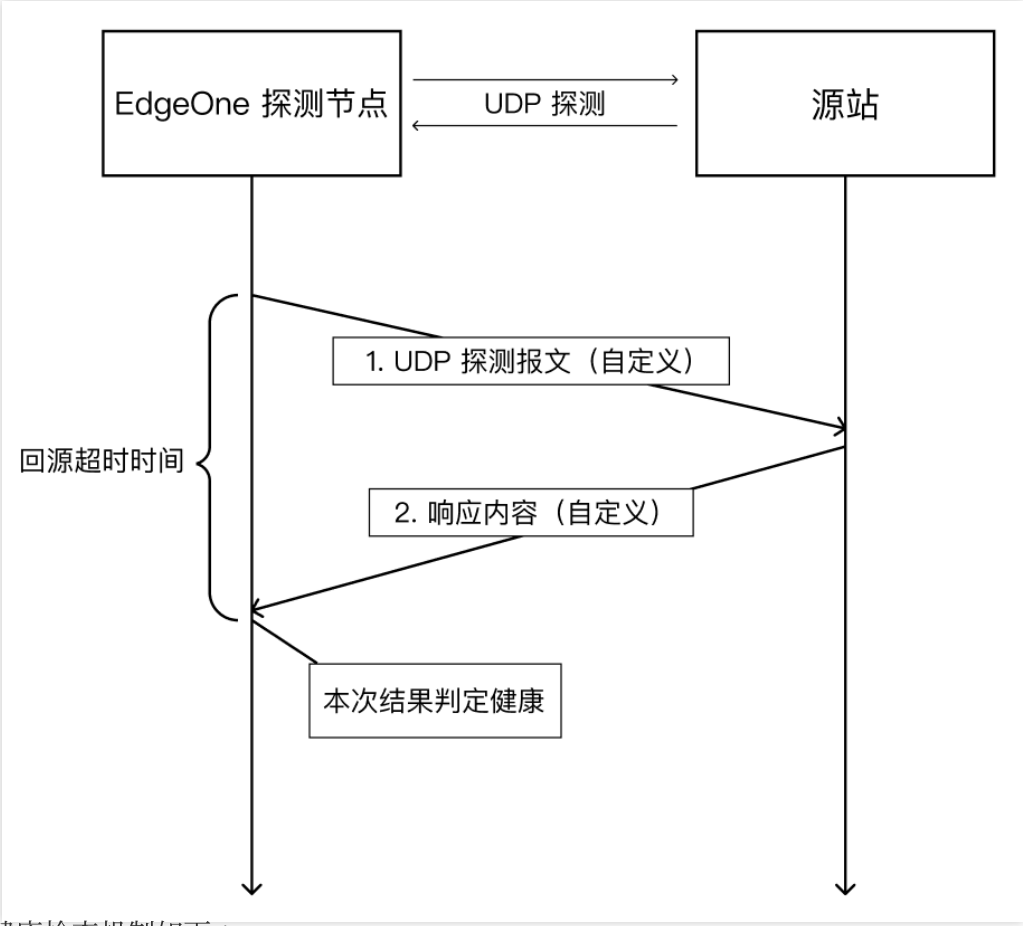
1. EdgeOne 探测节点向您的源站发送 HTTP 请求，需要配置相应的 URL 和端口，可携带自定义的 HOST。
2. 若在回源超时时间内，EO 探测节点收到了源站返回的 HTTP 状态码，若与设置的 HTTP 状态码匹配成功，则本次结果判定为健康。
3. 若在回源超时时间内，EO 探测节点未收到源站的响应或收到与设置不匹配的状态码，则本次结果判定为不健康。



TCP 健康检查机制如下：

1. EdgeOne 探测节点向您的源站的特定端口（可配置）发送 SYN 连接请求报文。
2. 源站收到 SYN 请求报文后，若相应端口处于正常监听状态，则会返回 SYN+ACK 响应报文。
3. 若在回源超时时间内，探测节点收到源站返回的 SYN+ACK 响应报文，则表示服务运行正常，本次结果判定为健康，并向源站回复 ACK 报文以及发送 RST 复位报文中断 TCP 连接。
4. 若在回源超时时间内，探测节点未收到源站返回的 SYN+ACK 响应报文，则表示服务运行异常，本次结果判定为不健康，并向源站发送 RST 复位报文中断 TCP 连接。

版权所有：腾讯云计算（北京）有限责任公司



UDP 健康检查机制如下：

1. EdgeOne 探测节点向您的源站的特定端口（可配置）发送自定义的探测报文。
2. 若在回源超时时间内，探测节点收到源站返回的自定义的响应报文，则表示服务运行正常，本次结果判定为健康。
3. 若在回源超时时间内，探测节点未收到源站返回的自定义的响应报文或者收到与定义内容不支持的响应报文，则表示服务运行异常，本次结果判定为不健康。

说明：

请求内容和响应内容都是自定义的，同时您需要在源站配置相应的请求-响应内容。

探测请求标识

主动探测时不会携带特殊请求标识，当您选择 ICMP Ping 探测或 TCP 探测时没有相关特征；选择 UDP 探测时可以通过配置的自定义内容进行判断；HTTP/HTTPS 探测中可以配置单独的自定义请求头来进行标识。

查看源站健康状态

最近更新时间：2024-05-29 10:33:37

节点探测结果将展示边缘安全加速平台 EO 在全球可用区内不同节点及地区发起的对当前源站组探测后的结果，用户可以根据此结果查看各不同区域对源站是否健康的探测结果。

注意：

EdgeOne 负载均衡功能在内测中，如您需要使用请 联系我们。

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**源站配置** > **负载均衡**。
3. 在负载均衡页面，单击所需的**负载均衡实例**。

4. 在实例详情页中，单击**查看详情**。

5. 在节点探测结果中，分为以下三种颜色的节点：

绿色节点：表明该地区的探测节点判定源站组中所有源站都健康。

红色节点：表明该地区的探测节点判定源站组中存在不健康的源站。

灰色节点：表明该地区的探测节点检测不到任何源站。探测是 IP 维度的，即如果是域名源站，则会将域名解析为 IP 后再进行探测。该情况通常会出现在您填写了一个错误的域名源站，无法解析出 IP，此时建议您排查一下是否存在源站域名拼写错误或者对应的域名已过期。

说明：

不同地区的探测节点是独立决策的，边缘节点将根据实际各区域就近的探测节点的探测结果进行回源。

例如：您的源站在中国香港，位于新加坡的探测节点认为源站不健康，位于德国的探测节点认为该源站健康，那么新加坡地区的流量就不会被调度至该源站，而德国地区的流量还是会正常调度至该源站。

出现上述情况时，您可以综合参考其他地区的探测结果，如果只有少数节点认为源站不健康，那么可能是部分地区存在网络波动，如果大部分节点都认为源站不健康，那么建议您检查一下源站是否出现故障。

