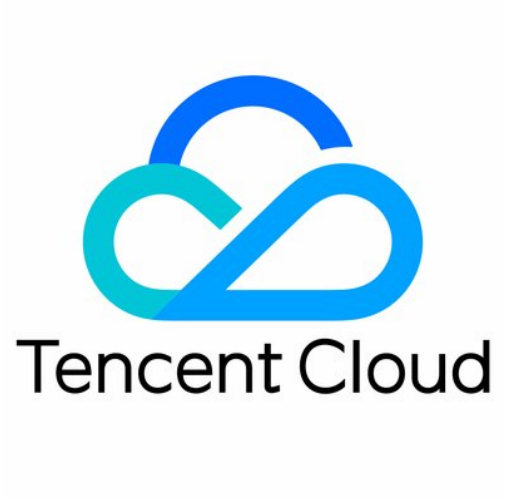
Tencent Cloud EdgeOne

Origin Configuration

Product Documentation



Contents

Origin Configuration
Origin Group Configuration

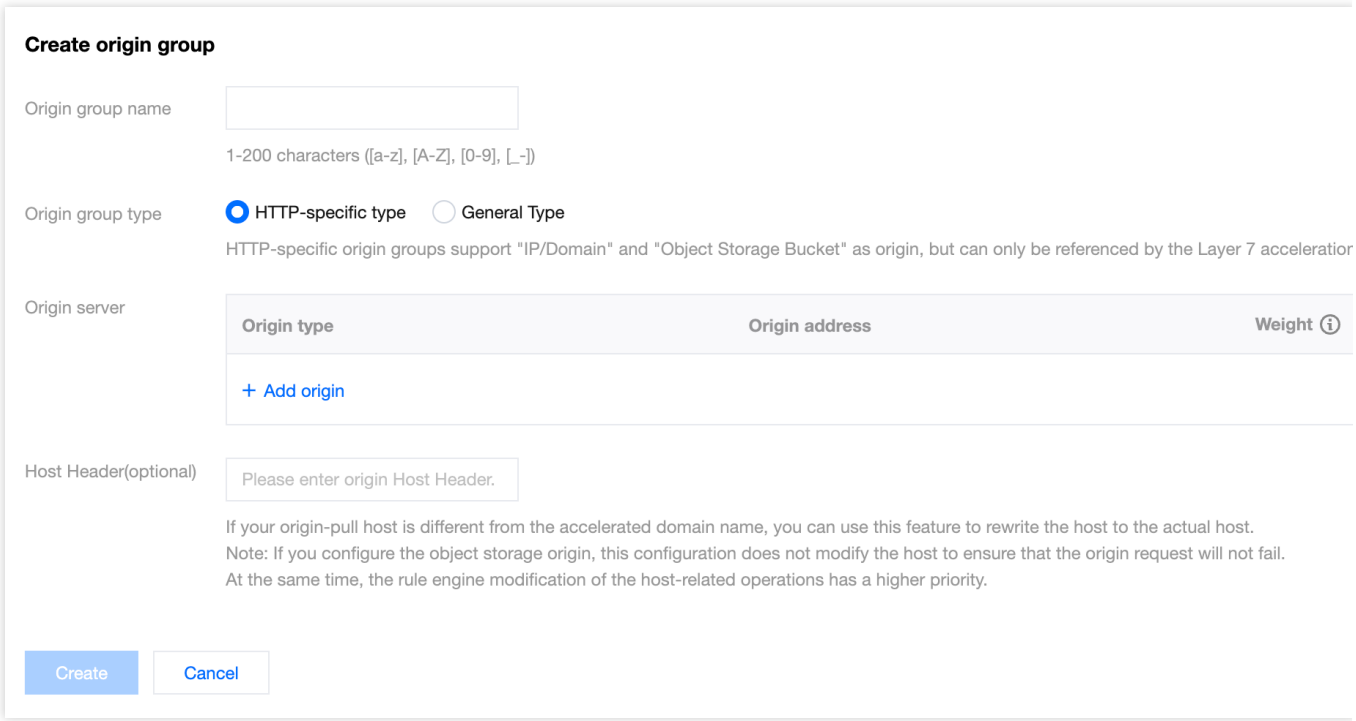
Last updated：2023-12-15 09:51:57

Overview

Manage business origins in the form of origin groups. The origin groups configured here can be used in functions such as adding acceleration domain names and L4 proxy.

Create Origin Group

1. Log in to the EdgeOne console and click Site List in the left sidebar. In the **site list**, click the target site to enter the site details page.
2. On the site details page, click **origin configuration > origin group**.
3. Click **Create origin group**.
4. Fill in the origin group name and select the origin type. The specific type descriptions are as follows:
HTTP Dedicated: Supports adding **IP/domain name origins** and **object storage origins**, and can only be used for site acceleration-related services (e.g., Domain Name Service and rule engine - Modify origin).
Universal: Only supports adding **IP/domain name** as origin, does not support adding **object storage origin,** and can be used for site acceleration services (such as Domain Name Service and rule engine) and L4 proxy.
Note:
After the configuration is complete, the origin group type cannot be modified.



5. Click the **Add Origin** button to configure the origin. The supported origin types are as follows, with up to 100 origins supported.

Object storage origin: Tencent Cloud COS or other object storage buckets compatible with AWS S3.

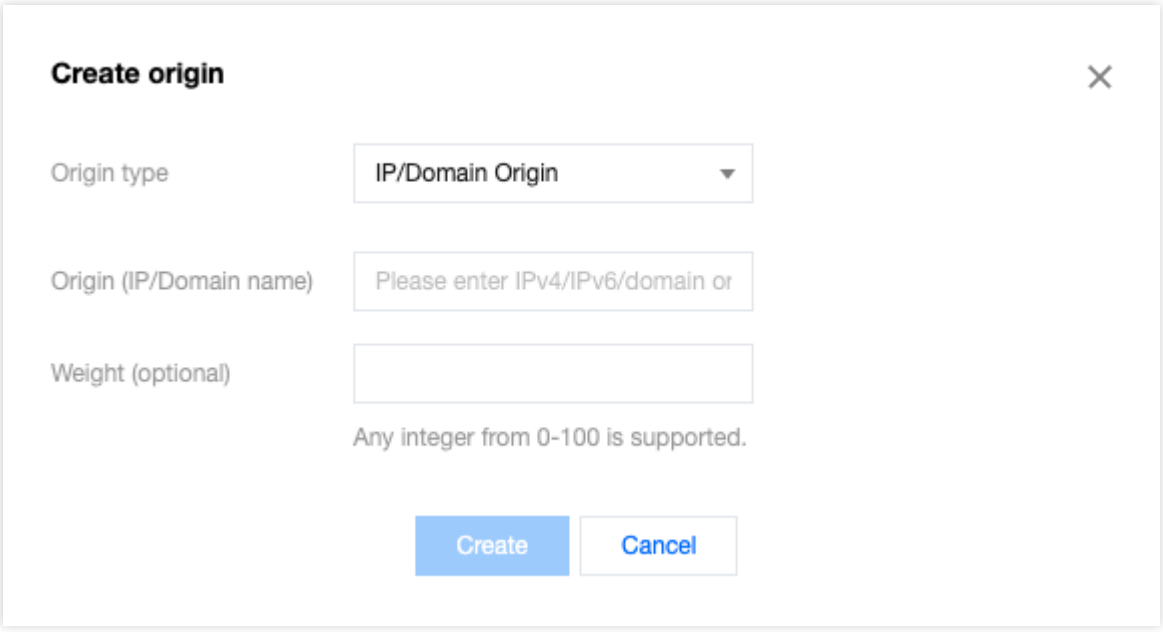
IP/domain name origin: Supports IPv4 addresses, IPv6 addresses, and domain names as origins.

