边缘安全加速平台 EO

域名服务与源站配置

腾讯云

文档目录

域名服务与源站配置
域名服务
概述

最近更新时间：2024-10-30 15:14:42

流量调度管理是腾讯云 EdgeOne 提供的多 CDN 智能解析调度工具，支持在源站、多个服务商之间自定义流量调度策略，实现流量平滑灰度迁移和灵活分配，保证服务高可用。当您的站点接入 EdgeOne 后，您可以通过域名服务模块来管理您的接入域名。在接入站点时，EdgeOne 为您提供了三种不同的接入模式，包括 NS 接入、CNAME 接入以及 DNSPod 托管接入，根据站点接入的不同，在域名服务模块内也将提供不同的能力。

接入方式介绍

为了让用户可以更灵活地根据实际业务需求接入至 EdgeOne 内，EdgeOne 当前已支持三种接入方式，分别是 NS 接入、CNAME 接入以及 DNSPod 托管接入，以下为三种方式的对比：

模式	NS 接入（推荐）	CNAME 接入	DNSPod 托管接入
适用场景	可修改域名的 DNS 解析服务商，将域名解析服务切换至 EdgeOne。	如果当前域名已托管在其他域名解析服务商处，不希望更改原有解析服务商，您可以使用 CNAME 接入。	当域名托管在腾讯云 DNSPod 时，建议使用该模式接入。
DNS 记录管理	接入后，统一在 EdgeOne 管理当前域名的 DNS 记录。	接入后，仍然在原域名解析服务商管理 DNS 记录。	接入后，仍然在腾讯云 DNSPod 控制台内管理 DNS 记录。
优势	可在 EdgeOne 内一站式管理域名的 DNS 记录，并且域名加速生效后，可支持默认直接解析 A 记录指向最近的 EdgeOne 边缘节点，减少域名解析耗时。	不要求变更域名的 DNS 解析服务商即可接入，使用方式更加灵活，可在多云厂商之间快速切换。	通过 DNSPod 托管接入可以免校验域名归属权，并支持一键添加域名 CNAME 记录实现快速开启加速。

支持的能力

根据接入方式的不同，在域名服务菜单内，将为您提供不同的能力：

功能	介绍	适用接入模式
DNS 记录	用于管理该域名的 DNS 解析记录，根据接入模式不同，能力有所区别： • **NS 接入：**在修改 DNS 服务器指向 EdgeOne 后，可在 DNS 记录内管理该域名的所有解析记录，支持解析记录的新增、修改、删除。 • **DNSPod 托管接入：**将自动同步您当前域名在 DNSPod 内配置的 A/AAA/CNAME 记录，仅允许查看，如需新增、修改、删除解析记录可前往 DNSPod 控制台内进行管理。	• NS 接入 • DNSPod 托管接入
DNS 配置	用于配置 DNS 高级能力，包括 DNSSEC、自定义 NS 服务器名称等。	NS 接入
域名管理	集中管理接入 EdgeOne 的加速域名信息，在该页面内支持配置该加速域名的源站、HTTPS 证书。	所有接入模式
流量调度管理	流量调度管理是 EdgeOne 提供的智能解析调度工具，支持在源站、多个服务商之间自定义流量调度策略，实现流量平滑灰度迁移和灵活分配，保证服务高可用。	• CNAME 接入 • DNSPod 托管接入

托管域名 DNS 解析
修改 DNS 服务器

最近更新时间：2024-04-19 14:43:51

本文介绍了当您选择 NS 接入站点时，如何修改 DNS 服务器，只有当您完成修改时，EdgeOne 才能够为您的站点提供解析、加速、安全一体化服务。

> **注意：**
> 该操作仅在 NS 接入模式下需要，如果您是 CNAME 模式接入，不需要进行该操作。

操作步骤

1. 前往您域名的注册商处登录管理员账号，域名注册服务商可以通过 ICANN WHOIS 查询。
2. 将您的 DNS 服务器地址修改为由 EdgeOne 提供的服务器地址。

部分域名注册商的配置可参考：

腾讯云

1. 登录 腾讯云域名注册控制台 。
2. 在**我的域名**页面，定位目标域名，单击操作列下的**管理**。

3. 在 DNS 解析窗口中，单击**修改 DNS 服务器**。

4. 在修改 DNS 服务器窗口中，选择**自定义 DNS** 并填写 EdgeOne 给您提供的 DNS 服务器地址。
5. 完成后单击**提交**即可。

阿里云

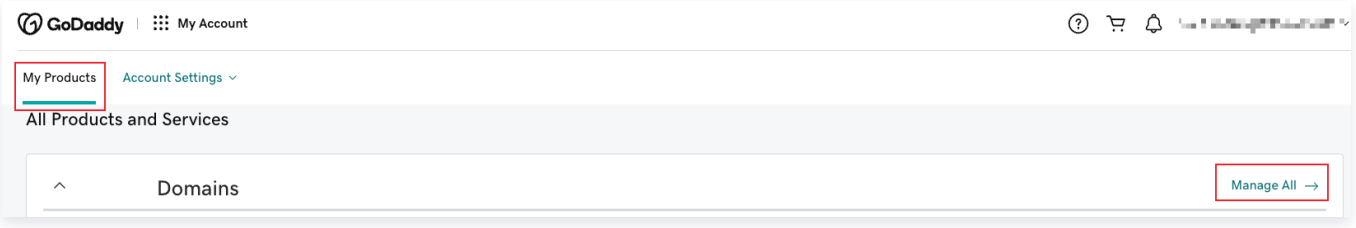
1. 登录 阿里云域名控制台 。
2. 在**域名列表**中定位目标域名，单击操作列下的**管理**。
3. 在左侧导航栏中，单击 **DNS 修改**。
4. 在 DNS 修改页面，单击**修改 DNS 服务器**。
5. 根据页面提示，输入 EdgeOne 提供的 DNS 服务器地址信息，完成后单击**确定**即可完成设置。

华为云

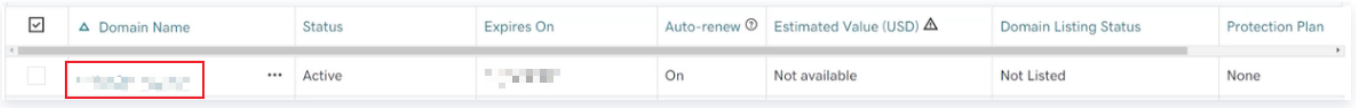
1. 登录 华为云域名控制台 。
2. 在域名列表中定位目标域名，单击操作列下的**更多 > 管理**，进入域名信息页面。
3. 在基本信息中，单击**修改**。
4. 在**修改 DNS 服务器**窗口中，输入 EdgeOne 提供的 DNS 服务器地址信息。
5. 单击**确定**即可完成设置。

Godaddy

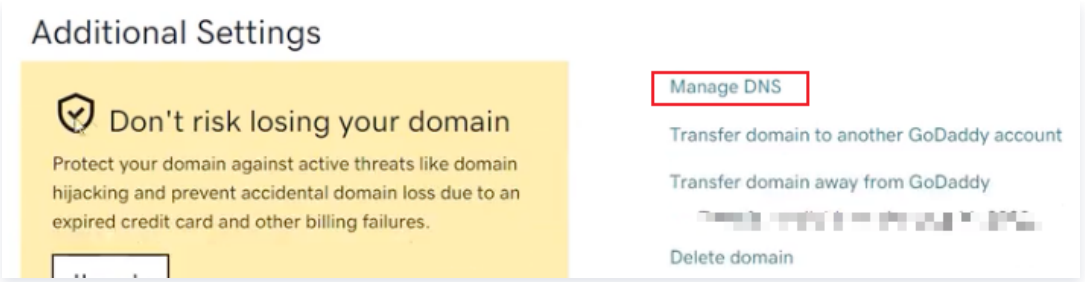
1. 登录 GoDaddy。
2. 单击 **My Products**，并选择 **Manage All**。



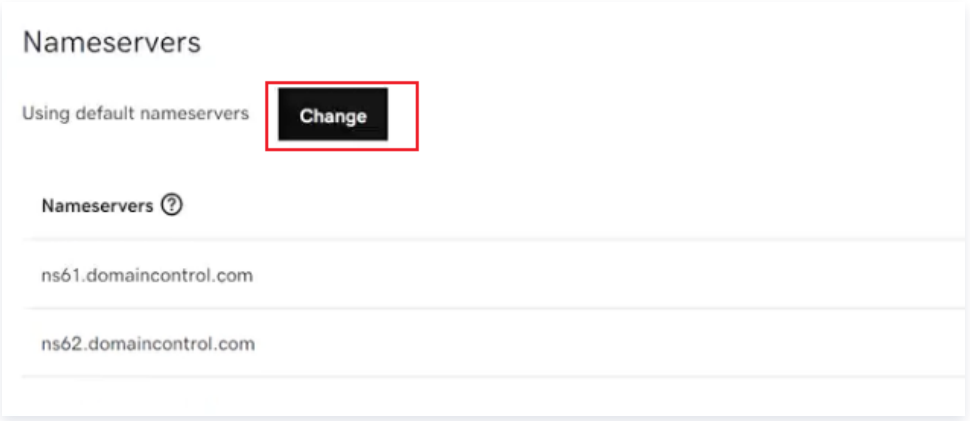
3. 单击需要变更的**域名**。



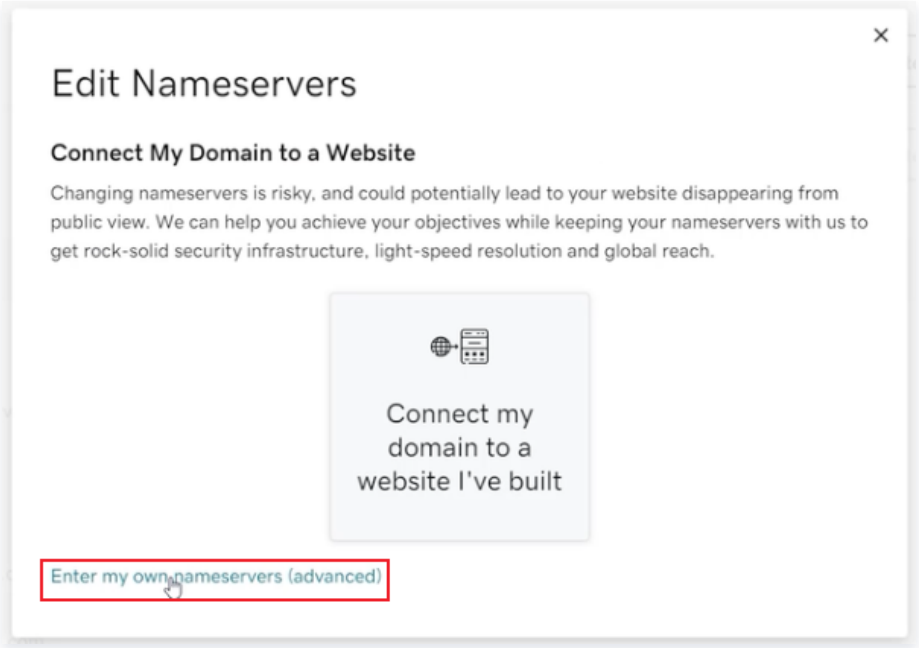
4. 在 Additional Settings 下，单击 **Manage DNS**。



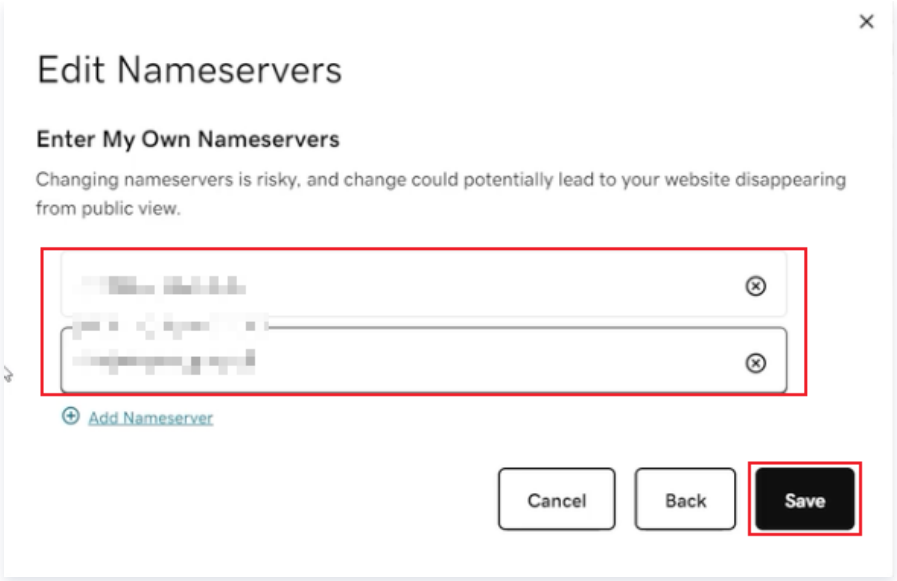
5. 在 Nameservers 下，单击 **Change**。



6. 选择 **Enter my own nameservers (advanced)**。



7. 输入 EdgeOne 提供的 DNS 服务器地址信息，完成后单击 **Save** 即可完成设置。



Google

1. 登录 Google 管理控制台。
2. 选择目标域名。
3. 依次单击左上角的**菜单**、**DNS**。
4. 在**域名服务器**下，选择使用自定义域名服务器。
5. 在**域名服务器**字段中，输入 EdgeOne 提供的 DNS 服务器地址信息。
6. 单击**保存**即可完成设置。

Name

1. 登录 Name 管理控制台 。
2. 单击 **My Domains**。
3. 选择目标域名。
4. 单击 **Nameservers column** 列中的 **Manage Nameservers**。
5. 单击 **Delete All** 以清除当前的名称服务器。
6. 在标有 **Add Nameserver** 的空白框中输入 EdgeOne 提供的 DNS 服务器地址信息，然后单击蓝色的 **Add** 。确保一次只添加一个。
7. 单击 **Save Changes** 保存更改。

3. 修改完成后，域名注册商需要一定的时间来处理 DNS 服务器的更新，请耐心等待生效，EdgeOne 将会定时检测 DNS 服务器记录是否已生效。

> ⚠ **注意：**
> 如果您原 DNS 上存在正在使用的解析记录值，建议您先前往 **DNS 记录**内导入所有 DNS 解析记录再切换 DNS 服务器，避免原 DNS 解析服务中断。详情操作步骤可参见 配置域名 DNS 解析记录 。

配置域名 DNS 解析记录

最近更新时间：2024-11-04 20:48:01

本文介绍了如何在 EdgeOne 上配置 DNS 解析记录。

> **注意：**
> 本功能仅在站点为 NS 接入模式下支持，CNAME 模式下不支持。

前提条件

1. 您的站点是以 NS 模式接入。
2. 已将您域名的 DNS 服务器修改为 EdgeOne 提供的 DNS 服务器地址。详情请参见 修改 DNS 服务器 。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，单击需配置的站点，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务 > DNS 记录**。
3. 在 DNS 记录页面，单击**添加记录**，选择所需记录，填写相关参数，单击**保存**。相关参数说明可参考：DNS 相关概念介绍 。

> **说明：**
> 在添加 DNS 记录后，该记录仅提供 DNS 解析能力，如果您希望该域名接入 EdgeOne 进行安全加速，可单击操作列中的**添加为加速域名**，参考 添加加速域名 文档，将该域名接入 EdgeOne 内。

DNS 相关概念介绍

主机记录

主机记录相当于子域名的前缀，用于将域名映射到特定的 IP 地址或者其他相关信息。当您在浏览器中输入一个网址时，您的设备会查询 DNS 服务器来获取这个网址对应的 IP 地址，这个过程就是通过查找 DNS 记录完成的。假设当前的站点为 `example.com`，想要接入的域名为 `www.example.com`，则主机记录即输入为 `www` 。

解析记录类型介绍

记录类型	说明	示例
A	将域名解析到 IPv4 地址，记录值仅允许输入 IPv4 格式的地址，不允许使用内网 IP。	如果您有一个域名 `example.com`，其 A 记录是 `1.1.1.1` 。当用户访问 `example.com` 时，DNS 会将其解析为该 IP 地址。
AAAA	将域名解析到 IPv6 地址，记录值仅允许输入 IPv6 格式的地址，不允许使用内网 IP。	如果您有一个域名 `example.com`，其 AAAA 记录是 `2001:0db8:85a3:0000:0000:8a2e:0370:7334` 。当用户访问 `example.com` 时，DNS 会将其解析为该 IP 地址，这使得用户可以通过 IPv6 访问该网站。
CNAME	将一个域名别名指向另一个域名，记录值仅允许输入域名。	如果您有一个子域名 `www.example.com`，其 CNAME 记录指向 `example.com` 。则用户访问 `www.example.com` 时会被重定向到 `example.com` 获取对应的解析记录结果。

MX	指定处理电子邮件的邮件服务器，MX 记录需要包含优先级及服务器地址，其中： • 优先级：允许输入范围为 0-50； • 域名服务器地址：仅允许输入域名。	如果您希望将发送到 `example.com` 的电子邮件转发到某个邮件服务器，您可以设置 MX 记录，例如 `10 mail.example.com`，其中 10 是优先级，数字越小优先级越高。
TXT	用于存储任意文本信息，通常用于验证和安全目的，记录值最长不允许超过 256 字节。	常见的用途包括 SPF（发件人策略框架）记录和域名验证。例如，您可以配置一个 TXT 记录 `v=spf1 include:_spf.example.com ~all`，用于指定哪些服务器可以代表您的域名发送电子邮件。
NS	指定负责管理该域名的 DNS 服务器，记录值仅允许使用域名格式。	如果您有一个域名 `example.com`，其 NS 记录可能是 `ns1.example.com` 和 `ns2.example.com`，这表示该域名由这些 DNS 服务器负责解析该域名的权威 DNS 查询。
SRV	用于定义特定服务的主机名和端口号，记录值应包含对应的主机域名及端口号。	如果您有一个服务（如 VoIP 或即时消息），您可以使用 SRV 记录来指定服务的主机名和端口。例如：`_sip._tcp.example.com` 可能指向 `sipserver.example.com` 的 5060 端口。

CAA	指定哪些证书颁发机构（CA）被授权可为域名颁发 SSL/TLS 证书。记录值格式需要包含标志、标记及值三个信息，以空格进行分隔：
	• 标志：仅允许设置为 0，即允许 CA 机构在无法识别 CAA 记录属性的情况下仍然可以为该域名颁发证书。
	• 标签：通常是 "issue"、"issuewild" 或 "iodef"：
	  ○ issue：允许指定的 CA 为所有子域名颁发证书。
	  ○ issuewild：允许指定的 CA 为所有子域名颁发通配符证书。
	  ○ iodef：提供一个 URL，CA 在遇到违反 CAA 政策的请求时可以发送报告到这个 URL。
	• 值：字符串类型，通常是允许颁发证书的 CA 的域名，需要包含双引号。
		您可以设置 CAA 记录来限制只有特定的 CA 可以为您的域名颁发证书，例如：`0 issue "letsencrypt.org"`，表示只有 Let's Encrypt 可以为该域名颁发证书。

解析记录冲突介绍

在进行递归解析查询时，各记录类型之间是有优先级的，例如：根据 RFC1034 和 RFC2181， CNAME 优先级最高，所以在解析请求过程中，会优先返回 CNAME 解析记录结果，因此，如果设置了 CNAME 记录，即不允许再配置 MX 和 TXT 记录，防止出现记录冲突。
✓：不冲突，在相同的主机记录下，该两种类型的解析记录可以共存。如：已经设置了 `www.example.com` 的 A 记录，还可以再设置 `www.example.com` 的 MX 记录。
×：冲突，在相同的主机记录下，该两种类型的解析记录不可以共存。如：已经设置了 `www.example.com` 的 A 记录，不可以再设置 `www.example.com` 的 CNAME 记录。

记录类型	A	AAAA	CNAME	MX	NS	TXT	SRV	CAA
A	✓	✓	×	✓	×	✓	✓	✓
AAAA	✓	✓	×	✓	×	✓	✓	✓
CNAME	×	×	×	×	×	×	×	×
MX	✓	✓	×	✓	×	✓	✓	✓
NS	×	×	×	×	✓	×	×	×

TXT	✓	✓	×	✓	×	✓	✓	✓
SRV	✓	✓	×	✓	×	✓	✓	✓
CAA	✓	✓	×	✓	×	✓	✓	✓

说明：
上表为主机记录为非 @ 时的冲突情况，当主机记录为 @ 时，CNAME 记录与 MX、TXT 记录不冲突，允许配置。但是配置后仍然可能会出现解析记录冲突，冲突说明及风险可参考，详情可参考：CNAME 和 MX、TXT 记录冲突说明 。

权重介绍

权重允许您在相同主机记录、记录类型及解析线路下，设置不同的记录值，在解析时，EdgeOne 将根据权重按照比例来随机返回对应的解析结果。仅支持 A/AAAA/CNAME 类型记录允许配置权重，权重默认为空，即不配置权重，允许输入范围为 0-100，当权重配置为 0 时代表不解析，但不允许所有权重设置为 0。配置权重后，如果存在多条同名的解析记录，将按照权重返回解析记录结果，权重的计算方式为：**最终生效的权重 = 当前记录权重/所有同名记录权重之和**。
示例如下：
假设当前存在 3 条相同的主机记录名称的 CNAME 记录， 分别为记录 A、记录 B、记录 C，权重设置分别是 0、60、40，则最终权重生效结果为记录 A 不解析，记录 B 的权重比例为：60/（60+40）= 60%， 记录 C 的权重比例为：40/（60+40）=40%。

说明：
- 相同主机记录的 A/AAAA/CNAME 记录最多允许同时添加 15 条。
- 如果存在多条相同主机记录名称的 A/AAAA/CNAME 记录并配置权重，则所有记录的权重开关必须保持一致，即必须全部配置权重或者全部关闭权重。

解析线路介绍

默认情况下，请求 DNS 解析时，权威服务器不会判断用户的 IP 来源来返回解析记录值。EdgeOne 支持解析线路分配，可以在解析时根据用户的请求 IP 所归属的解析线路，返回对应线路的解析记录值，如果您希望根据用户的 IP 地域来源返回不同的解析记录，您可以根据地域来配置不同的记录值。例如：当前域名 `www.example.com`，配置了中国大陆区域线路 A 记录解析到 `1.1.1.1`，默认线路为 A 记录解析到 `2.2.2.2`，则来源于中国大陆的用户，访问域名 `www.example.com` 时都将被解析到 `1.1.1.1`，其它区域访问该域名时都将被解析到 `2.2.2.2`。

说明：
- 该功能仅标准版及企业版套餐支持。
- 当前仅 A/AAAA/CNAME 记录支持配置解析线路，相同主机记录下最多支持配置 15 条解析线路。

TTL

TTL（Time To Live）表示 DNS 记录在各级 DNS 服务器的缓存时间（以秒为单位）。当 DNS 记录的 TTL 到期后，Local DNS 服务器需要重新向权威 DNS 服务器请求获取该记录解析，以确保 DNS 记录的信息是最新的。 TTL 设置的时间越短，将需要越频繁地向权威请求该记录解析，可能略微影响解析的性能，TTL 设置较长，如果在出现记录更新时，将可能影响该记录实际的生效时间。默认情况下，EdgeOne 的 TTL 时间设置为 5 分钟，您可以根据实际业务需求进行修改。

DNS 高级配置

最近更新时间：2024-09-19 14:44:42

本文将介绍 EdgeOne 支持的 DNSSEC、自定义 NS 服务器、CNAME 加速等高级配置原理及配置方式。

> **说明：**
> 以下 DNS 高级配置相关功能仅在 NS 接入模式下支持。

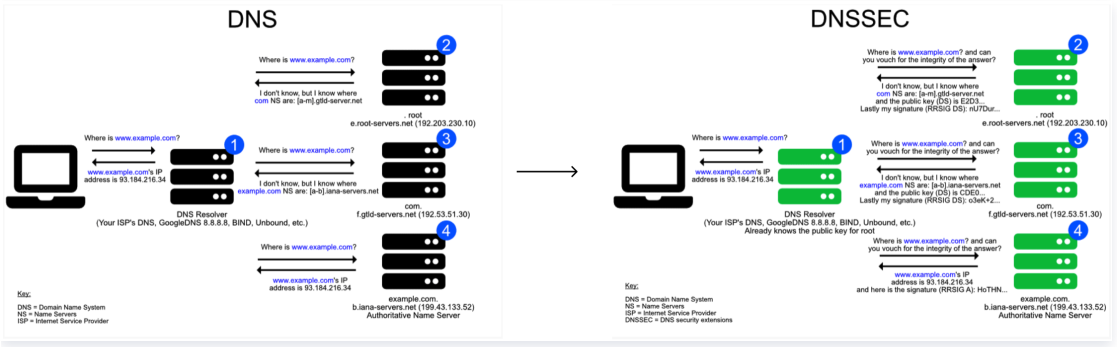
DNSSEC

功能介绍

域名系统安全扩展（DNS Security Extensions），简称 DNSSEC。开启 DNSSEC，可有效防止 DNS 欺骗和缓存污染等攻击。它是通过数字签名来保证 DNS应答报文的真实性和完整性，能够保护用户不被重定向到非预期地址，从而提高用户对互联网的信任，并保护您的核心业务。如果您希望提高您站点解析的安全性以防止被劫持篡改，建议启用该配置。

原理介绍

DNSSEC 通过向现有 DNS 记录添加加密签名的方式来建立一种更安全的 DNS。这个签名会与常见的记录类型（如 AAAA 和 MX 记录）一起存储在 DNS 名称服务器中。随后只需检查所请求的 DNS 记录对应的签名，即可验证该记录是否直接来自权威名称服务器。这意味着 DNS 记录在数字化传输过程中不会被投毒或以其他方式篡改，因而可有效防止引入伪造的记录。



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**域名服务** > **DNS 配置**，进入 DNS 配置页面。
3. 在 DNS 配置页面，单击 DNSSEC 模块的  ，经过二次确认后，开启 DNSSEC 功能。
4. EdgeOne 会向您提供如下图所示的 DS 记录信息。其中，摘要类型及算法的对应关系，请参考：摘要类型 和 算法 。

5. 接下来，您需要根据上述信息，在域名注册商处添加 DS 记录。如果您是在腾讯云注册域名，可参考：域名系统安全扩展（DNSSEC）配置 。如果在其它厂商注册的域名，请查阅相应域名注册商指引文档进行配置。
6. 配置完成后，等待域名注册服务商处生效即可。

自定义 NS 服务

功能介绍

自定义 NS 允许您创建自己站点专属的名称服务器，以替代所分配默认名称服务器。创建后 EdgeOne 会自动为自定义 NS 分配对应的 IP 地址。

操作场景

当您选择 NS 接入您的站点，并且您希望自定义站点的 DNS 服务器的名称时，您可以使用该配置。

> **说明**
> 自定义 NS 服务器有如下限制：
> - 只能以当前站点 (例如：example.com) 的子域名 (例如：ns.example.com) 作为自定义 NS 服务器名称。
> - 自定义 NS 至少需要添加 2个域名，并且不能和当前已有 DNS 记录冲突。

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**域名服务** > **DNS 配置**，进入 DNS 配置页面。
3. 在 DNS 配置页面，单击自定义 NS 服务模块的  ，添加自定义的 NS 服务器主机记录。

4. 单击**确定**，添加完成后，您还需要在域名注册商添加该自定义 NS 的胶水记录，才能真正生效。如果您是在腾讯云注册域名，可参考：自定义 DNS Host。如果在其它厂商注册的域名，请查阅相应域名注册商指引文档进行配置。