版权所有：腾讯云计算（北京）有限责任公司

相关参考
负载均衡相关概念

最近更新时间：2024-05-29 10:33:37

本文将为您介绍负载均衡中涉及到的相关概念。

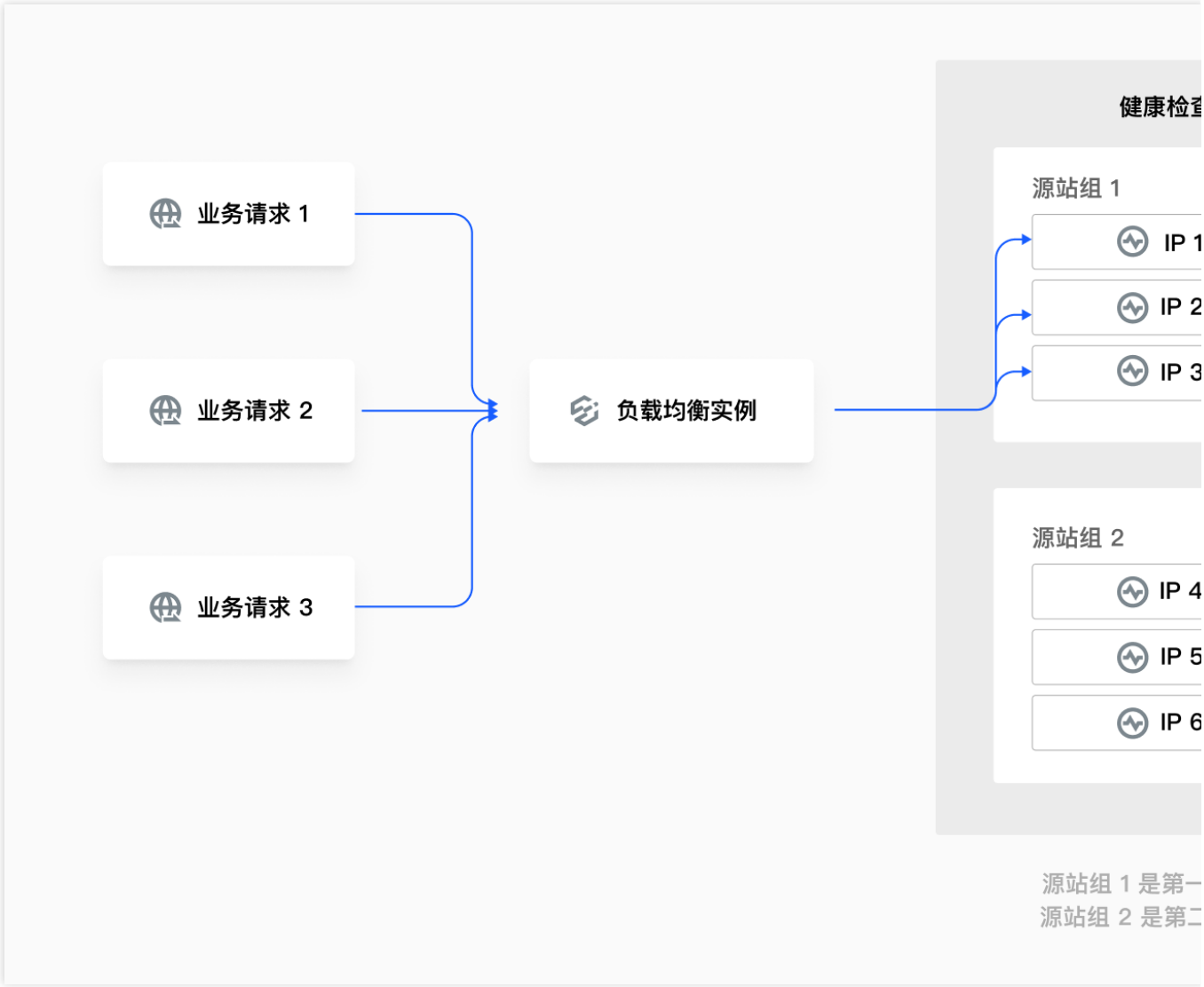
注意：

EdgeOne 负载均衡功能在内测中，如您需要使用请 联系我们。

负载均衡实例

负载均衡实例是一个虚拟的概念，它由源站组和健康检查策略组成。一个负载均衡实例中可以按照优先级顺序配置至多十个源站组以及一个健康检查策略，负载均衡实例将会根据探测结果以及配置的流量调度策略智能地分配业务流量。

版权所有：腾讯云计算（北京）有限责任公司



源站组

源站组是负载均衡中最小的源站配置单元，可以添加单个或多个源站。添加多源站时可以配置权重来调整流量负载，详情请参见 源站组操作指引。

健康检查策略

健康检查策略是由探测方式和健康判定条件组成。当前支持 ICMP Ping、HTTP/HTTPS、TCP 和 UDP 这四种探测方式，详情请参见 健康检查详解。

流量调度策略

流量调度策略只有当健康检查策略启用时才会生效，当前支持按“优先级顺序进行故障转移”策略，即根据探测结果，屏蔽故障源站，按照源站组的优先级顺序，将流量路由到健康源站。

请求重试策略

负载均衡可以在业务正常请求至某个源站出现请求失败时，根据请求重试策略将该请求调度至其它源站再次重试，以减少因网络问题、源站故障等原因导致的业务请求失败。详情请参见 请求重试策略介绍。

请求重试策略介绍

最近更新时间：2024-05-29 10:33:37

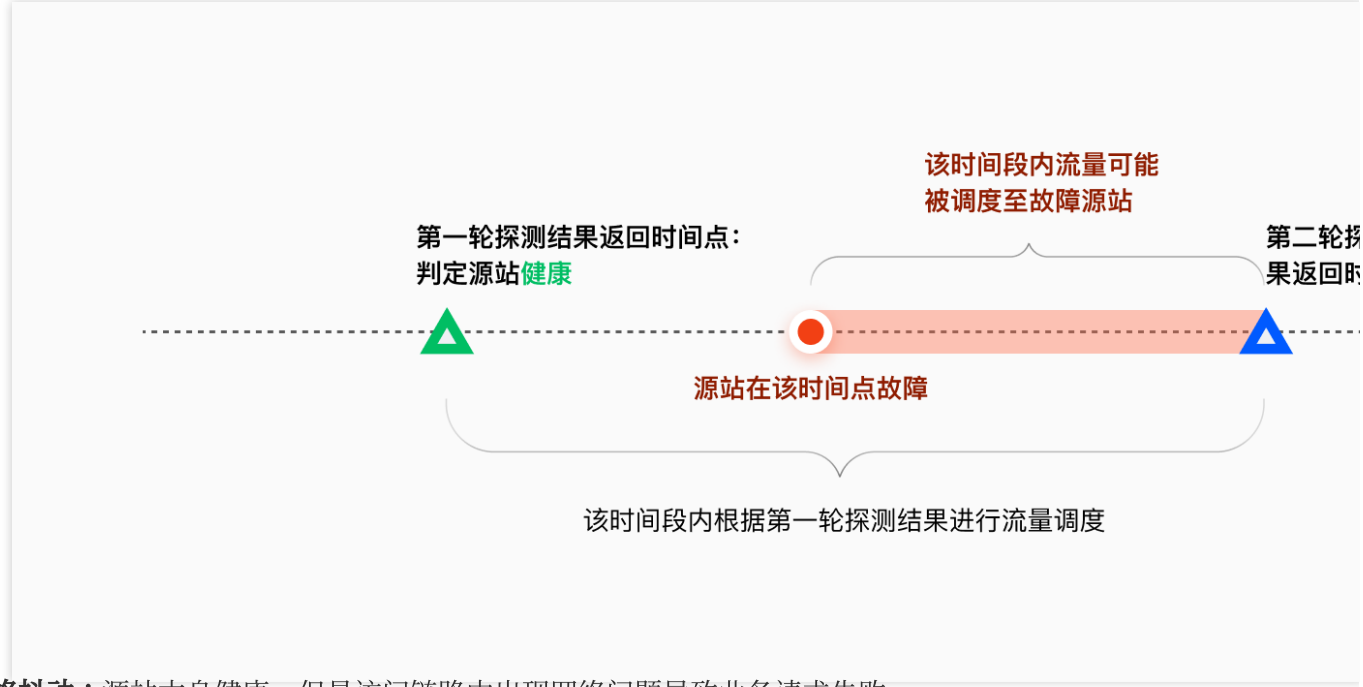
负载均衡可以在业务正常请求至某个源站出现请求失败时，根据请求重试策略将该请求调度至其它源站再次重试，以减少因网络问题、源站故障等原因导致的业务请求失败。

注意：

EdgeOne 负载均衡功能在内测中，如您需要使用请 联系我们。

实际业务请求可能会因为以下情况出现业务请求失败：

1. **源站故障后还未被主动探测屏蔽：**配置了健康检查策略后，主动探测是周期性进行的，在新一轮探测结果返回之前，会根据上一轮探测结果进行流量分配。如果源站在两轮探测结果之间从健康变成了不健康，此时业务流量就可能仍然被调度至不健康源站，从而导致业务请求失败。



2. **网络抖动：**源站本身健康，但是访问链路中出现网络问题导致业务请求失败。

说明：

请求失败包括回源建连失败和回源接收失败。

针对以上情况，EdgeOne 为您提供以下两种兜底的请求重试策略：

策略一：当真实业务请求访问某个源站失败时，直接重试到下一优先级源站组中的源站。适用于高优先级源站组和低优先级源站组性能相近的场景。

策略二：当真实业务请求访问某个源站失败时，直接重试到当前优先级源站组中的其他源站。适用于高优先级源站组性能远大于低优先级源站组的场景。

源站组操作指引

最近更新时间：2024-08-01 21:32:16

功能简介

以源站组的方式管理业务源站。此处配置的源站组可于 添加加速域名 和 四层代理 等功能中引用。

新建源站组

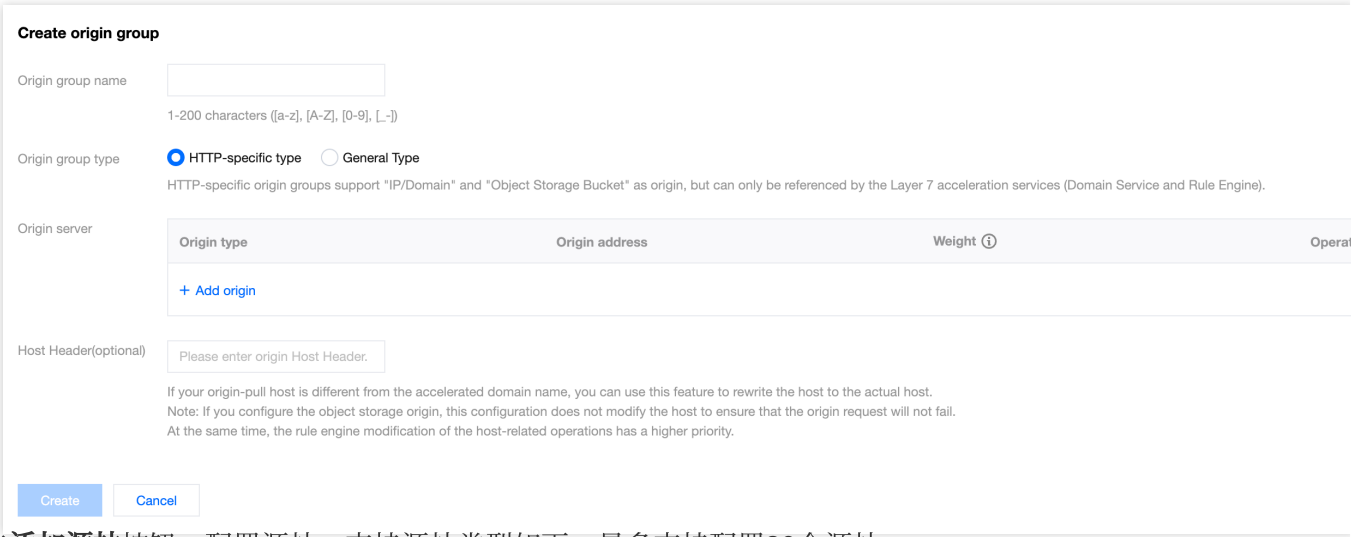
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**源站配置** > **源站组**。
3. 单击**新建源站组**。
4. 填入源站组名称，并且选择源站类型，具体类型说明如下：

