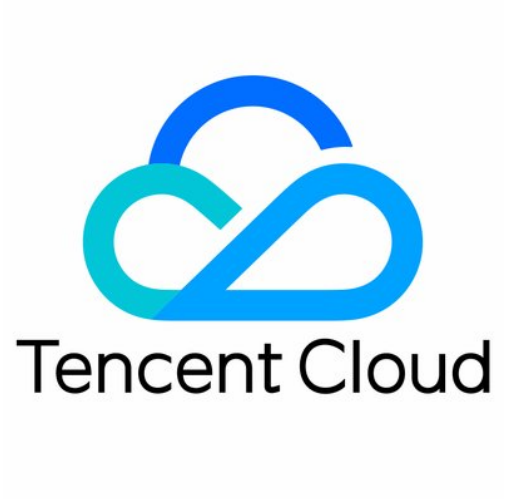
Content Delivery Network

Tools Instructions

Product Introduction



Contents

Tools Instructions
Advanced Tools
Manage Certificates

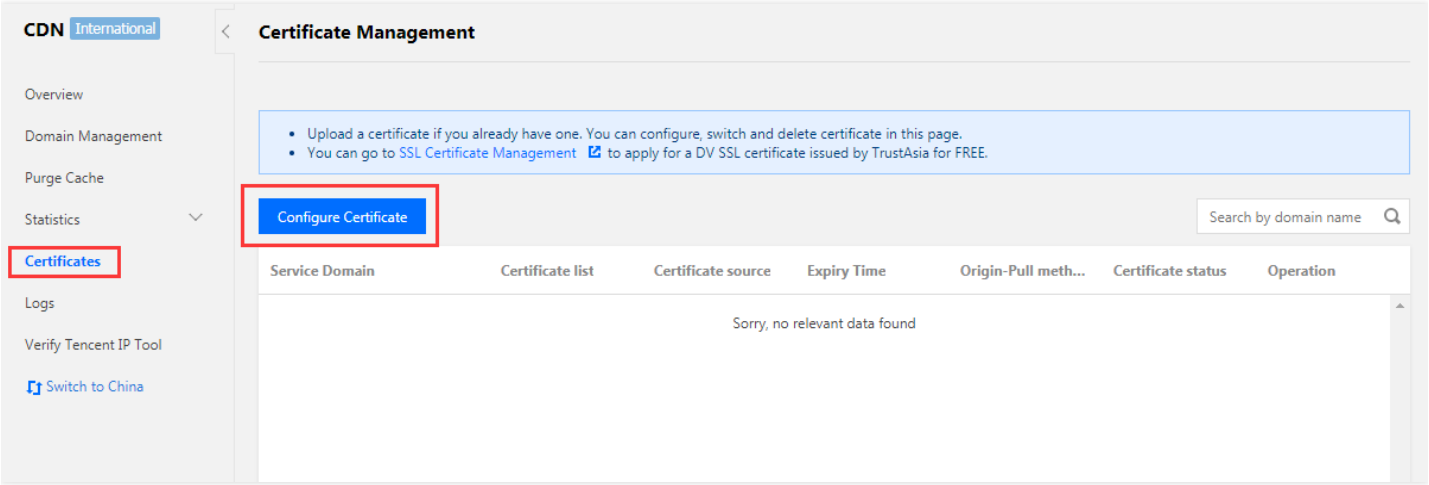
Last updated：2018-09-19 15:54:20

You can configure HTTPS certificate for a domain that has been connected to CDN. You can upload your existing certificate for deployment, or directly deploy the certificate hosted or issued by SSL Certificate Management platform.

You can apply for a free third party certificate from TrustAsia on SSL Certificate Management page.