> **说明：**
> 开启并添加自定义 NS 服务后，EdgeOne 将自动为您在当前域名添加对应的 A 记录解析，您无需配置。

5. 配置完成后，等待域名注册服务商处生效即可。

CNAME 加速

功能介绍

开启后可有效提升解析速度，当域名在 EdgeOne DNS 设置多级 CNAME 记录时，系统将直接给出最终 IP 解析结果，减少解析次数。此功能默认开启，正常情况下无需更改，如果您需要给用户提供完整的解析路径，可选择关闭。示例：
假设您的站点为 `example.com`，您配置了如下图所示多级解析记录：`loopthree.example.com` -> `looptwo.example.com` -> `loopone.example.com` -> `1.2.3.4`。

记录类型	主机记录	记录值	TTL	操作
CNAME	loopthree	looptwo.	自动	编辑 开启加速 暂停 删除
CNAME	looptwo	loopone	自动	编辑 开启加速 暂停 删除
A	loopone	1.2.3.4	自动	编辑 开启加速 暂停 删除

共 3 条　　10 条 / 页　　1 / 1 页

在没有开启 **CNAME 加速**时，解析结果会如下所示：

```
;; ANSWER SECTION:
loopthree.          300     IN      CNAME   looptwo.
looptwo.            289     IN      CNAME   loopone.
loopone.            289     IN      A       1.2.3.4
```

开启了 **CNAME 加速** 时，解析结果会直接展示为 IP 地址：

```
;; ANSWER SECTION:
loopthree.          272     IN      A       1.2.3.4
```

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**域名服务 > DNS 配置**，进入 DNS 配置页面。
3. 在 DNS 配置页面，单击 CNAME 加速模块的“开关”，可关闭或开启 CNAME 加速功能。

> **说明**
> 多级 CNAME 必须全部在 EdgeOne DNS，才能实现直接解析出对应的 IP 信息。

批量导入 DNS 记录

最近更新时间：2024-07-25 16:21:41

如果您的站点需要使用 NS 模式接入 EdgeOne，建议您在修改 DNS 服务器前，先将当前已生效中的 DNS 记录通过批量导入的方式完成添加，以避免当前的 DNS 解析服务时效。

> **说明：**
> - 单次导入最多100条记录，如果记录数量较多，建议分多次导入。
> - 当前导入来源支持选择腾讯云 DNSPod、阿里云云解析 DNS、CloudFlare，如果您当前的 DNS 解析不是托管在以上服务商，或者 EdgeOne 在解析以上 DNS 解析服务商格式有误时（不同厂商的记录格式可能随时产生变化），建议您使用模板导入的方式。

场景一：在站点接入过程中批量导入 DNS 记录

示例场景

当前新增一个 `example.com`，需要使用 NS 接入，当前域名解析托管在阿里云云解析 DNS 服务中，需要将当前 DNS 记录批量导入至 EdgeOne。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，在服务总览中，单击右上角的**新增站点**。
2. 参考 从零开始快速接入 EdgeOne，完成站点创建的步骤1和步骤2。
3. 在步骤3中，选择接入模式时，选择为 NS 接入模式，单击**批量导入**。
4. 选择导入来源，以该场景为例，选择导入来源为阿里云云解析 DNS。选择文件为阿里云云解析 DNS 导出的 DNS 记录文件，导出方式请参考对应厂商的产品文档指引。

5. 单击**下一步**，识别导入文件内容，如果文件格式校验无误，则需要再次确认需导入的 DNS 记录内容，如果 DNS 记录内容有误，可以在该界面内进行修改。
6. 确认无误后，单击**确认导入**，等待后台导入完成即可。

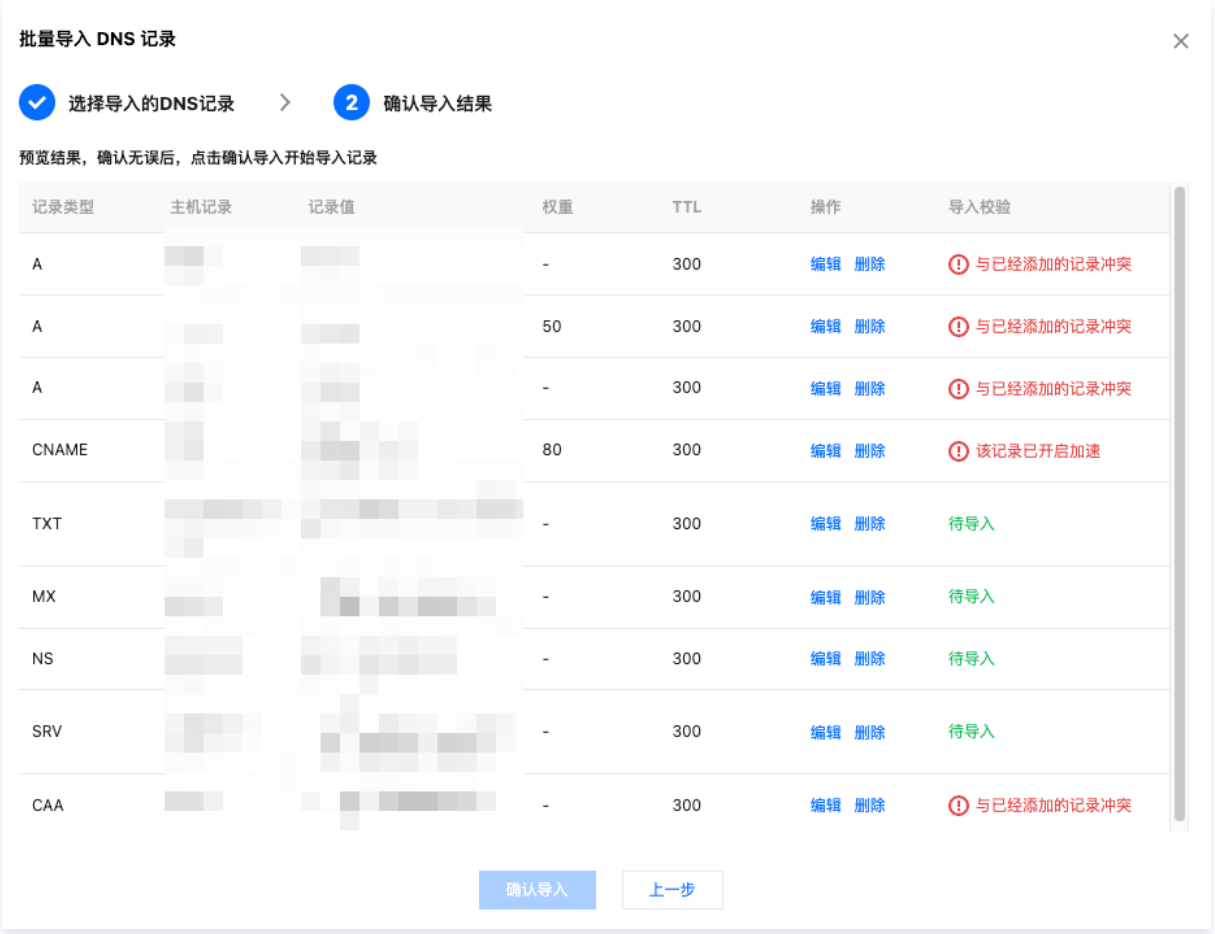
场景二：在域名管理界面内批量导入 DNS 记录

示例场景

当前已有一个站点 `example.com`，使用了 NS 接入的方式，需要批量新增多个 DNS 解析记录。

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**。
2. 在站点详情页面，单击**域名服务 > DNS 记录** 。
3. 单击**批量导入**，选择批量导入来源为**模板导入**，并下载相应的模板，支持 csv 模板、xlsx 表格、txt 文件、zone 文件四种格式。
4. 将需要导入的 DNS 记录按照模板格式填写并保存，通过选择文件的方式选择对应填写好的导入模板，或者将该文件直接通过拖拽的方式到控制台内。
5. 单击**下一步**，识别模板内容，如果文件格式校验无误，则需要再次确认需导入的 DNS 记录内容，如果 DNS 记录内容有误，可以在该界面内进行修改。



6. 确认无误后，单击**确认导入**，等待后台导入完成即可。

解析线路及对应代码枚举

最近更新时间：2024-11-12 15:21:11

亚洲

国家/地区	代码	国家/地区	代码
阿富汗	AF	马尔代夫	MV
亚美尼亚	AM	蒙古	MN
阿塞拜疆	AZ	缅甸	MM
巴林	BH	尼泊尔	NP
孟加拉	BD	朝鲜	KP
不丹	BT	阿曼	OM
英属印度洋领地	IO	巴基斯坦	PK
柬埔寨	KH	巴勒斯坦	PS
圣诞岛	CX	菲律宾	PH
中国香港	HK	卡塔尔	QA
印度	IN	沙特阿拉伯	SA
印度尼西亚	ID	新加坡	SG
伊朗	IR	韩国	KR
伊拉克	IQ	斯里兰卡	LK
以色列	IL	叙利亚	SY
日本	JP	中国台湾	TW
约旦	JO	塔吉克斯坦	TJ
哈萨克斯坦	KZ	泰国	TH
科威特	KW	土库曼斯坦	TM
吉尔吉斯斯坦	KG	阿联酋	AE
老挝	LA	乌兹别克斯坦	UZ
黎巴嫩	LB	越南	VN
中国澳门	MO	也门	YE
马来西亚	MY		

欧洲

国家/地区	代码	国家/地区	代码
奥兰群岛	AX	意大利	IT
阿尔巴尼亚	AL	泽西岛	JE

安道尔	AD	立陶宛	LT
奥地利	AT	卢森堡	LU
白俄罗斯	BY	马其顿	MK
比利时	BE	马耳他	MT
波黑	BA	摩尔多瓦	MD
保加利亚	BG	摩纳哥	MC
荷兰加勒比区	BQ	黑山	ME
克罗地亚	HR	荷兰	NL
捷克	CZ	挪威	NO
丹麦	DK	波兰	PL
爱沙尼亚	EE	葡萄牙	PT
法罗群岛	FO	罗马尼亚	RO
芬兰	FI	俄罗斯	RU
法国	FR	圣马力诺	SM
德国	DE	塞尔维亚	RS
直布罗陀	GI	荷属圣马丁	SX
希腊	GR	斯洛伐克	SK
根西岛	GG	西班牙	ES
匈牙利	HU	瑞典	SE
冰岛	IS	瑞士	CH
爱尔兰	IE	乌克兰	UA
马恩岛	IM	英国	GB

非洲

国家/地区	代码	国家/地区	代码
阿尔及利亚	DZ	马里	ML
安哥拉	AO	毛里塔尼亚	MR
贝宁	BJ	毛里求斯	MU
博茨瓦纳	BW	马约特	YT
布基纳法索	BF	摩洛哥	MA
布隆迪	BI	莫桑比克	MZ
喀麦隆	CM	纳米比亚	NA
佛得角	CV	尼日尔	NE
中非	CF	尼日利亚	NG

乍得	TD	卢旺达	RW
科摩罗	KM	圣赫勒拿	SH
吉布提	DJ	圣多美和普林西比	ST
埃及	EG	塞内加尔	SN
赤道几内亚	GQ	塞舌尔	SC
厄立特里亚	ER	塞拉利昂	SL
埃塞俄比亚	ET	索马里	SO
加蓬	GA	南非	ZA
冈比亚	GM	南苏丹	SS
加纳	GH	苏丹	SD
几内亚	GN	斯威士兰	SZ
几内亚比绍	GW	坦桑尼亚	TZ
肯尼亚	KE	多哥	TG
莱索托	LS	突尼斯	TN
利比里亚	LR	乌干达	UG
利比亚	LY	西撒哈拉	EH
马达加斯加	MG	赞比亚	ZM
马拉维	MW	津巴布韦	ZW

大洋洲

国家/地区	代码	国家/地区	代码
澳大利亚	AU	诺福克岛	NF
库克群岛	CK	北马里亚纳群岛	MP
东帝汶	TL	帕劳	PW
关岛	GU	巴布亚新几内亚	PG
基里巴斯	KI	所罗门群岛	SB
马绍尔群岛	MH	汤加	TO
瑙鲁	NR	图瓦卢	TV
新西兰	NZ		

北美洲

国家/地区	代码	国家/地区	代码
安圭拉	AI	海地	HT
安提瓜和巴布达	AG	洪都拉斯	HN

阿鲁巴	AW	牙买加	JM
巴哈马	BS	墨西哥	MX
巴巴多斯	BB	蒙塞拉特岛	MS
百慕大	BM	尼加拉瓜	NI
加拿大	CA	巴拿马	PA
开曼群岛	KY	波多黎各	PR
哥斯达黎加	CR	圣基茨和尼维斯	KN
古巴	CU	圣卢西亚	LC
库拉索	CW	法属圣马丁	MF
萨尔瓦多	SV	特立尼达和多巴哥	TT
格陵兰岛	GL	特克斯和凯科斯群岛	TC
格林纳达	GD	美国	US
危地马拉	GT		

南美洲

国家/地区	代码	国家/地区	代码
阿根廷	AR	圭亚那	GY
玻利维亚	BO	巴拉圭	PY
巴西	BR	秘鲁	PE
智利	CL	苏里南	SR
哥伦比亚	CO	乌拉圭	UY
厄瓜多尔	EC	委内瑞拉	VE
法属圭亚那	GF		

南极洲

国家/地区	代码
南极洲	Antarctica

中国大陆省份

省份	代码	省份	代码
中国大陆	CN	江苏	CN.JS
安徽	CN.AH	江西	CN.JX
北京	CN.BJ	吉林	CN.JL
重庆	CN.CQ	辽宁	CN.LN
福建	CN.FJ	宁夏	CN.NX

甘肃	CN.GS	青海	CN.QH
广东	CN.GD	陕西	CN.SN
广西	CN.GX	山东	CN.SD
贵州	CN.GZ	上海	CN.SH
海南	CN.HI	山西	CN.SX
河北	CN.HE	四川	CN.SC
黑龙江	CN.HL	天津	CN.TJ
河南	CN.HA	西藏	CN.XZ
湖北	CN.HB	新疆	CN.XJ
湖南	CN.HN	云南	CN.YN
内蒙古	CN.NM	浙江	CN.ZJ

中国大陆运营商

运营商	代码	运营商	代码
教育网	CN/CERNET	电信	CN/CT
中国广电	CN/CBN	联通	CN/CU
移动	CN/CM	铁通	CN/CTT

中国大陆省份运营商

省份运营商	代码	省份运营商	代码
安徽移动	CN.AH/CM	江苏联通	CN.JS/CU
安徽电信	CN.AH/CT	江西移动	CN.JX/CM
安徽联通	CN.AH/CU	江西电信	CN.JX/CT
北京移动	CN.BJ/CM	江西联通	CN.JX/CU
北京电信	CN.BJ/CT	吉林移动	CN.JL/CM
北京联通	CN.BJ/CU	吉林电信	CN.JL/CT
重庆移动	CN.CQ/CM	吉林联通	CN.JL/CU
重庆电信	CN.CQ/CT	辽宁移动	CN.LN/CM
重庆联通	CN.CQ/CU	辽宁电信	CN.LN/CT
福建移动	CN.FJ/CM	辽宁联通	CN.LN/CU
福建电信	CN.FJ/CT	宁夏移动	CN.NX/CM
福建联通	CN.FJ/CU	宁夏电信	CN.NX/CT
甘肃移动	CN.GS/CM	宁夏联通	CN.NX/CU
甘肃电信	CN.GS/CT	青海移动	CN.QH/CM

甘肃联通	CN.GS/CU	青海电信	CN.QH/CT
广东移动	CN.GD/CM	青海联通	CN.QH/CU
广东电信	CN.GD/CT	陕西移动	CN.SN/CM
广东联通	CN.GD/CU	陕西电信	CN.SN/CT
广西移动	CN.GX/CM	陕西联通	CN.SN/CU
广西电信	CN.GX/CT	山东移动	CN.SD/CM
广西联通	CN.GX/CU	山东电信	CN.SD/CT
贵州移动	CN.GZ/CM	山东联通	CN.SD/CU
贵州电信	CN.GZ/CT	上海移动	CN.SH/CM
贵州联通	CN.GZ/CU	上海电信	CN.SH/CT
海南移动	CN.HI/CM	上海联通	CN.SH/CU
海南电信	CN.HI/CT	山西移动	CN.SX/CM
海南联通	CN.HI/CU	山西电信	CN.SX/CT
河北移动	CN.HE/CM	山西联通	CN.SX/CU
河北电信	CN.HE/CT	四川移动	CN.SC/CM
河北联通	CN.HE/CU	四川电信	CN.SC/CT
黑龙江移动	CN.HL/CM	四川联通	CN.SC/CU
黑龙江电信	CN.HL/CT	天津移动	CN.TJ/CM
黑龙江联通	CN.HL/CU	天津电信	CN.TJ/CT
河南移动	CN.HA/CM	天津联通	CN.TJ/CU
河南电信	CN.HA/CT	西藏移动	CN.XZ/CM
河南联通	CN.HA/CU	西藏电信	CN.XZ/CT
湖北移动	CN.HB/CM	西藏联通	CN.XZ/CU
湖北电信	CN.HB/CT	新疆移动	CN.XJ/CM
湖北联通	CN.HB/CU	新疆电信	CN.XJ/CT
湖南移动	CN.HN/CM	新疆联通	CN.XJ/CU
湖南电信	CN.HN/CT	云南移动	CN.YN/CM
湖南联通	CN.HN/CU	云南电信	CN.YN/CT
内蒙移动	CN.NM/CM	云南联通	CN.YN/CU
内蒙电信	CN.NM/CT	浙江移动	CN.ZJ/CM
内蒙联通	CN.NM/CU	浙江电信	CN.ZJ/CT
江苏移动	CN.JS/CM	浙江联通	CN.ZJ/CU
江苏电信	CN.JS/CT		

美国各州

州	代码	州	代码
亚拉巴马州	US.AL	内布拉斯加州	US.NE
阿拉斯加州	US.AK	内华达州	US.NV
亚利桑那州	US.AZ	新罕布什尔州	US.NH
阿肯色州	US.AR	新泽西州	US.NJ
加利福尼亚州	US.CA	新墨西哥州	US.NM
科罗拉多州	US.CO	纽约州	US.NY
康涅狄格州	US.CT	北卡罗来纳州	US.NC
特拉华州	US.DE	北达科他州	US.ND
佛罗里达州	US.FL	俄亥俄州	US.OH
乔治亚州	US.GA	俄克拉荷马州	US.OK
夏威夷州	US.HI	俄勒冈州	US.OR
爱达荷州	US.ID	宾夕法尼亚州	US.PA
伊利诺伊州	US.IL	罗得岛州	US.RI
印第安纳州	US.IN	南卡罗来纳州	US.SC
爱荷华州	US.IA	南达科他州	US.SD
堪萨斯州	US.KS	田纳西州	US.TN
肯塔基州	US.KY	德克萨斯州	US.TX
路易斯安那州	US.LA	美属维京群岛	US.VI
缅因州	US.ME	犹他州	US.UT
马里兰州	US.MD	佛蒙特州	US.VT
马萨诸塞州	US.MA	弗吉尼亚州	US.VA
密歇根州	US.MI	哥伦比亚特区	US.DC
明尼苏达州	US.MN	华盛顿州	US.WA
密西西比州	US.MS	西弗吉尼亚州	US.WV
密苏里州	US.MO	威斯康星州	US.WI
蒙大拿州	US.MT	怀俄明州	US.WY

印度各邦

邦	代码	邦	代码
安达曼-尼科巴群岛	IN.AN	中央邦	IN.MP
安得拉邦	IN.AP	马哈拉施特拉邦	IN.MH

阿鲁纳恰尔邦	IN.AR	曼尼普尔邦	IN.MN
阿萨姆邦	IN.AS	梅加拉亚邦	IN.ML
比哈尔邦	IN.BR	米佐拉姆邦	IN.MZ
昌迪加尔	IN.CH	那加兰邦	IN.NL
恰蒂斯加尔邦	IN.CG	奥里萨邦	IN.OR
达德拉-纳加尔哈维利	IN.DN	本地治里	IN.PY
达曼-第乌	IN.DD	旁遮普邦	IN.PB
德里	IN.DL	拉贾斯坦邦	IN.RJ
果阿邦	IN.GA	锡金	IN.SK
古吉拉特邦	IN.GJ	泰米尔纳德邦	IN.TN
哈里亚纳邦	IN.HR	特伦甘纳邦	IN.TG
喜马偕尔邦	IN.HP	特里普拉邦	IN.TR
查谟-克什米尔邦	IN.JK	北阿坎德邦	IN.UT
贾坎德邦	IN.JH	北方邦	IN.UP
卡纳塔克邦	IN.KA	西孟加拉邦	IN.WB
喀拉拉邦	IN.KL		

接入加速域名
站点/域名归属权验证

最近更新时间：2024-08-23 15:07:21

什么情况下需要验证站点/域名归属权

当您的站点/域名首次接入 EdgeOne 时，为了确保您是当前接入站点/域名的所有者，我们需要您验证该站点/域名的归属权。

> ⚠ **注意：**
> 该操作仅在 CNAME 接入模式下需要，如果您的站点是 NS 模式接入，可直接通过切换 DNS 服务器至 EdgeOne 即视为完成归属权验证。

站点与域名归属权验证的区别

假设您的业务域名为：`a.example.com`，`b.example.com`，`c.example.com`，此时您接入的站点为 `example.com`

- **站点归属验证：**当您拥有根域名 DNS 解析的操作权限或者根域名源站服务器的操作权限时，建议您使用站点归属权验证，可以有效降低操作成本。
  - 站点归属权验证通过后，EdgeOne 认定您拥有该域名下所有多级域名的归属权，接入 `a.example.com`，`b.example.com`，`c.example.com` 及其他子域名都无需再验证归属权。
- **域名归属权校验：**当您的公司存在多级架构或为代运维域名时，如果您只拥有子域名的 DNS 解析操作权限或子域名源站服务器的操作权限时，EdgeOne 允许您在接入站点时跳过站点归属权验证，之后单独验证域名的归属权，将会增加接入操作成本。
  - 使用域名归属权验证，接入 `a.example.com`，`b.example.com`，`c.example.com` 都需要单独验证归属权。
  - 子域名归属权验证通过后，该域名下的其他域名无需再次验证，例如：`a.example.com` 验证通过后，`test.a.example.com` 无需再次验证。

如何验证站点/域名归属权

站点和域名验证归属权的实际操作步骤是一致的，下面以验证站点归属权为例。

DNS 解析验证

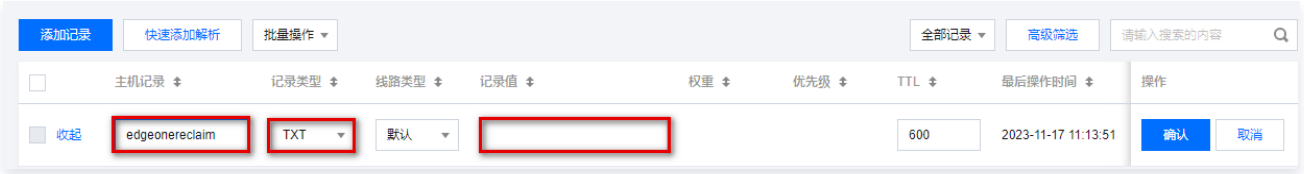
1. 在站点验证页面，选择 **DNS 解析验证**，在该页面内，可以获取到 DNS 解析验证所需要添加的主机记录、记录类型以及记录值。

2. 登录该域名的 DNS 解析服务商，为新增一条 TXT 记录用于验证站点归属权，以下为不同 DNS 解析服务商的添加示例。

腾讯云 DNSPod 添加示例

a. 登录 云解析 DNS 控制台，在**我的解析**中找到当前待验证的域名，单击该**域名**进入域名配置页。
b. 在记录管理页面，单击**添加记录**，为当前域名新增一条用于归属权校验的解析记录。

c. 填写步骤1中的主机记录、记录类型和记录值。



参数名称	参数说明
主机记录	edgeonereclaim
记录类型	TXT
线路类型	默认
记录值	填写 EdgeOne 提供的记录值
TTL	600

d. 单击**确认**，完成添加。

阿里云解析 DNS 添加示例

a. 登录阿里云的 云解析 DNS 控制台 。

b. 在**域名解析**页面，找到当前待验证的域名，在域名右侧单击**解析设置**，进入解析设置页面。

c. 单击**添加记录**，为当前域名新增一条用于归属权校验的解析记录。

d. 填写步骤1中的记录类型、主机记录和记录值。

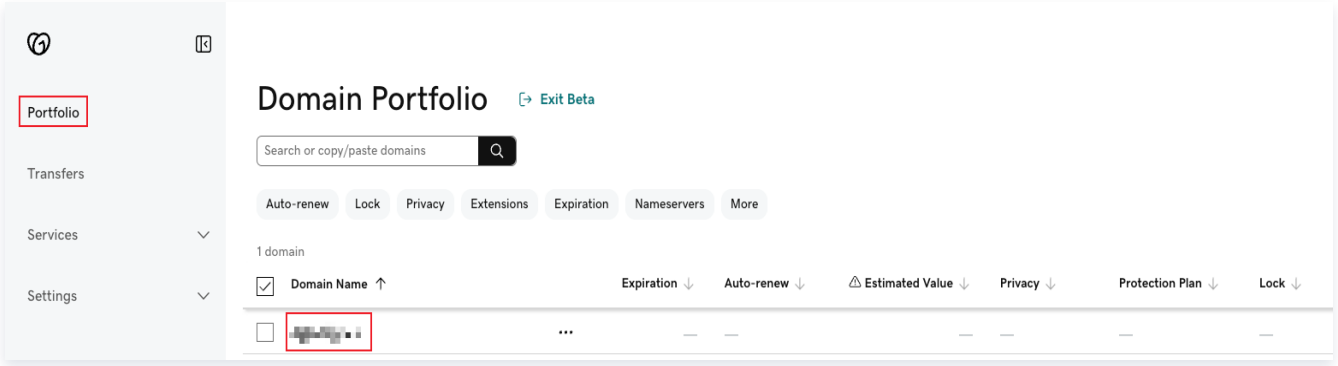
参数名称	参数说明
记录类型	TXT
主机记录	edgeonereclaim
线路类型	默认
记录值	填写 EdgeOne 提供的记录值
TTL	10分钟