Note：

Explanation of weight-related configurations in the origin group:

1. If a weight is set for an origin in the origin group, all origins in the group must also set corresponding weights. Weights can be integers between 0 and 100. If the weight of an origin is set to 0, no origin-pull requests will be allocated to that origin. Other non-zero weight origins will be allocated origin-pull requests based on their respective weight ratios.

2. If you do not set a weight, all origins in the origin group should not set weights at the same time. In this case, if "smart acceleration" is not enabled, EdgeOne will distribute origin-pull requests equally to each origin. If "smart acceleration" is enabled, EdgeOne will select the best quality origin for each origin-pull request.



6. Click **Create** to complete the origin group creation.

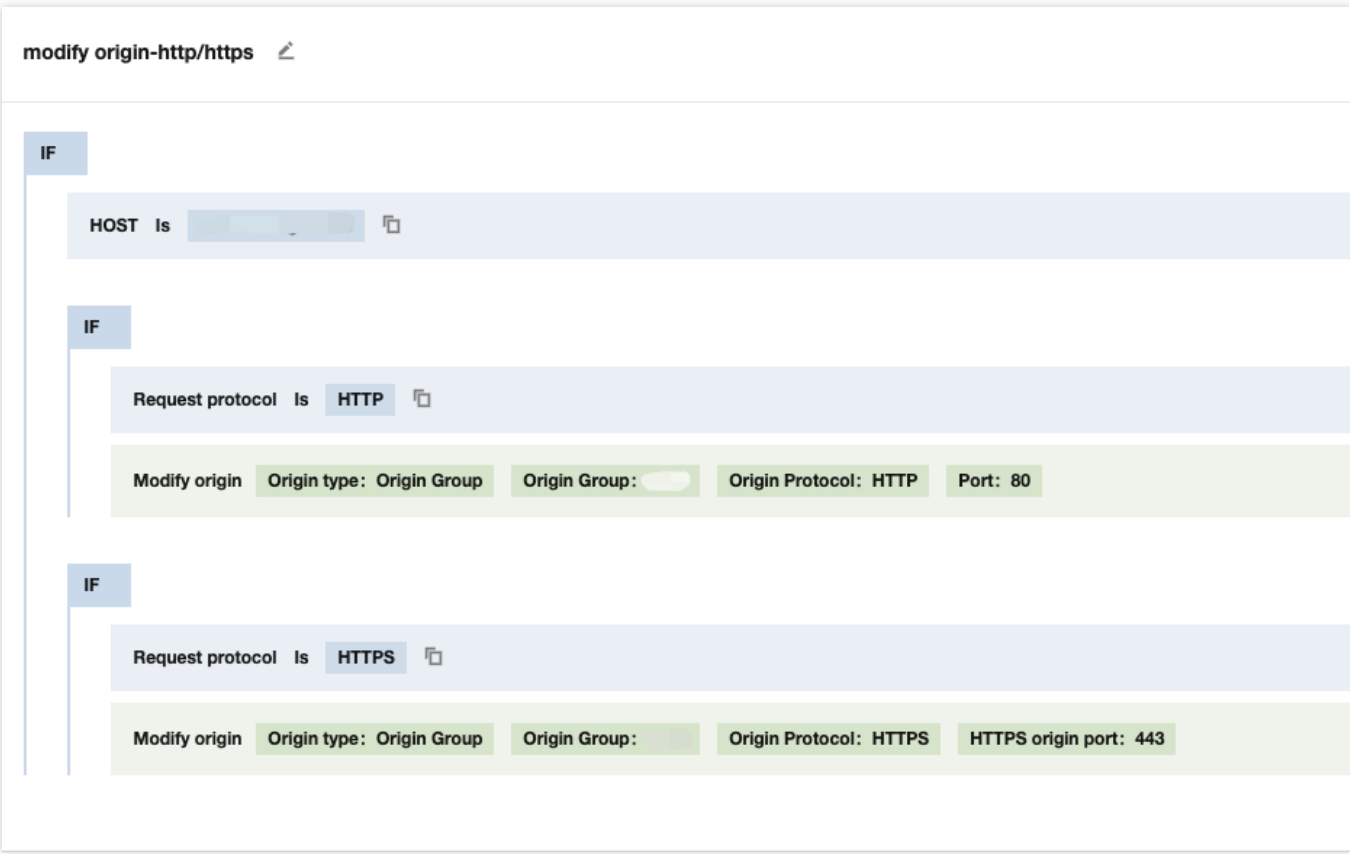
Id Version Origin Group Compatible Related Issues

