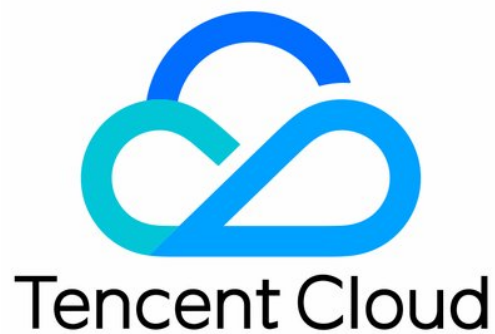


Tencent Cloud EdgeOne

FAQs

Product Documentation



Copyright Notice

©2013-2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

FAQs

Last updated : 2023-09-12 14:56:59

How can I connect my site to EdgeOne?

EdgeOne supports NS and CNAME connection.

What security capabilities does EdgeOne have?

It can prevent web application layer, DDoS, CC, bot, and crawler attacks and allows you to configure complicated custom access control rules based on your business needs.

Does EdgeOne support cross-region acceleration?

EdgeOne deploys edge nodes in to fully meet your cross-region business needs. For specific available regions, [contact us](#).

Does EdgeOne support sites not deployed on Tencent Cloud?

Yes. For more details, please [contact us](#).

Does EdgeOne support API operations?

Yes. EdgeOne supports TencentCloud API and Terraform API.

Does EdgeOne support dynamic acceleration?

Yes. It supports scenarios where requests for dynamic/static hybrid resources need to be accelerated. It can optimize the request response time and stability to deliver a high-quality and smooth access experience for websites.

What site business security protection capabilities does EdgeOne offer?

EdgeOne provides web and bot protection for HTTP and HTTPS-based website businesses. Specific web protection rules include those for web security, OWASP rules, custom characteristics, and frequency control.

What non-site business security protection capabilities does EdgeOne offer?

EdgeOne provides DDoS attack protection for TCP and UDP applications with specified ports, such as detection and protection against common types of DDoS attack, filtering rules by port, protocol, source IP region, and custom packet characteristic, and UDP watermark protection (coming soon).

The monitoring data I see in Tencent Cloud Observability Platform and EdgeOne are not the same.

Data trends on Tencent Cloud Observability Platform and EdgeOne are generally consistent. However when it comes to the 1-minute granularity, the data can be slightly different. See below for details:

Tencent Cloud Observability Platform: Collect data from edge servers and aggregate the data with 1-minute granularity on the domain name level. This can guarantee the timeliness and stability. But it only provides data related to key metrics on the domain name level.

EdgeOne: Collect and analyze logs in real-time upon receiving the request, and then print out the result. It supports more metrics, such as traffic and requests by the device type and browser type. But the print-out time can be affected in case of request surges.

Assume that a user requests a 1 GB file. The download starts at 10:00:00 and ends at 10:01:40.

Tencent Cloud Observability Platform: Every edge server reports the metric data at a 1-minute interval. Data of this event is recorded at both 10:01 and 10:02.

EdgeOne: Every edge server prints a log when the download ends (10:01:40). The data is recorded at 10:01.

Therefore, data from Tencent Cloud Observability Platform and EdgeOne can differ at a 1-minute granularity due to the difference of sampling rules.