HTTP 专用型：支持添加 **IP/域名源站**和**对象存储源站**，仅支持被站点加速相关服务引用（例如：域名服务和规则引擎-修改源站）。

通用型：仅支持添加 **IP/域名**为源站，不支持添加**对象存储源站**，能被站点加速服务（如域名服务和规则引擎）和四层代理引用。

注意：

配置完成后，源站组类型不支持修改。



5. 单击**添加源站**按钮，配置源站，支持源站类型如下，最多支持配置20个源站。

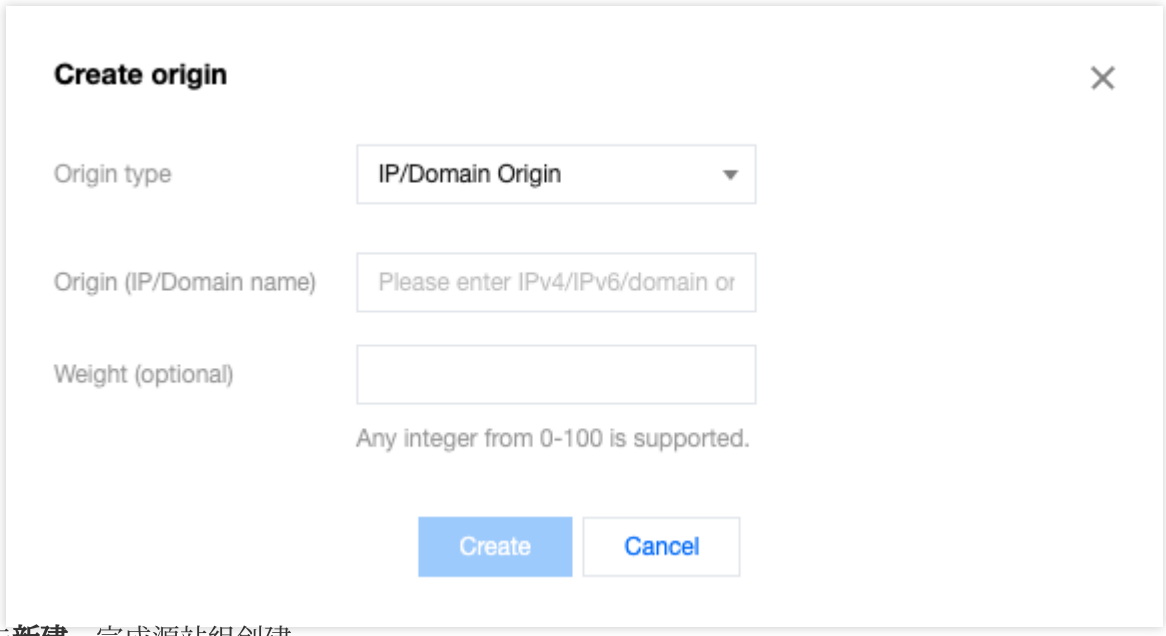
对象存储源站：腾讯云 COS 或者兼容 AWS S3 的其他对象存储桶。

IP/域名源站：支持 IPv4 地址，IPv6 地址，域名作为源站。

说明：

关于源站组中权重相关配置的说明：

1. 如果源站组内某个源站设定了权重，则源站组内所有源站都需同时设定相应的权重。权重支持填写0-100的整数。如果将某个源站的权重设定为0，则不会有任何回源请求分配至该源站。其它非0权重的源站将根据各自的权重比例分配回源请求。
2. 如果您没有设定权重，那么源站组内所有源站都应同时不设定权重。在这种情况下，如果未启用「智能加速」，EdgeOne 将等比例分配回源请求到每个源站。如果启用了「智能加速」，每次回源请求 EdgeOne 将选择最优质的源站。



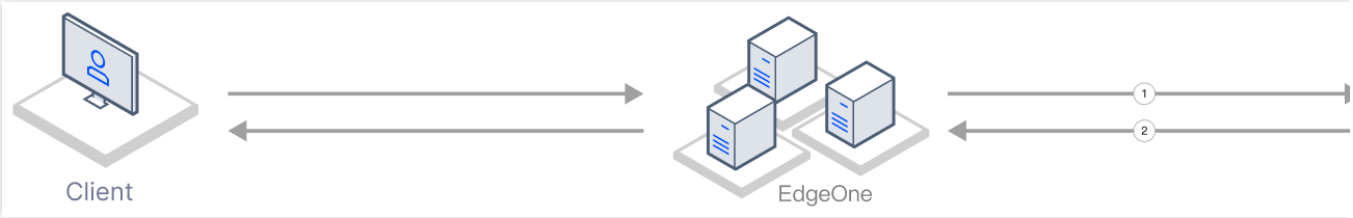
6. 单击**新建**，完成源站组创建。

回源配置
配置回源 HTTPS

最近更新时间：2023-12-13 11:10:23

功能说明

回源 HTTPS 用于指定 EdgeOne 在回源时所使用的请求协议。
在安全要求较高的场景下，需要采用 HTTPS 协议访问来保护网站的数据安全，通过指定回源协议为 HTTPS，可以确保从 EdgeOne 到源站的回源请求都采用了 HTTPS 协议，避免数据在传输过程中被篡改或窃取。
在一些需要快速响应的场景下，可以采用 HTTP 协议回源来加速网站的访问速度，通过指定回源协议为 HTTP，可以避免在 EdgeOne 和源站之间进行 SSL 握手等复杂的操作，从而加速网站的访问速度。或您的源站尚未支持 HTTPS，可选择 HTTP 回源。



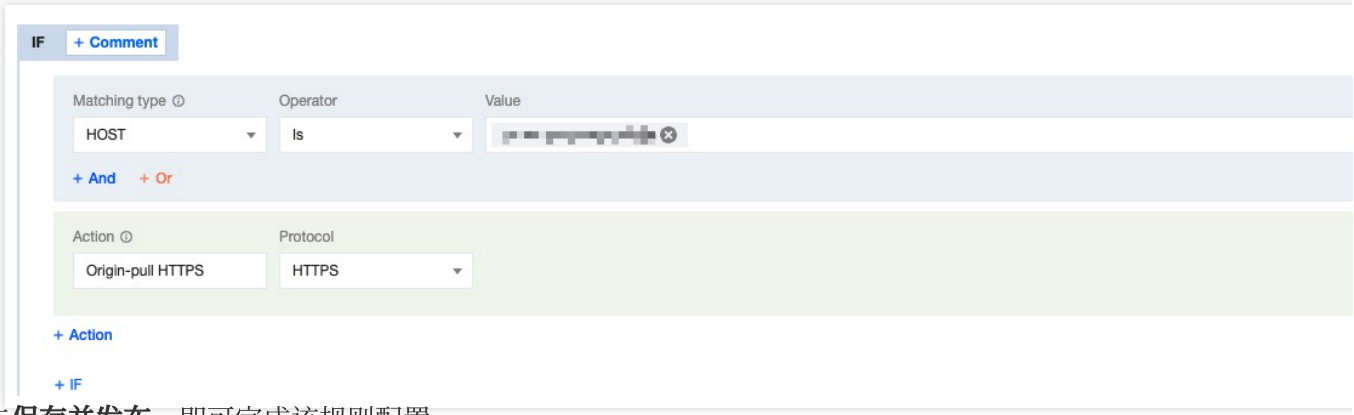
1. 节点发起回源请求，此时将使用平台指定的回源协议进行回源请求。
2. 源站响应节点请求，使用与节点请求相同的协议建连。

说明：
规则引擎的配置优先级更高，如果在域名服务、规则引擎内同时配置了回源协议规则，最终以规则引擎内为准。

场景一：针对多个域名在规则引擎内批量配置回源 HTTPS

若您需要针对多个不同域名统一将回源协议修改为回源 HTTPS，例如：`www.example.com`、`vod.example.com`、`image.example.com`。可参考以下步骤：

1. 登录 边缘安全加速平台 EO控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**。
2. 在站点详情页面，单击**规则引擎**。
3. 在规则引擎管理页面，单击**创建规则**，进入新规则的编辑页面。
4. 在规则编辑页面，输入规则名称，选择 Host 匹配类型以匹配指定域名的请求，以当前场景为例，选择域名`www.example.com`、`vod.example.com`、`image.example.com`。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为**回源 HTTPS**。