e. 单击**确认**，完成添加。

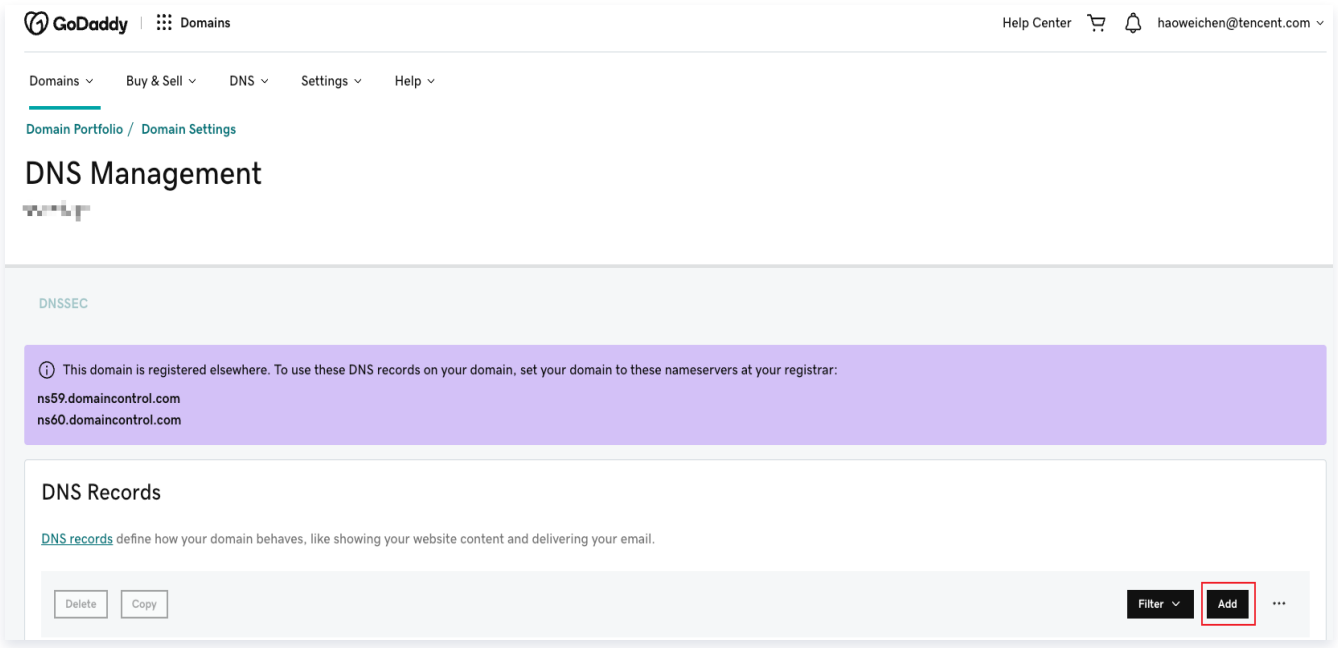
Godaddy 添加示例

a. 登录 Godaddy Domain Portfolio 控制台。

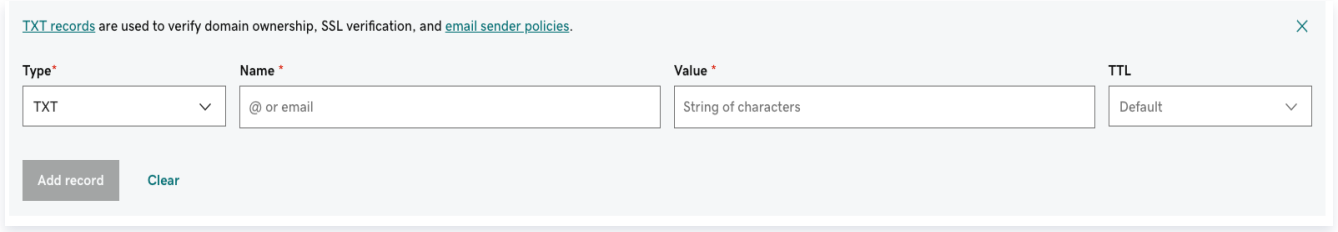
b. 在 **Portfolio** 页面，找到当前待验证的域名，单击该**域名**进入解析设置页面。



c. 单击 **Add**，为当前域名新增一条用于归属权校验的解析记录。



d. 填写步骤1中的记录类型、主机记录和记录值。



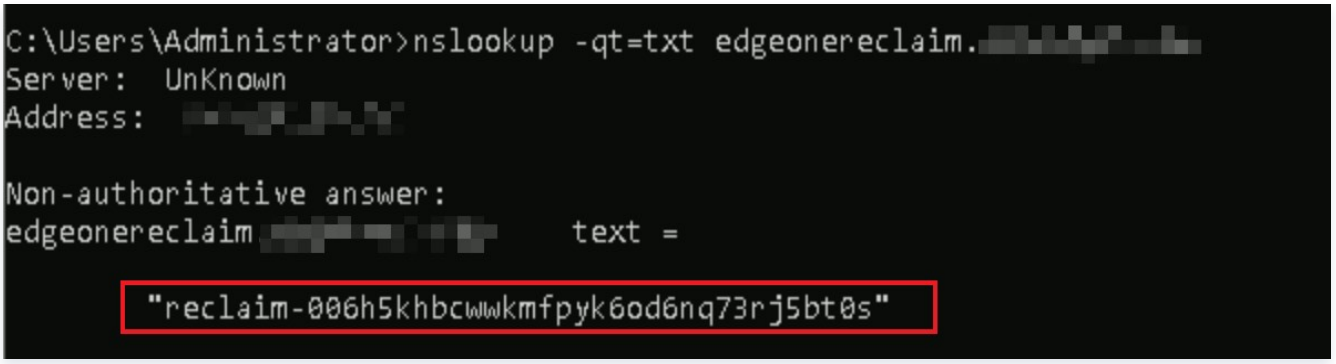
参数名称	参数说明
Type	TXT
Name	edgeonereclaim
Value	填写 EdgeOne 提供的记录值
TTL	Default

e. 单击 **Add Record**，完成添加。

3. 手动验证当前 TXT 记录解析是否生效，您可以通过以下方式验证：

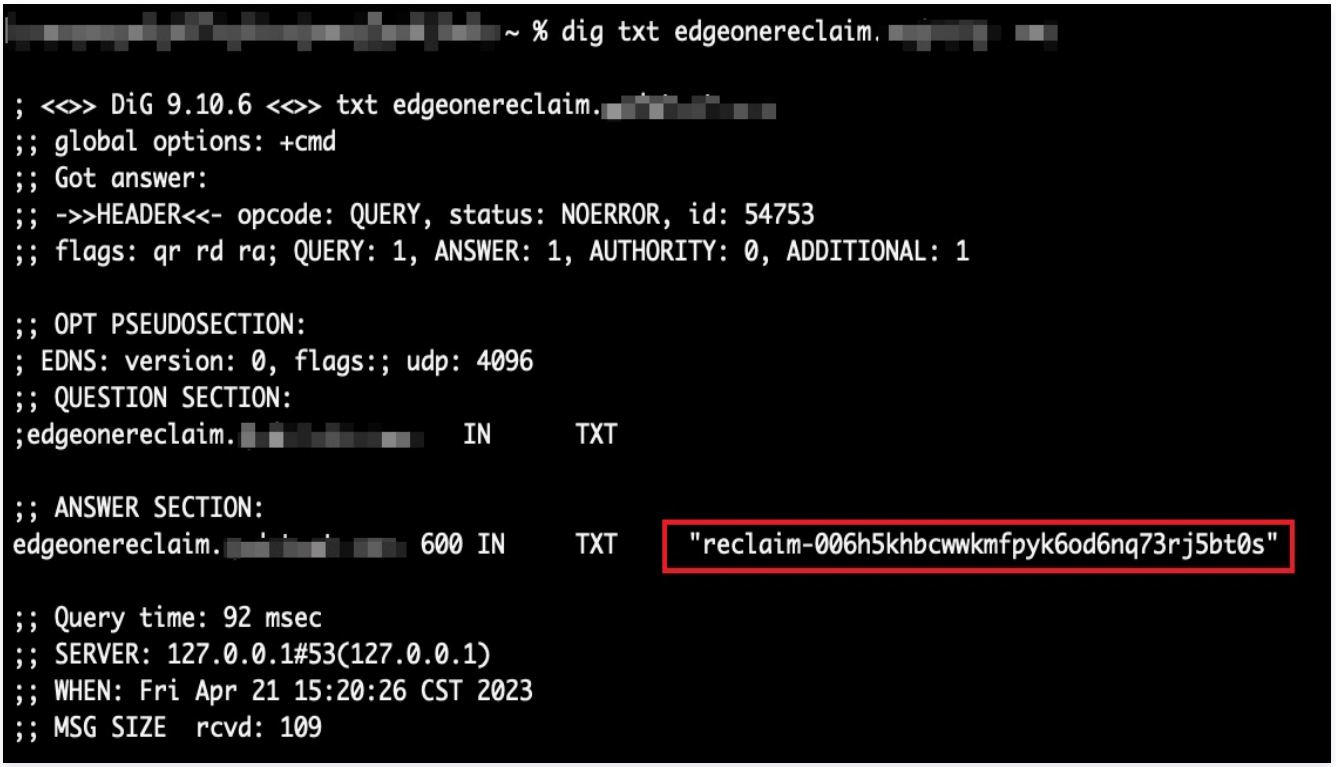
Windows

在 Windows 系统中，打开 cmd 运行程序，以接入站点为 `www.example.com` 为例，您可以在 cmd 内运行：`nslookup -qt=txt edgeonereclaim.example.com`，根据运行的解析结果内，可以查看该域名的 TXT 解析记录信息。若 TXT 解析记录值与步骤1提供的记录值相同，则当前 TXT 记录解析已生效。



Mac/Linux

在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以接入站点为 `example.com` 为例，您可以在终端内运行命令：`dig txt edgeonereclaim.example.com`，根据运行的解析结果内，可以查看该域名的 TXT 记录信息。若 TXT 记录信息与步骤1提供的记录值相同，则当前 TXT 记录解析已生效。



4. 确认 TXT 记录生效后，单击**验证**，完成站点归属权验证。

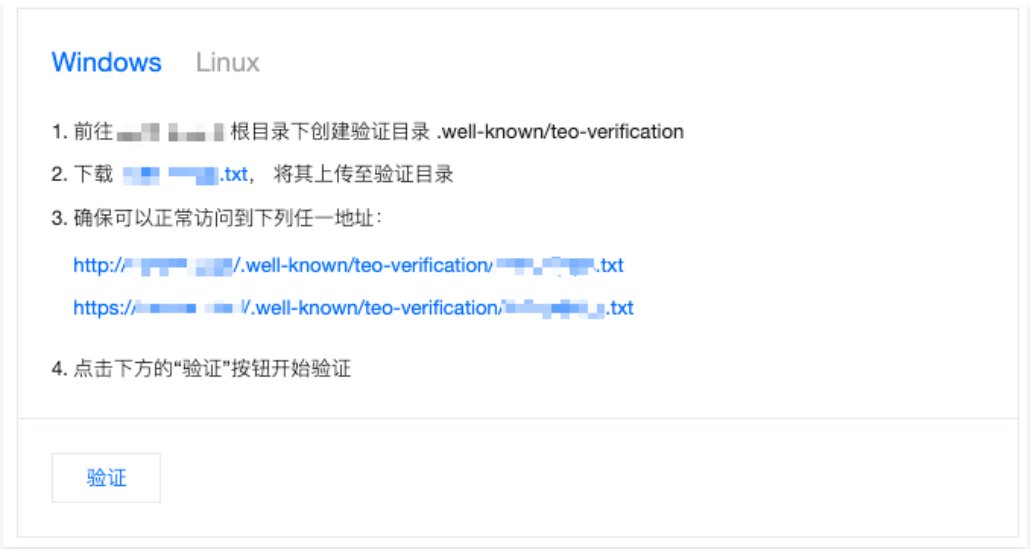
文件验证

1. 在站点验证页面，选择**文件验证**。

2. 文件验证根据操作系统区分为两种操作方式：

Windows Server

1. 前往服务器的根目录下创建验证目录 `.well-known/teo-verification` 。
2. 单击图中第二步文件链接获取验证文件，将其上传至验证目录。



3. 复制图中第三步中 URL 链接到您的浏览器中，确保能够正常访问到该资源。
4. 单击下方**验证**，验证通过即可。

Linux Server

1. 通过命令行进入 Web 服务器根目录下。
2. 复制图中第二步代码至命令行，并执行。

3. 复制图中第三步中 URL 链接到您的浏览器中，确保能够正常访问到该资源。
4. 单击下方**验证**，验证通过即可。

添加加速域名

最近更新时间：2025-02-26 15:46:02

本文将介绍如何将您的业务域名接入 EdgeOne 并开启加速。

> **说明：**
> 域名创建完成后，EdgeOne 将为该域名分配一个 CNAME 地址，您需要完成配置 CNAME 才能使该域名的安全加速生效。配置方式请参考：修改 CNAME 解析 。

准备工作

1. 您已经完成了站点的接入，例如：`example.com` 。如果您想要加速的区域是中国大陆可用区或者全球可用区，请先对您的域名进行备案。详情介绍参见 备案指引 。
2. 已有一个可供对外访问的服务，可以是云服务器或者是腾讯云 COS 服务。例如：已有一个通过腾讯云服务器搭建的跨境电商网站，当前服务器 IP 地址为：`10.1.1.1` 。
3. 如果您的站点是 CNAME 接入，需要您完成域名的归属权校验；如果您的站点是 NS 接入，需要您先完成 DNS 服务器地址修改 。

场景一：快速添加域名

如果您的域名不需要复杂的配置，为了能够快速接入 EdgeOne，可以单击**快速添加**来添加域名。

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的**站点**，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务** > **域名管理** ，进入域名管理详情页面。
3. 单击**快速添加**，新增加速域名。参考 域名各配置项说明 填写域名配置信息后，单击**保存**即可下发域名配置。

场景二：添加域名并完成基础配置

如果您当前需要完整配置域名的基础信息，例如回源协议、回源端口，则建议使用添加域名来进行。根据您所选择接入模式不同，添加子域名的步骤也会有所区别。

NS 接入

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的**站点**，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务** > **域名管理** ，进入域名管理详情页面。
3. 单击添加域名，参考 域名各配置项说明 填写域名配置信息后，单击**下一步**。
4. 在添加域名时，EdgeOne 根据各个常见业务场景，为您提供了推荐配置，以保障您的业务更安全顺畅运行，您可以根据业务场景选择对应的推荐配置，相应配置会在规则引擎模块以一条规则的形式进行展示。可单击**完成**下发推荐配置并创建加速域名，或者直接单击**跳过**，不下发任何推荐配置，仅创建加速域名。
5. 在 NS 接入模式下，EdgeOne 将根据域名为您在后台自动添加一条指向 EdgeOne 的 CNAME 地址。您可以通过**一键添加**来立即开启加速，如果您还需要完成其它域名配置，也可以单击**稍后添加**，参考 修改 CNAME 解析 配置。

CNAME 接入

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的**站点**，进入站点管理二级菜单。

2. 在左侧导航栏中，单击**域名服务** > **域名管理**，进入域名管理详情页面。
3. 单击**添加域名**，参考 域名各配置项说明 填写域名配置信息后，单击**下一步**。
4. 在添加域名时，EdgeOne 根据各个常见业务场景，为您提供了推荐配置，以保障您的业务更安全顺畅运行，您可以根据业务场景选择对应的推荐配置，相应配置会在规则引擎模块以一条规则的形式进行展示。可单击**下一步**下发推荐配置并创建加速域名，或者直接单击**跳过**，不下发任何推荐配置，仅创建加速域名。
5. 在 CNAME 接入模式下，EdgeOne 将为该域名分配一个 CNAME 地址，您需要完成配置 CNAME 才能使该域名的安全加速生效。配置方式请参考：修改 CNAME 解析。配置完成后，单击**完成**即可。

DNSPod 托管接入

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的**站点**，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务** > **域名管理**，进入域名管理详情页面。
3. 单击**添加域名**，参考 域名各配置项说明 填写域名配置信息后，单击**下一步**。
4. 在添加域名时，EdgeOne 根据各个常见业务场景，为您提供了推荐配置，以保障您的业务更安全顺畅运行，您可以根据业务场景选择对应的推荐配置，相应配置会在规则引擎模块以一条规则的形式进行展示。可单击**下一步**下发推荐配置并创建加速域名，或者直接单击**跳过**，不下发任何推荐配置，仅创建加速域名。
5. 在 DNSPod 托管接入模式下，EdgeOne 将为该域名分配一个 CNAME地址，您可以通过**一键添加**来由 EdgeOne 自动完成该域名的 CNAME 配置，如果您还需要完成其它域名配置，也可以单击**稍后添加**，参考 修改 CNAME 解析 配置。

相关参考

域名各配置项说明

配置项	说明
加速域名	用于提供给客户端访问的域名，填写域名对应的主机记录值即可，支持泛域名接入，如果需要接入主域名，请直接填写@即可。例如：需要加速网站为 `www.example.com`，这里填写为 `www` 即可。
源站配置	源站为客户端发起请求时，最终访问的资源地址，可选 IP/域名、对象存储源站、源站组三种方式： • **IP/域名：**用于接入单个源站，可填写单个 IP 或单个域名作为源站 • **对象存储源站：**用于添加添加腾讯云 COS 和兼容 AWS S3 鉴权的对象存储桶作为源站。如果存储桶为公有读写访问，您也可以直接使用 IP/域名的源站类型接入。 • 源站组：如果源站为多个 IP，可通过配置源站组的方式添加。 • 云点播：云点播中授权的存储桶，分发范围可选择应用内所有文件或指定存储桶的文件生效 • 负载均衡：主动探测源站时延和健康状况，配置智能流量调度策略，提供更安全快捷的流量分发服务。 例如：已有一个使用腾讯云服务器搭建的跨境电商网站，该服务器的 IP 地址：`10.1.1.1`。配置源站时，源站配置选择为 IP/域名，填写该服务器地址即可。 **⚠ 注意：** 1. 建议您的源站根据加速区域配置相同地域的源站，例如，加速区域为中国大陆可用区，请配置为境内源站回源，如果源站位于全球可用区（不含中国大陆），由于回源存在跨境访问，将无法为您保障回源效果。如果您需要加速中国大陆客户的访问，且源站在全球可用区（不含中国大陆），可以参考跨地域安全加速（海外站点）。 2. 如果您的加速区域为全球可用区，可以在规则引擎中，添加相应的规则，匹配条件选择客户端地理位置，操作选择修改源站，根据不同区域回源到不同的源站内，以保障回源效果。 3. 如果您的源站类型为 IP/域名，回源 HOST 默认为加速域名，如果您的回源 Host 需要指定域名，可参考 修改回源 HOST 进行配置。如果您的源站为对象存储源站，回源 HOST 默认为对象存储源站域名。
IPv6 访问	选择是否启用支持使用 IPv6 访问，可参考文档：IPv6 访问。默认为遵循站点配置。
回源协议	选择您源站支持的访问协议，默认为协议跟随，可选：

	• **协议跟随**：回源时所使用协议与用户访问请求协议相同 • **HTTP**：回源时使用 HTTP 协议。 • **HTTPS**：回源时使用 HTTPS 协议。
回源端口	指定回源时使用的端口，请确保您的源站指定端口是可连通的，默认 HTTP 回源使用 80 端口，HTTPS 回源使用 443 端口。

如何验证加速域名已经生效

根据您所选择接入模式不同，访问测试的验证方式也会有所区别，请根据所选择的站点接入模式来进行访问测试验证。

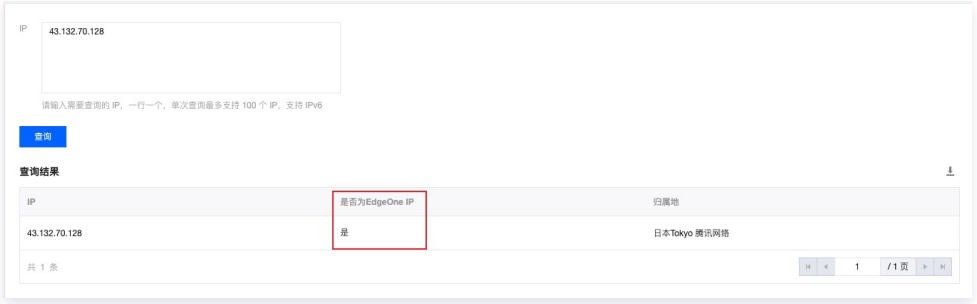
NS 接入模式

NS 接入模式下，针对已开启加速的域名，客户端访问时，EdgeOne 将自动调度至最近的边缘节点中，您可以通过访问验证当前所分配的服务节点是否为 EdgeOne IP 来进行验证。
测试获取当前访问节点 IP，可通过以下方式手动获取。

Windows

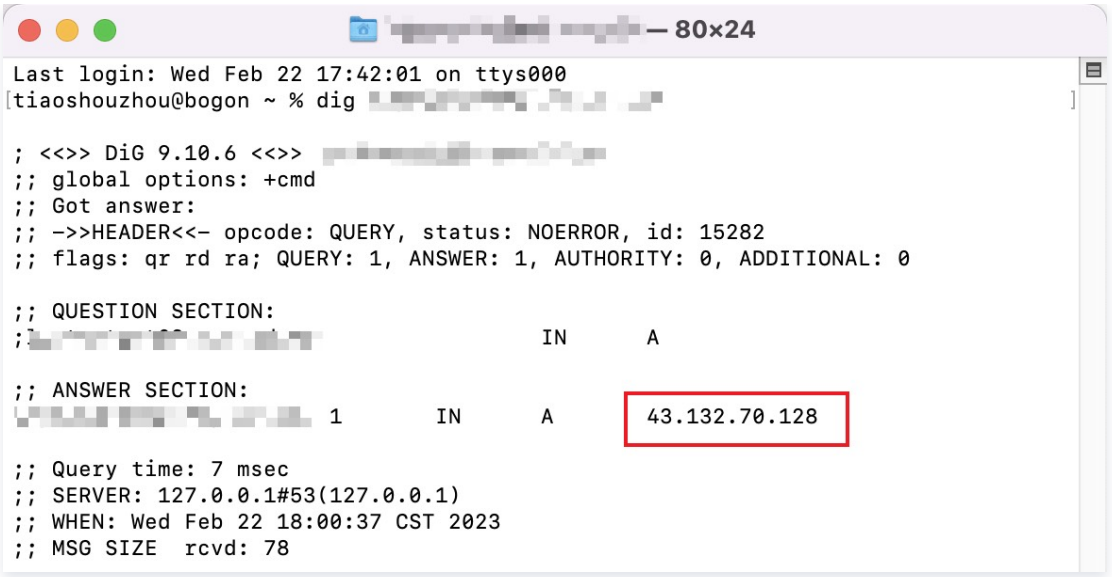
1. 在 Windows 系统中，打开 cmd 运行程序，以域名 `www.example.com` 为例，您可以在 cmd 内运行：`nslookup -qt=A www.example.com`，在运行的解析结果内，可以获取到当前域名 A 记录解析的 IP 地址。

2. 在 IP归属查询 页面，输入当前获取到的域名解析 IP 地址，查询该 IP 是否属于 EdgeOne，如果是，则当前加速解析已切换至 EdgeOne 内服务。

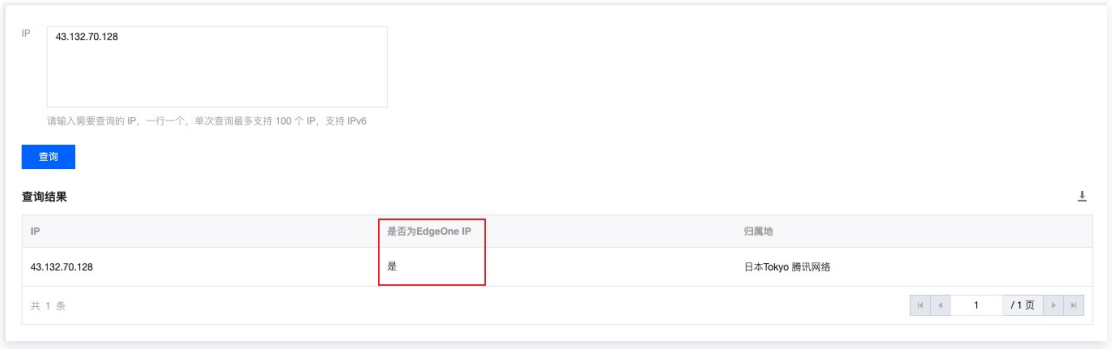


Mac/Linux

1. 在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以域名 `www.example.com` 为例，您可以在终端内运行命令：`dig www.example.com`，在运行的解析结果内，可以获取到当前域名 A 记录解析的 IP 地址。



2. 在 IP 归属查询 页面，输入当前获取到的域名解析 IP 地址，查询该 IP 是否属于 EdgeOne，如果是，则当前加速解析已切换至 EdgeOne 内服务。



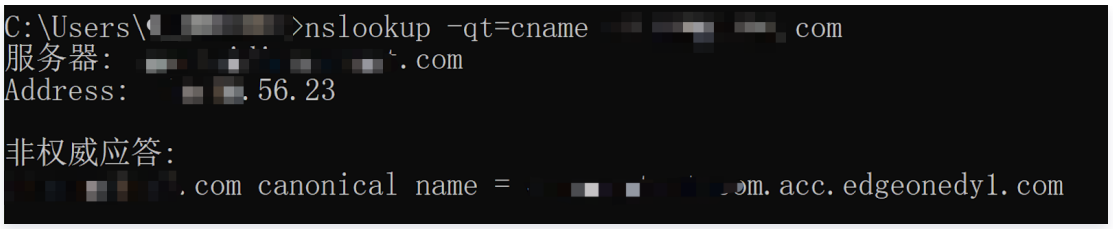
CNAME 接入模式

完成 CNAME 配置后，平台将自动检测当前 CNAME 状态是否已生效，如果在域名管理列表的状态一栏显示当前 CNAME 已生效，则当前域名已正确配置并开启加速。

如果您已正确配置 CNAME，当前状态仍显示未生效，也可能是域名解析服务商的 CNAME 解析生效延迟，您也可以通过以下方式手动验证。

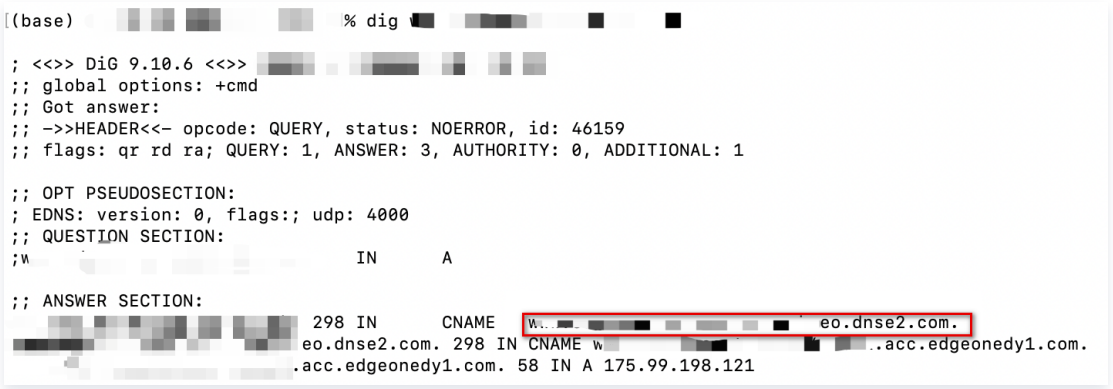
Windows

在 Windows 系统中，打开 cmd 运行程序，以域名 `www.example.com` 为例，您可以在 cmd 内运行：`nslookup -qt=cname www.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若 CNAME 结果为 EdgeOne 内分配的 CNAME 地址，即已切换至 EdgeOne 加速。



Mac/Linux

在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以域名 `www.example.com` 为例，您可以在终端内运行命令：`dig www.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若 CNAME 信息与 EdgeOne 分配的 CNAME 地址相同，即域名加速已切换至 EdgeOne。



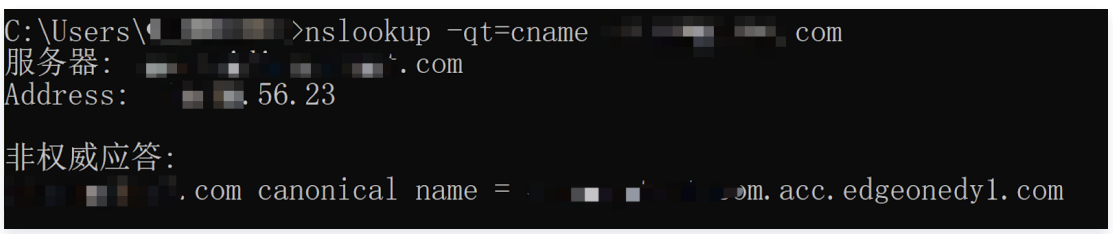
DNSPod 托管接入模式

完成 CNAME 配置后，平台将自动检测当前 CNAME 状态是否已生效，如果在域名管理列表的状态一栏显示当前 CNAME 已生效，则当前域名已正确配置并开启加速。