Configuring Certificate

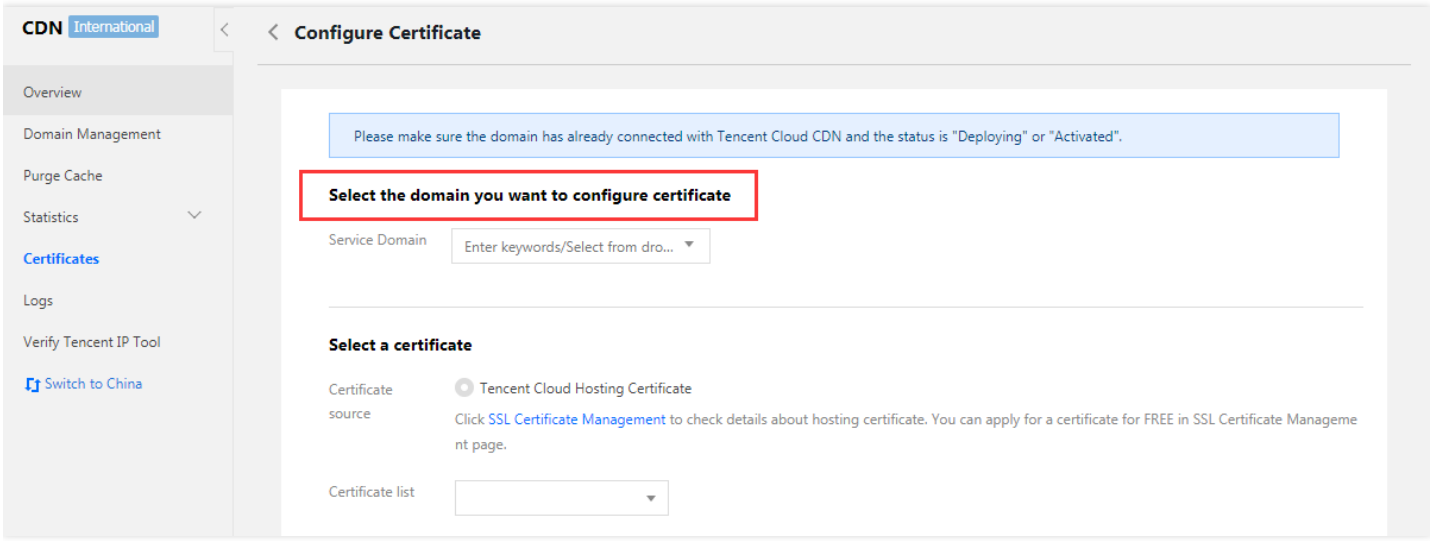
If you already have a certificate, you can upload it directly to the CDN page for configuration. Log in to CDN Console, and go to **Certificates** page in **Advanced** and click "Configure Certificate":



1. Selecting a Domain

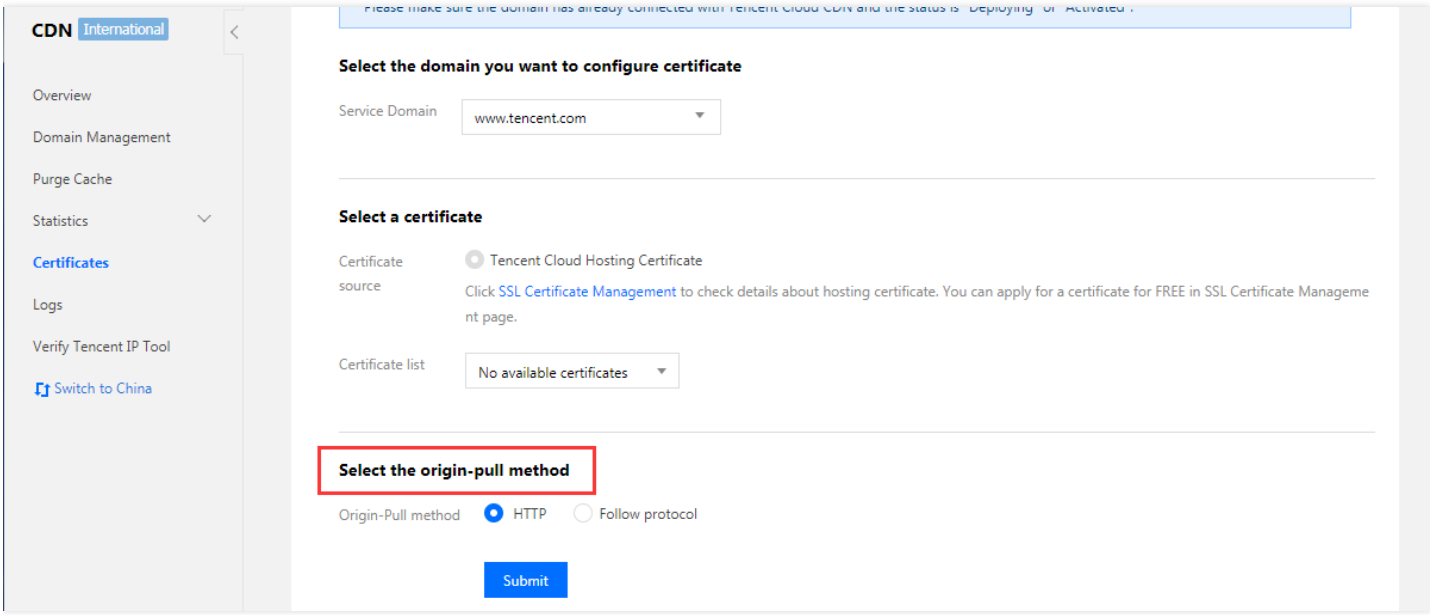
Select the accelerated domain for which you want to configure a certificate. Note:

- The domain is required to be connected to CDN with a status of **Deploying** or **Activated**. For a deactivated domain, certificate deployment is not allowed;
- When CDN acceleration has been activated for COS or Cloud Image, certificate cannot be deployed for domain `.file.myqcloud.com` or `.image.myqcloud.com` by default;
- Certificate cannot be deployed for SVN hosted origin currently.