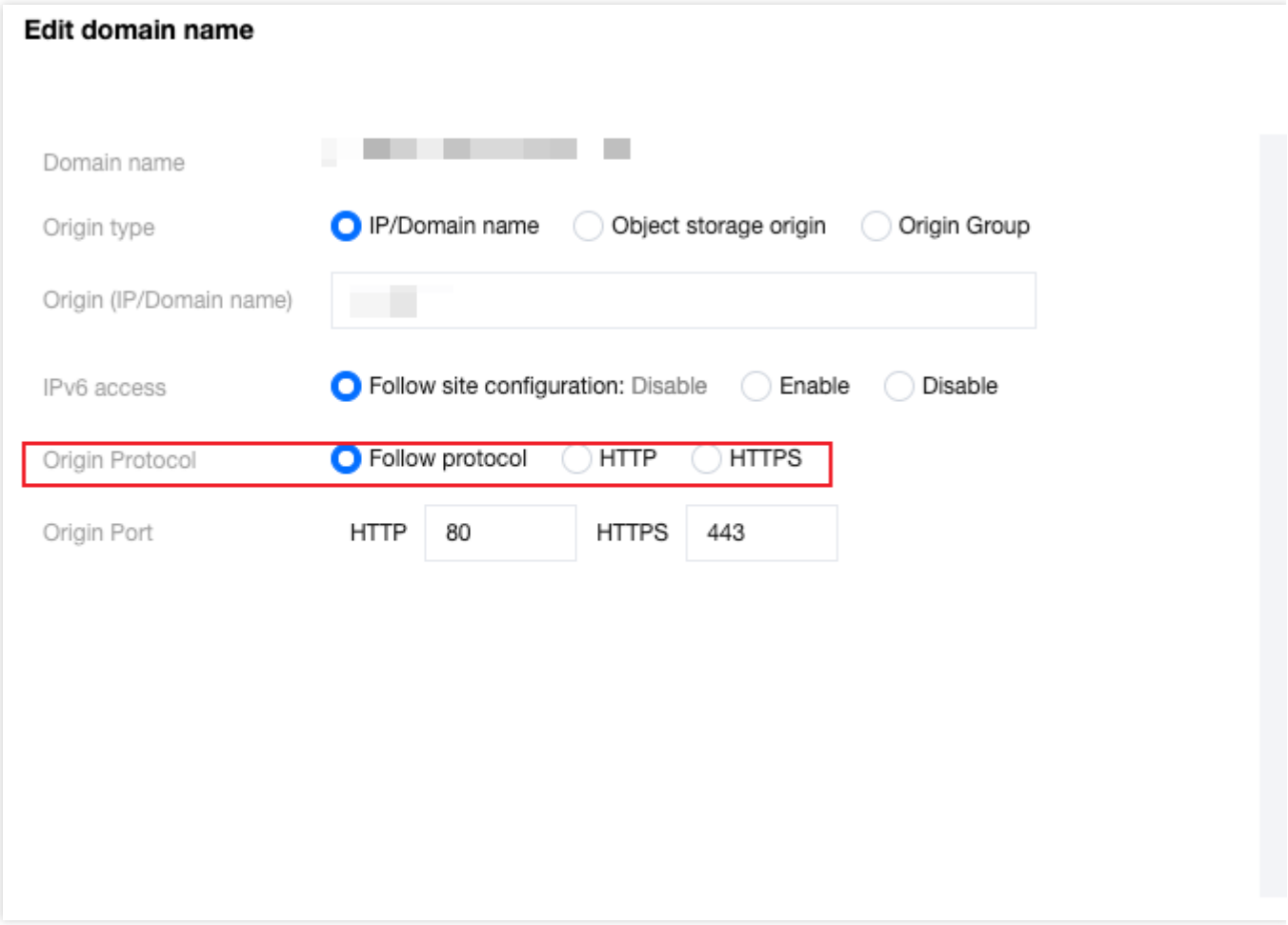
6. 单击**保存并发布**，即可完成该规则配置。

场景二：针对指定域名配置回源 HTTPS

若您需要指定某个特定域名将回源协议修改为回源 HTTPS，例如：`www.example.com`。可参考以下步骤：

1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**。
2. 在站点详情页面，单击**域名服务** > **域名管理**。
3. 在域名管理页面，选择当前需要修改的域名，单击**编辑**。

4. 在回源协议内，选择为 **HTTPS**，单击**完成**，即可完成修改。


Edit domain name
Domain name
Origin type
IP/Domain name
Object storage origin
Origin Group
Origin (IP/Domain name)
IPv6 access
Follow site configuration: Disable
Enable
Disable
Origin Protocol
Follow protocol
HTTP
HTTPS
Origin Port
HTTP
80
HTTPS
443

Host Header 重写

最近更新时间：2023-10-11 10:27:52

功能简介

重写 Host 头字段。若您的回源 Host 与 负载均衡 任务中接入的加速域名不同，可使用此功能重写 Host 至实际回源 Host。

操作步骤

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**源站配置 >规则引擎**。
2. 在规则引擎页面，选择所需站点，单击

可按需配置 Host Header 重写规则。
3. 在规则引擎页面，匹配类型 **Host**，操作选择 **Host Header 重写**，并按需配置其他参数，单击**保存发布**或**仅保存**。

说明

目前支持的匹配类型为 Host。

回源请求参数设置

最近更新时间：2023-12-14 17:43:30

功能简介

默认情况下，回源时会保留请求中原有的全部查询字符串和 Cookie。如果您的业务源站仅允许携带指定查询字符串或者 Cookie 信息回源请求时，可通过删除指定的回源请求参数，来确保回源请求正常。

操作步骤

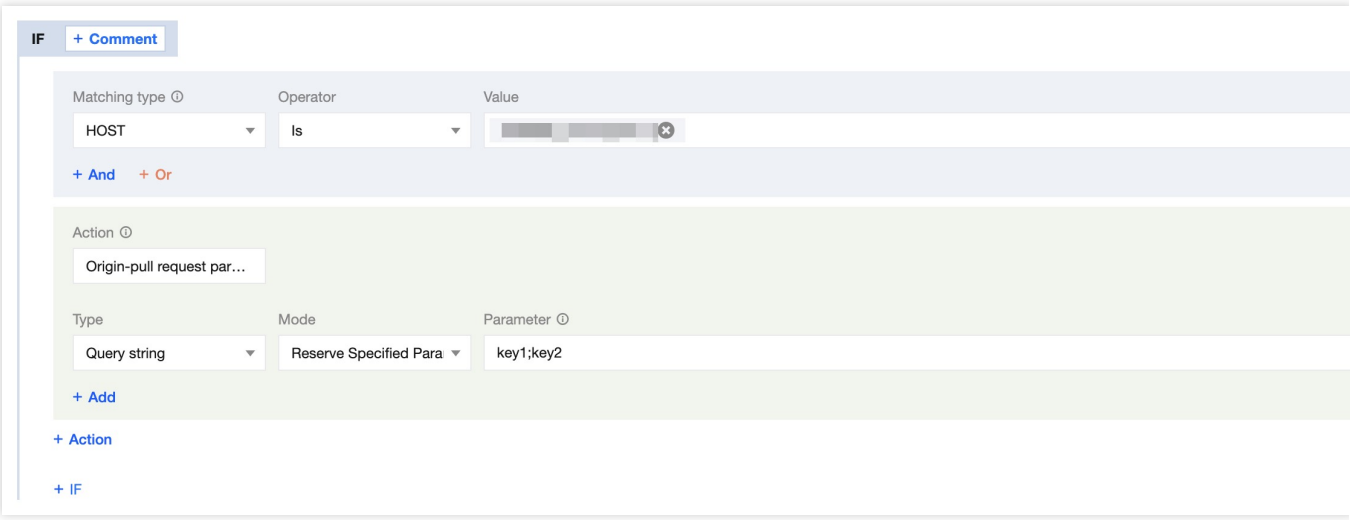
例如：客户端请求 URL： `http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d` ，回源时仅需保留 `key1=a` 参数。您可以参照以下步骤配置：

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**。
2. 在站点详情页面，单击**规则引擎**。
3. 在规则引擎管理页面，单击**创建规则**，进入新规则的编辑页面。

3.1 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。

3.2 单击**操作**，在弹出的操作列表内，选择操作为**回源请求参数设置**。

3.3 选择模式为保留指定参数，输入需保留的参数 `key1` 和 `key2` ，最多允许输入10个参数。



4. 单击**保存并发布**，即可完成该规则配置。

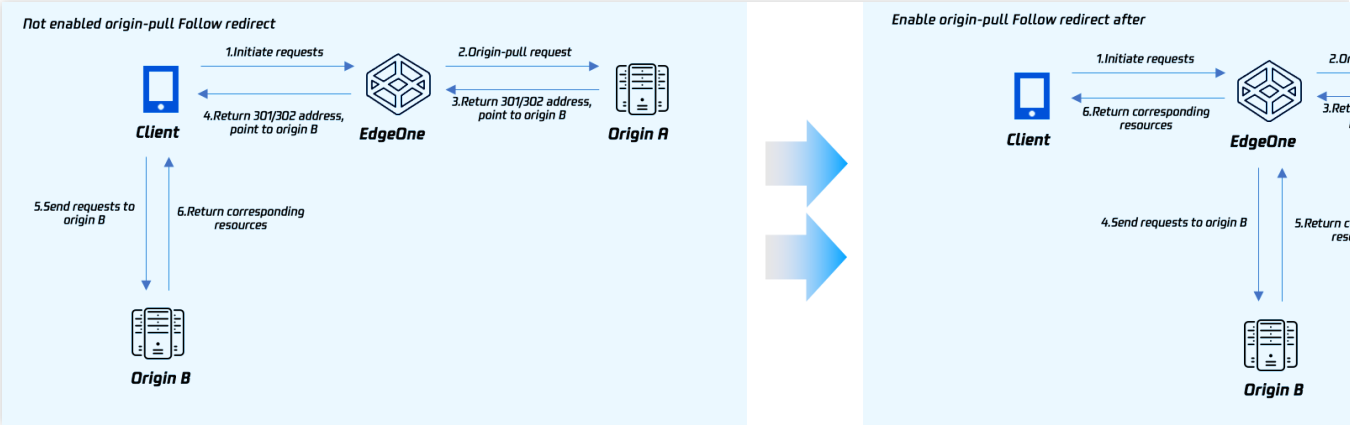
回源跟随重定向

最近更新时间：2023-10-11 10:25:40

功能简介

正常情况下，当源站返回 301/302 请求后，节点默认会将响应状态码返回给客户端，由客户端重定向到对应的资源进行访问。
EdgeOne 支持回源跟随重定向，开启后，节点回源时如收到 301/302 状态码，会主动跟随重定向（不超过设置的最大重定向次数）至指定的地址，直到获取对应文件后，再响应客户端实际资源，能够提高用户的访问响应速度。