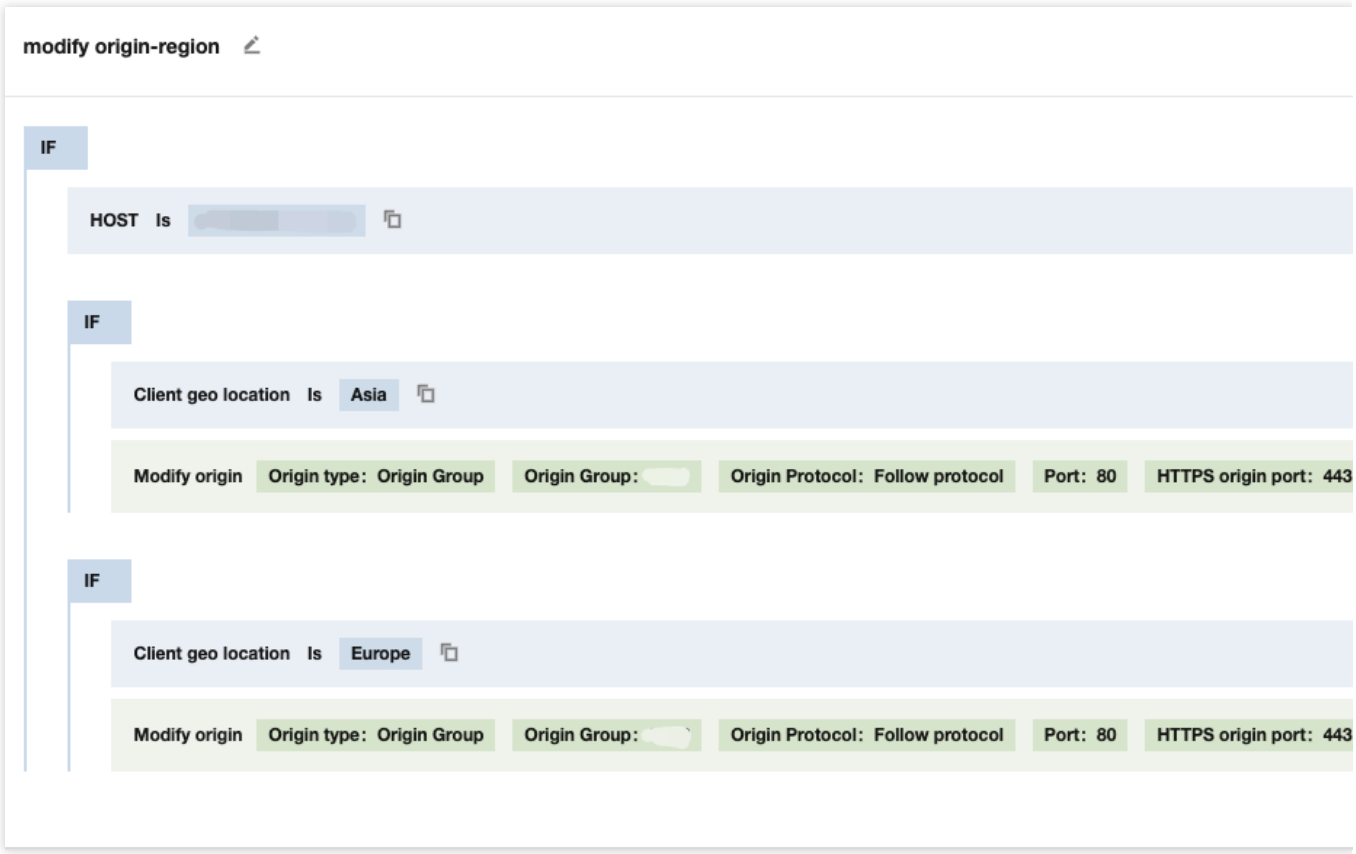
Last updated：2023-10-24 15:45:49

The origin group has carried out a product capability upgrade since October 24, 2023. After the upgrade, the old version of the origin group will be processed for compatibility in the following ways. At the same time, we also suggest you switch to the usage of the new version of the origin group.

Origin type & Configuration method compatibility

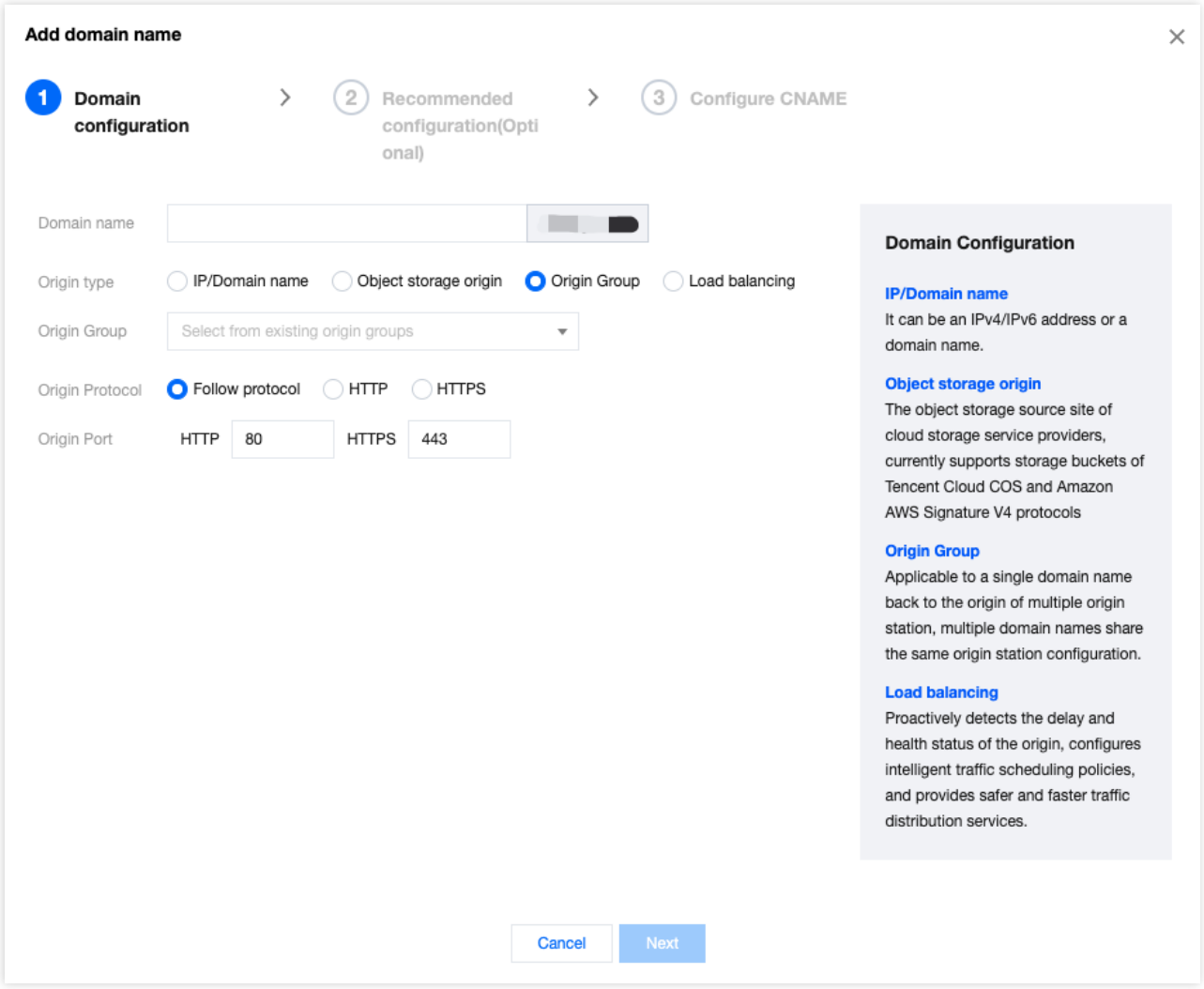
The new version of the origin group will no longer distinguish between **self-owned origin**, **object storage origin**, and **Tencent Cloud COS type origin**. The original origin groups with origin type of **object storage and Tencent Cloud COS** will be automatically updated to the new version of dedicated **HTTP origin group**, and the original origin groups with **self-owned origin** type will be automatically updated to the **universal origin** group.
The origin group will no longer support the configuration of origin-pull by region/protocol. If you have previously configured related origin-pull rules by region/protocol, the rules will be migrated to the rule engine as shown below:

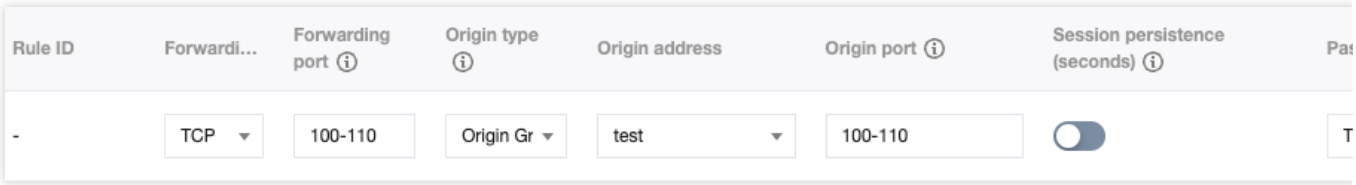




Origin group port migration description

The new version of the origin group will no longer support port configuration. All port configurations will be migrated to the service configuration entry, such as L4 proxy or Domain Management.