如果您已正确配置 CNAME，当前状态仍显示未生效，也可能是域名解析服务商的 CNAME 解析生效延迟，您也可以通过以下方式手动验证。

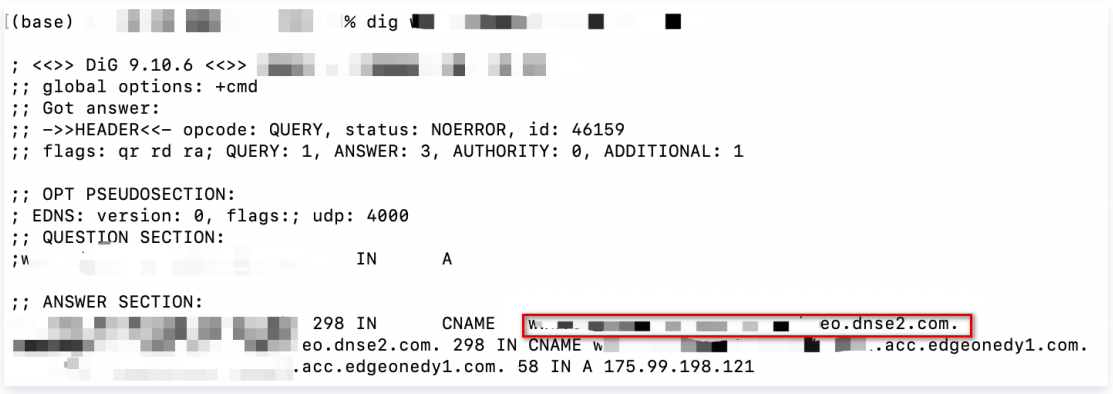
Windows

在 Windows 系统中，打开 cmd 运行程序，以域名 `www.example.com` 为例，您可以在 cmd 内运行：`nslookup -qt=cname www.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若 CNAME 结果为 EdgeOne 内分配的 CNAME 地址，即已切换至 EdgeOne 加速。



Mac/Linux

在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以域名 `www.example.com` 为例，您可以在终端内运行命令：`dig www.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若 CNAME 信息与 EdgeOne 分配的 CNAME 地址相同，即域名加速已切换至 EdgeOne。



验证业务访问

最近更新时间：2024-11-27 11:44:44

当您的域名接入至 EdgeOne 后，您还需要切换 DNS 解析，为该域名添加由 EdgeOne 分配的 CNAME 记录才能使服务生效。在执行该操作之前，为了确保您在切换后的业务能够正常访问，建议您在充分测试验证后再进行切换。本文档将指引您如何进行验证。

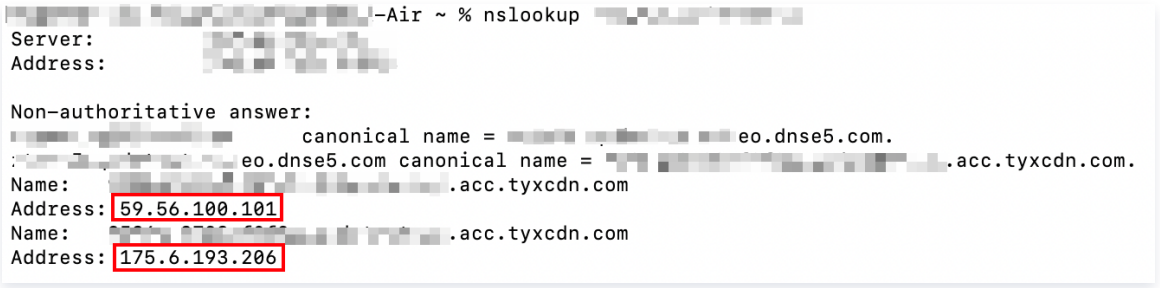
例如，您当前接入的加速域名为 `www.example.com`，接入后验证的步骤如下：

1. 登录 **边缘安全加速平台 EO 控制台**，通过站点列表，选择需配置的**站点**。
2. 在左侧导航栏中，单击**域名服务 > 域名管理**。
3. 在域名管理页面，如果您当前已完成添加域名，可以在该页面下看到 EdgeOne 为该域名分配的 CNAME 地址。

   例如：`www.example.com.eo.dnse5.com` 。

4. 通过命令行工具（CMD运行工具 或者终端），使用 `nslookup` 命令获取以上 CNAME 解析的边缘 IP，例如：

   `nslookup www.example.com.eo.dnse5.com`，获取到的 IP 如下所示，`59.56.100.101` 或者 `175.6.193.206` 均为 EdgeOne 边缘节点 IP。



5. 您可以继续参考以下两种方式来进行验证：

绑定 Host 验证

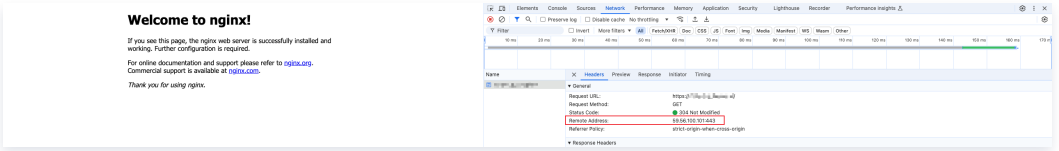
根据您操作系统的不同，您可以参考以下方式绑定 Host 进行测试验证：

Windows

在系统内找到 HOST 文件，将该 IP 地址与您的加速域名绑定，将步骤4获取的任一节点 IP（27.152.181.195）和加速域名（`www.example.com`）绑定到电脑本地 hosts 文件中，填写方法为 IP 地址在前，加速域名在后，中间用空格分隔。如下所示：

> **说明：**
> Win 系统的 host 文件所在目录为：`C:\Windows\System32\drivers\etc\` 。如果在该目录下无权限编辑该文件，可以复制该文件副本，在副本内编辑后替换原文件。

配置完成并保存后，通过浏览器进行业务访问测试，直接去访问当前的加速域名的测试 URL，打开浏览器的开发者工具，查看访问到的 IP，是否为当前已绑定的边缘节点 IP，同时查看访问效果是否符合您的预期。



Mac

在系统内找到 HOST 文件，将该 IP 地址与您的加速域名绑定，将步骤4获取的任一节点 IP（27.152.181.195）和加速域名（`www.example.com`）绑定到电脑本地 hosts 文件中，填写方法为 IP 地址在前，加速域名在后，中间用空格分隔。如下所示：

> **说明：**
> Mac 系统的 host 文件所在目录为：`/etc/`。如果在该目录下无权限编辑该文件，可以复制该文件副本，在副本内编辑后替换原文件。

hosts

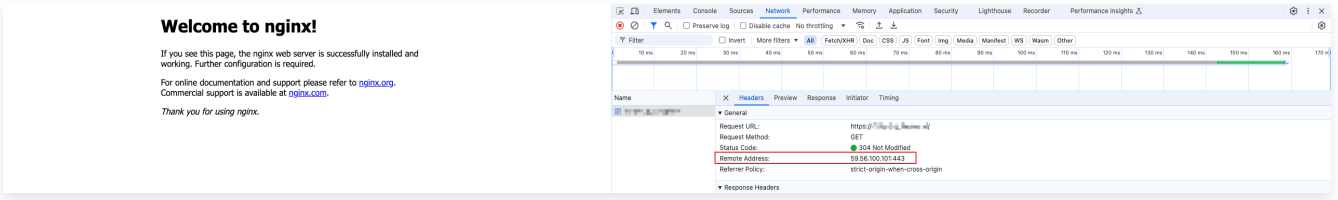
```
##
# Host Database
#
# localhost is used to configure the loopback interface
# when the system is booting.  Do not change this entry.
##


127.0.0.1       localhost
255.255.255.255 broadcasthost

59.56.100.101 www.example.com

::1             localhost
```

配置完成并保存后，通过浏览器进行业务访问测试，直接去访问当前的加速域名的测试 URL，打开浏览器的开发者工具，查看访问到的 IP，是否为当前已绑定的边缘节点 IP，同时查看访问效果是否符合您的预期。



Curl 命令验证

您可以参考以下 Curl 命令：

```
curl --resolve <hostname>:<port>:<ip> <url> -v
```

其中 hostname 即当前需要访问的域名 `www.example.com`，port 为访问时指定的端口号，如果是 HTTPS 访问，使用 443 端口，如果是 HTTP 访问，使用 80 端口，ip 即为步骤 4 中获取到的 IP 地址，url 即为当前访问测试使用的 url。例如：
`curl --resolve www.example.com:443:59.56.100.101 https://www.example.com/ -v`。
查看请求结果是否正常以及是否符合预期。

```
[ MacBook-Air ~ % curl --resolve :443:59.56.100.101 https://]
.cn/ -v
* Added :443:59.56.100.101 to DNS cache
* Hostname was found in DNS cache
*   Trying 59.56.100.101:443...
* Connected to (59.56.100.101) port 443
* ALPN: curl offers h2,http/1.1
* (304) (OUT), TLS handshake, Client hello (1):
*  CAfile: /etc/ssl/cert.pem
*  CApath: none
* (304) (IN), TLS handshake, Server hello (2):
* (304) (IN), TLS handshake, Unknown (8):
* (304) (IN), TLS handshake, Certificate (11):
* (304) (IN), TLS handshake, CERT verify (15):
* (304) (IN), TLS handshake, Finished (20):
* (304) (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / AEAD-AES256-GCM-SHA384 / [blank] / UNDEF
* ALPN: server accepted h2
* Server certificate:
*  subject: CN=
*  start date: Sep 16 12:20:26 2024 GMT
*  expire date: Dec 15 12:20:25 2024 GMT
*  subjectAltName: host "" matched cert's ""
*  issuer: C=US; O=Let's Encrypt; CN=R10
*  SSL certificate verify ok.
* using HTTP/2
* [HTTP/2] [1] OPENED stream for https://
* [HTTP/2] [1] [:method: GET]
* [HTTP/2] [1] [:scheme: https]
* [HTTP/2] [1] [:authority: ]
* [HTTP/2] [1] [:path: /]
* [HTTP/2] [1] [user-agent: curl/8.6.0]
* [HTTP/2] [1] [accept: */*]
> GET / HTTP/2
> Host:
> User-Agent: curl/8.6.0
> Accept: */*
>
< HTTP/2 200
< etag: "6179061b-267"
< server: nginx/1.21.3
< content-type: text/html; charset=utf8
< ohc-mp4-bitrate: 300kbps
```

6. 当验证访问符合预期后，即可将您的域名解析切换至 EdgeOne 服务，详情参考：修改 CNAME 解析 。

修改 CNAME 解析

最近更新时间：2024-10-15 11:19:11

域名创建完成后，EdgeOne 将为该域名分配一个 CNAME 地址，您需要完成配置 CNAME 才能使该域名的安全加速生效。

场景一：NS 模式或者 DNSPod 托管模式下，一键添加 CNAME

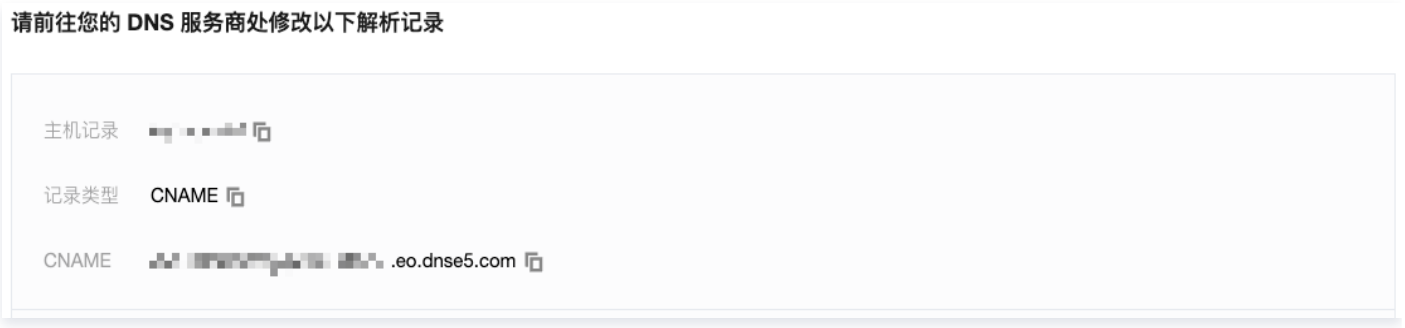
在 DNSPod 托管接入模式下，域名支持一键添加 CNAME，可以帮助您快速完成 CNAME 配置。

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的**站点**，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务 > 加速域名管理**，进入域名管理详情页面。
3. 如果当前域名还未配置 CNAME，在状态列中单击**一键添加**。

4. 在弹窗中确认 EdgeOne 将操作的相关 CNAME 信息后，单击**确定**。在二次弹窗中再次单击**确定**，即可由 EdgeOne 自动帮您完成 CNAME 配置。

场景二：手工配置 CNAME

1. 添加完域名后，EdgeOne 会为您提供指向 EdgeOne 节点的 CNAME。



2. 登录该域名的 DNS 解析服务商，添加一条 CNAME 记录，以下为不同 DNS 解析服务商的添加示例。

腾讯云 DNSPod

a. 登录 云解析 DNS，在**我的解析**中找到当前待验证的域名，单击该**域名**进入域名配置页。
b. 在域名配置页中，单击**添加记录**，为当前域名新增一条 CNAME 记录。

c. 填写步骤1中的记录类型、主机记录和记录值。

参数名称	参数说明

记录类型	CNAME
主机记录	填写您的域名
线路类型	默认
域名	填写 EdgeOne 提供的 CNAME
TTL	600

d. 单击**确认**，完成添加。

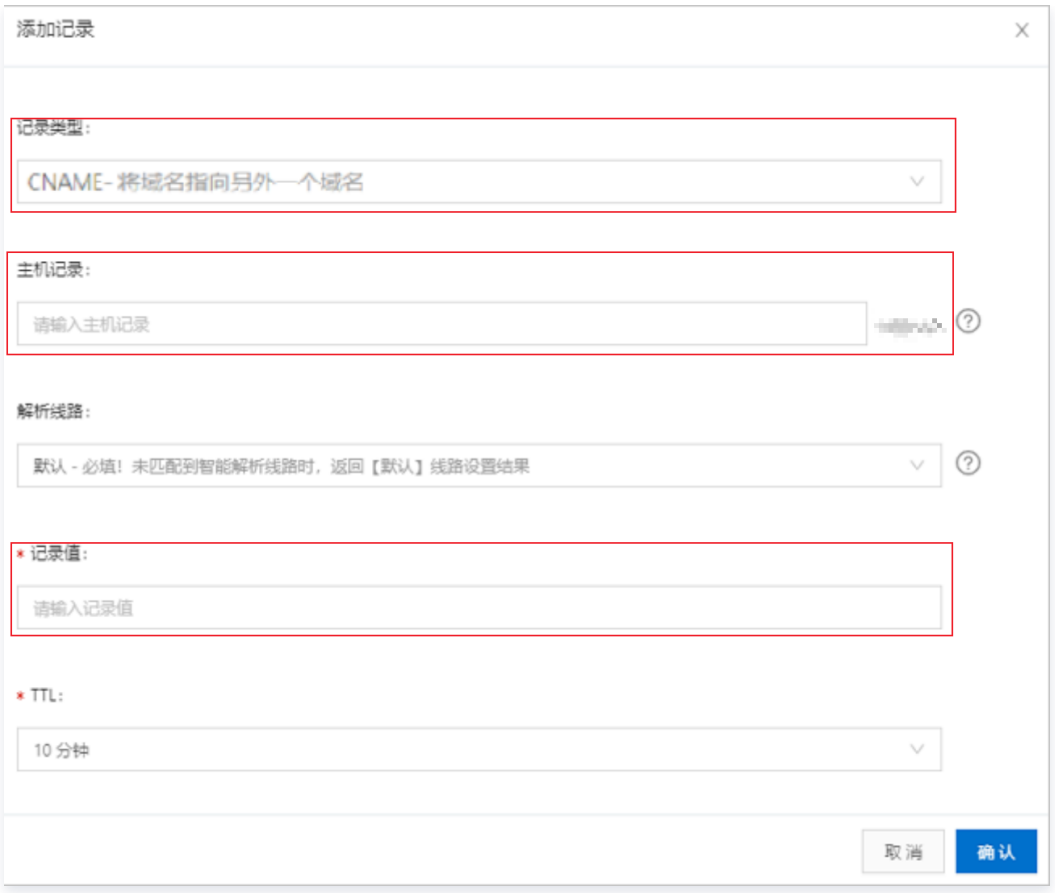
阿里云 DNS 添加示例

a. 登录阿里云的 云解析 DNS 控制台 。

b. 在**域名解析**页面，找到当前待验证的域名，在域名右侧单击**解析设置**，进入解析设置页面。

c. 单击**添加记录**，为当前域名新增一条 CNAME 记录。

d. 填写步骤1中的记录类型、主机记录和记录值。

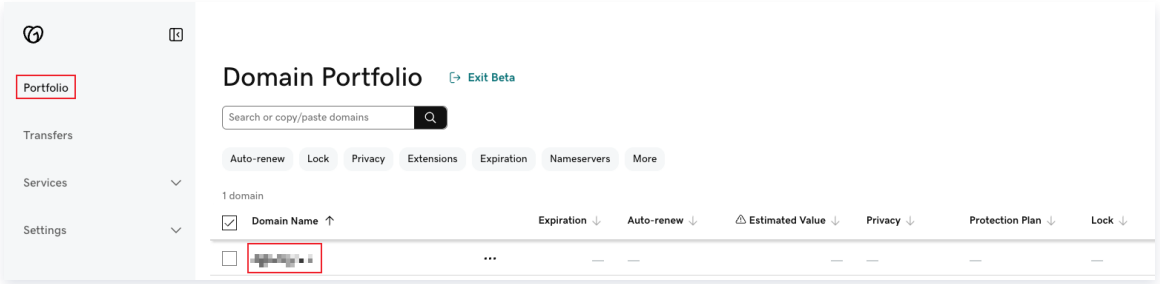


参数名称	参数说明
记录类型	CNAME
主机记录	填写您的域名
线路类型	默认
记录值	填写 EdgeOne 提供的 CNAME
TTL	10分钟

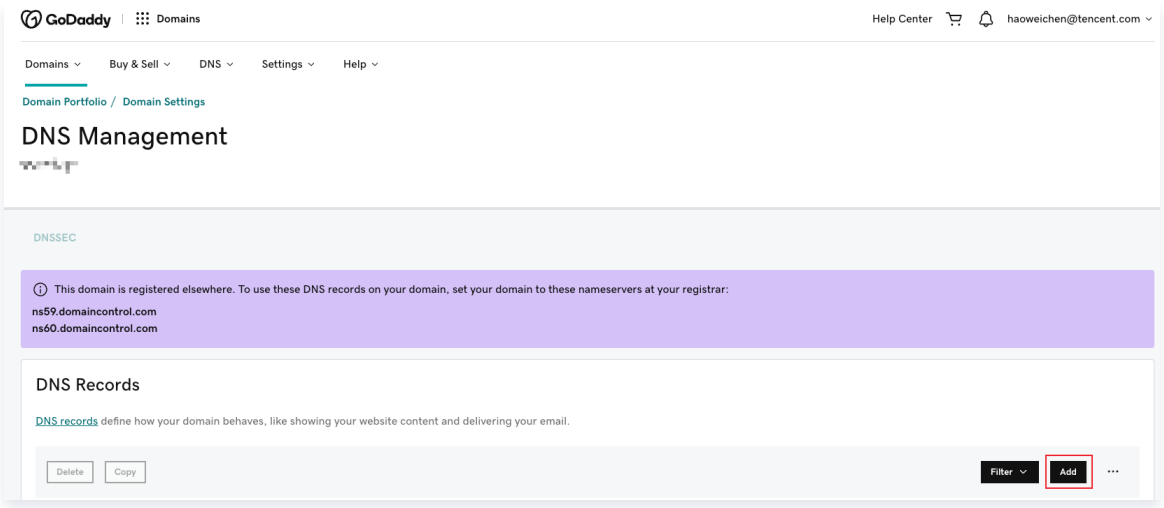
e. 单击**确认**，完成添加。

Godaddy 添加示例

a. 登录 Godaddy Domain Portfolio 控制台 。
b. 在 **Portfolio** 页面，找到当前待验证的域名，单击该**域名**进入解析设置页面。



c. 单击 **Add**，为当前域名新增一条用于归属权校验的解析记录。

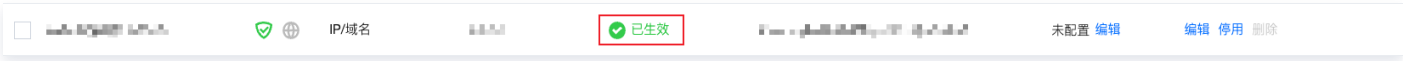


d. 填写步骤1中的记录类型、主机记录和记录值。

参数名称	参数说明
Type	CNAME
Name	填写您的域名
Value	填写 EdgeOne 提供的 CNAME
TTL	Default

e. 单击 **Add Record**，完成添加。

3. 配置完成之后，列表中，状态列出现展示为**已生效**则表示该 CNAME 记录已生效，该域名正常加速中。



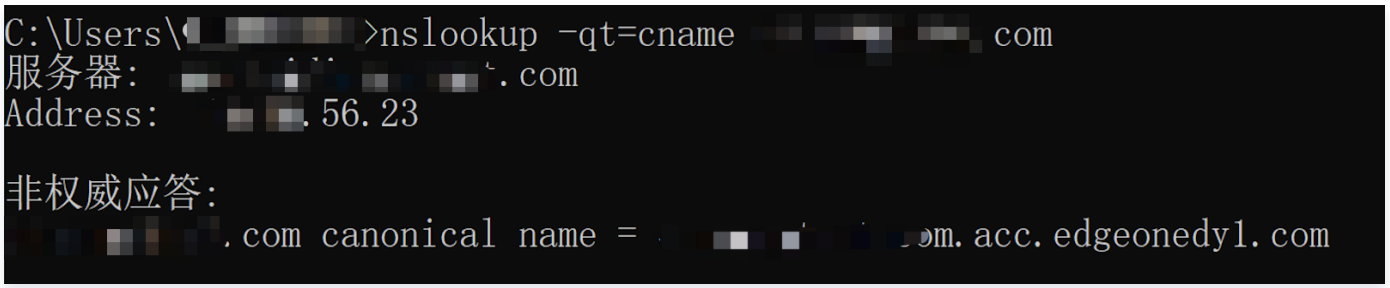
如何验证域名的 CNAME 解析是否生效

完成 CNAME 配置后，平台将自动检测当前 CNAME 状态是否已生效，如果在域名管理列表的状态一栏显示当前 CNAME 已生效，则当前域名已正确配置并开启加速。

如果您已正确配置 CNAME，当前状态仍显示未生效，也可能是域名解析服务商的 CNAME 解析生效延迟，您也可以通过以下方式手动验证。

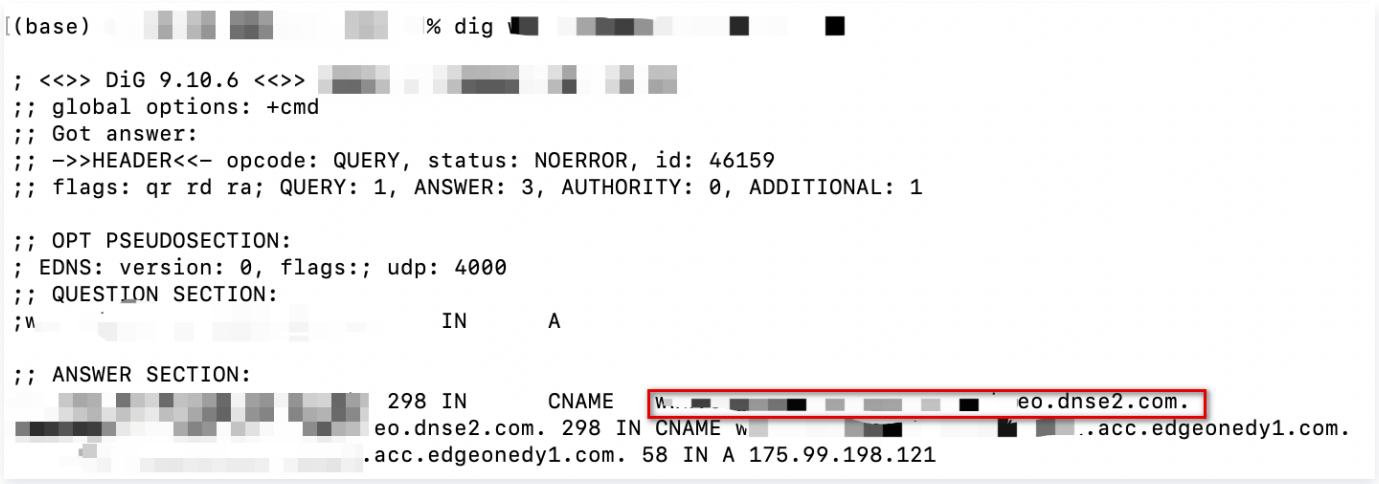
Windows

在 Windows 系统中，打开 cmd 运行程序，以域名 `www.example.com` 为例，您可以在 cmd 内运行：`nslookup -qt=cname www.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若 CNAME 结果为 EdgeOne 内分配的 CNAME 地址，即已切换至 EdgeOne 加速。



Mac/Linux

在 Mac/Linux 系统中，可以使用 dig 命令进行验证，以域名 `www.example.com` 为例，您可以在终端内运行命令：`dig www.example.com`，根据运行的解析结果内，可以查看该域名的 CNAME 信息。若 CNAME 信息与 EdgeOne 分配的 CNAME 地址相同，即域名加速已切换至 EdgeOne 。



流量调度
流量调度管理

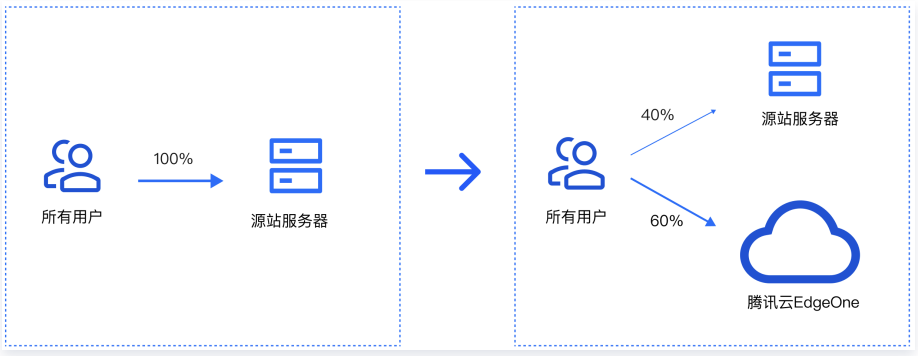
最近更新时间：2024-08-23 15:07:21

功能简介

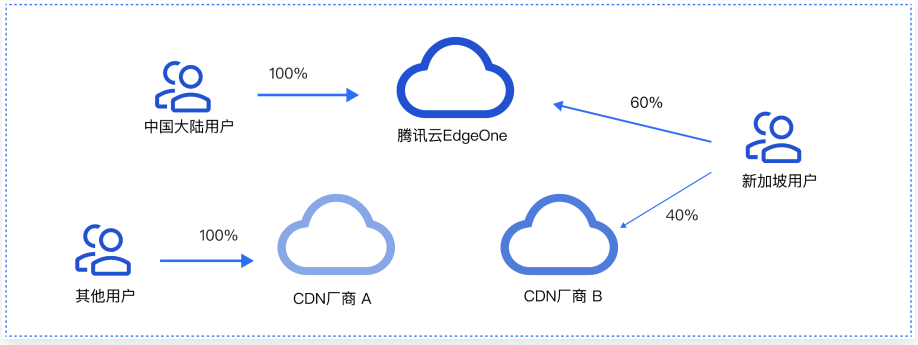
流量调度管理是腾讯云 EdgeOne 提供的多 CDN 智能解析调度工具，支持在源站、多个服务商之间自定义流量调度策略，实现流量平滑灰度迁移和灵活分配，保证服务高可用。