例如：客户端访问 URL 为 `https://a.example.com/test.jpg`，源站 A 将该 URL 302重定向至 `https://b.example.com/test.jpg`，并且域名 `a.example.com` 已接入 EdgeOne 服务，`b.example.com` 还未接入加速服务。则：
未开启回源跟随重定向：客户端发起访问后，如果 EdgeOne 节点内无缓存，则回源站 A 访问并收到302状态码后，会将该状态码响应至客户端，由客户端直接向源站 B 发起请求并获取对应资源。此时，因为源站 B 未接入加速服务，客户端自行发起访问速度较慢，且获取文件后无法缓存，当有其他用户访问相同文件时，需要再次重复该流程。
开启回源跟随重定向：客户端发起访问后，如果 EdgeOne 节点内无缓存，则回源站 A 访问并收到302状态码后，会根据该状态码及相应地址，直接向源站 B 发起请求并获取对应资源后，缓存该资源在节点中。此过程由 EdgeOne 节点来进行回源请求，请求速度更快，且获取文件后可缓存于节点中，当有其他用户访问相同文件时，无需重复回源，可直接命中文件并响应客户端。



操作步骤

例如：若您需要针对指定域名 `www.example.com` 开启回源跟随重定向，最大重定向次数为3次。可参考以下步骤：

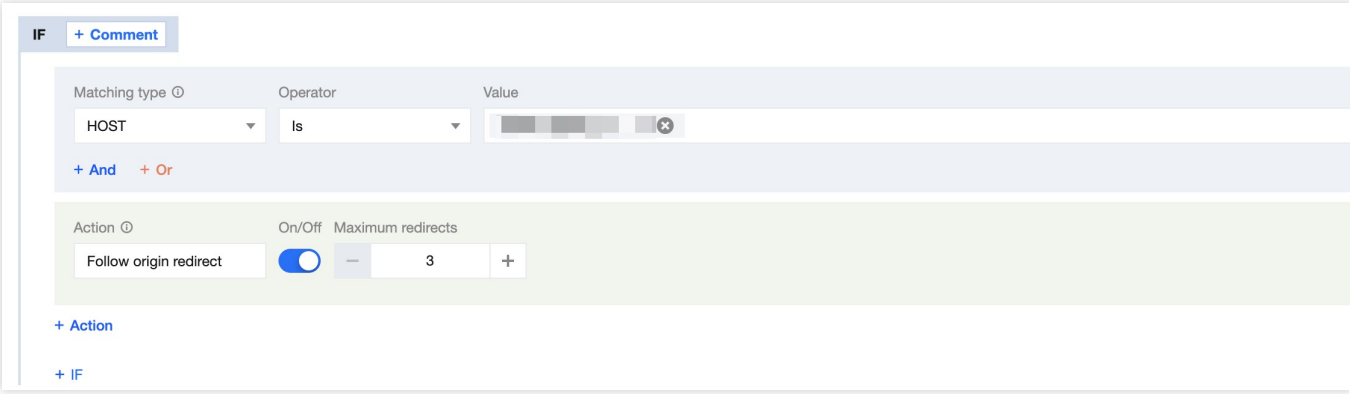
1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**。
2. 在站点详情页面，单击**规则引擎**。
3. 在规则引擎管理页面，单击**创建规则**，进入新规则的编辑页面。以当前场景为例，可按照如下步骤操作：

3.1 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。

3.2 单击**操作**，在弹出的操作列表内，选择操作为**回源跟随重定向**。

3.3 单击开关，单击开关切换为开启，可配置最大重定向次数为 3次，相关配置说明如下：

最大重定向次数：可配置1-5次，在最大重定向次数内，节点将跟随重定向地址直到获取相应资源，超出最大重定向次数后，将直接响应对应状态码给客户端。



4. 单击**保存并发布**，即可完成该规则配置。

HTTP/2 回源

最近更新时间：2023-10-11 10:28:34

功能简介

支持 EdgeOne 节点以 HTTP/2 协议进行回源。HTTP/2（即 HTTP 2.0，超文本传输协议第2版），是 HTTP 协议的第二个主要版本，能有效减少网络延迟，提高站点页面加载速度。

说明：

1. 开启后，需源站支持 HTTP/2 协议访问。
2. 若需配置 HTTP/2 访问，请参见 HTTP/2。

操作步骤

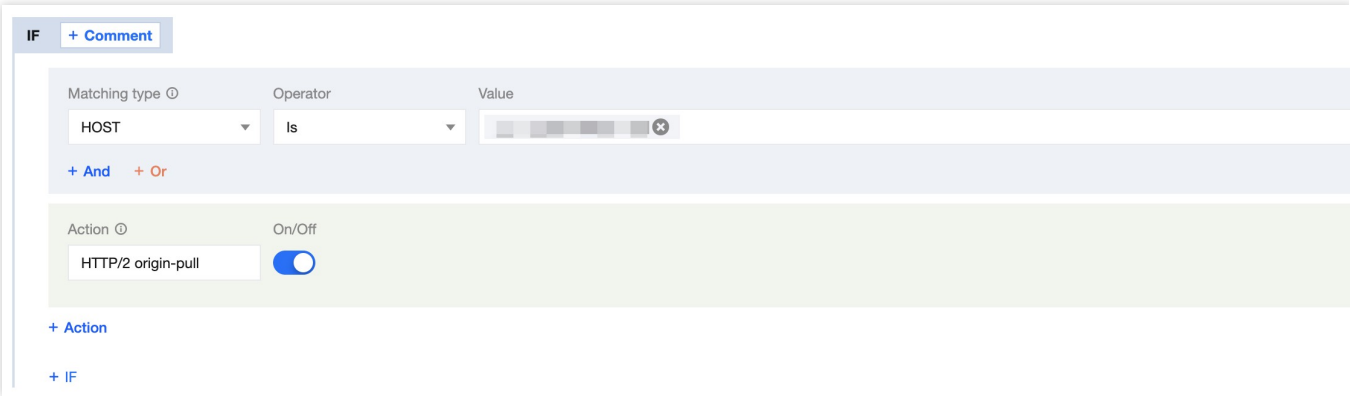
若您需要针对指定域名 `www.example.com` 开启或关闭 HTTP/2 回源，可参考以下步骤：

1. 登录 边缘安全加速平台控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**。
2. 在站点详情页面，单击**规则引擎**。
3. 在规则引擎管理页面，单击**创建规则**，进入新规则的编辑页面。以当前场景为例，可按照如下步骤操作：

3.1 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。

3.2 单击**操作**，在弹出的操作列表内，选择操作为**HTTP/2 回源**。

3.3 单击**开关**，开启/关闭 HTTP/2 回源即可。



4. 单击**保存并发布**，即可完成该规则配置。

分片回源

最近更新时间：2024-01-02 10:00:01

功能简介

开启后支持分片回源，有助于减少大文件回源消耗，缩短响应时间。

为什么分片回源可以提升大文件分发效率？

节点在缓存资源时，为提高缓存效率，会将资源文件分片缓存（所有分片在节点的缓存时间相同，遵循节点缓存过期 TTL 配置），同时支持 Range 请求。若客户端请求时携带 HTTP 头部 `Range: bytes = 0-999`，则只返回文件的前1000个字节，并非整个文件。
开启分片回源后，若客户端请求的并非整个文件，仅部分文件，且该部分文件在节点的缓存已过期，需回源获取最新的资源。节点会根据客户端请求分片回源，即仅回源拉取客户端需要的部分文件缓存至节点，同时返回给用户。有效减少回源消耗，提升了整体响应速度。
若未开启分片回源，客户端请求的是部分文件，节点回源时遵循客户端 range 范围回源拉取，也只会拉取请求的部分文件并缓存至节点，同时返回给客户端请求的部分文件，但是可能在性能上无法达到最优化。在大文件场景下，建议打开分片回源。

适用场景

若您的业务资源都是静态大文件，且源站已支持 Range 请求，或源站为腾讯云 COS 源站且**未使用**数据处理类功能（例如：图片处理），建议开启分片回源，提升分发效率和响应速度。

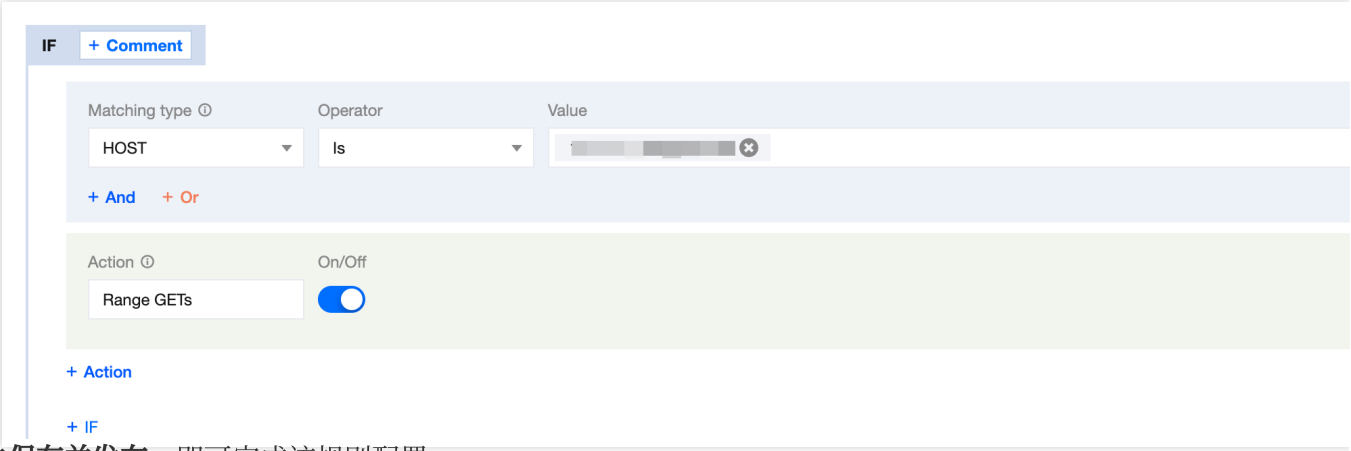
注意事项

业务源站需同步支持 Range 请求，否则可能会导致回源失败。
若请求资源都是静态小文件，或业务源站为腾讯云 COS 源站且已使用数据处理类功能（例如：图片处理），不建议开启分片回源，开启后会影响回源。