2. Origin-Pull Method

After the certificate is configured, you can select the back-to-origin method by which CDN nodes get resources from origin server:



- If HTTP is selected, the requests sent from users to CDN nodes support HTTPS/HTTP, and the requests sent from CDN nodes to origin server all use HTTP;
- If HTTPS is selected, the origin server is required to be already configured with a certificate, otherwise back-to-origin failure may occur. When this is checked, if the requests sent from users to CDN nodes use HTTP, the requests sent from CDN nodes to origin server also use HTTP; if the requests sent from users to CDN nodes use HTTPS, the requests sent from CDN nodes to origin server also use HTTPS;

- Currently, domains connected with COS origin or FTP origin do not support using HTTPS as the back-to-origin method;
- For the configuration of HTTPS, your origin server is required to have no port constraint or to be configured with port 443, otherwise the configuration may fail.

3. Finishing Configuration

Once the configuration is finished, you can see the domain and certificate that have been configured successfully on "Certificate Management" page.

Editing Certificate

For certificates that have been configured successfully, you can seamlessly update the certificates with "Edit" button.

- Seamless switching between self-owned certificate and Tencent Cloud hosted certificate is supported;
- Once the edited certificate is submitted, it will be deployed by seamlessly overwriting the original one without affecting your use of service.

PEM Certificate Format

The certificate issued by Root CA agency has a PEM format as show below:

```
-----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
hvcNAQEFBQADggEBALpFBXeG782QsTtGwEE9zBcVCuKjrsl3dWK1dFiq30P4y/Bi
ZBYEywBt8zNuYFUE25Ub/zmvmpe7p0G76tmQ8bRp/4qkJoiSesHJvFgJ1mksr3IQ
3gaE1aN2BSUIHxGLn9N4F09hYwwbeEZaCxfgBiLdEIodNwzcvGJ+2LlDWGJOGrNI
NM856xjqhJCPxYzk9buuCl1B4Kzu0CTbexz/iEgYV+DiuTxcfA4uhwMDSe0nynbn
1qiwRk450mCOnqH4ly4P4lXo02t4A/DI1I8ZNct/Qfl69a2Lf6vc9rF7BELT0e5Y
R7CKx7fc5xRaeQdyGj/dJevm9BF/mSdnclS5vas=
-----END CERTIFICATE-----
```

- [--- BEGIN CERTIFICATE ---, --- END CERTIFICATE ---] are the beginning and end, which should be uploaded with the content;
- Each line contains 64 characters, but the last line can contain less than 64 characters;

The certificate chain issued by intermediate agency:

```
---BEGIN CERTIFICATE---
---END CERTIFICATE---
---BEGIN CERTIFICATE---
---END CERTIFICATE---
---BEGIN CERTIFICATE---
---END CERTIFICATE---
```

Rules for certificate chain:

- No blank line is allowed between certificates;
- Each certificate shall comply with the certificate format rules described above;

PEM Private Key Format

RSA private key can include all private keys (RSA and DSA), public keys (RSA and DSA), and (x509) certificates. It stores DER data encoded with Base64 and is enclosed by ascii header, being suitable for textual transfer between systems. Example:

RSA private key rules:

- [---BEGIN RSA PRIVATE KEY---, ---END RSA PRIVATE KEY---] are the beginning and end, which should be uploaded with the content;
- Each line contains 64 characters, but the last line can contain less than 64 characters;

If the private key is generated using other methods than the one described above and has a format of [---BEGIN PRIVATE KEY ---, --- END PRIVATE KEY ---], you can convert the format as follows:

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

Then upload the content of new_server_key.pem and the certificate.

PEM Format Conversion

Currently, CDN only supports the certificate with a PEM format. Any non-PEM certificates are required to be converted to PEM format before being uploaded to Cloud Load Balance. It is recommended to use

openssl tool for the conversion. Here are some common methods for converting the certificate format to PEM format.

Converting DER to PEM

DER format generally occurs in Java platform.