应用场景

- 灰度迁移：引入新服务商时，为了保证服务可用性，需要进行灰度切换，实现业务平滑迁移。



- 多厂商调度：业务量级较大且敏感，为了分散风险，希望将流量灵活分配给多家服务商，实现业务容灾。



功能特点

- 管理简单：选择域名 > 添加服务商 > 添加调度策略，仅需三步添加即可实现流量调度管理。
- 快速接入：用户只需在 DNS 解析商处添加 EdgeOne 分配的 CNAME 记录即可实现快速接入。
- 多种调度模式：支持按比例、按区域的调度模式，可组合使用满足多样化需求。
- 覆盖场景多样：支持源站和 CDN 厂商作为调度服务商，可以满足灰度切换和同时使用多家服务商的场景。

前提条件

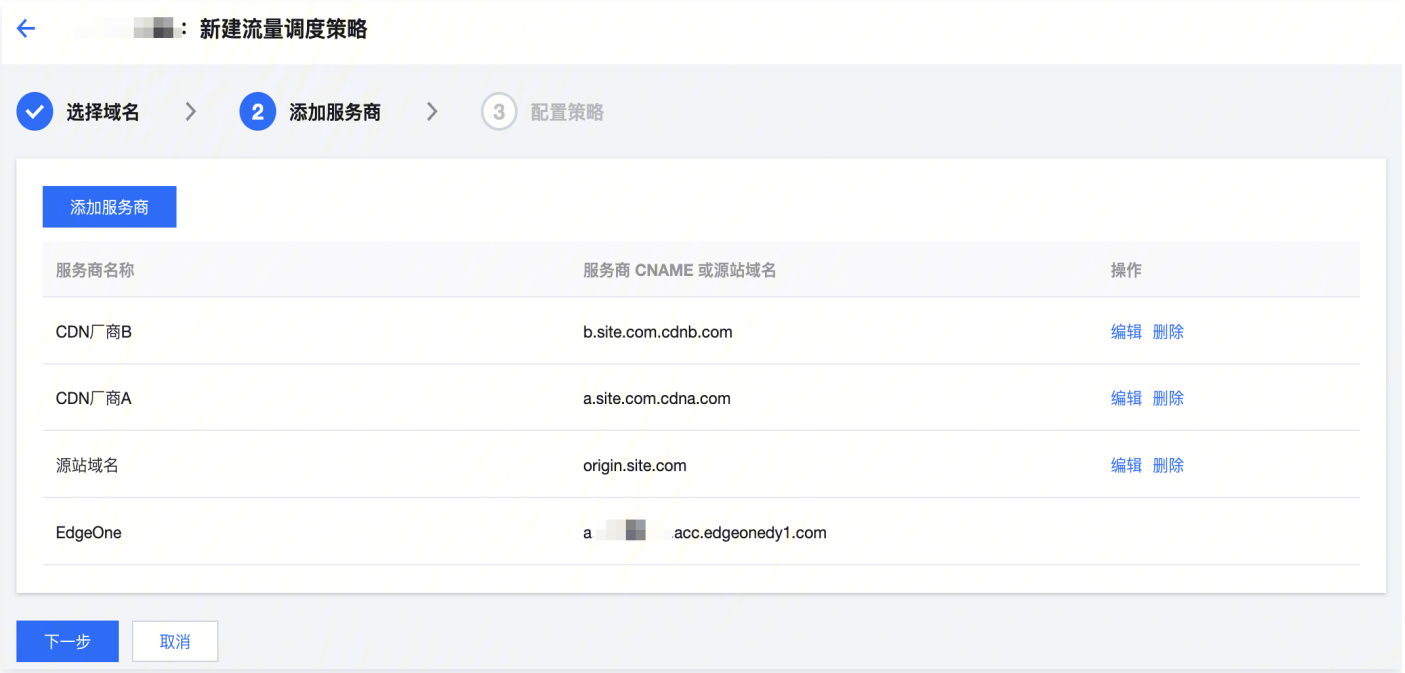
您需要成功 购买 边缘安全加速平台（EdgeOne）产品（企业版），且使用 CNAME 模式完成 站点接入。

添加流量调度策略

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** > **流量调度管理**。
3. 在流量调度管理页面，单击**添加调度策略**，选择需要开启流量调度的域名，单击**创建**。

4. 单击**添加服务商**，按照业务需求配置服务商名称、CNAME等参数，单击**下一步**。

> **说明：**
> 提供默认服务商 EdgeOne，不可修改和删除。支持新增源站域名和其他 CDN 服务商 CNAME 域名。



5. 单击**添加策略**，选择线路/区域，配置多服务商的调度策略，服务商支持多选以及权重设置，完成后单击**提交配置**。

> **说明：**
> - 默认策略为全部流量走 EdgeOne，该策略作为兜底策略不可删除，可支持修改为其他服务商。
> - 线路/区域支持国家地区，中国大陆运营商、省份、省份运营商，美国各州和印度各邦。
> - 细粒度区域/线路生效优先级更高，如配置北京调度源站、中国大陆调度服务商 A 、默认线路调度服务商 B，则北京地区走源站，中国大陆其他区域走服务商 A，境外区域走服务商 B。

6. 添加策略完成后，因流量调度CNAME和域名默认CNAME一致，如果域名解析已切换，则无需变更，策略立即生效现网；否则，需要在 DNS 服务商处完成域名解析切换，方可触发流量调度策略生效。

管理流量调度策略

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 > 流量调度管理**。
3. **流量调度管理**页面，可以编辑管理、停用、启用和删除策略。

停用策略

停用策略会导致流量调度策略失效，所有流量将全部调度使用 EdgeOne 进行服务。

启用策略

停用的策略可通过启用恢复使用流量调度管理，启用后流量会从全部调度使用 EdgeOne 变更为按配置的策略进行调度。

删除策略

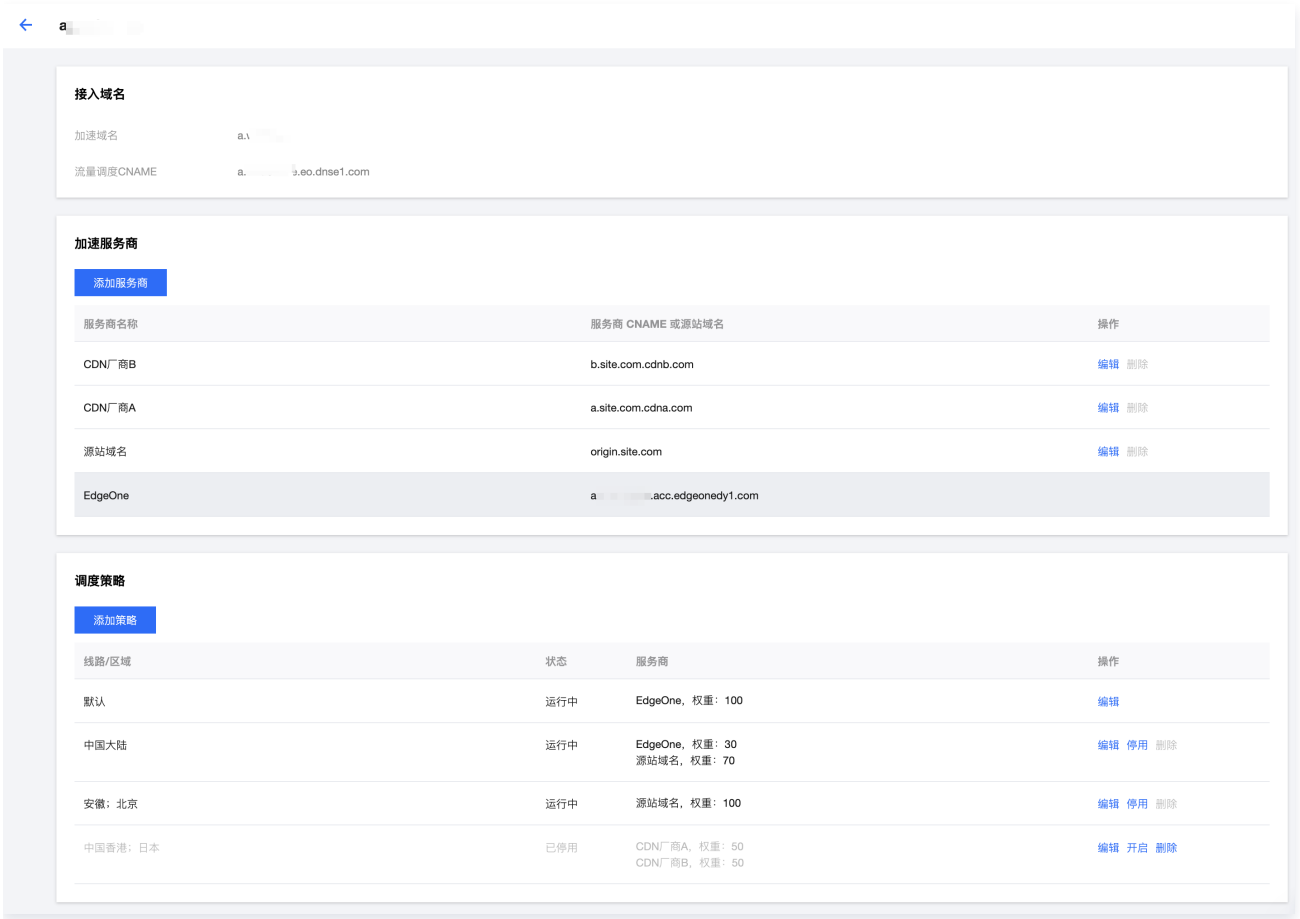
停用策略后，可删除策略，删除不影响服务，但策略不可恢复，请谨慎操作。

管理策略

单击**管理**可以进入**调度策略管理**页面，可以对服务商和调度策略进行增加、删除、修改以及停用。

> **说明：**
> - 变更已被策略引用的服务商，保存后会立即生效到策略。
> - 删除和修改策略、启用和停用策略均会立即生效。

- 已被策略引用的服务商，无法删除。



HTTPS 证书

概述

最近更新时间：2024-10-14 18:03:31

本文介绍了 HTTPS 相对 HTTP 协议的优势以及 EdgeOne 节点上支持部署的证书类型和加密算法。

HTTPS 介绍

HTTPS 是在 HTTP 的基础上，通过 SSL 协议构建了身份认证和传输加密的方法，SSL 协议需通过 HTTPS 证书来验证服务器的身份，为客户端浏览器和服务器之间构建可信的加密传输通道。相比 HTTP 传输，HTTPS 具有以下优势：

- **防劫持、防篡改、防监听：**HTTPS 协议可对用户与服务端间的数据交互进行加密，从而实现传输数据的防劫持、防篡改、防监听。
- **增加网站可信度：**用户通过 HTTPS 访问至网站并通过证书验证网站的可信身份时，在浏览器内将增加安全的绿色标识，来提升网站的可信度，避免用户访问至钓鱼网站。
- **提升网站的搜索排名：**搜索引擎将优先收录已支持 HTTPS 协议的可信网站，网站支持 HTTPS 协议访问后，有利于提高搜索引擎的排名。

EdgeOne 支持的 HTTPS 证书能力

功能名称	功能介绍
边缘 HTTPS 证书	边缘 HTTPS 证书可支持让用户在访问当前域名时，可通过 HTTPS 与 EdgeOne 边缘节点安全通信。当前 EdgeOne 已支持通过以下方式配置边缘 HTTPS 证书。 • 腾讯云 SSL 证书：如果您当前已经拥有域名证书，可将上传至腾讯云 SSL 控制台的证书部署至 EdgeOne 边缘节点上。最多支持同时部署一本 RSA、ECC、SM2 证书到 EdgeOne 节点中。 • 申请免费证书：如果您当前还未购买 SSL 证书，可通过 EdgeOne 自动完成免费证书申请、部署以及续签，减少运维工作量，当前申请的免费证书是来源于 Let‘s Encrypt 的 RSA 证书。
边缘双向认证	边缘双向认证则是指在通信过程中，客户端和服务器都需要向对方证明自己的身份。这通常用于高安全要求的场景，如企业内部网络或金融交易。EdgeOne 可支持在边缘节点内启用双向认证，在访问中要求客户端携带可信任的客户端证书进行验证，进一步加强通信的安全性。
强制 HTTPS 访问	强制 HTTPS 访问可将客户端 HTTP 请求通过301/302重定向至 HTTPS，最终以 HTTPS 访问 EdgeOne。以确保所有客户端都是以 HTTPS 向 EdgeOne 节点发起请求，保障通信的安全性。
HSTS	HSTS（HTTP Strict-Transport-Security）是国际互联网工程组织 IETE 推行的 Web 安全协议，用来通知浏览器使用更安全的 HTTPS 访问该站点。若您需要增强网站的安全性，防止恶意攻击者通过中间人攻击窃取用户敏感信息；或需要遵循数据隐私保护法规，保护用户的隐私信息；或需要提高网站的信誉度，增强用户对网站的信任感，均可以配置 HSTS 来提高网站的安全性和信誉度。
SSL/TLS 安全配置	当您的网站开启 HTTPS 访问后，EdgeOne 默认为您的站点支持了兼容性更高多种 SSL/TLS 版本访问，以适配不同用户终端的访问环境，正常情况下，您无需修改该配置。如果您的网站安全性要求较高，需要禁止用户通过安全较低的 SSL/TLS 版本访问，您可以通过修改此配置来自定义所使用的 SSL/TLS 版本。
OCSP 装订	OCSP（Online Certificate Status Protocol）是用来检验证书合法性和有效性的在线查询协议，由数字证书颁发机构 CA（Certificate Authority）提供。当用户每次通过 HTTPS 访问网站的时候，浏览器会通过 OCSP 查询验证网站的证书是否有效。 启用 OCSP 装订后，OCSP 查询的工作将由 EdgeOne 服务器完成，且 EdgeOne 可将查询结果缓存到服务器中。当客户端与 EdgeOne TLS 握手时，EdgeOne 直接响应客户端 OCSP 信息和证书，供客户端验证，无需再由客户端向 CA 发送查询请求，极大地提高了 TLS 握手效率，节省用户验证时间，优化 HTTPS 速度。

部署/更新 SSL 托管证书至 EdgeOne 域名

最近更新时间：2024-03-22 09:44:11

本文分别从 EdgeOne 控制台和 SSL 控制台介绍如何将自有证书部署/更新至 EdgeOne 域名。

部署证书

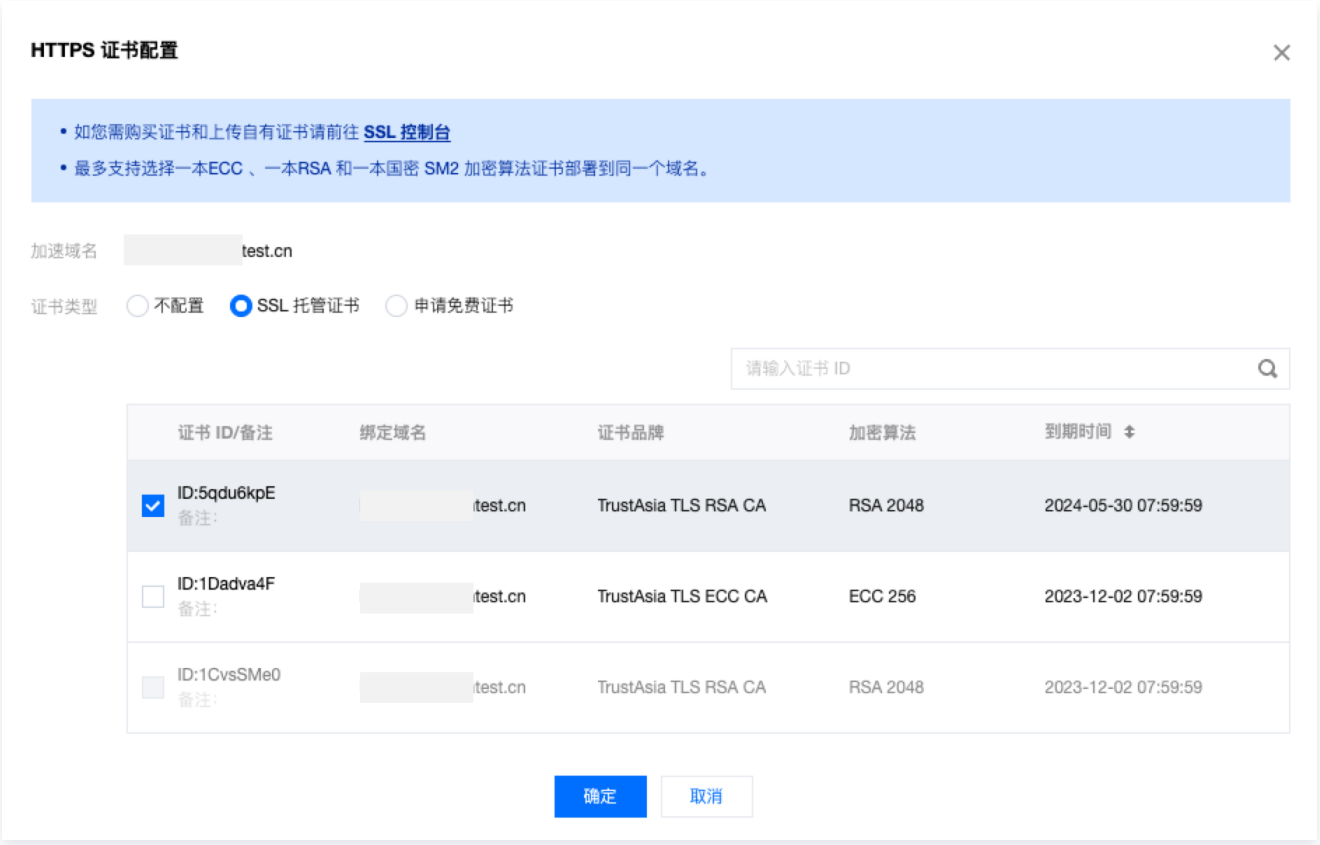
前提条件

已在 SSL 证书控制台 内购买 SSL 证书，或已上传自有证书托管至 SSL，如何上传托管证书请参见： 上传 SSL 证书 。

场景1：通过 EdgeOne 控制台部署自有证书

如果您希望直接通过 EdgeOne 控制台管理和使用自有证书，可参考以下步骤操作：

1. 登录 边缘安全加速平台控制台 ，通过站点列表，选择需配置的站点，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务 > 域名管理**。
3. 在域名管理列表页面，选择待配置 SSL 托管证书的域名，在 HTTPS 列内单击**编辑**，弹出 HTTPS 证书配置。
4. 在证书类型中，选择 SSL 托管证书，可自动带出当前可部署于该域名的证书列表，选择需关联的证书 ID，单击**确定**，即可下发证书配置。



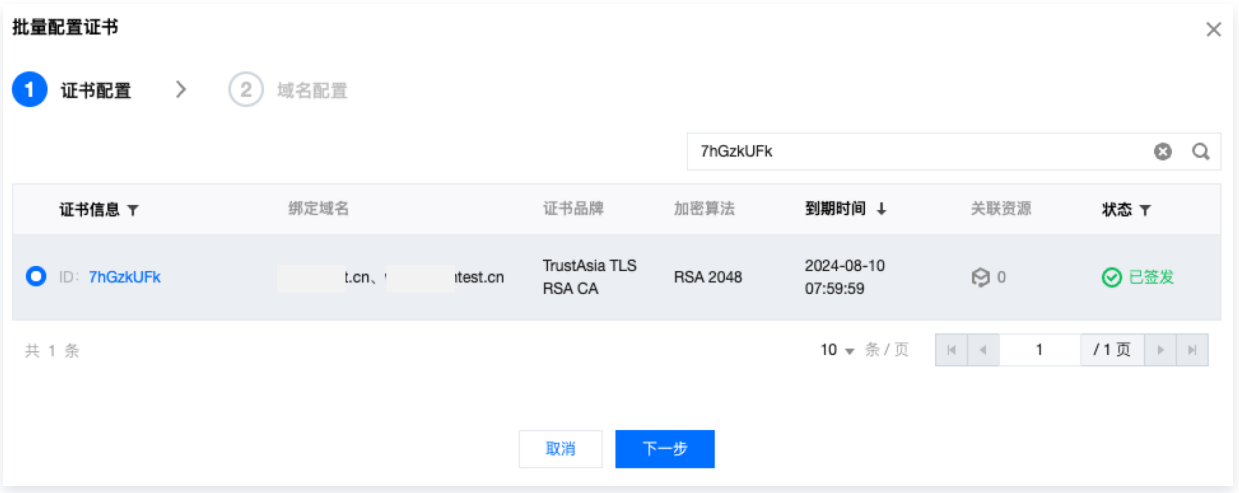
> ⚠ **注意：**
> 最多支持选择一本 ECC 、一本 RSA 和一本国密 SM2 加密算法证书部署到同一个域名。

5. 部署完成后，您可以在域名管理列表页中，将鼠标悬停于已配置图标上，可展示当前已部署的证书信息。

场景2：通过 EdgeOne 控制台批量配置证书

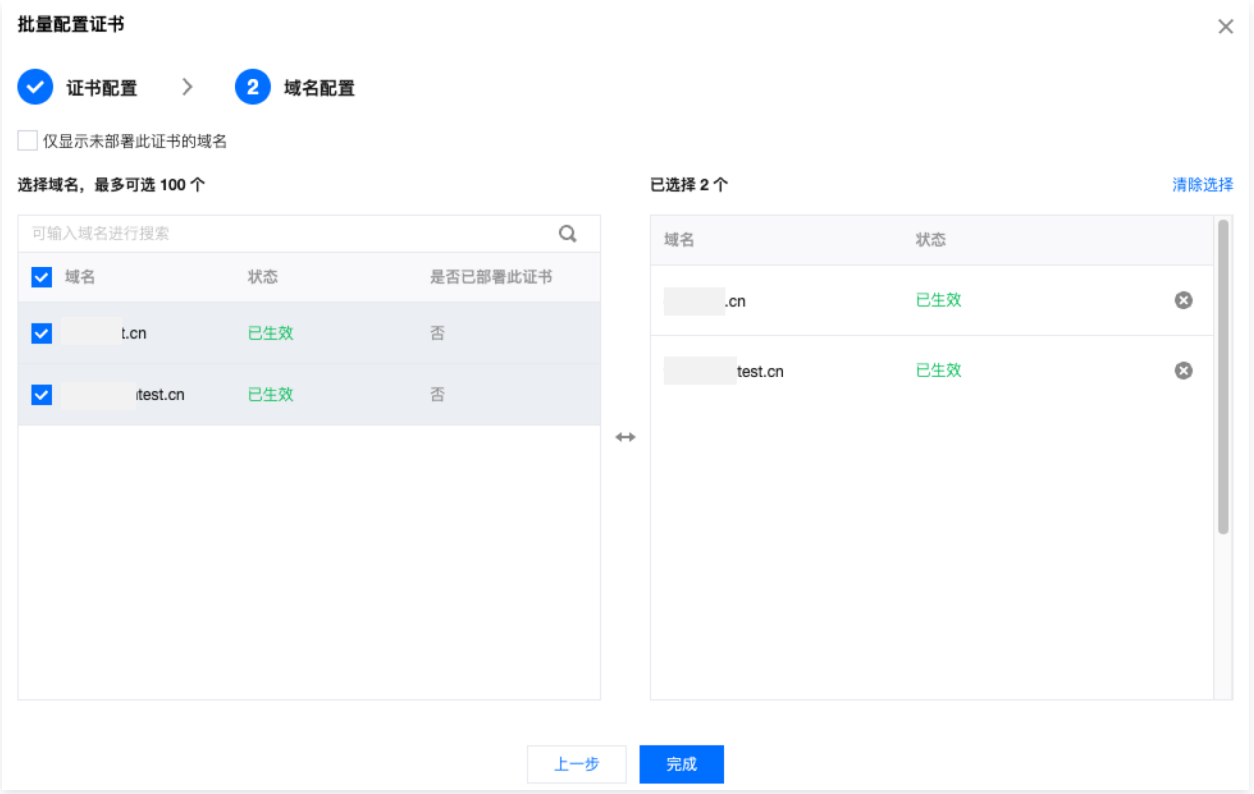
如果您的证书为多域名或泛域名证书，您期望在 EdgeOne 批量选中多个域名并部署同一本证书，减少多个不同域名重复配置同一本证书的操作，则批量配置证书适用于此场景，具体操作步骤如下：

1. 登录 边缘安全加速平台控制台，通过站点列表，选择需配置的站点，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务 > 域名管理**。
3. 在域名管理页面，单击**批量配置证书**，在**批量配置证书**的步骤中，选中需配置的证书。



4. 单击**下一步**，则进入域名配置步骤。批量选中需要部署的域名，单击**完成**即可下发证书部署。

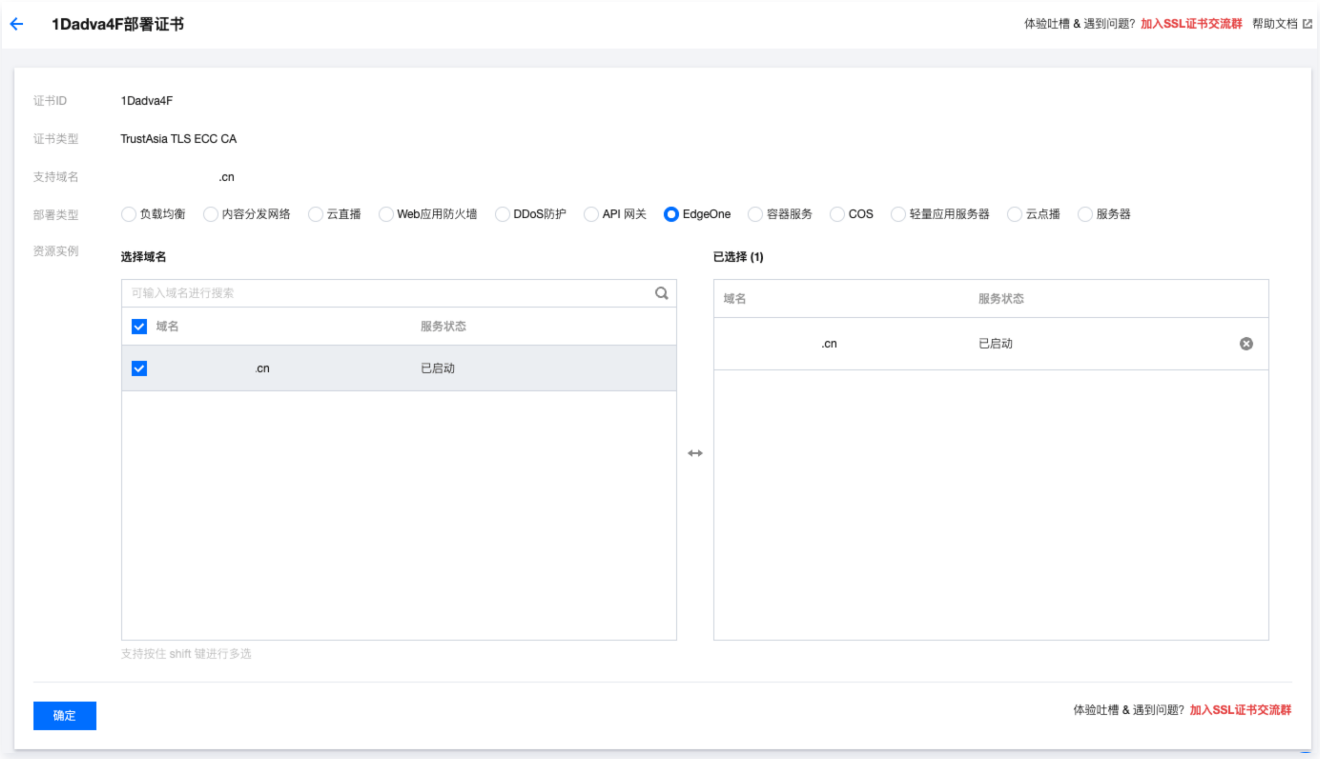
> **说明：**
> 1. 单次批量选中域名最多支持100个，如证书需部署超过100个域名，请分批操作。
> 2. 如需快速过滤掉已部署此证书的域名，请勾选：仅显示未部署此证书的域名。