Primary and Standby Origin Configuration Instructions

In the **Domain Management** and **Rule Engine - Modify Origin**, directly configuring primary and standby origins is no longer supported. Existing configurations will not be affected, but modifications are no longer supported. If you currently have a demand for primary and standby origin configurations, please contact us for support.

Collect EdgeOne origin-pull node IP

Last updated：2023-12-15 09:54:21

To obtain the EdgeOne's IPs for requesting origin, which can be used to set these EdgeOne's IPs as an allowlist in the origin firewall, only allowing fixed source (IP) requests to the origin, thus implementing protection for the origin.

Use Guide

1. Directly access https://api.edgeone.ai/ips through a browser or curl command. This will collect all IPv4 and IPv6 origin-pull node IP addresses of EdgeOne in the Global availability zone. The responded result is UTF-8 encoded plain text, with one IP segment per line.
2. If you only need to obtain the origin-pull node IP of a specified region or a specified IP Type, you can also filter the origin-pull node IP by carrying a specified query string. The supported query strings are as follows:

Query string	Explanation
version	Specifies the Type of origin-pull node IP address to be collected, with the following values: **v4:** All IPv4 origin-pull node IP addresses **v6:** All IPv6 origin-pull node IP addresses By default, all IPv4 and IPv6 IP addresses are returned when this parameter is not included.
area	Specifies the region of the origin-pull node IP to be collected, with the following values: **global:** All origin-pull node IP addresses in the Global availability zone **mainland-china:** All origin-pull node IP addresses in the Chinese mainland availability zone **overseas:** All origin-pull node IP addresses in the Global availability zone (excluding Chinese mainland) By default, all origin-pull node IP addresses in the Global availability zone are returned when this parameter is not included.

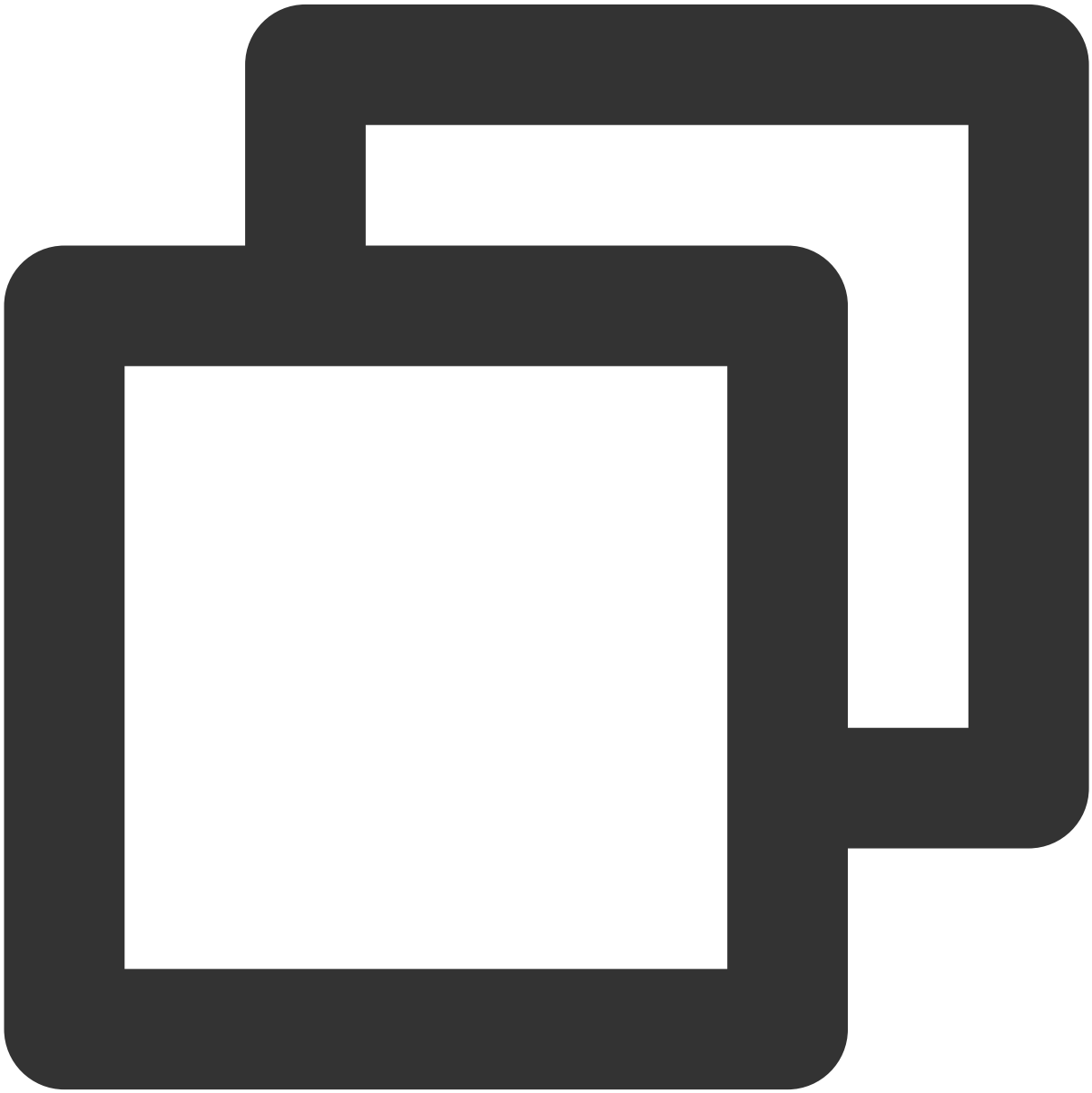
Note：

1. In general, it is suggested to select and obtain the origin-pull node IP address of the corresponding region based on your site's service area. For example, if the site's service area is in the Chinese mainland availability zone, you can obtain the origin-pull node IP address within the Chinese mainland availability zone, and the same applies to other service areas.
2. This function is mutually exclusive with the origin protection function. If you need to collect the latest origin-pull IP through the method in this Document, please confirm that you have turned the business origin protection function Off.

Request example

If you want to obtain all IPv6 origin-pull node IPs in the Global availability zone (excluding Chinese mainland), you can query the origin-pull IP address under this condition by carrying `version=v6&area=overseas` in the request URL. The specific URL is: `https://api.edgeone.ai/ips?version=v6&area=overseas`

The response result example is as follows (this result is for reference only, please refer to the real-time request result for the actual origin-pull IP):



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

Host Header Rewrite

Last updated：2023-10-11 10:28:05

Overview

Host header rewriting enables you to rewrite the host header to the actual origin domain when the origin domain is different from the acceleration domain in the load balancing task.

Directions

1. Log in to the EdgeOne console. Select **Origin Configuration** >**Rule Engine** on the left sidebar.
2. On the rule engine page, select the target site and click

to configure host header rules as needed.
3. On the rule engine page, select **Host** for the match type and **Rewrite host header** for the action, and configure other parameters as needed. Click **Save and publish** or **Save only**.