Certificate conversion:

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

Private key conversion:

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

Converting P7B to PEM

P7B format generally occurs in Windows Server and Tomcat.

Certificate conversion:

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

Obtain [--- BEGIN CERTIFICATE ---, --- END CERTIFICATE ---] content in outcertificat.cer as a certificate for upload.

Private key conversion: no private key

Converting PFX to PEM

PFX format generally occurs in Windows Server.

Certificate conversion:

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

Private key conversion:

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

Completion of Certificate Chain

CA agency mainly provide the following three certificates: Apache, IIS, Nginx.

CDN uses **Nginx**. Select the certificates with an extension of .crt or .key under **Nginx** folder. A certificate of PEM format can be directly opened in text editor. You just need to copy and upload it.

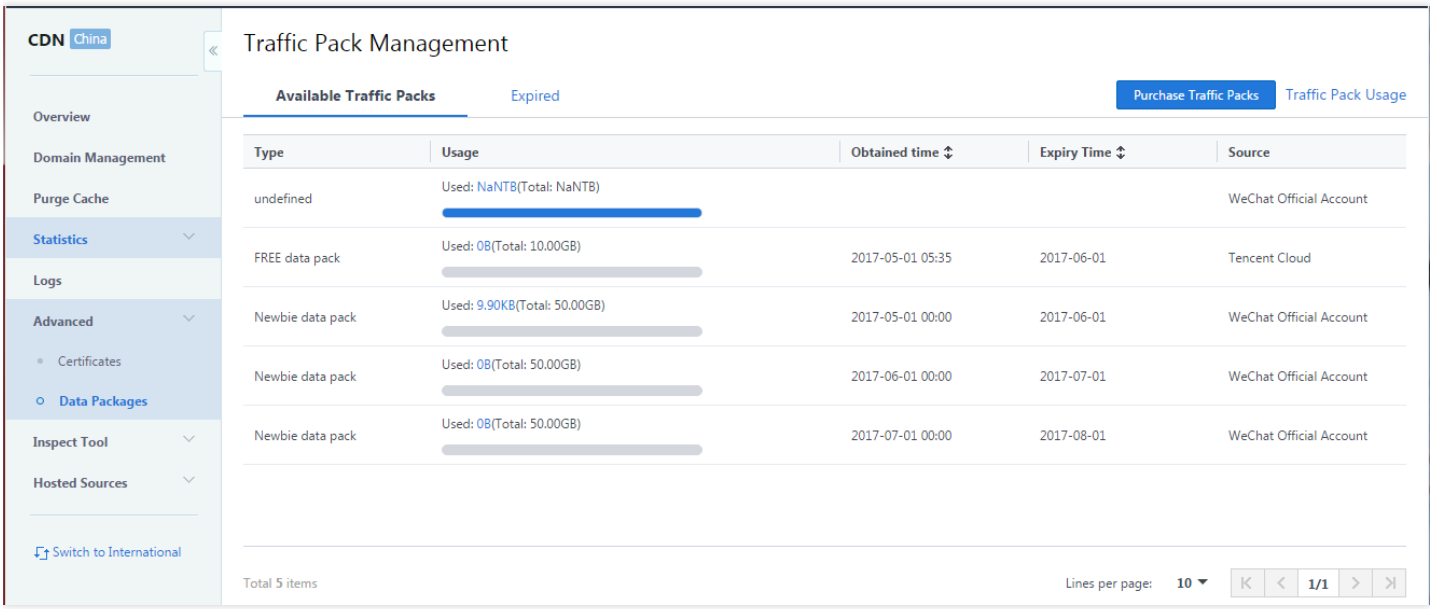
You can also complete the certificate chain by pasting the content of CA certificate (PEM format) to the bottom of domain certificate (PEM format).

Manage Traffic Packages

Last updated：2018-04-03 16:34:50

If your billing method is Pay by Traffic, you can purchase a traffic package for cost saving. You can check the usage of traffic package in CDN Console to keep track of the balance of traffic package in real time and top it up in time so that your use of CDN services will not be affected.

Log in to CDN Console and select **Advanced** page. You'll see the **Traffic Package Management** feature provided by CDN:



This page provides the history of purchase and usage of traffic packages.