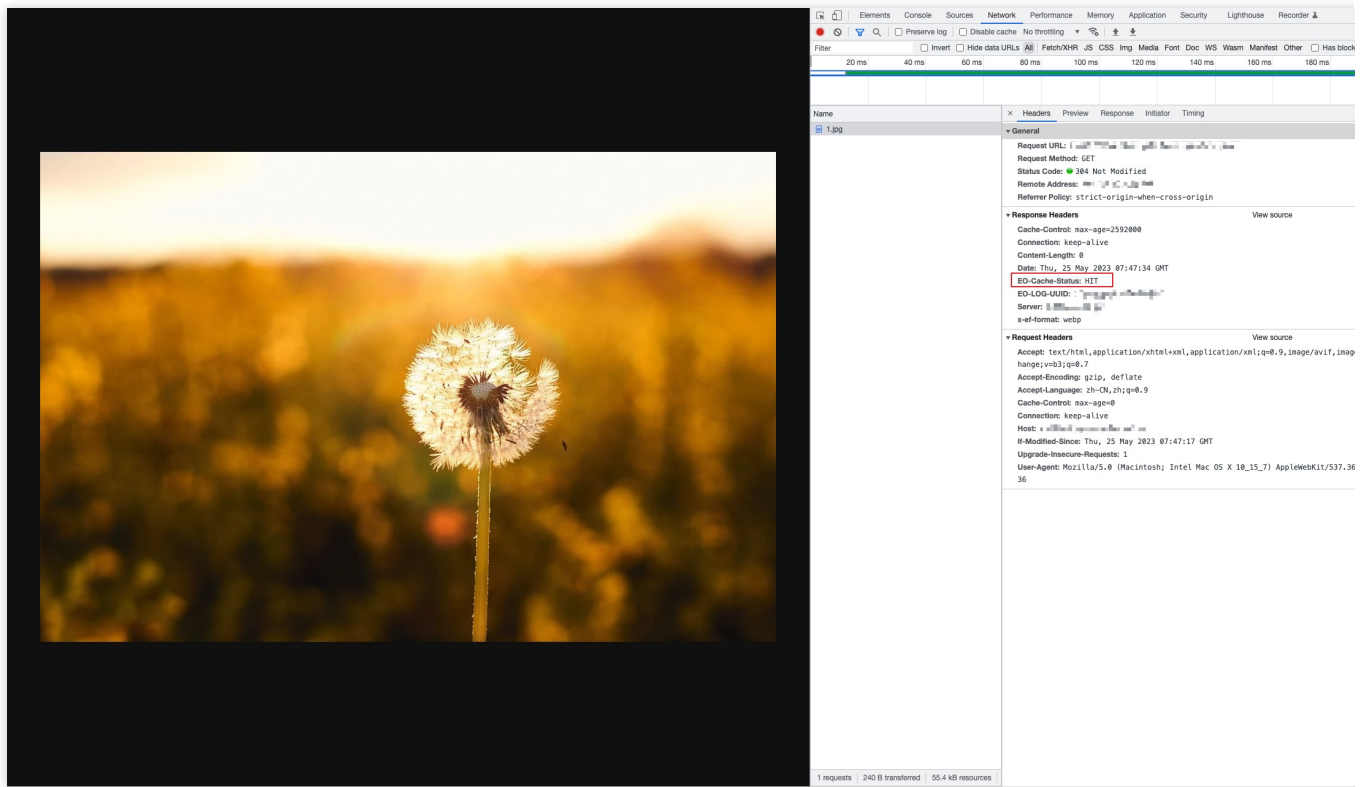
How do I tell whether user access has hit the EdgeOne cache?

EdgeOne identifies whether a request hit the cache via [EO-Cache-Status](#).

Open in browser

Curl command

Open the console in the browser and access the request URL (such as <https://example.com/test.webp>). Check the response header. If the value of `EO-Cache-Status` is `HIT`, the cache is hit.



For Mac/Linux OS, you can use curl command to verify (such as `curl https://example.com/test.webp -i`). Check the response header. If the value of `EO-Cache-Status` is `HIT`, the cache is hit.

```
~ % curl https://example.com/test.webp -i
HTTP/1.1 200 OK
EO-LOG-UUID: 10980868366293882628
Connection: keep-alive
EO-Cache-Status: HIT
Last-Modified: Mon, 24 Oct 2022 08:56:22 GMT
x-cos-hash-crc64ecma: 3381852570206268457
x-cos-request-id: NjQzOGZhMGFFmZU1N2U0MDlFMjAyYjZfNjhkYWYfMQ==
Server: tencent-cos
Accept-Ranges: bytes
Date: Fri, 14 Apr 2023 07:00:26 GMT
Content-Type: image/webp
Etag: "6df8274cf55de4cd1125c0003fd4e2b0"
Content-Length: 21676
```

Why do I get a CNAME and MX record conflict prompt when adding a DNS resolution record?

Take `example.com` as an example.

Record type	Host	Value

MX	www	mx.mail.com
CNAME	www	test.edgeone.com

When performing a recursive resolution query, each record type has different priority, and CNAME has the highest priority. See [RFC1034](#) and [RFC2181](#). Therefore, during the resolution request process, the CNAME resolution record result will be returned first. When the host record value is the same, CNAME record and MX record cannot be configured at the same time, and you will get a prompt about the conflict.