Note

Supported match types: "Host".

Range GETs

Last updated：2024-01-02 09:59:31

Overview

Range GETs can be enabled to reduce the consumption of large file origin-pulls and response time.

Why can Range GETs improve the efficiency of large file delivery?

When caching large files, nodes will split them into smaller parts in order to improve cache efficiency. All parts cached expire at the same time and follow the node cache TTL configuration. Range requests are also supported. For example, if a client request carries the HTTP header `Range: bytes = 0-999`, only the first 1000 bytes of the file will be returned to the user.
If Range GETs is enabled: When parts of the file are requested and their caches expire, nodes only pull and cache the requested parts and return them to the user, so that origin-pull consumption and response time are greatly reduced.
If Range GETs is disabled, when the client requests only parts of a file, the node will pull only the requested parts according to the `Range` header in the client request, cache them, and return them to the client at the same time. However, this may not be able to achieve the optimal performance. In large file scenarios, we recommend you enable Range GETs.

Use Cases

You can use Range GETs to cache large static files in either of the following cases: The origin server supports Range requests, or you use a Tencent Cloud COS origin server and do not apply any data processing methods such as image processing.

Notes

The origin server must support Range requests, or the origin-pull may fail.
The origin-pull may fail if Range GETs is enabled for small static files, or if you enable it while using a Tencent Cloud COS origin server and data processing methods such as image processing.

Directions

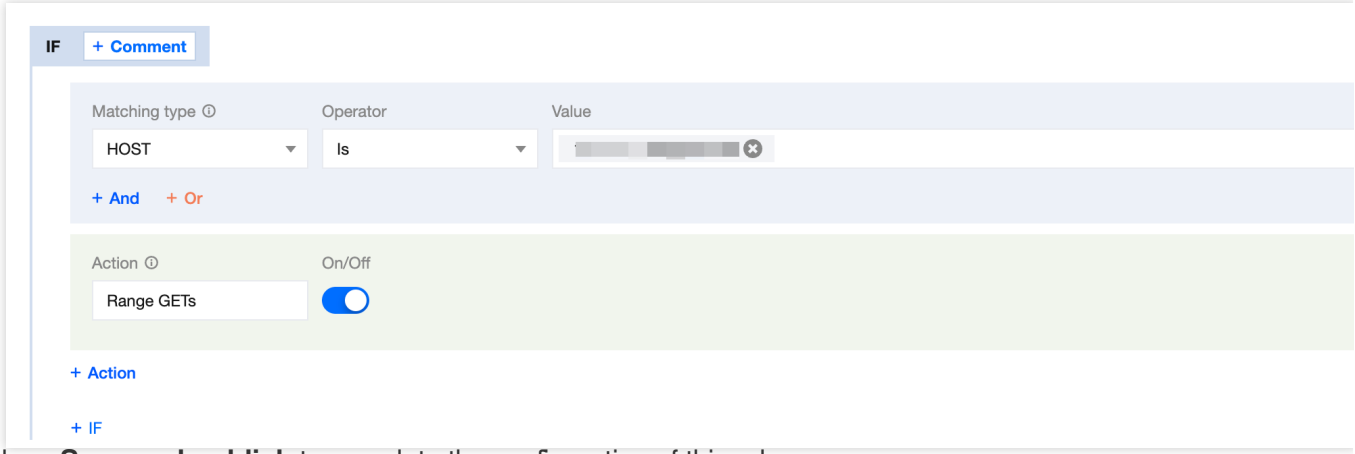
For instance, you have a video service website that provides online video watching through `video.example.com`. The videos are mainly long videos with large files. In order to reduce traffic consumption of large files and improve origin-pull speed, you need to support range requests and origin-pull. You can perform the following steps:

1. Log in to the EdgeOne console, click **Site List** in the left sidebar and click the **Site** to be configured in the site list.
2. On the site detail page, click on **Rule Engine**.
3. On the rule engine management page, click on **Create rule** to enter the new rule's editing page. In this scenario, you can operate as follows:

3.1 On the rule editing page, select the Matching type as `HOST` equals `video.example.com`.

3.2 Click on **Action**, in the displayed operation list, choose the operation as **Range GETs**.

3.3 Click on **On**/**Off** to enable Range GETs.



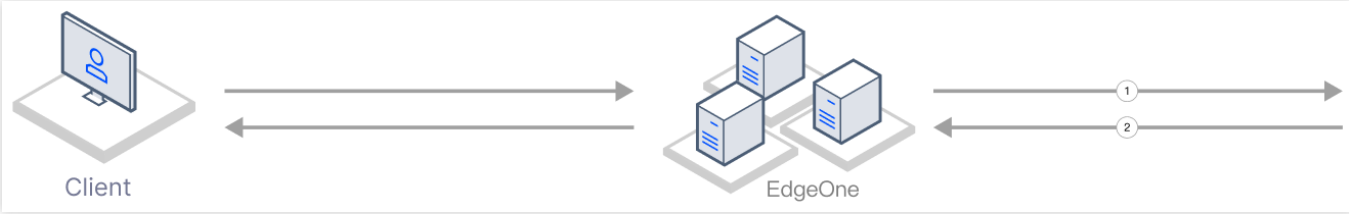
4. Click on **Save and publish** to complete the configuration of this rule.

Configuring Origin-Pull HTTPS

Last updated：2023-12-13 11:10:42

Overview

You can specify the protocol that EdgeOne uses in the origin-pull request.
In scenarios that requires a high level of security, HTTPS can be used to access a website to ensure the security of website data. When HTTPS is specified as the origin-pull protocol, all origin-pull requests from EdgeOne to the origin use HTTPS, which prevents data tampering or theft during transmission.
In scenarios where fast response is required, HTTP can be used for origin-pull requests to speed up website access. When HTTP is specified as the origin-pull protocol, you can avoid complex SSL handshakes and other operations between EdgeOne and the origin, thus improving the website access speed. If your origin does not support HTTPS, please select HTTP.



1. An EdgeOne node initiates an origin-pull request by using the specified origin-pull protocol.
2. The origin responds to the request and establishes a connection by using the same protocol as the request.

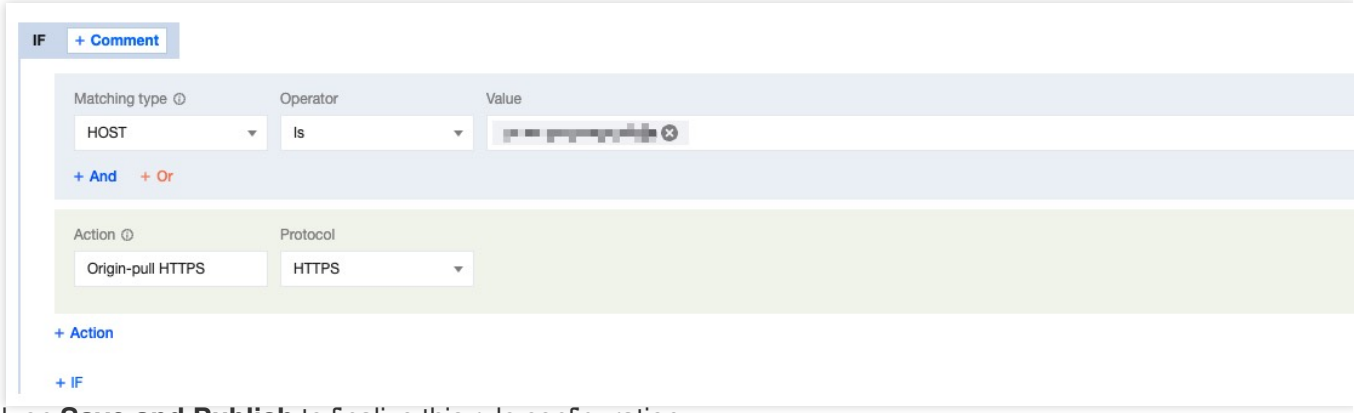
Note:
The configuration priority of the rule engine is superior. If the origin protocol rule is configured simultaneously within the domain name service and the rule engine, the final standard is determined by the rule engine.