Diagnosis Tools
Verify Tencent IP Tool

Last updated：2018-09-19 15:54:26

CDN 为您提供了节点 IP 归属查询工具。您可以通过本工具验证指定的 IP 是否为腾讯云 CDN 节点的 IP。

使用说明

登录 CDN 控制台，选择左侧【诊断工具】菜单中的【节点 IP 归属查询】。

在文本框中输入要查询的 IP，一行一个，最多可一次性查询 20 个。输入完成后，单击【验证】。若 IP 为 CDN 节点 IP，显示具体归属地。

若 IP 不是 CDN 节点 IP。则会显示归属地未知。

Self Troubleshooting Tool

Last updated：2018-06-07 19:15:05

Overview

CDN provides a self-diagnose tool that helps you perform self-inspection when you find that there is a problem while accessing a resource URL. The process of self-diagnose includes a series of inspection items such as checking the DNS resolution of connected domain, connection quality, the availability of sites and the consistency of data access, to help you locate the problem and provide solutions.

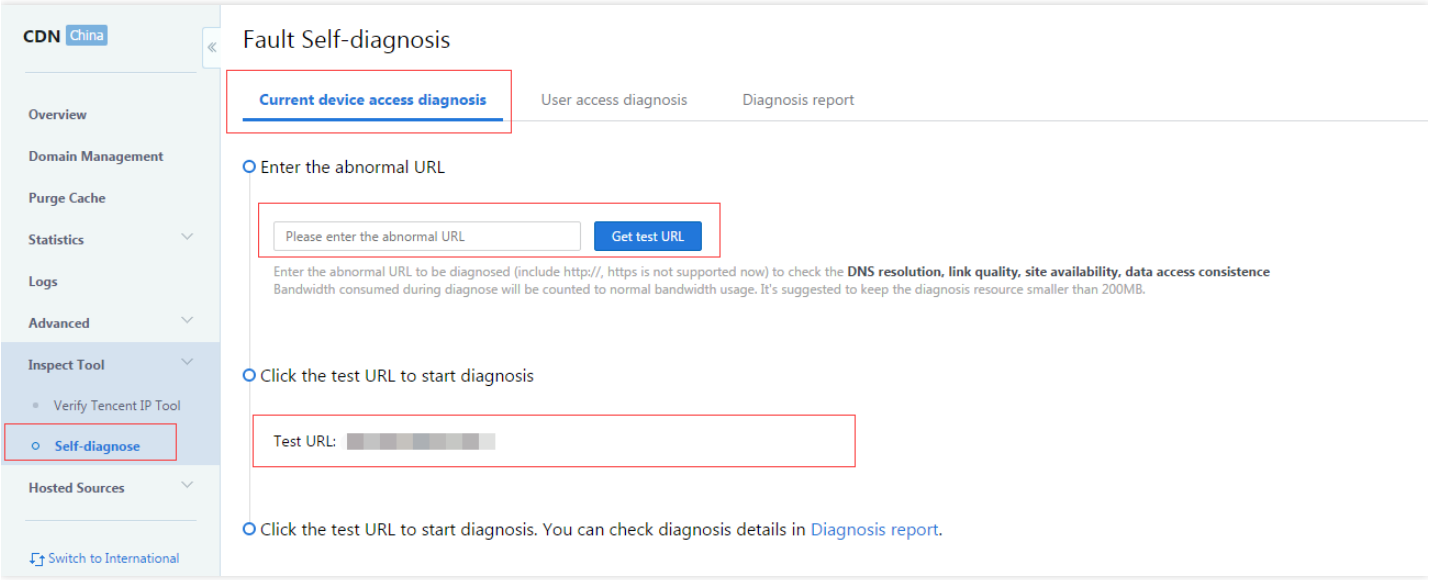
Note: The resource URL to be diagnosed must be an "Activated" domain under your account. The bandwidth generated during the diagnosis process will be calculated as billing bandwidth. It is suggested that the target resources to be diagnosed do not exceed 200MBytes.

Instructions

Current Device Access Diagnosis

You can initiate diagnosis through "Current device access diagnosis" when you find that there is a problem while accessing a resource. The procedure for current device access diagnosis is as follows:

1. From the console, go to Inspect Tool >> Self-diagnose page and select "Current device access diagnosis" tab;
2. Enter the resource URL to be diagnosed. Currently only URLs with the prefix "http://" are supported. Cannot diagnose URLs which start with "https" at this moment. Once the correct URL is entered, click "Get test URL", and a test address will be generated in the page;
3. Click the test address generated in step 2 to open the diagnosis page and start collecting diagnosis information. Please do not close the diagnosis page during the process, the page will close on its own when the process is completed;
4. After the diagnosis, you can go to "Diagnosis report" tab to review the results.