操作步骤

例如：当前您有一个视频服务网站通过 `video.example.com` 提供在线视频观看，视频以长视频为主，文件较大，为了减少大文件回源流量消耗并提高回源速度，需支持 range 请求和回源。您可以参照以下步骤操作：
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**。

2. 在站点详情页面，单击**规则引擎**。
3. 在规则引擎管理页面，单击**创建规则**，进入新规则的编辑页面。以当前场景为例，可按照如下步骤操作：
3.1 在规则编辑页面，匹配类型选择为 HOST 等于 video.example.com。
3.2 单击**操作**，在弹出的操作列表内，选择操作为**分片回源**。
3.3 单击**开关**，开启分片回源即可。



4. 单击**保存并发布**，即可完成该规则配置。

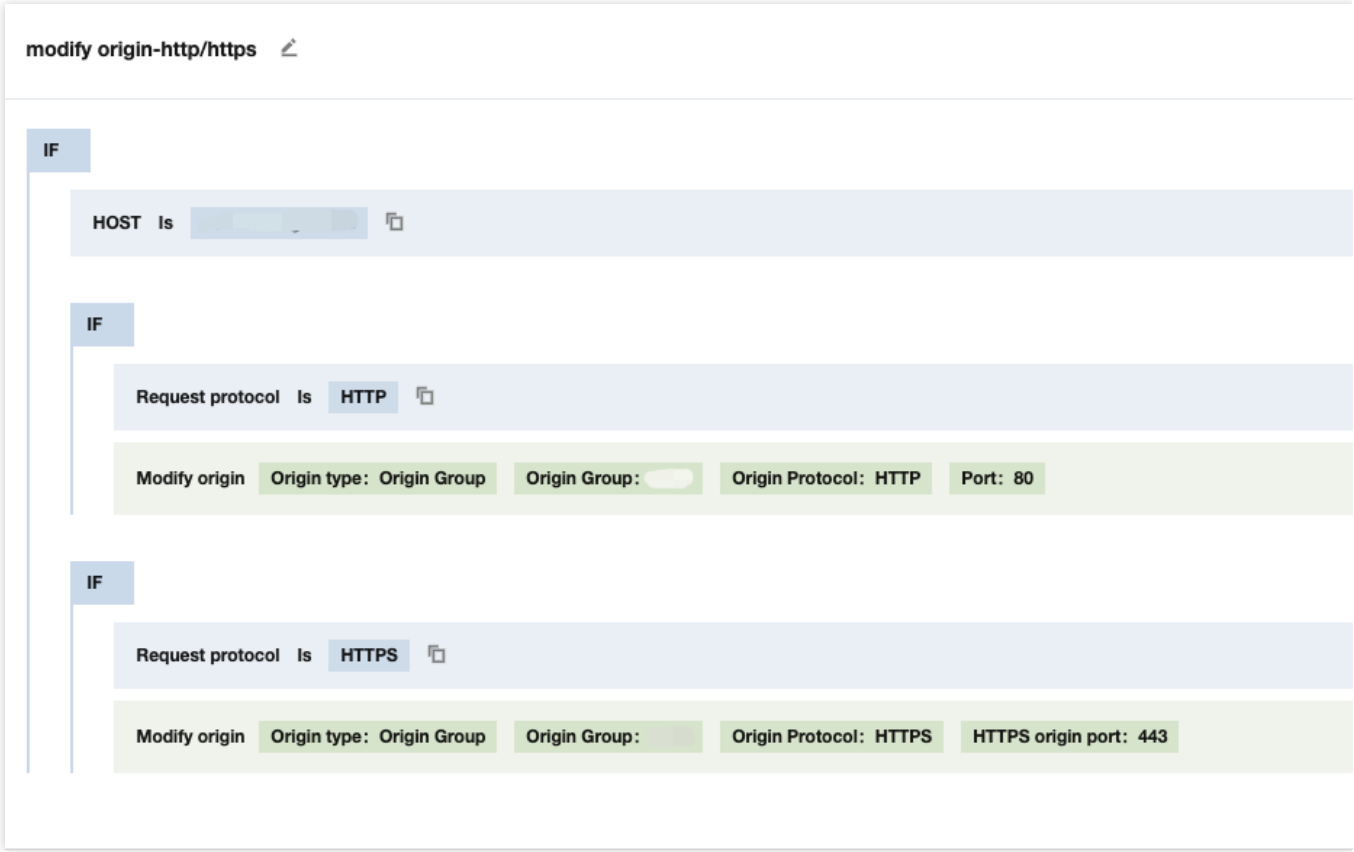
相关参考
旧版源站组兼容相关问题

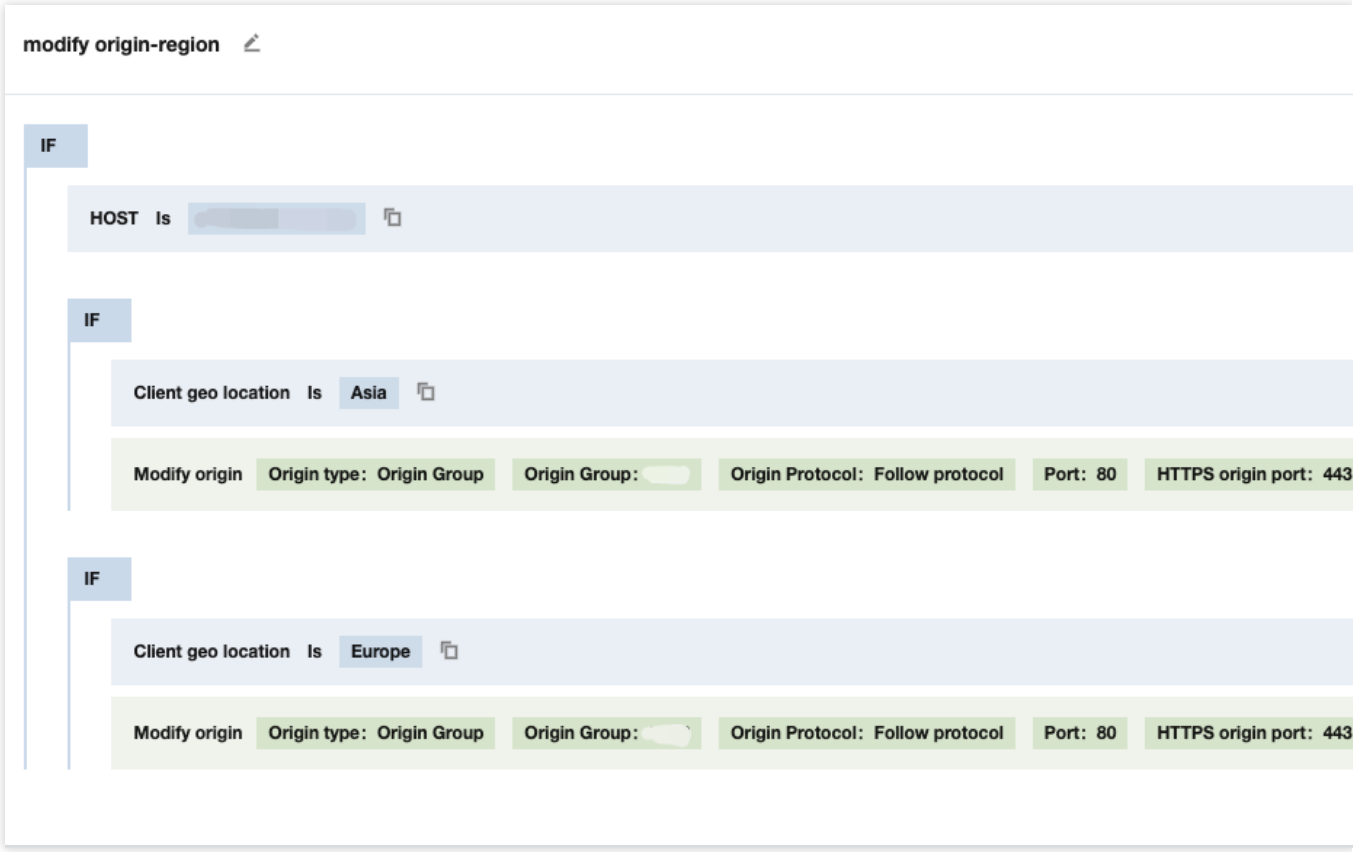
最近更新时间：2023-10-24 15:44:27

源站组已于 2023 年 10 月 24 日起进行产品能力升级。升级后，旧版源站组将以以下方式进行兼容性处理，同时，我们也建议您转换至新版源站组的使用。

源站类型&配置方式兼容

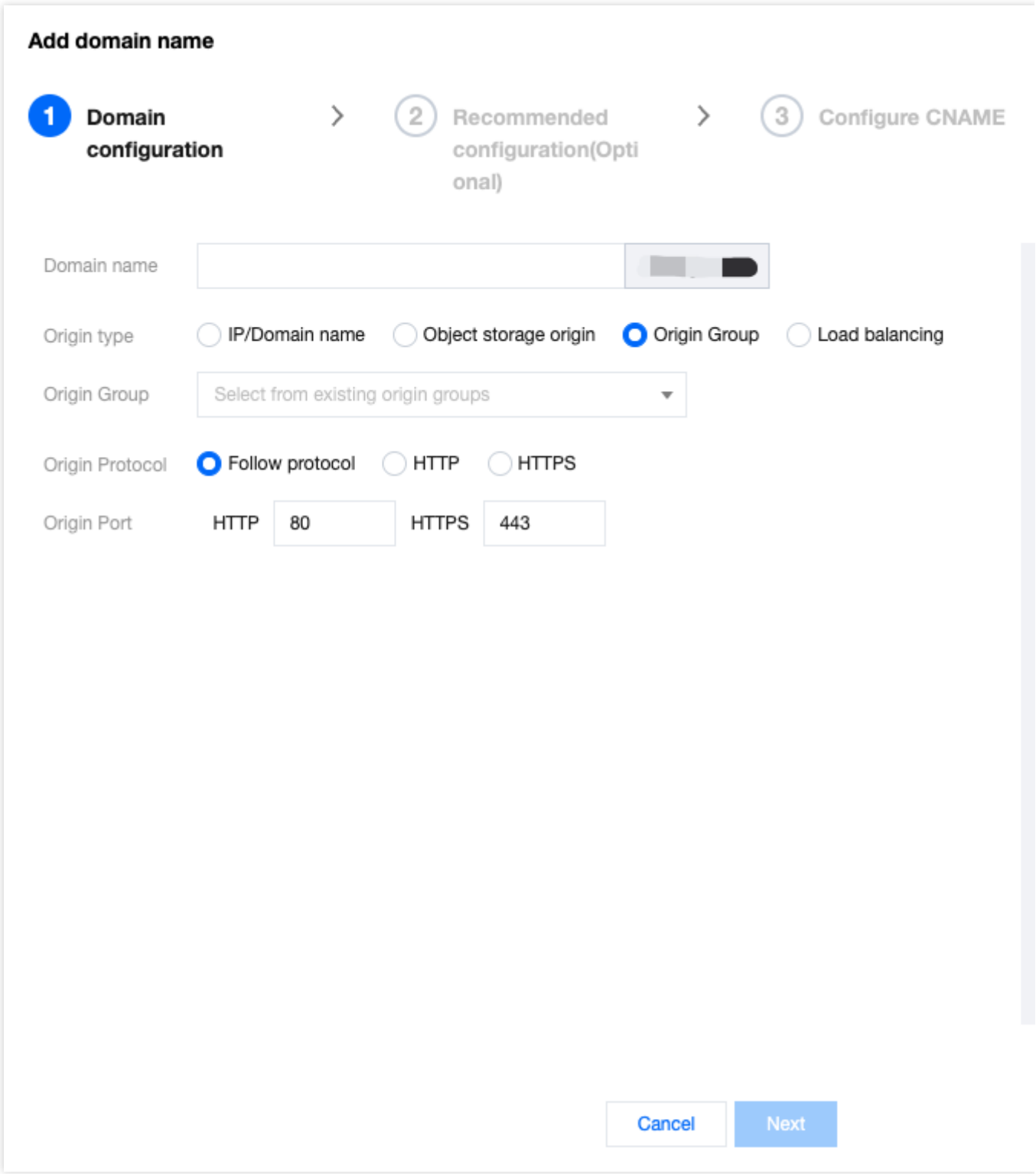
新版源站组将不再区分**自有源站、对象存储源站、腾讯云 COS** 类源站，原源站类型为**对象存储源站、腾讯云 COS** 的源站组将自动更新为新版 **HTTP 专用型**源站组，原源站类型为**自有源站**的源站组将自动更新为**通用型**源站组。
源站组内不再支持配置使用按地域/协议回源，如果您原来有配置相关的按地域/协议回源规则，该规则将迁移至规则引擎内，如下所示：

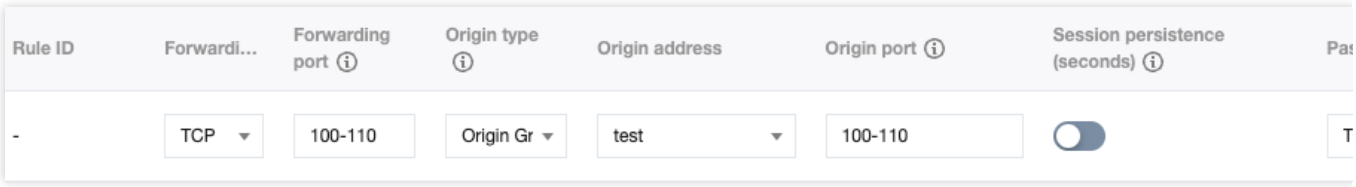




源站组端口迁移说明

新版源站组将不再支持配置端口，所有端口的配置将迁移到服务配置入口，例如：四层代理或者域名管理。


Add domain name
1 Domain configuration
2 Recommended configuration(Optional)
3 Configure CNAME
Domain name
Origin type
IP/Domain name
Object storage origin
Origin Group
Load balancing
Origin Group
Select from existing origin groups
Origin Protocol
Follow protocol
HTTP
HTTPS
Origin Port
HTTP
80
HTTPS
443
Cancel
Next



主备源站相关配置说明

加速域名管理和**规则引擎-修改源站**中，不再支持直接配置主备源站，存量配置不会受影响，但不再支持修改。如果您当前有主备源站配置需求，请联系我们支持。