Scenario 1: Configuring origin-pull HTTPS for multiple domain names in batches in the rule engine

If you need to uniformly change the origin-pull protocol to origin-pull HTTPS for multiple domain names, such as `www.example.com` , `vod.example.com` and `image.example.com` , please refer to the following steps:
1. Log in to the EdgeOne console and click **Site List** in the left sidebar. In the site list, click the target site.
2. On the site details page, click **Rule Engine**.
3. On the rule engine management page, click **Create rule**.

4. On the rule editing page, enter the rule name and select Host matching type to match the request of the specified domain name. In the current scenario, select domain names `www.example.com` , `vod.example.com` and `image.example.com` .

5. Click on **Action** > **Select Box**, select **Origin-pull HTTPS** from the dropdown action list that appears.

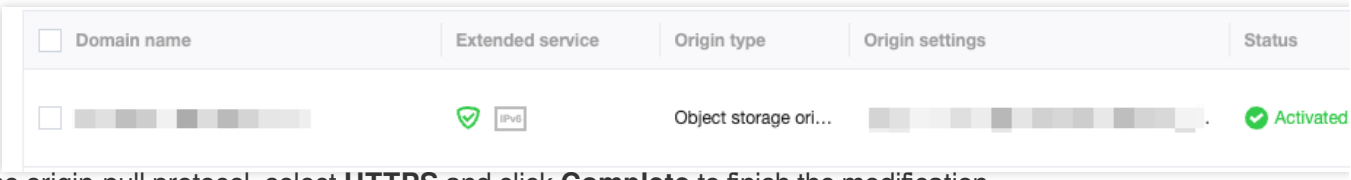


6. Click on **Save and Publish** to finalize this rule configuration.

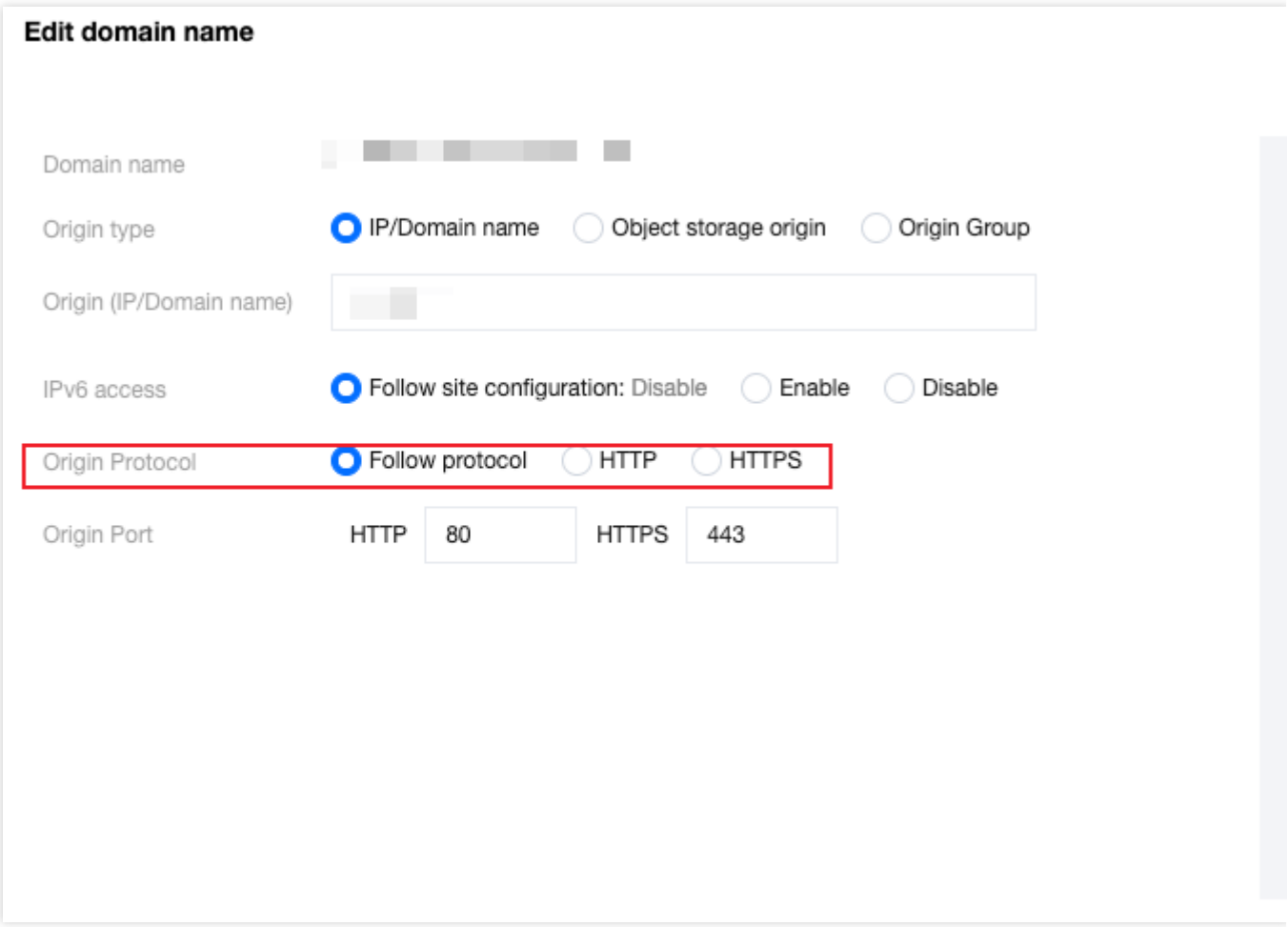
Scenario 2: Configuring origin-pull HTTPS for the specified domain name

If you need to specify a domain name to modify the origin-pull protocol into origin-pull HTTPS, such as `www.example.com,` please follow these steps:

1. Log in to the EdgeOne console, click **Site List** on the left sidebar, and click the **Site** to be configured in the site list,
2. Choose **Domain Name Service** > **Domain Name Management** on the **Site Details** page.
3. Select the domain name that needs to be modified and click **Edit** on the **Domain Management** page.