场景3：通过腾讯云 SSL 控制台部署自有证书至 EdgeOne 域名

如果您主要使用腾讯云 SSL 控制台上统一管理所有腾讯云产品证书并进行维护，可以参考以下步骤操作：

1. 登录 SSL证书控制台，单击**我的证书**。
2. 在我的证书页面，通过查看证书绑定的域名，找到当前需配置证书的域名可使用的证书，单击操作列的**部署**。
3. 在部署类型选中 EdgeOne，选择将要部署证书到 EdgeOne 的域名，单击**确定**即可下发部署。



更新证书

- 场景一：如果您的证书是自有证书，上传至 SSL 证书托管，在需要更新时，需要将新的证书内容重新上传至 SSL 证书控制台内，然后参考 部署证书 的方式进行重新部署后更新。
- 场景二：如果您已在 SSL 证书控制台内购买 SSL 证书，建议您开启证书托管实现证书的自动续期及更新，您可以参考：证书托管 。

使用免费证书部署至 EdgeOne 域名

最近更新时间：2024-11-28 10:20:31

使用场景

如果您当前网站还未购买 HTTPS 证书，且加速域名不包含泛域名，可申请使用免费证书来测试支持 HTTPS 访问。

说明：

1. 免费证书由 Let's Encrypt 机构颁发，如果您的站点当前为 NS 接入的方式，可申请泛域名证书，如果当前为 CNAME 接入，EdgeOne 只支持申请单域名证书，不支持申请泛域名证书。
2. 证书有效期为90天，到期前平台将自动为您申请续期，无需您手动更新。如果您当前是 NS 接入，切换至 CNAME 接入后，申请的泛域名证书到期后将无法自动续期。
3. 免费证书不支持下载。
4. 如果域名是 CNAME 接入，您还需要完成 CNAME 配置并等待 CNAME 状态生效，才可以为该域名申请免费 SSL 证书。

操作步骤

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的**站点**，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务 > 域名管理**。
3. 在域名管理页面，选择待配置证书的域名，在 HTTPS 列内单击**编辑**，弹出 HTTPS 证书配置。

4. 选择申请免费证书后，单击**确定**，即可完成免费证书的申请和安装。
5. 部署完成后，您可以在域名管理列表页中，将鼠标悬停于已配置图标上，可展示当前已部署的证书信息。

双向认证

最近更新时间：2024-10-14 18:03:31

功能简介

HTTPS 双向认证，又称为双向 TLS 认证或客户端认证，是一种安全通信协议，其中服务器和客户端都需要验证对方的身份。在标准 HTTPS 中，主要是服务器向客户端证明自己的身份（通过服务器证书），从而建立起一个安全的、加密的通信通道。双向认证在此基础上更进一步，要求客户端也提供证书，由服务端验证客户端的身份。这种方式常用于需要高度安全的系统，以确保通信双方都是可信任的。

准备工作

- 一本服务端证书，分别是 server.pem、server.key；
- 一本客户端证书，分别是 client.pem、client.key；
- 根证书：CA.pem，该证书需要将完整的证书链提前上传至至 腾讯云 SSL 控制台，该证书需要包含完整的证书链，格式要求可参考：CA 证书格式和证书链规范 。

> **说明：**
> 如果您当前还没有购买服务端证书和客户端证书，在测试环境下，您也可以参考使用 OpenSSL 生成自签名证书来生成自签名证书。

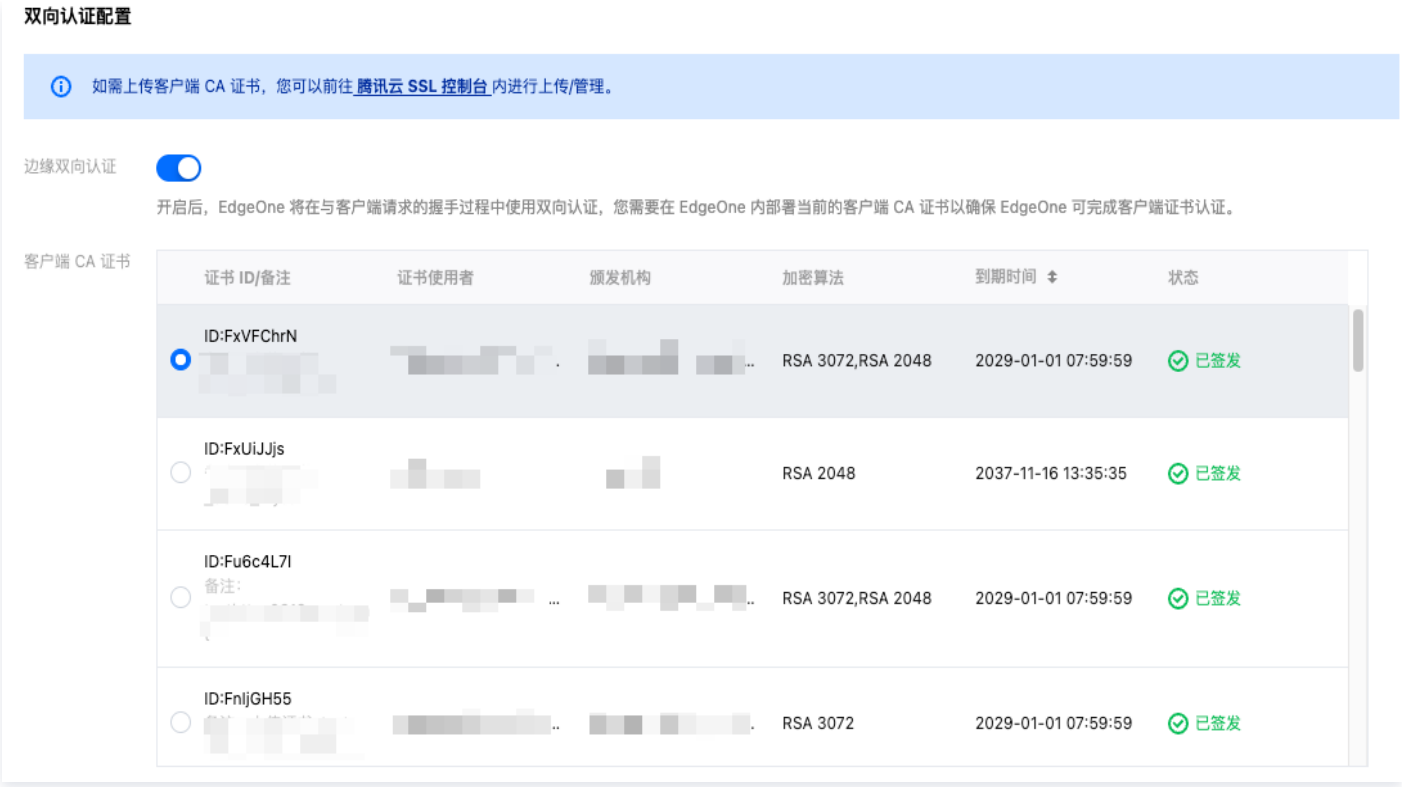
使用限制

- 当前每个域名仅支持配置 1 本客户端 CA 证书，支持 RSA、ECC 或者 SM2 国密算法证书。
- 如果服务端配置的是国密算法证书，客户端 CA 证书也必须为国密算法证书。

操作步骤

例如：需要针对 `www.example.com` 域名配置双向认证， 客户端 CA 证书已上传至腾讯云 SSL 控制台内。

1. 登录 边缘安全加速平台 EO 控制台，通过站点列表，选择需配置的站点，进入站点管理二级菜单。
2. 在左侧导航栏中，单击**域名服务 > 域名管理**。
3. 在域名管理页面，选择待配置证书的域名，在 HTTPS 列内单击**编辑**，弹出 HTTPS 证书配置，在双向认证配置中，打开边缘双向认证开关并选择已有的客户端 CA 证书进行配置。



4. 单击**确定**，即可下发配置，部署完成后即可生效。配置完成后，客户端需要携带由该客户端 CA 证书签发的客户端证书进行访问，否则无法完成 HTTPS 握手。您也可以通过参照以下 curl 命令，携带客户端证书信息来验证是否握手成功。

```
curl https://www.example.com --cert client.crt --key client.key -v -k
```

其中，--cert 为客户端公钥证书在本地的路径，--key 为客户端私钥证书在本地的路径。

热点问题

测试时报错，返回：Empty reply from server?

这种情况下，最常见的可能性是由于当前配置的客户端 CA 证书的证书链不完整，您需要将完整的证书链内容拼接到一起，上传到腾讯云 SSL 控制台内，拼接内容的顺序需要严格按照 CA 证书格式和证书链规范 的顺序进行拼接。

HTTPS 配置
强制 HTTPS 访问

最近更新时间：2024-07-22 16:02:31

功能说明

将客户端 HTTP 请求通过301/302重定向至 HTTPS，最终以 HTTPS 访问 EdgeOne。强制 HTTPS 访问的功能通常用于提高网站的安全性和保护用户隐私，若您的业务需要保护用户隐私和一些其他敏感信息，为了提高安全性，建议开启此功能，确保数据在传输过程中加密。

1. 客户端发起 HTTP 请求。
2. 节点响应301/302至 HTTPS 请求。
3. 客户端重定向至 HTTPS，发起 HTTPS 请求。

场景一：针对站点所有域名开启强制 HTTPS 访问

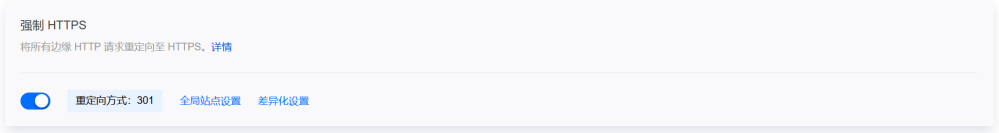
若您需要对整个接入站点开启强制 HTTPS 访问，可参考以下步骤：

前提条件

当前站点的访问域名，均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，在右侧导航栏中，单击**HTTPS**。
3. 找到强制 HTTPS 配置卡片，单击**开关**开启全局配置。



   - 关闭（默认）：不论客户端是何请求协议，EdgeOne 一律不做任何重定向，维持原请求协议访问至 EdgeOne 节点。
   - 开启：可选择通过301或302将客户端 HTTP 请求重定向为 HTTPS 请求，客户端 HTTPS 请求保持不变。

场景二：针对指定域名开启强制 HTTPS 访问

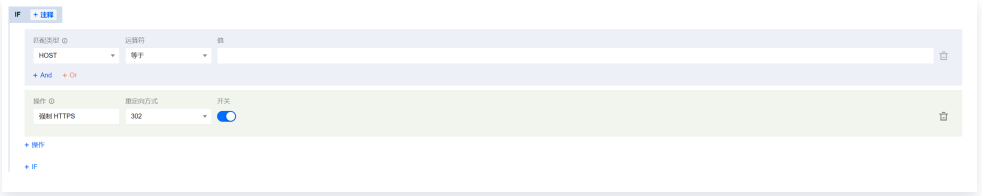
若您只需要针对指定域名开启强制 HTTPS 访问，其它域名仍然允许通过 HTTP 访问，可参考以下步骤：

前提条件

当前指定需开启强制 HTTPS 访问的域名，均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
4. 在规则编辑页面，选择 Host 匹配类型以匹配指定域名的请求。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为**强制 HTTPS**，单击**开关**。



6. 单击**保存并发布**，即可完成该规则配置。

启用 HSTS

最近更新时间：2024-07-22 16:02:31

功能说明

HSTS（HTTP Strict-Transport-Security）是国际互联网工程组织 IETE 推行的 Web 安全协议，用来通知浏览器使用更安全的 HTTPS 访问该站点。若您需要增强网站的安全性，防止恶意攻击者通过中间人攻击窃取用户敏感信息；或需要遵循数据隐私保护法规，保护用户的隐私信息；或需要提高网站的信誉度，增强用户对网站的信任感，均可以配置 HSTS 来提高网站的安全性和信誉度。

当客户端使用 HTTP 协议向 EdgeOne 节点发起请求时，即使开启了强制 HTTPS 访问将请求重定向至 HTTPS，因为第一次请求时仍然使用 HTTP 请求，该过程可能被拦截或恶意篡改。

为了提升访问安全，可通过 HSTS 来强制浏览器直接发起 HTTPS 访问，HSTS 是高安全等级网站的重要安全机制，启用 HSTS 后，EdgeOne 在响应 HTTPS 请求时会增加一个响应头部 `Strict-Transport-Security`，通过该头部告诉浏览器在指定的时间内直接使用 HTTPS 协议发起请求。

> **注意：**
> 1. HSTS 的 `Strict-Transport-Security` 头部仅在 HTTPS 响应中生效，如果在 HTTP 响应中包含该头部，浏览器会忽略它。因此，开启 HSTS 时，建议配置 强制 HTTPS 访问，为域名配置 SSL 证书，确保用户首次访问时通过 HTTPS 请求进行。这样，EdgeOne 将通过 HTTPS 响应，从而确保 HSTS 配置生效。
> 2. 当配置了响应 HSTS 头部时，浏览器如果验证当前站点存在证书安全风险，将提示用户并拦截当前的用户访问行为，以进一步保护用户数据安全。

场景一：针对站点所有域名启用 HSTS

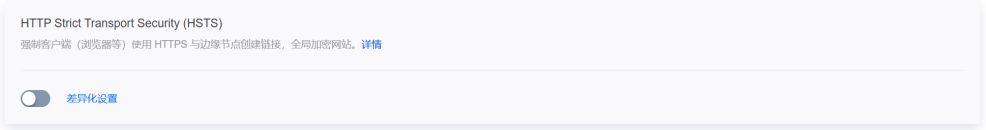
若您需要对整个接入站点启用 HSTS，可参考以下步骤：

前提条件

当前站点的访问域名，均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，在右侧导航栏中，单击**HTTPS**。
3. 找到 HSTS 配置卡片，单击**开关**，可开始配置 HSTS 。



4. 在弹出的配置窗中，可对 `Strict-Transport-Security` 头部内容进行配置。
   - **配置状态：**开启/关闭 HSTS 配置。
   - **缓存时间：**即 max-age 字段内容，可配置1-31536000整数。
   - **包含子域名：**开启后，将包含 includeSubDomains 指令。
   - **预加载：**开启后，将包含 preload 指令。

场景二：针对指定域名启用 HSTS

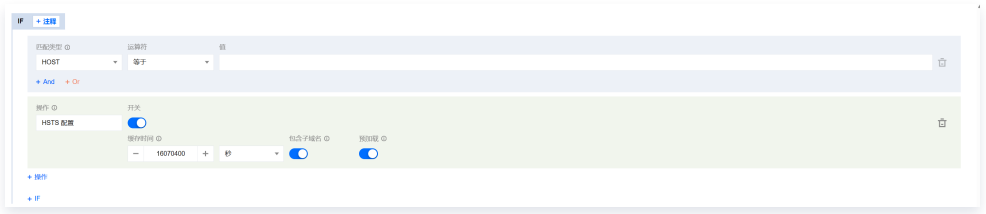
若您只需要针对指定域名开启 HSTS 或需要针对不同域名配置不同的 HSTS，可参考以下步骤。

前提条件

当前指定需要启用 HSTS 的域名，均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
4. 在规则编辑页面，选择 Host 匹配类型以匹配指定域名的请求。
5. 单击**操作 > 选择框**，在弹出的操作列表内，选择操作为 **HSTS配置**，单击**开关**。



6. 单击**保存并发布**，即可完成该规则配置。

了解更多

`Strict-Transport-Security` 头部内包含的各字段含义说明如下：

字段	说明
`max-age=<expire-time>`	HSTS 头部的过期时间，单位为秒，在该时间内浏览器始终以 HTTPS 发起请求。
`includeSubDomains`（可选）	若包含此指令，则当前域名及其子域名均会启用 HSTS。
`preload`（可选）	该指令用于表示同意当前域名加入所有主流的 Web 浏览器的 HSTS 预加载列表。加入浏览器内置的 HSTS 列表后，浏览器在发起该域名请求时，均会使用 HTTPS 请求。若需要加入浏览器的内置 HSTS 列表，需要满足以下条件： • `max-age` 至少是31536000（一年）。 • 必须包含 `includeSubDomains` 。 • 必须包含 `preload` 。 您可以查看 HSTS preload list 来验证当前域名是否在浏览器预加载列表内，主流浏览器将定期在版本更新中将 HSTS preload list 通过硬编码的方式写入。

SSL/TLS 安全配置
配置 SSL/TLS 安全等级

最近更新时间：2024-07-22 16:02:31

使用场景

当您的网站开启 HTTPS 访问后，EdgeOne 默认为您的站点支持了兼容性更高多种 SSL/TLS 版本访问，以适配不同用户终端的访问环境，正常情况下，您无需修改该配置。如果您的网站安全性要求较高，需要禁止用户通过安全较低的 SSL/TLS 版本访问，您可以通过修改此配置来自定义所使用的 SSL/TLS 版本。

> **说明：**
> 不同 TLS版本及密码套件的区别请参见：TLS 版本及密码套件说明 。

场景一：针对站点所有域名调整 SSL/TLS 安全配置

若您需要对整个接入站点配置 SSL/TLS 版本，可参考以下步骤。

前提条件

当前站点的访问域名均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，在右侧导航栏中，单击**HTTPS**。
3. 找到SSL/TLS 安全配置的卡片，单击**全局站点设置**进行修改。

默认配置：

- TLS 版本：开启 `TLS1.0、TLS1.1、TLS1.2、TLS1.3` 。
- 密码套件：`eo-loose-v2023` 。

场景二：针对指定域名调整 SSL/TLS 安全配置

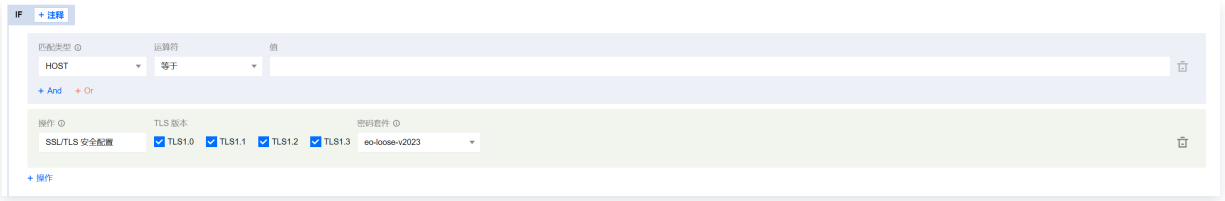
若您只需要针对指定域名自定义修改 SSL/TLS 版本，可参考以下步骤。

前提条件

当前指定需要 SSL/TLS 安全配置的域名均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
4. 在规则编辑页面，选择 Host 匹配类型以匹配指定域名的请求。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为 **SSL/TLS 安全配置**。



6. 单击**保存并发布**，即可完成该规则配置。

TLS 版本及密码套件说明

最近更新时间：2023-11-21 09:49:42

本文介绍了 EdgeOne 对 TLS 握手时允许使用的协议版本和密码套件的支持情况。

什么是 TLS 协议版本?

TLS（Transport Layer Security）协议是一种用于加密网络通信的安全协议，它是 SSL（Secure Sockets Layer）协议的继任者，允许客户端/服务器应用程序之间进行加密通信。TLS 协议有多个版本，包括 TLS 1.0、TLS 1.1、TLS 1.2 和 TLS 1.3，TLS 1.3是最新的版本，提供了更安全、更高效的加密机制。

什么是密码套件?

密码套件是一组加密算法，用于安全传输层协议（TLS）中的安全连接。TLS 密码套件由认证，加密和消息认证码（MAC）三个部分组成，它们提供安全性和可靠性，保护传输中的数据免受第三方窃取。在 TLS 握手过程中，客户端和服务器会协商一个可以使用的密码套件（客户端和服务器会根据它们支持的密码套件列表来确定使用哪个密码套件），以便客户端和服务器之间的通信可以使用该密码套件进行加密。

使用场景

EdgeOne 默认启用所有 TLS 版本，密码套件为 `eo-loose-v2023`，可以满足大部分客户需求，若您对安全性有更高要求，可自定义调整：

业务场景	TLS 版本	密码套件
注重兼容旧版浏览器，对安全性要求可适当放宽。	1.0、1.1、1.2	`eo-loose-v2023`
需兼顾浏览器的兼容性和安全性，安全性和兼容性均为适中	1.2、1.3	`eo-general-v2023`
安全性要求高，可降低浏览器兼容性，需屏蔽所有可能存在安全漏洞的 TLS 版本和密码套件	1.2、1.3	`eo-strict-v2023`

当前 EdgeOne 支持的 TLS 协议版本和密码套件

EdgeOne 支持的 TLS 版本如下：

- TLS 1.0
- TLS 1.1
- TLS 1.2
- TLS 1.3

OpenSSL 密码套件	TLS 1.3	TLS 1.2	TLS 1.1	TLS 1.0
TLS_AES_256_GCM_SHA384	✓	-	-	-
TLS_CHACHA20_POLY1305_SHA256	✓	-	-	-
TLS_AES_128_GCM_SHA256	✓	-	-	-
TLS_AES_128_CCM_SHA256	✓	-	-	-
TLS_AES_128_CCM_8_SHA256	✓	-	-	-
ECDHE-ECDSA-AES256-GCM-SHA384	-	✓	-	-
ECDHE-ECDSA-AES128-GCM-SHA256	-	✓	-	-
ECDHE-RSA-AES256-GCM-SHA384	-	✓	-	-
ECDHE-RSA-AES128-GCM-SHA256	-	✓	-	-
ECDHE-ECDSA-CHACHA20-POLY1305	-	✓	-	-

ECDHE-RSA-CHACHA20-POLY1305	-	✓	-	-
ECDHE-ECDSA-AES256-SHA384	-	✓	-	-
ECDHE-ECDSA-AES128-SHA256	-	✓	-	-
ECDHE-RSA-AES256-SHA384	-	✓	-	-
ECDHE-RSA-AES128-SHA256	-	✓	-	-
ECDHE-RSA-AES256-SHA	-	-	✓	✓
ECDHE-RSA-AES128-SHA	-	-	✓	✓
AES256-GCM-SHA384	-	✓	-	-
AES128-GCM-SHA256	-	✓	-	-
AES256-SHA256	-	✓	-	-
AES128-SHA256	-	✓	-	-
AES256-SHA	-	-	✓	✓
AES128-SHA	-	-	✓	✓

EdgeOne 支持在 TLS 协议版本的基础之上，为用户提供不同的强度的密码套件选择：

- `eo-strict-v2023`：**安全性要求高，禁用所有不安全的密码套件。**
- `eo-general-v2023`：**需兼顾浏览器的兼容性和安全性，安全性和兼容性均为适中。**
- `eo-loose-v2023`**（默认）：注重兼容旧版浏览器，对安全性要求可适当放宽。**

OpenSSL 密码套件	eo-strict-v2023	eo-general-v2023	eo-loose-v2023
TLS_AES_256_GCM_SHA384	✓	✓	✓
TLS_CHACHA20_POLY1305_SHA256	✓	✓	✓
TLS_AES_128_GCM_SHA256	✓	✓	✓
TLS_AES_128_CCM_SHA256	-	✓	✓
TLS_AES_128_CCM_8_SHA256	-	✓	✓
ECDHE-ECDSA-AES256-GCM-SHA384	✓	✓	✓
ECDHE-ECDSA-AES128-GCM-SHA256	✓	✓	✓
ECDHE-RSA-AES256-GCM-SHA384	✓	✓	✓
ECDHE-RSA-AES128-GCM-SHA256	✓	✓	✓
ECDHE-ECDSA-CHACHA20-POLY1305	✓	✓	✓
ECDHE-RSA-CHACHA20-POLY1305	✓	✓	✓
ECDHE-ECDSA-AES256-SHA384	-	✓	✓
ECDHE-ECDSA-AES128-SHA256	-	✓	✓
ECDHE-RSA-AES256-SHA384	-	✓	✓
ECDHE-RSA-AES128-SHA256	-	✓	✓
ECDHE-RSA-AES256-SHA	-	-	✓

ECDHE-RSA-AES128-SHA	-	-	✓
AES256-GCM-SHA384	-	-	✓
AES128-GCM-SHA256	-	-	✓
AES256-SHA256	-	-	✓
AES128-SHA256	-	-	✓
AES256-SHA	-	-	✓
AES128-SHA	-	-	✓

您可根据自身业务的安全和兼容性需求配置 TLS 版本及密码套件，最终支持的 OpenSSL 密码套件取 TLS 版本和密码套件选项对应内容的交集，例如：
TLS 版本开启 `TLS 1.3` **，且密码套件选项选择** `eo-strict-v2023` **，则最终支持的 OpenSSL 密码套件为** `TLS 1.3` **与** `eo-strict-v2023` **支持的交集：** `TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256, TLS_AES_128_GCM_SHA256`。

了解更多

如何配置 SSL/TLS 安全配置

开启 OCSP 装订

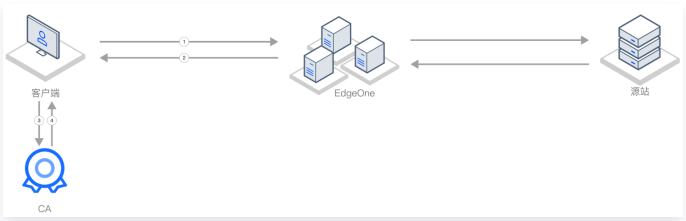
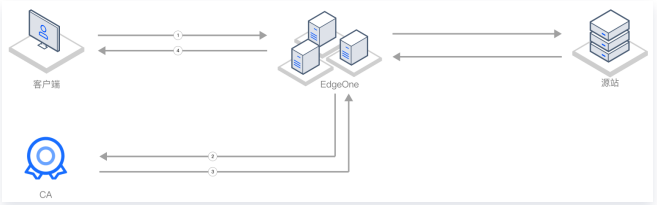
最近更新时间：2024-07-22 16:02:31

功能说明

OCSP（Online Certificate Status Protocol）是用来检验证书合法性和有效性的在线查询协议，由数字证书颁发机构 CA（Certificate Authority）提供。当用户每次通过 HTTPS 访问网站的时候，浏览器会通过 OCSP 查询验证网站的证书是否有效。

启用 OCSP 装订后，OCSP 查询的工作将由 EdgeOne 服务器完成，且 EdgeOne 可将查询结果缓存到服务器中。当客户端与 EdgeOne TLS 握手时，EdgeOne 直接响应客户端 OCSP 信息和证书，供客户端验证，无需再由客户端向 CA 发送查询请求，极大地提高了 TLS 握手效率，节省用户验证时间，优化 HTTPS 速度。