VOD 源站相关说明

最近更新时间：2024-07-29 15:38:48

源站介绍

腾讯云点播 面向音视频、图片等媒体，提供制作上传、存储、转码、媒体处理、媒体 AI、版权保护、播放等一体化的高品质媒体服务。

VOD 源站优势

优势	说明
多维成本优化	腾讯云点播为媒体服务提供媒资降冷、智能降码等策略，通过实时媒体播放情况进行精细成本优化，有效节省用户的存储及分发成本。
场景化转码	腾讯云点播为各行业场景提供更优质的转码能力，通过智能场景识别、动态编码、CTU/行/帧三级码率精准控制模型等技术，以更低的码率（近50%）获得更高的主观画质，实现**高画质低码率**，同时节约网络流量和存储成本。
稳定存储	腾讯云点播支持媒体文件跨多架构、多设备备份存储，提供异地容灾和用户资源隔离，极大提升存储稳定性。
优质上传	腾讯云点播通过调度优化、全球多存储园区覆盖优化、链路补充、传输优化、QUIC 协议等多种上传加速措施，改善数据传输的效率和在弱网环境中的稳定性，提高上传的速度和成功率。
版权保护	腾讯云点播版权保护提供防盗链、幽灵水印、HLS 私有加密和商业级 DRM 加密，为内容版权商提供高级别的安全保障。
音视频分发调优	当用户选择 VOD 源站时，EdgeOne 加速服务默认开启音视频文件预拉取能力，支持在客户端请求时预先对 HLS/DASH/MP4/FLV 格式文件进行分片拉取并缓存至边缘节点，提高视频文件的响应速度，从而**优化视频启播耗时、播放卡顿率**等。

VOD 源站适用场景

使用场景	场景说明
在线教育	在线教育指以网络为介质的教学方式，学员与教师通过网络开展教学活动。平台一般都有大量音视频教学资源，大部分通过入驻的教师录制课程并上传。腾讯云点播为该场景

	提供多端播放、智能字幕、版权保护、时移回看、点播转直播、内容审核等功能，帮助用户快速搭建音视频教学平台。
电商 App	电商 App 是为企业或个人提供网上交易洽谈的平台，商家为更好地展示商品，一般都会制作上传推广的商品图片、视频。消费者可以上传商品体验视频用于购物分享，或者商品评论，供其他消费者参考。腾讯云点播为该场景提供高清低码、智能截图封面、多码率智能切换、上传加速、标签分类等功能，从而帮助客户更好展示电商商品。
广电 OTT	广电 OTT 主要基于电视终端提供流媒体服务，腾讯云点播为该场景提供极速高清转码、多码率智能切换、版权保护、媒体 AI 识别、点播转直播、视频制作等功能，帮助客户快速搭建智能媒资库，并提供云端剪辑、视频导播等多元应用。
直播 App	直播 App 指主播通过网络实时进行某种现场播报、解说或表演的平台，包括秀场直播、游戏直播、网络直播课、直播带货、直播答题等。腾讯云点播为该场景提供直播录制、时移回看、直播剪辑、极速高清、点播转直播等能力，帮助客户快速搭建稳定可用的直播平台。

使用限制

使用云点播源站将为您自动提供更适合媒体内容的分发加速配置，因此云点播源站类型在使用规则引擎及站点加速配置时，部分操作将使用云点播默认配置，以提供更优的分发加速效果。为避免自定义配置与默认配置冲突，将不支持部分站点加速配置及规则引擎中的操作，详细限制情况如下：