4. In the origin-pull protocol, select **HTTPS** and click **Complete** to finish the modification.



HTTP/2 Origin-Pull

Last updated：2023-08-30 15:05:42

Overview

Support EdgeOne nodes to origin-pull using HTTP/2 protocol. HTTP/2 (i.e., HTTP 2.0, Hypertext Transfer Protocol version 2) is the second major version of the HTTP protocol, which can effectively reduce network latency and improve site page loading speed.

Note：

1. When enabled, the origin must support HTTP/2 protocol access.
2. If you need to configure HTTP/2 access, please refer to HTTP/2.

Directions

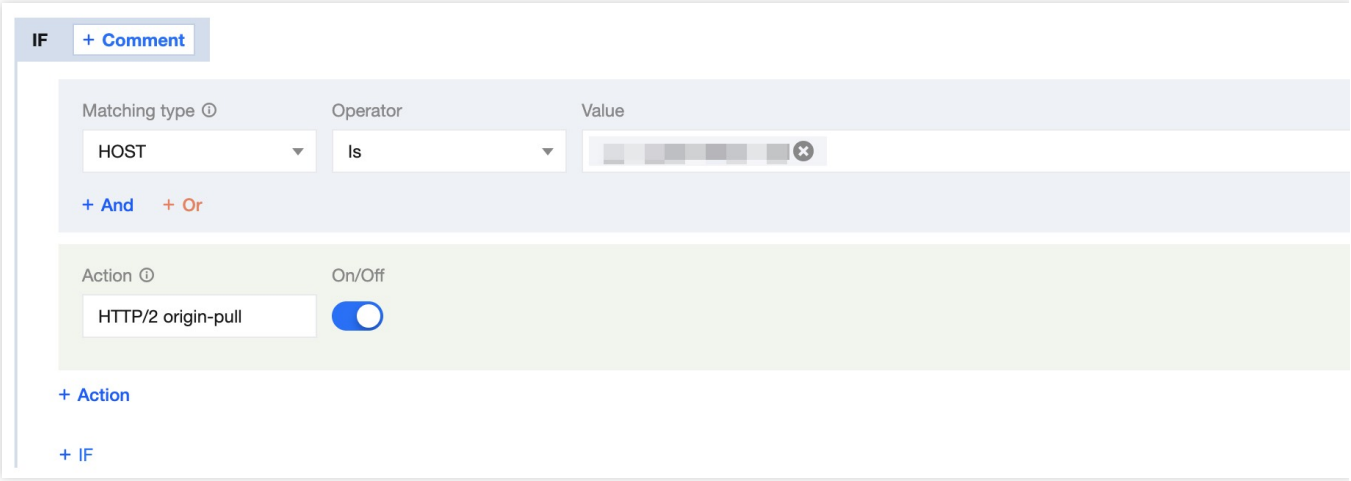
If you need to enable or disable HTTP/2 origin-pull for the specified domain `www.example.com`, you can follow the steps below:

1. Log in to the EdgeOne console, click on the site list in the left sidebar, and click on the site you need to configure within the site list.
2. On the site details page, click on the **rule engine**.
3. On the rule engine management page, click on **create rule** to enter the new rule editing page.

3.1 On the rule editing page, select the matching type as HOST equals `www.example.com`.

3.2 Click on the **action**, and in the pop-up operation list, select the operation as **HTTP/2 origin-pull**.

3.3 Click on the switch to enable/disable HTTP/2 origin-pull.



4. Click on Save and Publish to complete the rule configuration.

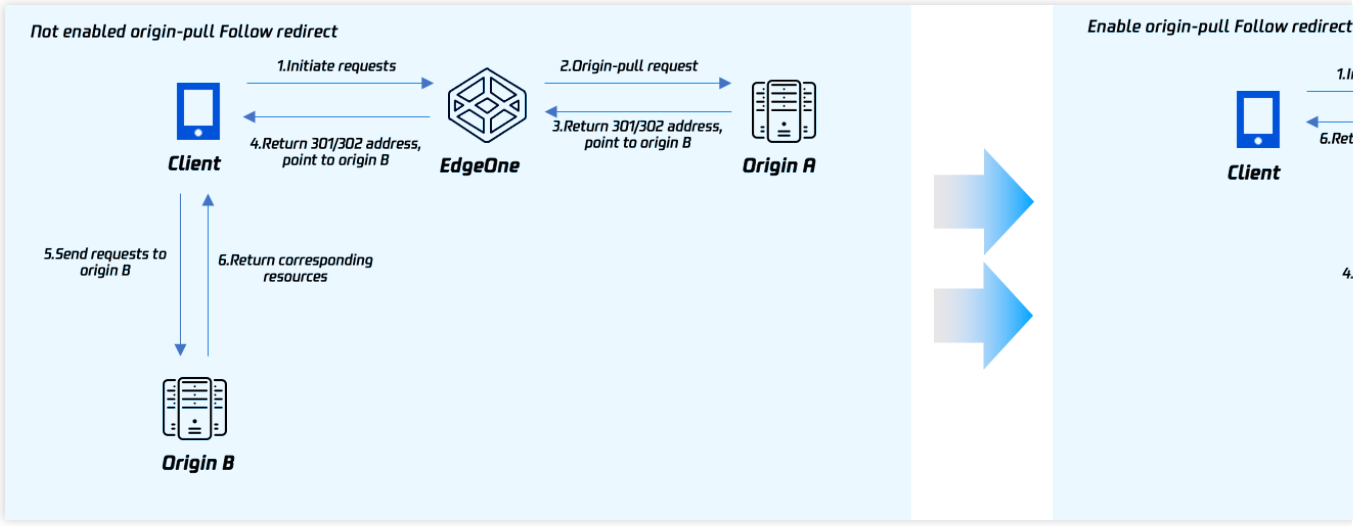
Redirect Following During Origin-Pull

Last updated：2023-08-30 15:08:04

Overview

Under normal circumstances, when the origin returns a 301/302 request, the node will return the status code to the client by default, and the client will redirect to the corresponding resources for access. EdgeOne supports follow origin redirects. When enabled, if the node receives a 301/302 status code during origin-pull, it will actively follow the redirect (not exceeding the set maximum redirects) to the specified address until the corresponding file is obtained, and then respond to the client with the actual resources, which can improve the user's access response speed.

For example: The client accesses the URL `https://a.example.com/test.jpg`, the origin A redirects the URL 302 to `https://b.example.com/test.jpg`, and the domain `a.example.com` has accessed the EdgeOne Service, while `b.example.com` has not yet accessed the acceleration service. Then:
Without enabling origin-pull follow redirect: After the client initiates the visit, if there is no cache in the EdgeOne node, it will visit the origin A and receive the 302 status code, and then respond to the client with the status code, and the client will directly request the origin B for the corresponding resources. At this time, since the origin B has not accessed the acceleration service, the client's self-initiated access speed is slower, and the obtained file cannot be cached. When other users access the same file, the process needs to be repeated.
Enable origin-pull follow redirect: After the client initiates the visit, if there is no cache in the EdgeOne node, it will visit the origin A and receive the 302 status code, and then, according to the status code and the corresponding address, directly request the origin B for the corresponding resources, and cache the resources in the node. This process is carried out by the EdgeOne node for origin-pull requests, the request speed is faster, and the obtained file can be cached in the node. When other users access the same file, there is no need to repeat the origin-pull, and the file can be directly hit and responded to the client.