若您希望提高 HTTPS 握手中证书状态校验的效率，提升网站访问性能，可开启 OCSP 装订。

未启用 OCSP 装订	启用 OCSP 装订
	
1. 客户端发起 TLS 握手请求。 2. EdgeOne 响应 TLS 握手（返回证书）。 3. 客户端发起 OCSP 查询。 4. CA 返回查询结果。	1. 客户端发起 TLS 握手请求。 2. EdgeOne 发起 OCSP 查询。 3. CA 返回查询结果，EdgeOne 缓存结果。 4. EdgeOne 响应 TLS 握手（返回证书和 OCSP 信息）。 因 EdgeOne 已缓存 OCSP 信息，后续请求若发起查询，则由 EdgeOne 直接响应，无需再次发起查询。

场景一：针对站点所有域名开启 OCSP 装订

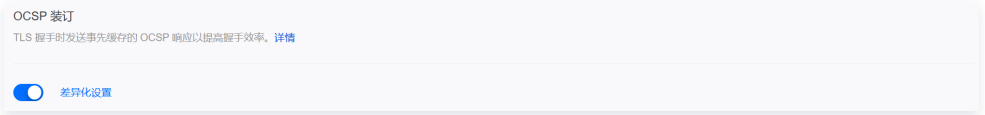
若您需要对整个接入站点开启 OCSP 装订，可参考以下步骤：

前提条件

当前站点的访问域名均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，在右侧导航栏中，单击 **HTTPS**。
3. 找到 OCSP 装订配置卡片，单击**开关**。



- 关闭（默认）：客户端发起请求，TLS 握手时，客户端需自行向 CA 发送证书验证请求，实时查询证书状态。
- 开启：EdgeOne 向 CA 发送证书验证请求，并缓存查询结果。客户端向 EdgeOne 节点发起 HTTPS 请求时，直接由 EdgeOne 响应证书查询结果供客户端验证。

场景二：针对指定域名开启 OCSP 装订

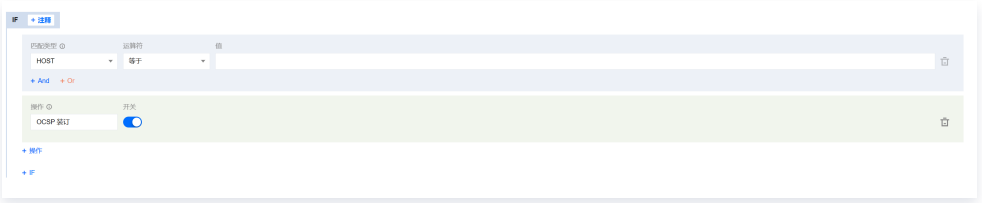
若您只需要针对指定域名开启 OCSP 装订，可参考以下步骤：

前提条件

当前指定需开启 OCSP 装订的域名均已配置 SSL 证书。如何配置 SSL 证书请参考：证书配置 。

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**。
2. 在站点详情页面，单击**站点加速**，进入站点全局配置页面，单击右**规则引擎 Tab 页**。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
4. 在规则编辑页面，选择 Host 匹配类型以匹配指定域名的请求。
5. 单击**操作 > 选择框**，在弹出的操作列表内，选择操作为 **OCSP 装订**,单击**开关**开启配置。



6. 单击**保存并发布**，即可完成该规则配置。

相关参考
使用 OpenSSL 生成自签名证书

最近更新时间：2024-11-19 14:19:01

所有的服务端和客户端证书一般情况下都需要向权威 CA 证书机构去申请，以保障能够被不同的操作系统和浏览器信任，CA 机构一般会收取一定的证书费用。如果您当前只是需要一本 HTTPS 证书进行测试使用，或者在企业内部使用，也可以自行通过 OpenSSL 颁发自签名证书。参考步骤如下：

步骤一：生成根证书

1. 通过以下命令创建根证书私钥，这将生成一个2048位的私钥，并将其保存到 .key 文件中。

```
openssl genrsa -out root.key 2048
```

2. 根据根证书私钥，生成证书签名请求文件（CSR）。

```
openssl req -new -key root.key -out root.csr
```

在生成 CSR 的过程中，需要提供组织名、公共名称等信息，可以根据实际使用情况填写。

3. 执行以下命令，创建根证书。

```
openssl x509 -req -in root.csr -out root.crt -signkey root.key -CAcreateserial -days 3650
```

即可得到一个有效期为10年的根证书 root.crt，后续可以用该根证书自行签发所需要的服务端证书和客户端证书。

步骤二：签发证书

以签发一本服务端证书为例，您可以通过 步骤一 生成的根证书，开始为您自签发证书：

1. 生成服务端证书的私钥。

```
openssl genrsa -out server.key 2048
```

2. 根据服务端证书私钥，生成证书签名请求文件（CSR）。

```
openssl req -new -out server.csr -key server.key
```

在生成 CSR 的过程中，与根证书一样，需要提供组织名、公共名称等信息，可以根据实际使用情况填写。

3. 生成服务端公钥证书。

```
openssl x509 -req -in server.csr -out server.crt -signkey server.key -CA root.crt -CAkey root.key
-CAcreateserial -days 3650
```

通过上述三个步骤，您将获得有效期为10年的自签名服务端证书 server.crt 和 server.key。您可以重复这些步骤，使用同一根证书继续生成其他所需的服务端证书或客户端证书。

证书格式要求

最近更新时间：2024-10-15 10:35:51

- 如果您的证书是由根 CA 机构颁发，您将获得一份唯一的证书。无需额外证书，配置的站点便可被浏览器等访问设备视为可信。
- 如果您的证书是由中级 CA 机构颁发，您将收到包含多份证书的文件。您需要手动将中间根证书和根证书按顺序拼接后上传。拼接规则是：先放中间根证书，其次放根证书，两者之间不留空行。

> **说明：**
> 一般情况下，机构在颁发证书的时候会有对应说明，请注意查阅。

CA 证书格式和证书链格式范例

如下为证书格式和证书链格式范例，请确认格式正确后上传：

1. 根 CA 机构颁发的证书，以 PEM 格式为例，样例如下：

```
-----BEGIN CERTIFICATE-----
MIIE+TCCA+GgAwIBAgIQU306HIX4KsioTW1s2A2krTANBgkqhkiG9w0BAQUFADCB
tTELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQL
ExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMTswOQYDVQQLEzJUZXJtcyBvZiB1c2Ug
YXQgaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL3JwYSoAYykwOTEvMC0GA1UEAxMm
VmVyaVNpZ24gQ2xhc3MgMyBTZWN1cmUgU2VydmVyIENBIC0gRzIwHhcNMTAxMDA4
MDAwMDAwWhcNMTMxMDA3MjM1OTU5WjBqMQswCQYDVQQGEwJVUzETMBEGA1UECBMK
V2FzaGluZ3RvbjEQMA4GA1UEBxQHU2VhdHRsZTEYMBYGA1UEChQPQW1hem9uLmNv
bSBJbmMuMRowGAYDVQQDFBFpYW0uYW1hem9uYXdzLmNvbTCBnzANBgkqhkiG9w0B
AQEFAAOBjQAwgYkCgYEA3Xb0EGea2dB8QGEUwLcEpwvGawEkUdLZmGL1rQJZdeeN
3vaF+ZTm8Qw5Adk2Gr/RwYXtpx04xvQXmNm+9YmksHmCZdruCrW1eN/P9wBfqMMZ
X964CjVov3NrF5AuxU8jgtw0yu//C3hWnOuIVGdg76626ggOoJSaj48R2n0MnVcC
AwEAAaOCAdEwggHNMAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMEUGA1UdHwQ+MDww
OqA4oDaGNGh0dHA6Ly9TVlJTZWN1cmUtRzItY3JsLnZlcmlzaWduLmNvbS9TVlJT
ZWN1cmVHMi5jcmwwRAYDVR0gBD0wOzA5BgtghkgBhvhFAQcXAzAqMCgGCCsGAQUF
BwIBFhxodHRwczovL3d3dy52ZXJpc2lnbi5jb20vcnBhMB0GA1UdJQQWMBQGCCsG
AQUFBwMBBggrBgEFBQcDAjAfBgNVHSMEGDAWgBSl7wsRzsBBA6NKZZBIshzgVy19
RzB2BggrBgEFBQcBAQRqMGgwJAYIKwYBBQUHMAGGGGh0dHA6Ly9vY3NwLnZlcmlz
aWduLmNvbTBABggrBgEFBQcwAoY0aHR0cDovL1NWUlNlY3VyZS1HMi1haWEudmVy
aXNpZ24uY29tL1NWUlNlY3VyZUcyLmNlcjBuBggrBgEFBQcBDARiMGChXqBcMFow
WDBWFglpbWFnZS9naWYwITAfMAcGBSsOAwIaBBRLa7kolgYMu9BSOJsprEsHiyEF
GDAmFiRodHRwOi8vbG9nby52ZXJpc2lnbi5jb20vdnNsb2dvMS5naWYwDQYJKoZI
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq3OP4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

证书格式为：

- `---BEGIN CERTIFICATE---`, `---END CERTIFICATE---` 开头和结尾。
- 每行 64 字符，最后一行不超过64字符。

2. 如果证书由中级机构颁发，CA 证书需要包含多级证书链，证书链结构如下所示：

```
-----BEGIN CERTIFICATE-----
CA 中间证书机构
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
CA 根证书机构
-----END CERTIFICATE-----
```

证书链规则为：

- 证书之间不能有空行。
- 每一份证书遵循上文的证书格式要求。

证书转换为 PEM 格式说明

通常情况下，HTTPS 证书使用 PEM 格式，其他格式的证书需要转换成 PEM 格式时，建议通过 openssl 工具进行转换。下面是几种比较流行的证书格式转换为 PEM 格式的方法。

DER 转换为 PEM

DER 格式一般出现在 Java 平台中。
证书转换：

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

私钥转换：

```
openssl rsa -inform DER -outform PEM -in privatekey.der -out privatekey.pem
```

P7B 转换为 PEM

P7B 格式一般出现在 Windows Server 和 tomcat 中。
证书转换：

```
openssl pkcs7 -print_certs -in incertificat.p7b -out outcertificate.cer
```

获取 outcertificat.cer 里面 `-----BEGIN CERTIFICATE-----`， `-----END CERTIFICATE-----` 的内容作为证书上传。
私钥转换：私钥一般在 IIS 服务器里可导出。

PFX 转换为 PEM

PFX 格式一般出现在 Windows Server 中。
证书转换：