说明：

如您需要针对云点播源站修改以下不支持的配置项，请 联系我们。

功能模块	操作类型	操作	限制情况
规则引擎	缓存配置	节点缓存 TTL	不支持自定义配置，如已配置则配置内容不生效
		浏览器缓存 TTL	不支持自定义配置，如已配置则配置内容不生效
		自定义 CacheKey	不支持自定义配置，如已配置则配置内容不生效
		状态码缓存 TTL	不支持自定义配置，如已配置则配置内容不生效
		缓存预刷新	不支持自定义配置，如已配置则配置内容不生效
		离线缓存	不支持自定义配置，如已配置则配置内容不生效
	网络优化	HTTP/2	支持自定义配置
		HTTP/3 (QUIC)	支持自定义配置
		WebSocket	不支持自定义配置，如已配置则配置内容不生效

		最大上传大小	不支持自定义配置，如已配置则配置内容不生效
		智能压缩	不支持自定义配置，如已配置则配置内容不生效
		智能加速	不支持自定义配置，如已配置则配置内容不生效
		HTTP/2 回源	不支持自定义配置，如已配置则配置内容不生效
		回源超时时间	不支持自定义配置，如已配置则配置内容不生效
	HTTPS优化	强制 HTTPS	支持自定义配置
		HSTS 配置	支持自定义配置
		SSL/TLS 安全配置	支持自定义配置
		OCSP 装订	支持自定义配置
		回源 HTTPS	不支持自定义配置，如已配置则配置内容不生效
	修改HTTP头	修改 HTTP 节点响应头	支持自定义配置
		客户端 IP 头部	不支持自定义配置，如已配置则配置内容不生效
		客户端 IP 地理位置	不支持自定义配置，如已配置则配置内容不生效
		修改 HTTP 回源请求头	不支持自定义配置，如已配置则配置内容不生效
		Host Header 重写	不支持自定义配置，如已配置则配置内容不生效
	高级配置	访问 URL 重定向	支持自定义配置
		Token 鉴权	支持自定义 A/D 鉴权方式，不支持自定义 B/C 鉴权方式
		修改源站	不支持自定义配置，如已配置则配置内容不生效
		回源 URL 重写	不支持自定义配置，如已配置则配置内容不生效
		回源请求参数设置	不支持自定义配置，如已配置则配置内容不生效
		回源跟随重定向	不支持自定义配置，如已配置则配置内容不生效
		自定义错误页面	不支持自定义配置，如已配置则配置内容不生效
		分片回源	不支持自定义配置，如已配置则配置内容不生效
		HTTP 应答	支持自定义配置

版权所有：腾讯云计算（北京）有限责任公司

站点加速	缓存配置	查询字符串	不支持自定义配置，如已配置则配置内容不生效
		忽略大小写	不支持自定义配置，如已配置则配置内容不生效

获取 EdgeOne 回源节点 IP

最近更新时间：2023-12-15 09:55:22

获取 EdgeOne 的回源节点 IP，可以用于在源站防火墙中将 EdgeOne 的回源节点 IP 设为白名单，只允许固定来源（IP）请求源站，以实现对源站的保护。

获取方式

1. 通过浏览器或 curl 命令直接访问 https://api.edgeone.ai/ips。即可获取所有 EdgeOne 在全球可用区内的 IPv4 和 IPv6 回源节点 IP 地址，响应结果为 UTF-8 编码的纯文本，一行一个 IP 段。
2. 如果您只需要获取指定区域或指定 IP 地址类型的回源节点 IP，您也可以通过携带指定查询字符串（QueryString）来筛选回源节点 IP，支持的查询字符串如下：

查询字符串	释义
version	指定获取的回源节点 IP 地址类型，参数取值如下： **v4**：所有的 IPv4 的回源节点 IP 地址 **v6**：所有的 IPv6 的回源节点 IP 地址 不带此参数的时候默认返回所有IPv4 和 IPv6 的 IP 地址。
area	指定获取的回源节点 IP 区域，参数取值如下： **global**：全球可用区内所有回源节点 IP 地址 **mainland-china**：中国大陆可用区内的回源节点 IP 地址 **overseas**：全球可用区（不含中国大陆）内的所有回源节点 IP 地址 不带此参数的时候默认返回全球可用区内所有回源节点 IP 地址

说明：

1. 一般情况，建议可以根据您的站点服务区域选择获取对应的区域的回源节点 IP 地址即可。例如：站点服务区域为中国大陆可用区，获取中国大陆可用区内的回源节点 IP 地址即可，其他服务地域同理。
2. 本功能与 源站防护 功能互斥，若您需要通过本文档方法获取最新回源 IP，请确定您已关闭业务 源站防护 功能。

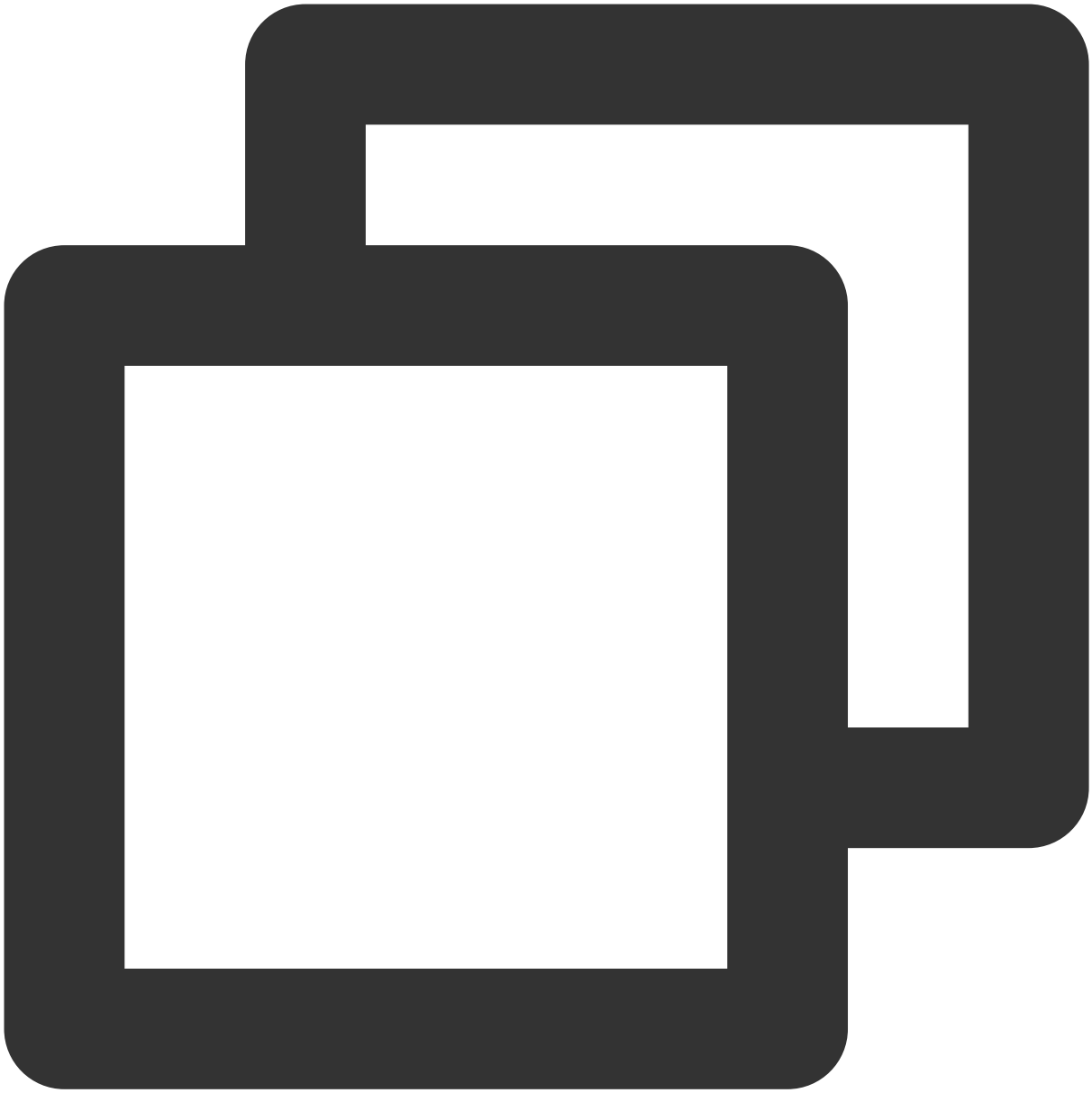
请求示例

若您想获得全球可用区（不含中国大陆）的所有 IPv6 回源节点 IP，可以通过在请求的 URL 中携带 `version=v6&area=overseas` 来查询此条件下的回源 IP 地址，具体的 URL 为：

```
https://api.edgeone.ai/ips?version=v6&area=overseas
```

响应结果示例如下（此结果仅为示例，具体回源 IP 请参照实时请求结果）

版权所有：腾讯云计算（北京）有限责任公司



```
240d:c010::/28
2001:ee0:324b:100::/64
2405:3200:101:63::/64
2405:4800:a601::/64
2602:ffe4:c02:1001::/64
2602:ffe4:c12:101::/64
2602:ffe4:c12:105::/64
2602:ffe4:c15:124::/64
2602:ffe4:c18:c003::/64
2602:ffe4:c18:c201::/64
2602:ffe4:c18:c203::/64
```

版权所有：腾讯云计算（北京）有限责任公司

```
2602:ffe4:c27:1003::/64
2604:980:4002:2::/64
2604:980:5003:2::/64
2604:980:7002:6::/64
2a02:b60:2001::/64
```