Directions

For example: If you need to enable origin-pull follow redirect for the specified domain `www.example.com` , with a maximum of 3 redirects. You can refer to the following steps:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, and click on the site to be configured in the site list.

2. On the site details page, click on the rule engine.

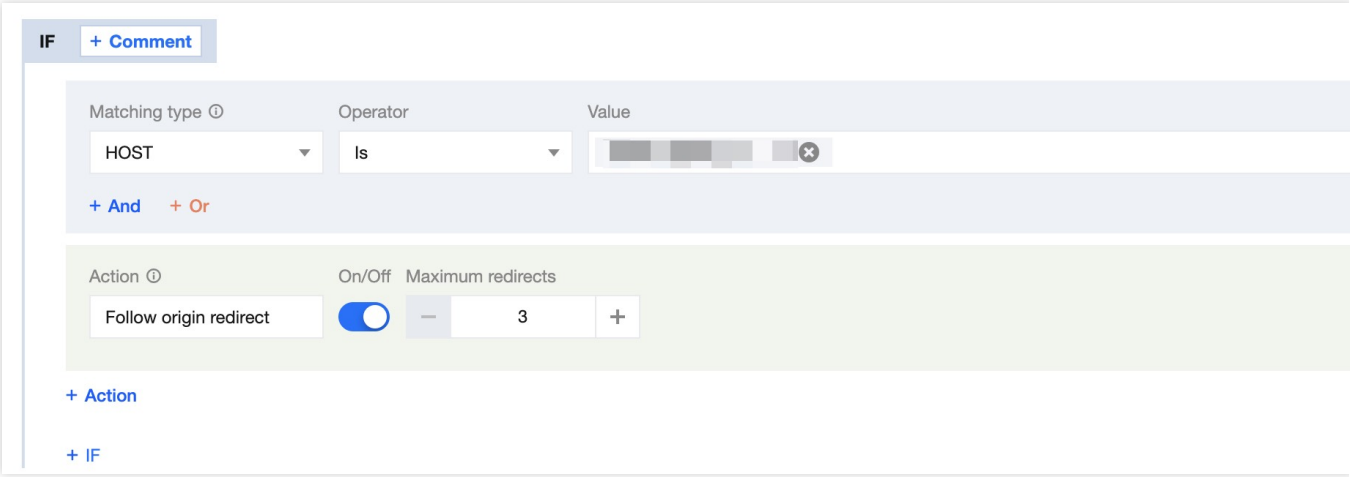
3. On the rule engine management page, click Create Rule to enter the editing page of the new rule. In this scenario, you can follow the steps below:

3.1. On the rule editing page, select the matching type as HOST equals `www.example.com` .

3.2. Click on the **action**, and in the pop-up operation list, select the operation as **follow origin redirect**.

3.3. Click on the switch, click on the switch to enable, and set the maximum redirects to 3 times. The related configuration instructions are as follows:

Maximum redirects: You can set it between 1-5 times. Within the maximum redirects, the node will follow the redirect address until the corresponding resources are obtained. If the maximum redirects are exceeded, the corresponding status code will be directly responded to the client.



4. Click on **Save and Publish** to complete the rule configuration.

Controlling Origin-pull Requests

Last updated：2023-08-30 15:09:23

Overview

By default, when origin-pulling, all query strings and Cookies within the request will be retained. If your business origin only allows specified query strings or Cookie information to be carried in the origin-pull request, you can ensure the normal origin-pull request by deleting the specified origin-pull request parameters.

Directions

For example, Client requests Request URL: `http://www.example.com/path/demo.jpg?key1=a&key2=b&key3=c&key4=d` , and only `key1=a` parameter needs to be retained when origin-pulling. You can follow the steps below to configure:

1. Log in to the EdgeOne console, click on the site list in the left menu bar, and click on the site to be configured within the site list.

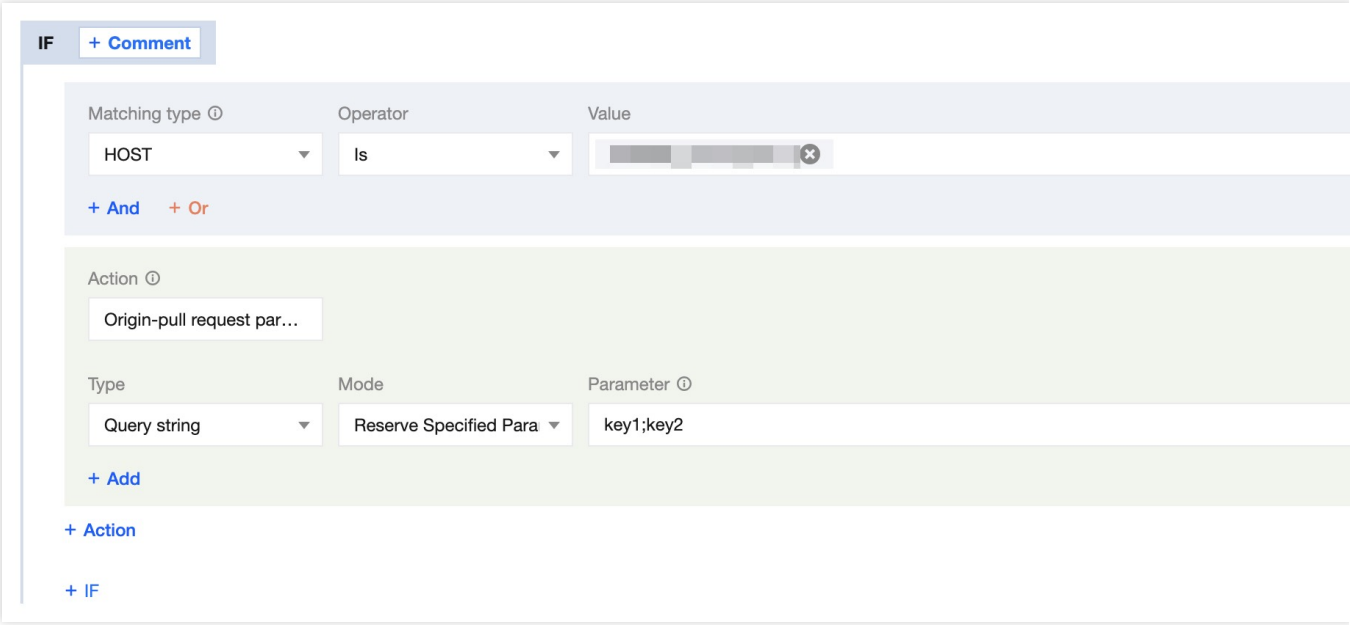
2. On the site details page, click on the **rule engine**.

3. On the rule engine Management page, click **Create rule** to enter the edit page of the new rule.

3.1. On the rule edit page, select the matching type as HOST equals `www.example.com` .

3.2. Click on the **action**, and in the pop-up operation list, select the operation as **origin-pull request parameter settings**.

3.3. Select the mode as retaining specified parameters, Enter the parameters `key1` and `key2` to be retained, up to 10 parameters are allowed.



4. Click **Save and Publish** to complete the rule Configuration.