If you do need to add CNAME and MX records at the same time when the host record is @, EdgeOne allows you to configure CNAME and TXT records at the same time:

Record type	Host	Value
MX	@	mx.mail.com
CNAME	@	test.edgeone.com

Reminder:

This configuration will lead to unstable mailbox reception. If the Local DNS of the mailbox server prioritizes the resolution of the CNAME type of the @ record, the resolution of the MX type of the @ record will be affected, resulting in a resolution failure. If the host record is not @, but the MX and CNAME records still indicate a conflict, please refer to the description of other record type conflicts below.

Why do I get a CNAME and TXT record conflict prompt when adding a DNS resolution record?

Take `example.com` as an example.

Record type	Host	Value
TXT	www	edgeone-txt-flag
CNAME	www	test.edgeone.com

The CNAME record has the highest priority, so if the host record is the same, configuring the CNAME record and the TXT record at the same time may cause the TXT record to fail to be parsed. **In this case, EdgeOne will prompt record conflict.**

If you do need to add CNAME and MX records at the same time when the host record is @, EdgeOne allows you to configure CNAME and TXT records at the same time:

Record type	Host	Value
-------------	------	-------

TXT	@	edgeone-txt-flag
CNAME	@	test.edgeone.com

Reminder:

This configuration will cause the TXT verification to fail, you can remove the CNAME record to solve this problem. TXT and CNAME records will still conflict when the host record is not @.

How do the record types conflict with one another?

See below for details:

✓: No conflict. When the HOST is the same, these two record types can both be configured. For example, after configuring the A record for `www.example.com`, you can still configure the MX record.

×: Conflict. When the HOST is the same, these two record types cannot be both configured. For example, after configuring the A record for `www.example.com`, you can not configure the CNAME record.

Record type	A	AAAA	CNAME	MX	NS	TXT	SRV	CAA
A	✓	✓	×	✓	×	✓	✓	✓
AAAA	✓	✓	×	✓	×	✓	✓	✓
CNAME	×	×	×	×	×	×	×	×
MX	✓	✓	×	✓	×	✓	✓	✓
NS	×	×	×	×	✓	×	×	×
TXT	✓	✓	×	✓	×	✓	✓	✓
SRV	✓	✓	×	✓	×	✓	✓	✓
CAA	✓	✓	×	✓	×	✓	✓	✓

Note

The table above shows the conflict relationship when the HOST is not @. If the HOST is @, a CNAME record does not conflict with an MX or TXT record.

When the record type is A/AAAA/CNAME, can I configure both the resolution and acceleration when the HOST is the same?

Take the following configuration as an example:

Record type	Host	Value
A	www	1.1.1.1

A	www	2.2.2.2
---	-----	---------

In this case, if you want to enable acceleration for one record, there will be a conflict. To enable acceleration for `1.1.1.1`, you need to delete `2.2.2.2` first.

Note

The above conflict happens on A/AAAA/CNAME records.

How to handle cross-origin errors when prefetching?

Since resources are prefetched through URLs, cross-origin headers are not required. When a cross-origin request is initiated, the request fails because these headers are not present in the cache.

To enable cross-origin support for your resources when prefetching, you can customize the HTTP response header in EdgeOne.

How long does it take for Cache Purge and Cache Pre-Warming to take effect after each content submission?

Cache Purge :

Type	Single Submission quantity	Effective Time
URL	1-5000 URLs	5-50 minutes
Directory	1-1000 directories	5-220 minutes
Hostname	1-1000 Hostname	5-220 minutes
Cache-Tag	1-100 Cache-Tag	5-10 minutes
All Cache	-	5-220 minutes

Cache Pre-Warming:

Type	Single Submission quantity	Effective Time
URL	1-5000 URLs	5-30 minutes

Note :

1. When the cache TTL configured for a file is less than 5 minutes, it is suggested not to use the purge tool, but to wait for the timeout update.
2. The actual total time for any type of cache purge mainly depends on the quantity of submitted content, the more content, the longer the waiting time.
3. The actual total time for cache pre-warming mainly depends on the file size, the larger the file, the longer the waiting time. The pre-warming effective time for more large files ($\geq 100\text{MB}$) may be extended, exceeding 30 minutes.