```
openssl pkcs12 -in certname.pfx -nokeys -out cert.pem
```

私钥转换：

```
openssl pkcs12 -in certname.pfx -nocerts -out key.pem -nodes
```

CER/CRT 转换为 PEM

对于 CER/CRT 格式的证书，您可通过直接修改证书文件扩展名的方式进行转换。例如，将 “servertest.crt” 证书文件直接重命名为 “servertest.pem” 即可。

源站配置
负载均衡
概述

最近更新时间：2024-03-26 16:29:01

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：2024-05-10 11:01:02

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 。

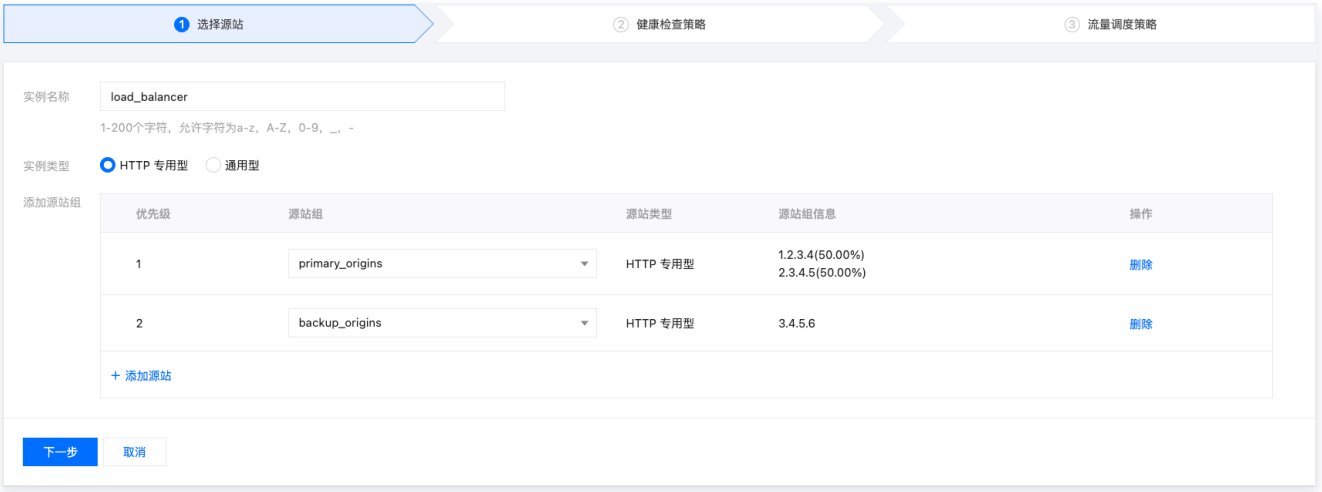
示例场景

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

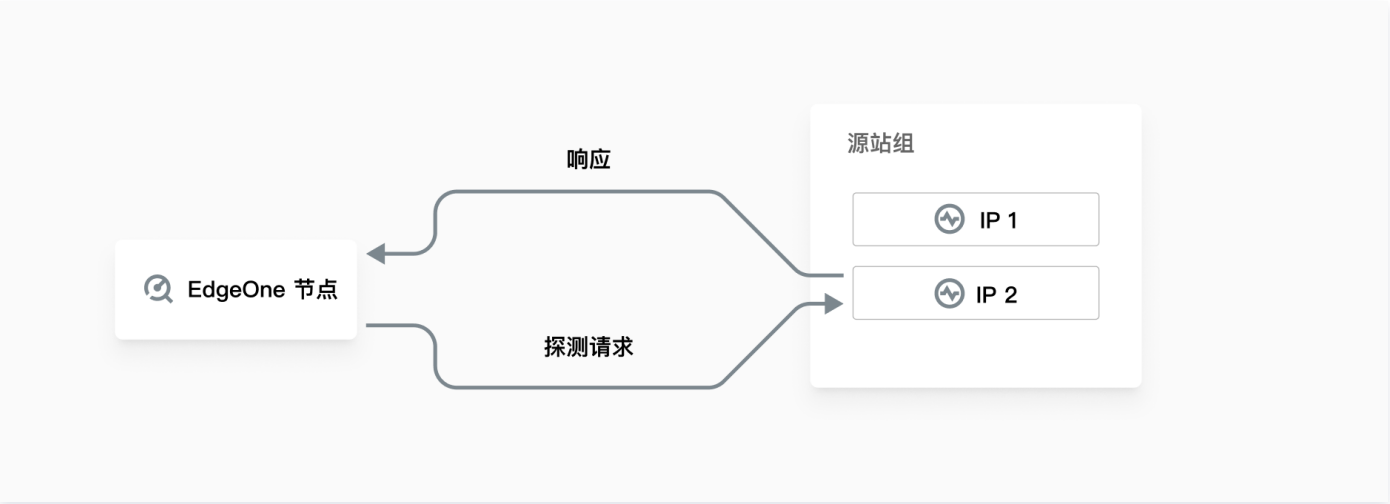
最近更新时间：2024-03-08 15:52:41

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。

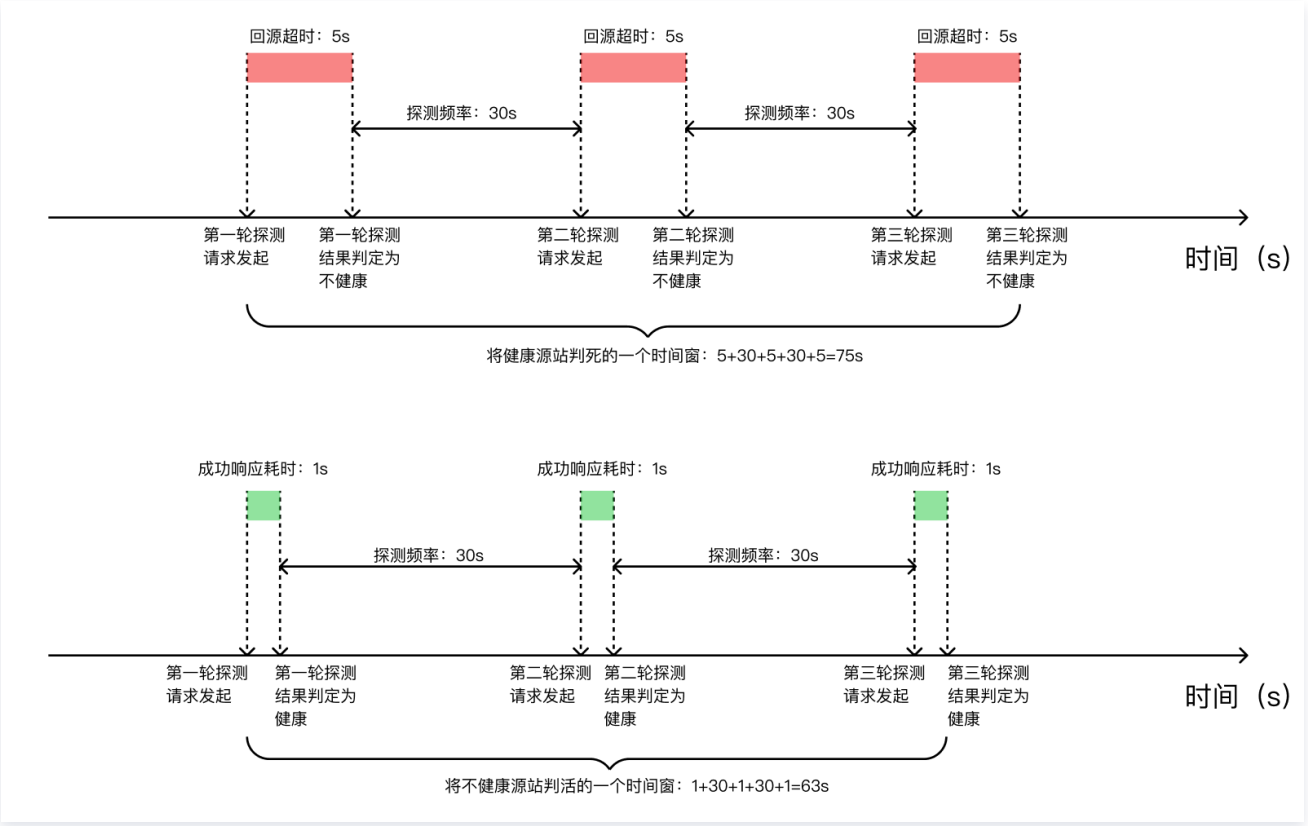
源站健康判定条件

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

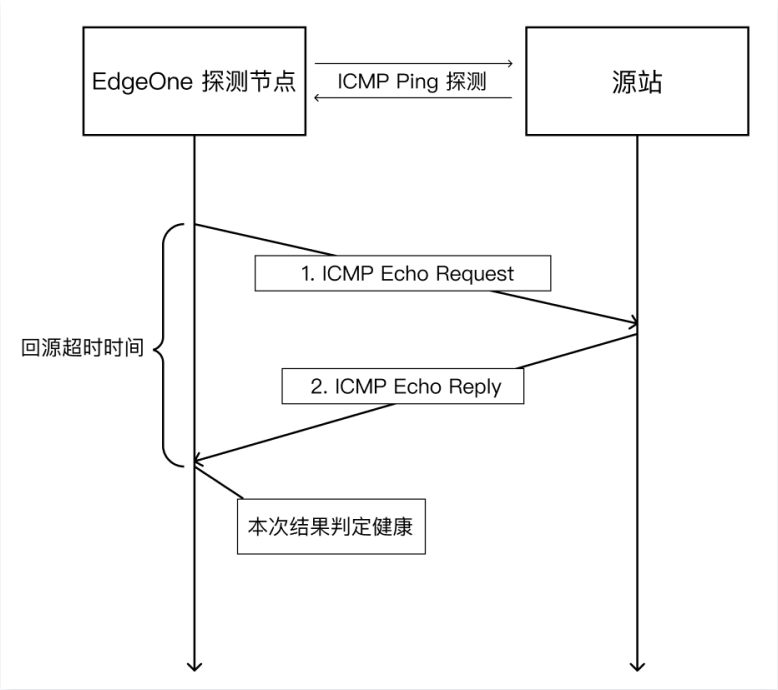


例如：当前设置源站健康判定条件为超时时间5s，不健康阈值为3次，健康阈值为3次，每30秒探测一次。
则判断该源站为不健康所需耗时为：5+30+5+30+5=75秒。
恢复该源站为健康状态所需耗时为（假定主动探测收到成功响应耗时需1秒）：1+30+1+30=63秒。

了解更多

探测方式的原理介绍

ICMP Ping

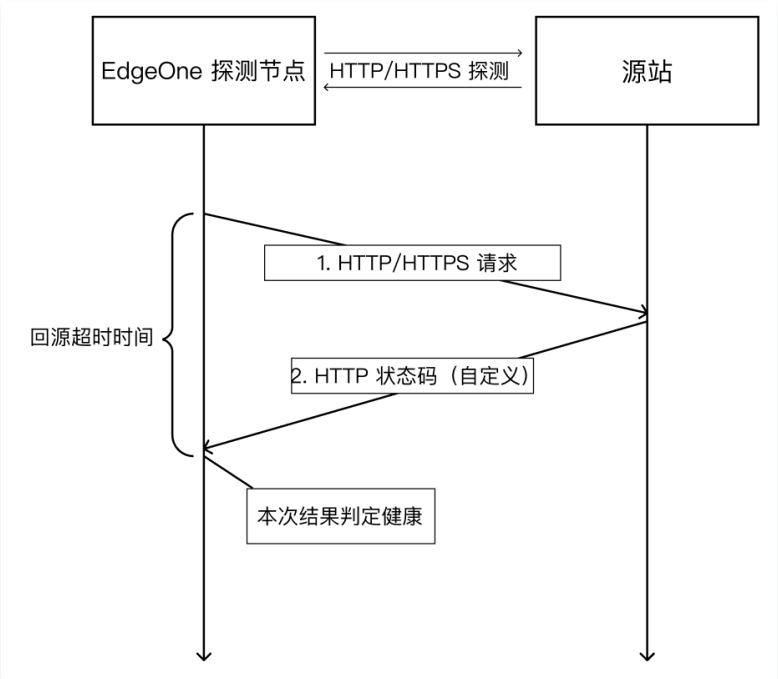


ICMP Ping 健康检查机制如下：

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。

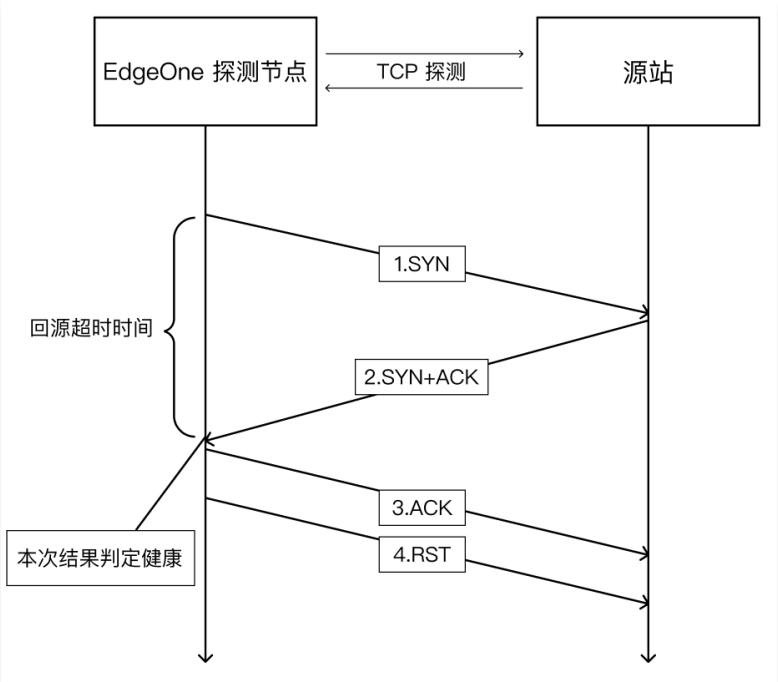
HTTP/HTTPS



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。

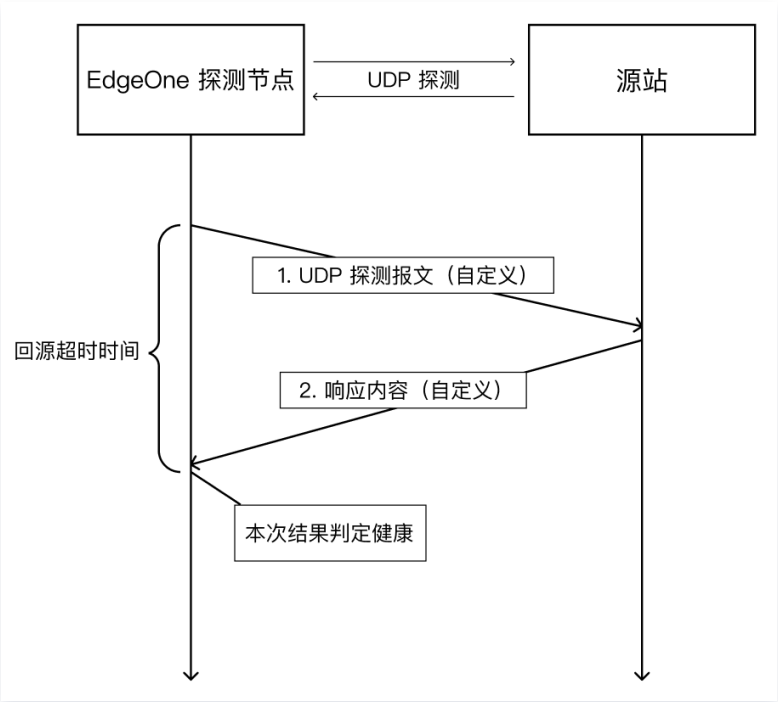
TCP



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。

UDP



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：2024-05-10 11:01:02

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 。

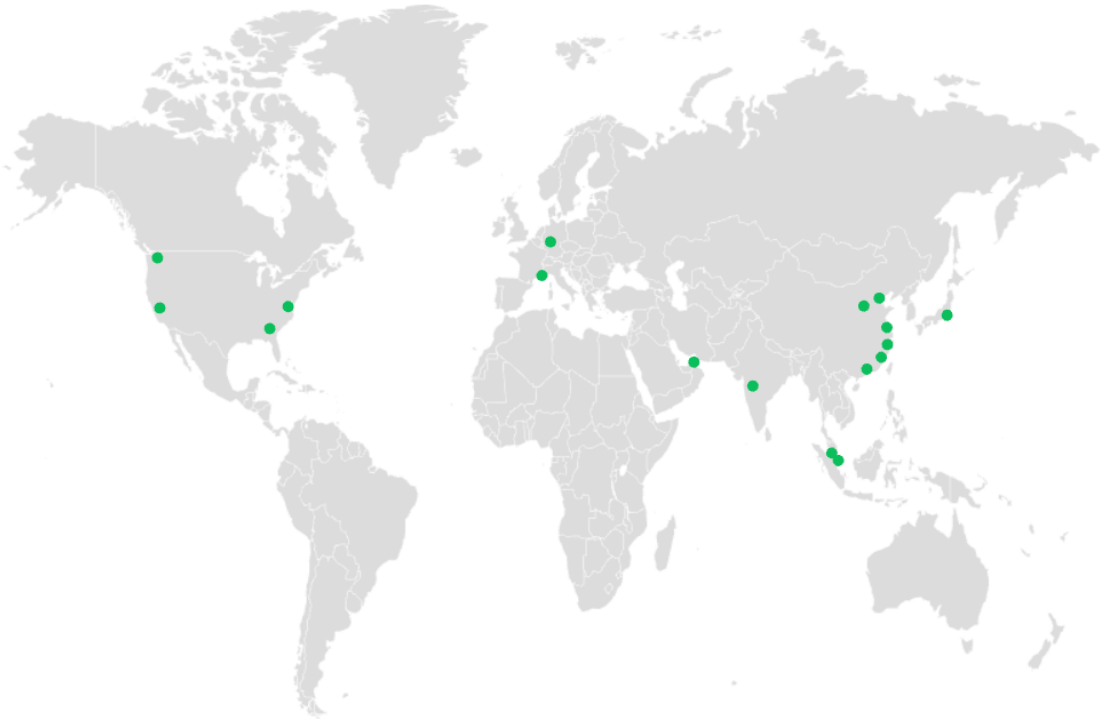
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**源站配置 > 负载均衡**。
3. 在负载均衡页面，单击所需的**负载均衡实例**。

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。

节点探测结果

总探测节点数	源站全部健康的节点数	存在不健康源站的节点数	未探测到任何源站的节点数
17 个	17 个	0 个	0 个



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。

相关参考
负载均衡相关概念

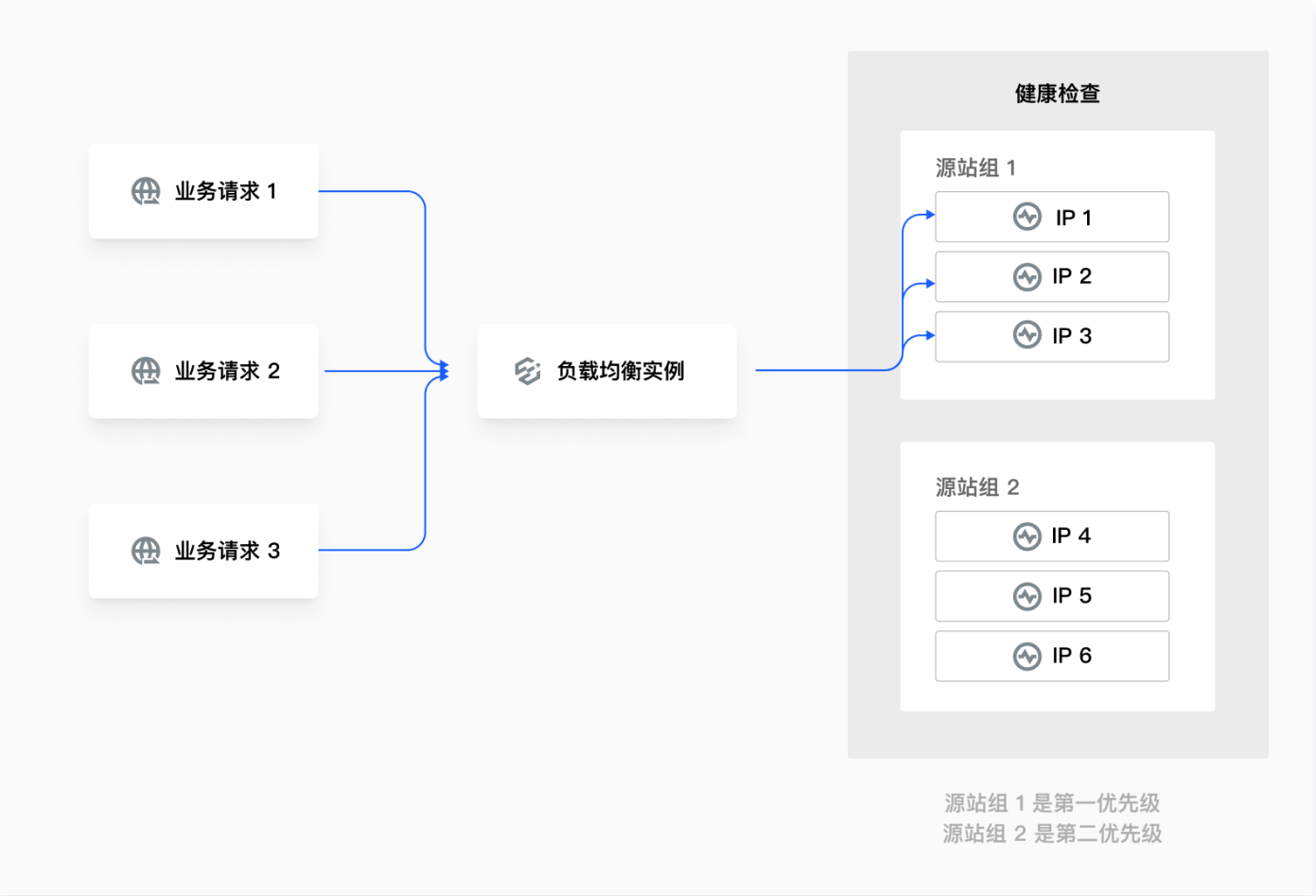
最近更新时间：2024-03-08 15:55:52

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。



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：2025-01-17 11:49:11

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。

> **说明：**
> POST 请求不支持回源重试。

源站组操作指引

最近更新时间：2024-12-19 11:20:12

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. 在源站组页面，单击**新建源站组**。
4. 在新建源站组页面，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**，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，则所有源站都需同时设置权重，权重支持填写0-100的整数。如果您没有设定权重，那么所有源站都不应设置权重。
> 2. 智能加速和源站组权重两部分能力组合使用时，将按照以下逻辑生效：

场景	生效逻辑
源站组中多源站配置权重，开启智能加速	优先按照权重选择源站，然后智能加速会对回源链路做优化。
源站组中多源站配置权重，不开启智能加速	按照权重比例回源。

源站组中多源站不配置权重，开启智能加速	按照智能加速选择的最优源站回源。
源站组中多源站不配置权重，不开启智能加速	轮询源站组中每个源站，等比例回源。

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：2024-07-22 16:02:31

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**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**。
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**。

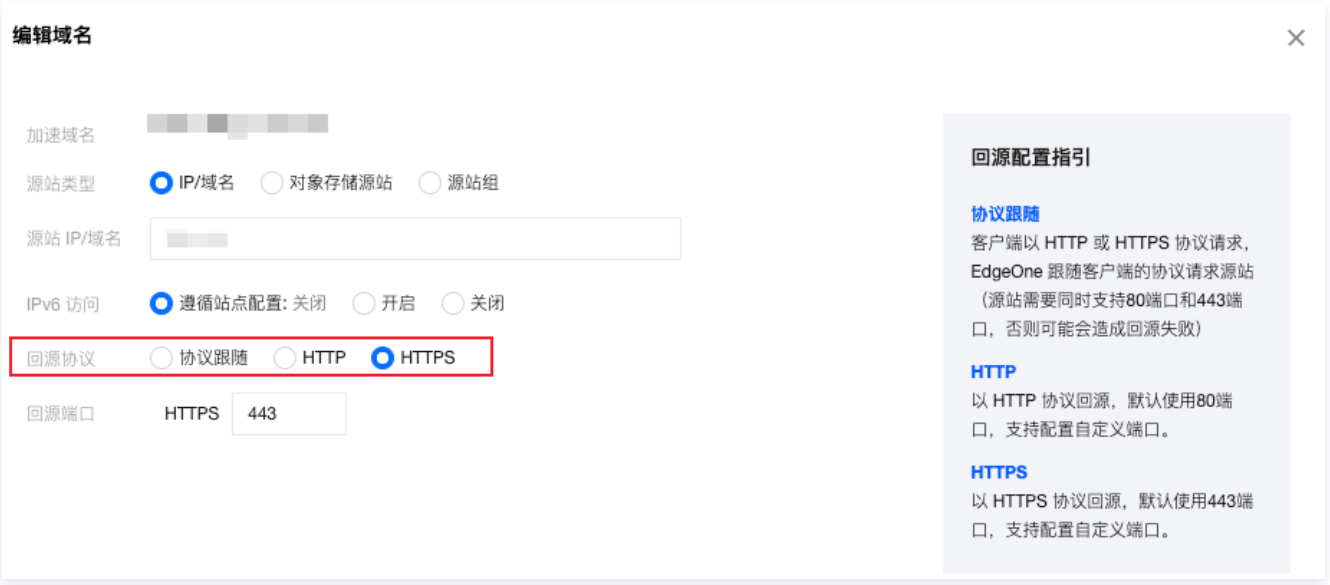
6. 单击**保存并发布**，即可完成该规则配置。

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。



Host Header 重写

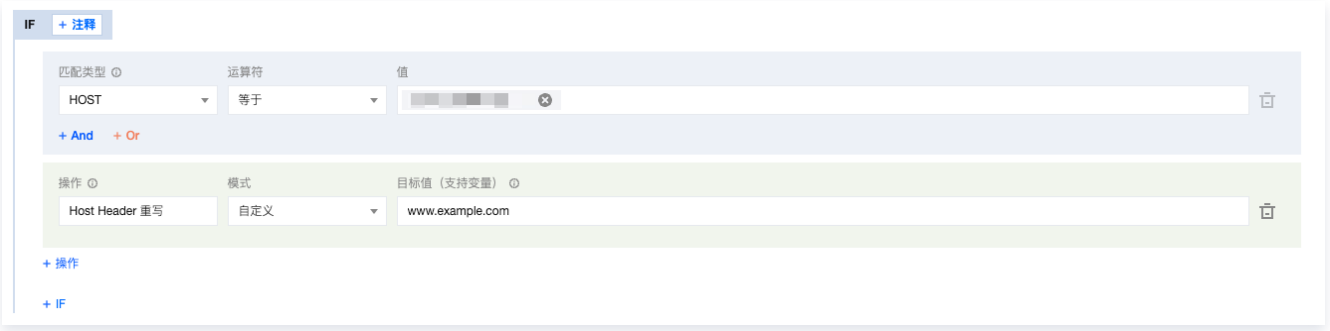
最近更新时间：2024-07-22 16:02:31

功能简介

重写 Host 头字段。若您的回源 Host 与 源站组列表 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 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**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**，进入新规则的编辑页面。
4. 在规则编辑页面，选择 Host 为匹配类型，配置需要修改的域名，例如：`www.example.com` 。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为 **Host Header 重写**，模式可选择为自定义或者跟随源站域名。



6. 单击**保存并发布**，即可完成该规则配置。

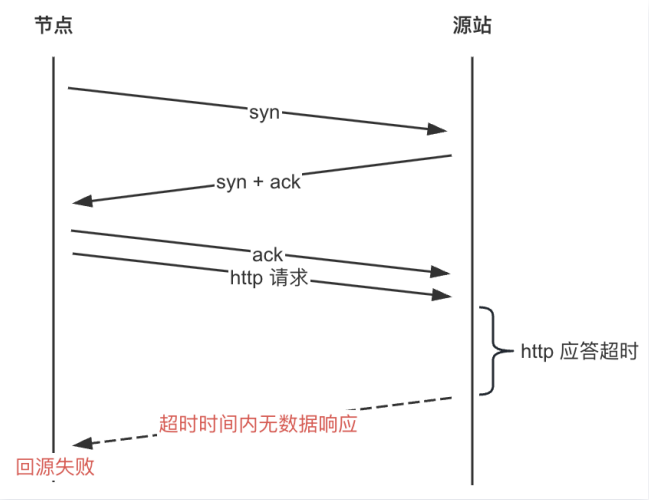
回源超时时间

最近更新时间：2024-12-25 16:15:42

功能简介

EdgeOne 规则引擎支持自定义设置回源超时时间，您可以根据网络链路情况以及源站数据处理能力，合理设置回源请求超时时间，让请求能够正常回源。回源超时时间的定义为节点发起回源请求，源站在多长时间内无数据响应则节点可以判定为超时，并主动断开与源站的连接。
目前可支持配置 HTTP 应答超时时间（TCP 连接超时时间配置即将上线，敬请期待），支持设置 5~600 之间的整数，默认值为 15，即节点和源站建连成功后，节点向源站发起 HTTP 请求，在 15 秒内，源站无任何应答数据（包括完全无数据响应或响应部分数据中断的场景），则节点判定为 HTTP 应答超时，此时会响应给客户端 524 状态码。

> **说明：**
> 该超时时间不适用于 HTTP/2 回源，HTTP/2 回源场景下，若 600s 内（暂不支持调整）没有帧发送/接收，则连接会超时断开，同时连接上的请求也会同步断开。



场景：配置 HTTP 应答超时时间为 60 s

若您 `example.com` 站点下的 `www.example.com` 域名业务对应源站负载较高，处理耗时长，为了避免由于超过节点默认 HTTP 超时时间 15s 后主动断开导致访问失败的问题，需延长至 60s。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**站点加速**，进入站点全局配置页面，单击**规则引擎 Tab 页**。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**，进入新规则的编辑页面。
4. 规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。
5. 单击**操作 > 选择框**，在弹出的操作列表内，选择操作为**回源超时时间**，配置 HTTP 应答超时时间为 60s。
6. 完整的规则配置如下所示，单击**保存并发布**，即可完成该规则配置。

回源请求参数设置

最近更新时间：2024-08-01 17:28:41

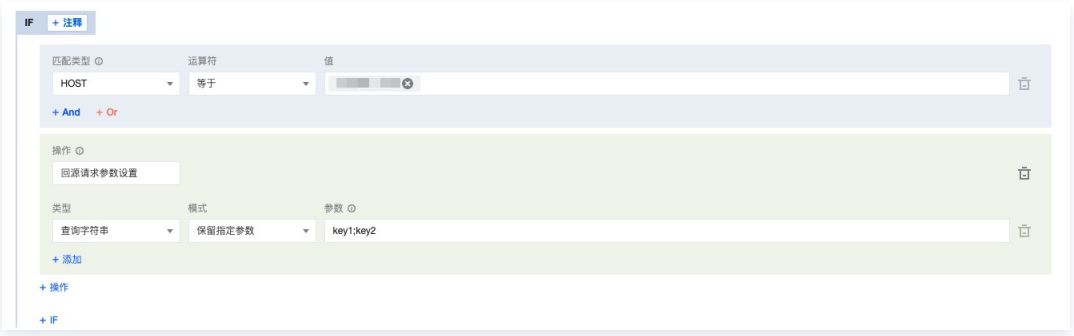
功能简介

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 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**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**，进入新规则的编辑页面。
4. 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为**回源请求参数设置**。
6. 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。



7. 单击**保存并发布**，即可完成该规则配置。

回源跟随重定向

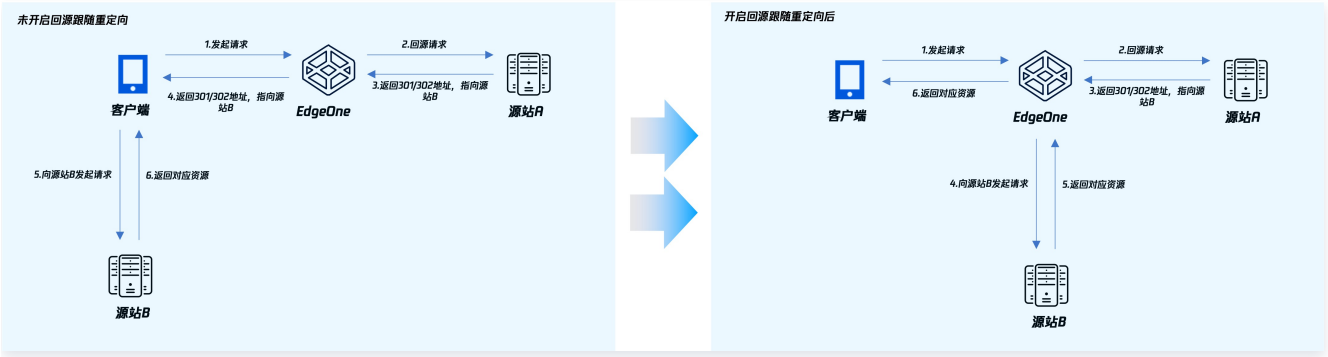
最近更新时间：2024-07-22 16:02:31

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。

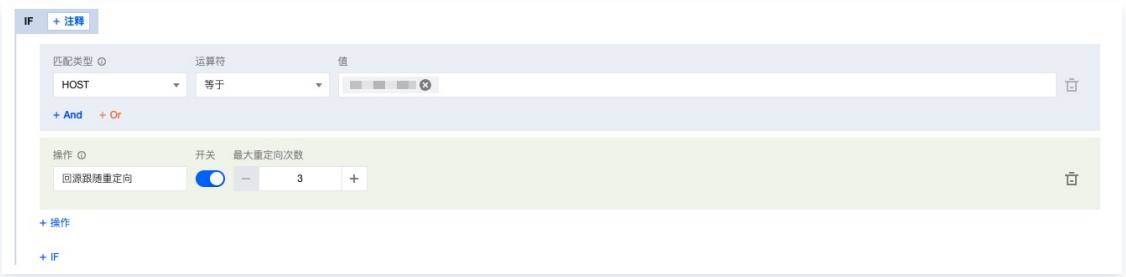


操作步骤

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 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**站点加速**，进入站点全局配置页面，单击右**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**，进入新规则的编辑页面。
4. 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com`。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为**回源跟随重定向**。
6. 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。



7. 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：2024-07-22 16:02:31

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 。

使用限制

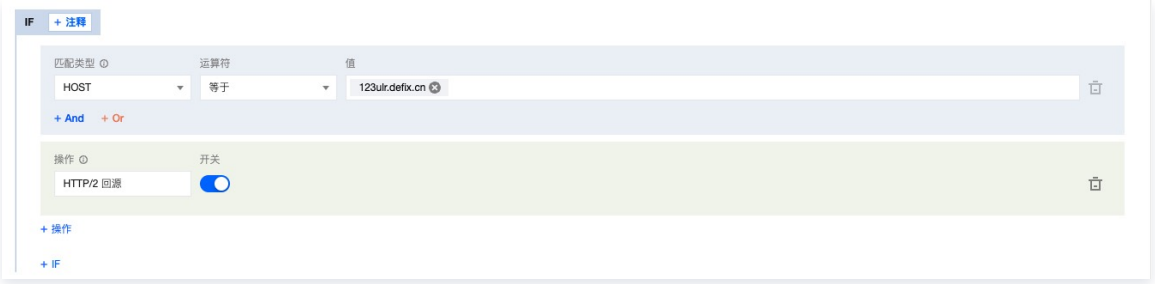
当开启 HTTP/2 回源，并且回源协议设置为协议跟随的场景下，如果客户端请求 HTTP，EdgeOne 节点将使用 H2C 进行回源。然而，如果源站不支持 H2C，将导致回源失败。
因此，如果您当前的源站不支持 H2C，且回源协议使用协议跟随，为了降低回源失败的风险，我们建议您将 HTTP/2回源的站点/域名保持为关闭状态。
如果您的回源协议使用 HTTPS 回源，则不受此影响。

> **说明：**
> H2C 是 HTTP/2 的非加密版本，"C" 代表 "clear text"，即明文。HTTP/2 协议是 HTTP 协议的第二个主要版本，它在性能上有显著的改进，包括请求和响应的多路复用，减少延迟，优化数据流，头信息压缩等。然而，HTTP/2 协议通常在安全的 HTTPS 上使用，这就需要使用 TLS（传输层安全协议）进行加密。但是，H2C 协议允许在没有加密的情况下使用 HTTP/2，这就使得在不需要或不能使用加密的情况下，也能享受到 HTTP/2 带来的性能优势。因此在开启 HTTP/2 回源并且使用 HTTP 回源的情况下，EdgeOne 使用了 H2C 进行回源。

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 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**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**，进入新规则的编辑页面。
4. 在规则编辑页面，匹配类型选择为 HOST 等于 `www.example.com` 。
5. 单击**操作** > **选择框**，在弹出的操作列表内，选择操作为**HTTP/2 回源**，单击**开关**开启配置。



6. 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：2024-07-22 16:02:31

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。

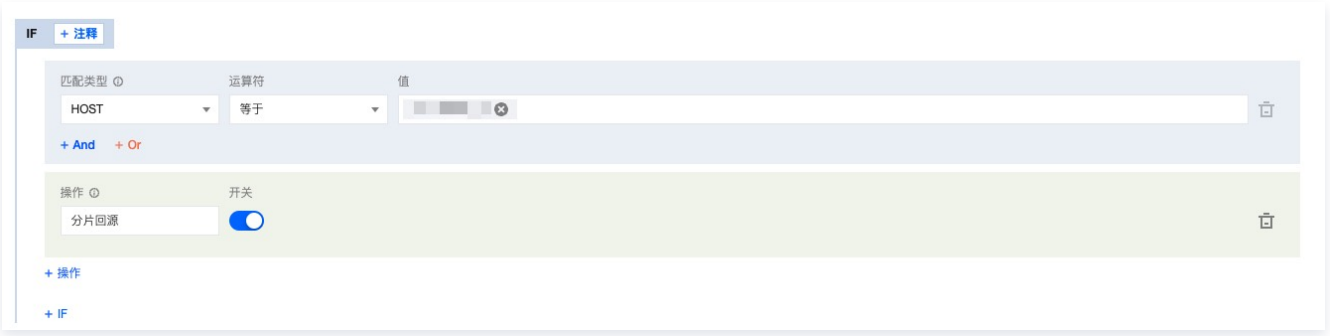
注意事项

- 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**站点加速**，进入站点全局配置页面，单击**规则引擎** Tab 页。
3. 在规则引擎页面，单击**创建规则**，选择**新增空白规则**，进入新规则的编辑页面。
4. 在规则编辑页面，匹配类型选择为 HOST 等于 `video.example.com` 。
5. 单击**操作 > 选择框**，在弹出的操作列表内，选择操作为**分片回源**，单击**开关**开启配置。



6. 单击**保存并发布**，即可完成该规则配置。

源站防护

最近更新时间：2024-08-07 17:46:41

功能简介

获取四层代理和站点加速服务最新的回源 IP 信息，更新业务源站防火墙规则，仅允许经过固定 IP(s) 的流量回源至源站，实现源站防护。

操作步骤

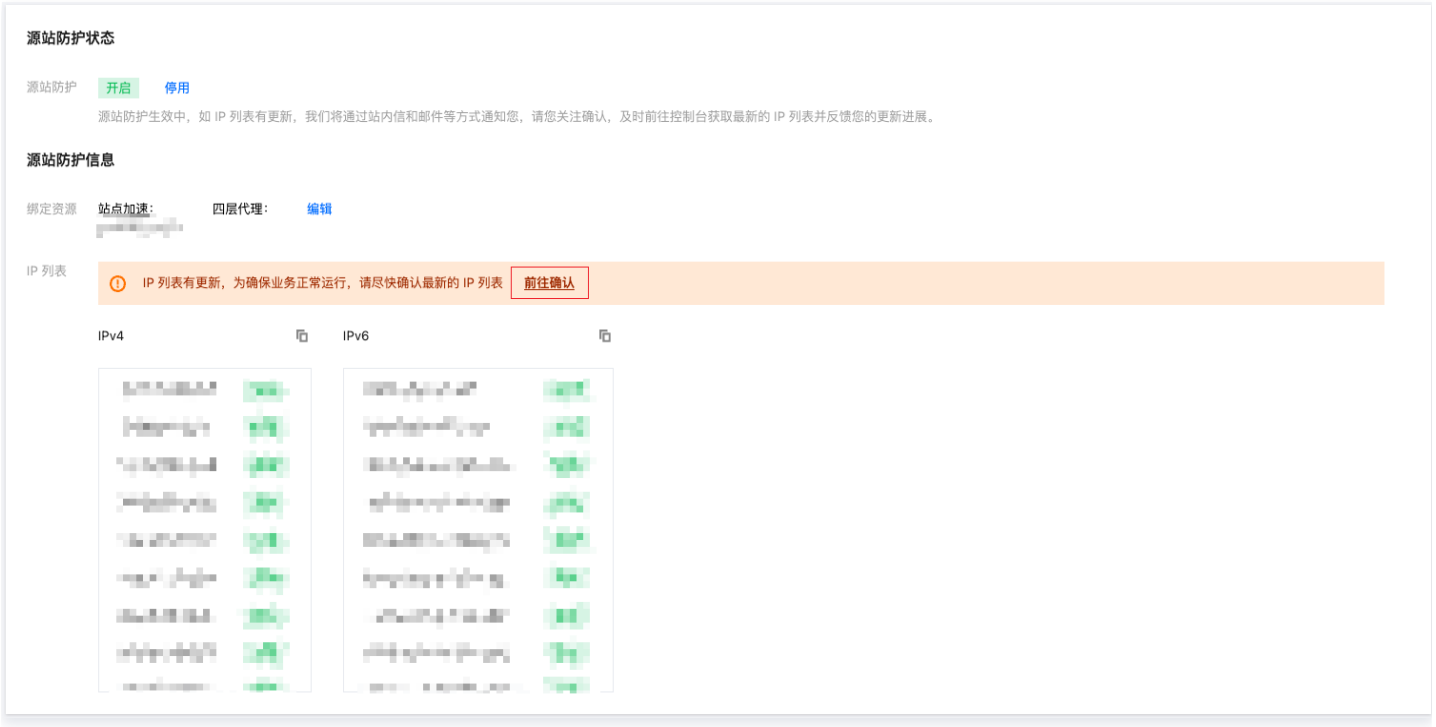
1. 登录 边缘安全加速平台 EO 控制台，在左侧菜单栏中，单击**站点列表**，在站点列表内单击需配置的**站点**，进入站点详情页面。
2. 在站点详情页面，单击**安全防护** > **源站防护**。
3. 在源站防护页面，单击源站防护状态的**启用**，选择站点加速/四层代理服务，单击**确认启用**为所选资源启用源站防护。

> **说明**
> 选择站点加速/四层代理服务：请绑定需要使用源站防护服务的资源。

4. 成功启用后：
   - 您可查看到这些资源目前使用的回源 IP 列表，请将其更新至您的源站防火墙规则中。
   - 后续如果回源 IP 列表有更新，我们将发出消息通知，直到您确认并反馈后，再为绑定的资源正式使用更新后的回源 IP 列表。

注意事项

为了您的业务能正常运行，当收到 IP 列表更新的消息，请您及时前往控制台确认并更新。



> **说明**
> 如未及时更新至最新的回源 IP，则可能影响正常业务，如延时不能达到最优，高并发时可能不稳定等。

相关参考
旧版源站组兼容相关问题

最近更新时间：2024-08-23 14:25:12

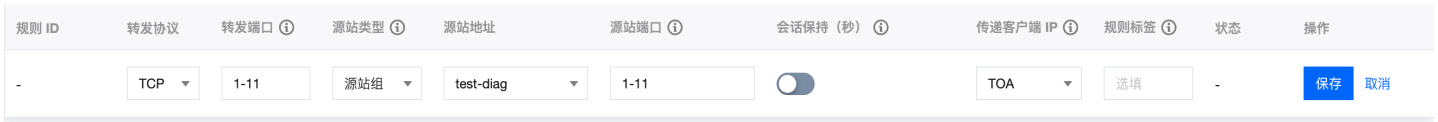
源站组已于2023年10月24日起进行产品能力升级。升级后，旧版源站组将以下方式进行兼容性处理，同时，我们也建议您转换至 新版源站组 的使用。

源站类型和配置方式兼容

- 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 。



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。

> **说明：**
> EdgeOne 负载均衡能力即将上线，可支持主备源站配置场景需求，敬请期待。