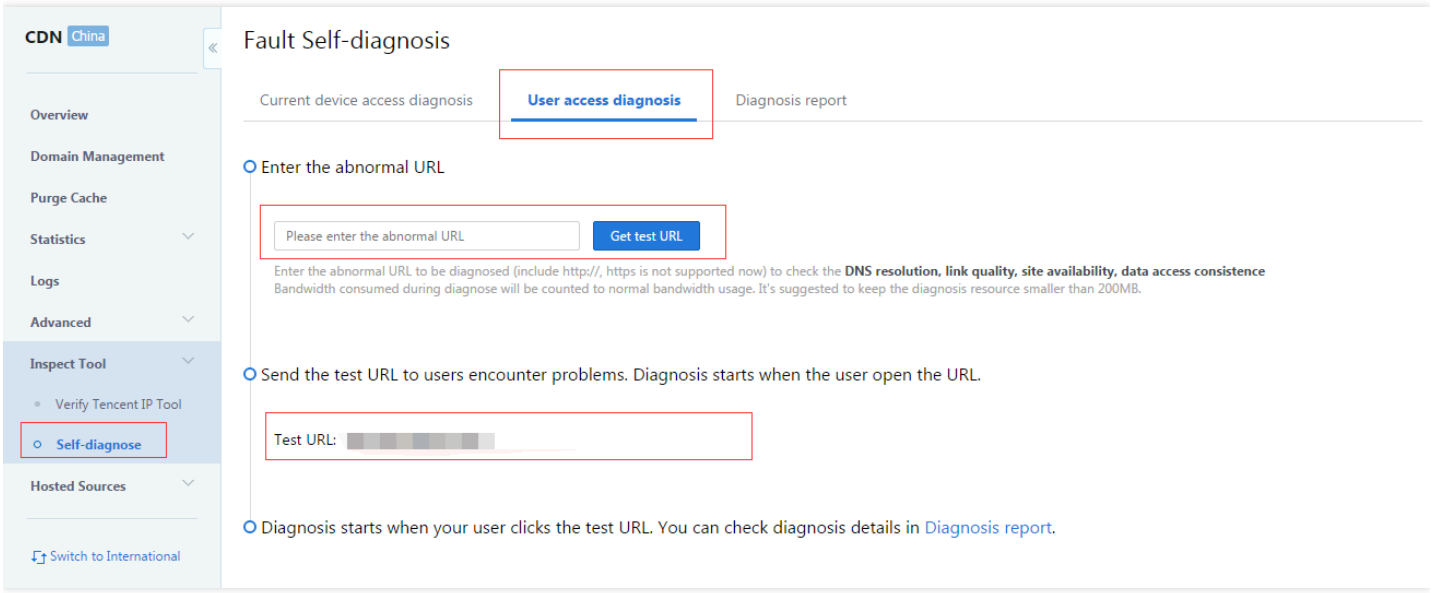
User Access Diagnosis

When a user reports that there is a problem while accessing resource, you can locate the problem using "User access diagnosis", and solve the problem through actions suggested by Tencent Cloud. The procedure for user access diagnosis is as follows:

1. From the console, go to Inspect Tool >> Self-diagnose page and select "User access diagnosis" tab;

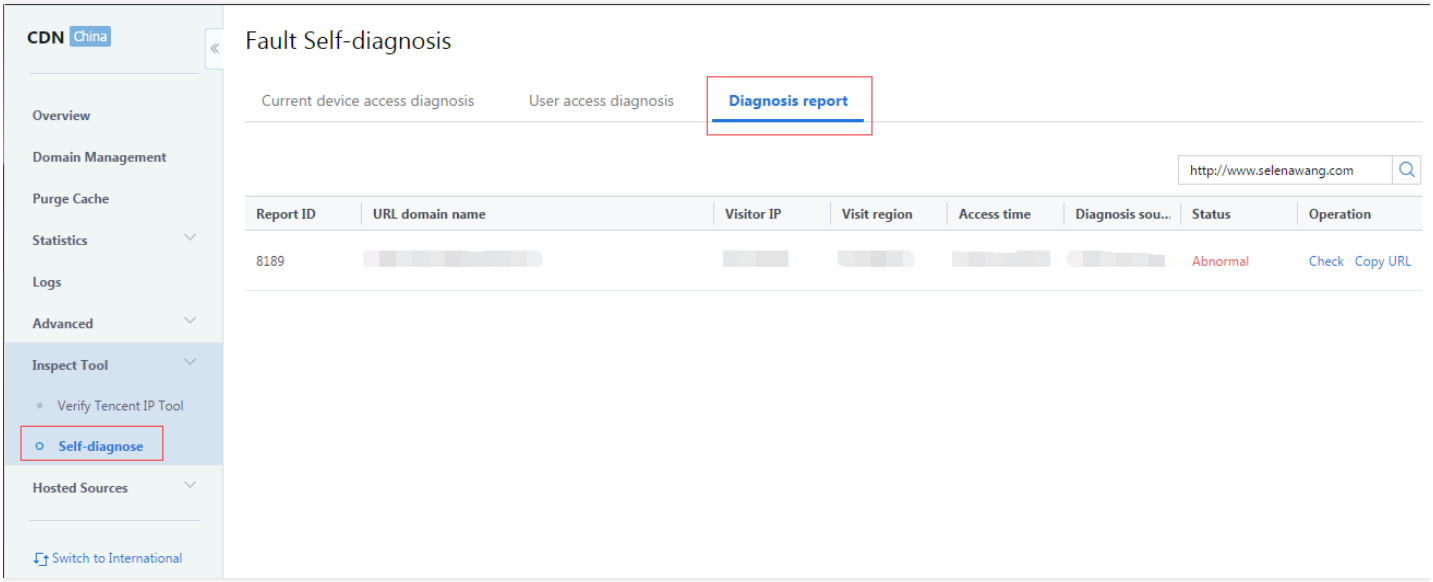
2. Enter the resource URL to be diagnosed. Currently only URLs with the prefix "http://" are supported. Cannot diagnose URLs which start with "https" at this moment. Once the correct URL is entered, click "Get test URL", and a test address will be generated in the page;

3. Send this test address to your user. Diagnosis information will be collected when your user opens the test URL. Please do not close the page during the process.
4. After the diagnosis, you can go to "Diagnosis report" tab to review the results that have been collected from the user.

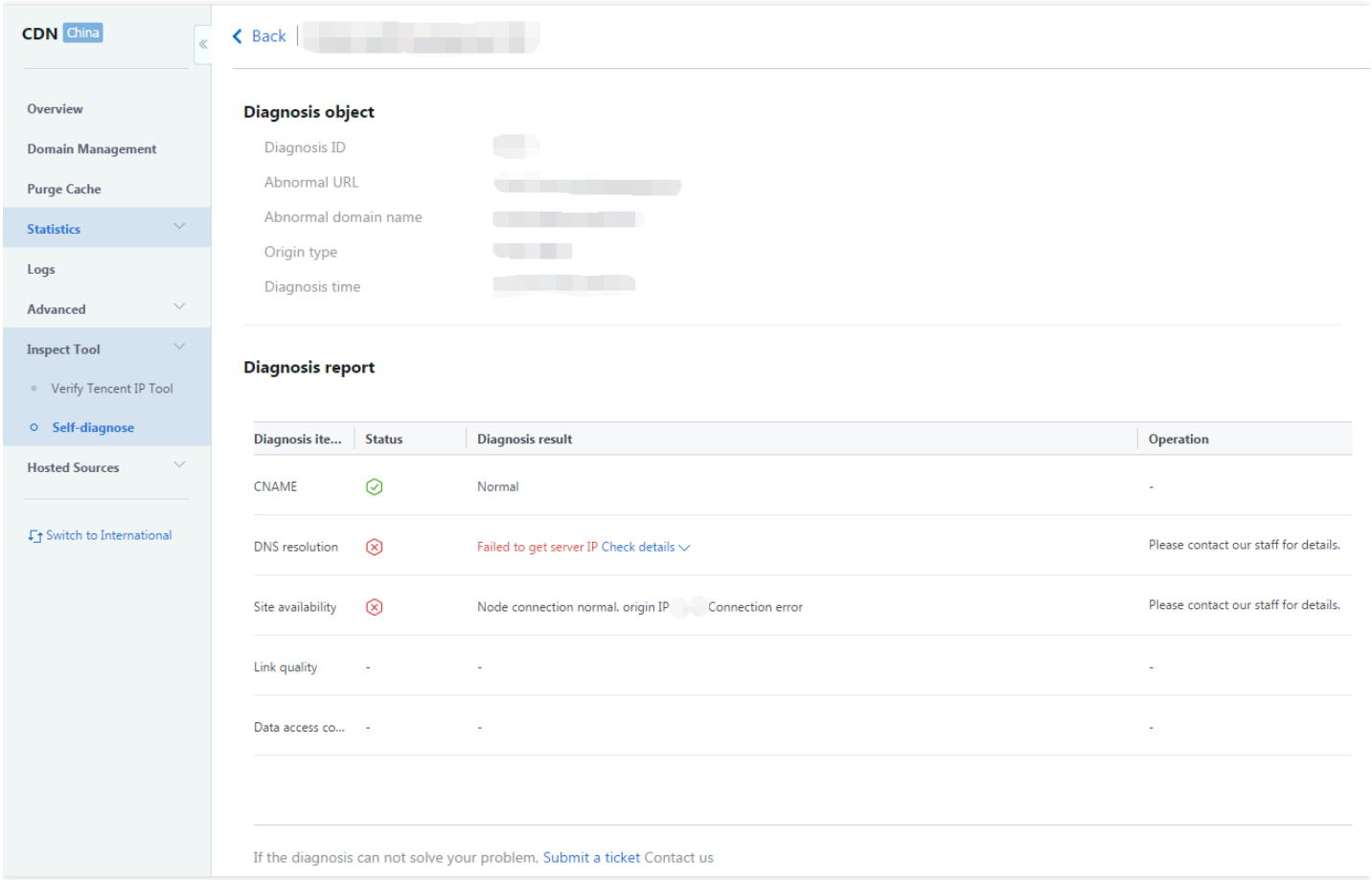


Reviewing the Diagnosis Report

From the console, go to Inspect Tool >> Self-diagnose page and select "Diagnosis report" tab to see a list of diagnosis reports. Diagnosis reports that have been generated will be presented in the page, sorted by time of creation.



You can click "Check" to view the details of the report.



The Report Details page is divided into two sections, "Diagnosis object" and "Diagnosis report":

Diagnosis object: Contains Diagnosis ID, abnormal URL, abnormal domain name, origin type information.
Diagnosis report: Contains diagnosis results about CNAME, DNS resolution, site availability, link quality, and data access consistency.

Item 1: CNAME

1. Normal: If the CNAME that is actually resolved from the diagnosis domain is consistent with the CNAME that should be deployed and resolved, the result will be "normal".
2. Abnormal CNAME Configuration: If the CNAME that is actually resolved from the diagnosis domain is not consistent with the CNAME that should be deployed and resolved, the result will be "abnormal". You can click "Check details" to review the CNAME that is actually resolved and the one that should be deployed and resolved as well as its CDN provider. Only one CNAME is presented in the details if multiple CNAMEs are actually resolved from the diagnosis domain. In this case, it is suggested that you change the CNAME configuration at the DNS service provider. If the CNAME configuration is abnormal, other diagnosis items will not be commenced.

Item 2: DNS Resolution

1. Normal: If the actual node accessed by the diagnosis domain is consistent with the optimal node, the result will be "normal". You can click "Check details" to review Client IP, Local DNS, IPs of the actual node and the optimal node, regions and ISP information
2. Non-optimal path: If the actual node accessed by the diagnosis domain is different from the optimal node, the result will be "non-optimal path". It is suggested that you contact Tencent Cloud technicians.
3. Failed to obtain node IP: Under circumstances such as when the IP of the diagnosis domain is hijacked, or the connection to the node failed, the diagnosis result will be "failed to obtain node IP". It is suggested that you contact Tencent Cloud technicians.

Item 3: Site availability

1. Normal: If the connections to the node and the origin server are normal, the diagnosis result will be "normal connections to node and origin server"
2. Abnormal: If the connections to the node or the origin server are abnormal, the diagnosis result will be "abnormal connection to node" or "abnormal connection to origin server" or "abnormal connection to both node and origin server". It is suggested that you contact Tencent Cloud technicians.

Item 4: Link quality

1. Normal: If the access to the diagnosis domain is normal, the diagnosis result will be "normal", and the total resource access latency will be presented. You can also click "Check details" to review details about the time spent within every part of the link.
2. Abormal: If the access to the diagnosis domain failed, the diagnosis result will be "abnormal". It is suggested that you contact Tencent Cloud technicians. If link quality is diagnosed as abnormal, data access consistency diagnosis will not be commenced.

Item 5: Data Access Consistency

1. Normal: If diagnosed resources can be normally accessed at the origin and the node plus they have the same MD5, the diagnosis result will be "normal". You can click "Check details" to review the information about the resources at origin server and node.
2. Abnormal origin server resource: If a status code such as 4XX, 5XX occurred when accessing resources at the origin server, or the MD5 values of resources on different origin servers are inconsistent, the diagnosis result will be "abnormal origin server resource". It is suggested to check the resources at the origin server. You can also click "Check details" to review more details about the resources at origin server and node.
3. Abnormal CDN resource: If resources at origin server are normal, but a status code of 4XX or 5XX was returned when accessing resources at the node, or the MD5 values of resources at origin and node are inconsistent, the diagnosis result will be "abnormal CDN resource". It is suggested that you contact

Tencent Cloud technicians. You can also click "Check details" to review more details about the resources at origin server and node.

If you're not able to solve the problem using the diagnosis report, we suggest that you submit a ticket, or contact Tencent Cloud technicians for troubleshooting.