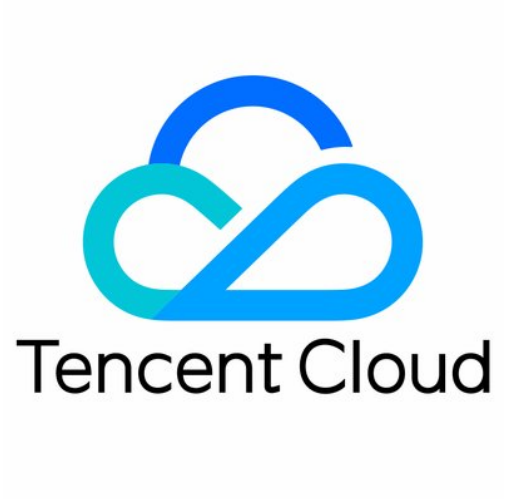
SSL Certificate Service

Domain Ownership Validation

Product Documentation



Contents

Domain Ownership Validation
DNS Validation

Last updated：2022-03-28 15:51:14

Overview

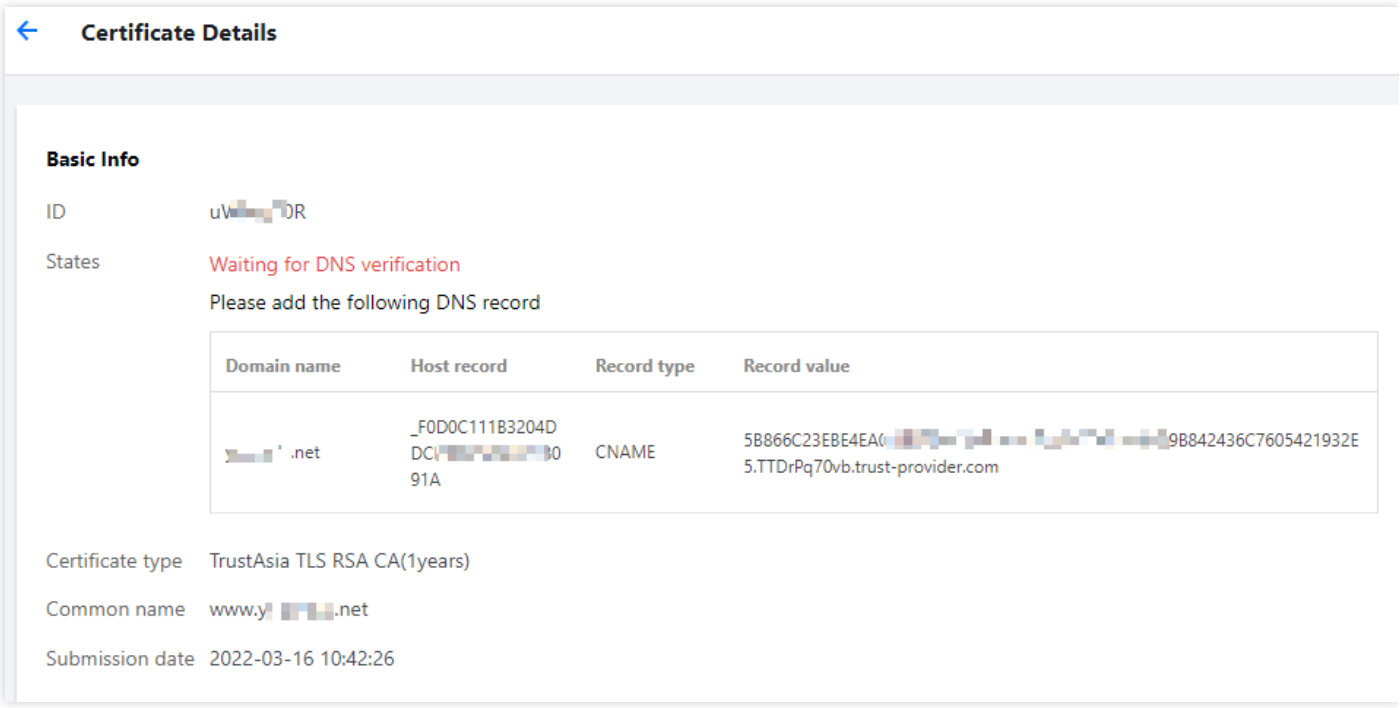
This document describes how to validate a domain when you apply for a certificate or add a domain in the certificate management console and the domain validation mode is DNS validation.

Directions

Step 1. View validation information

1. Log in to the SSL Certificate Service console.
2. Select a certificate in the **Validating** state. On the **Validate Domain** page displayed, obtain the host record and record value. See the figure below.

> Note：
> Take note of the host record and record value before you go to step 2 to add a DNS record.

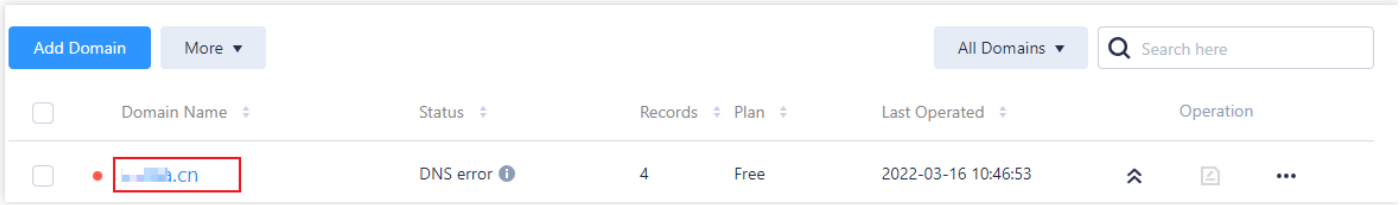


Step 2. Add a DNS record

Note：

The following operations apply only to domain names hosted with Tencent Cloud. For domain names hosted with other platforms, go to the corresponding **DNS service provider** for DNS. To query DNS service providers, go to DNS.TECH.

1. Obtain the host record and record value, which can be obtained on the **Validate Domain** page, as described in step 1.
2. Log in to the DNSPod console to view the domain name for which a certificate has been applied, and then click **DNS** in the **Operation** column to go to the **Record Management** page. See the figure below.

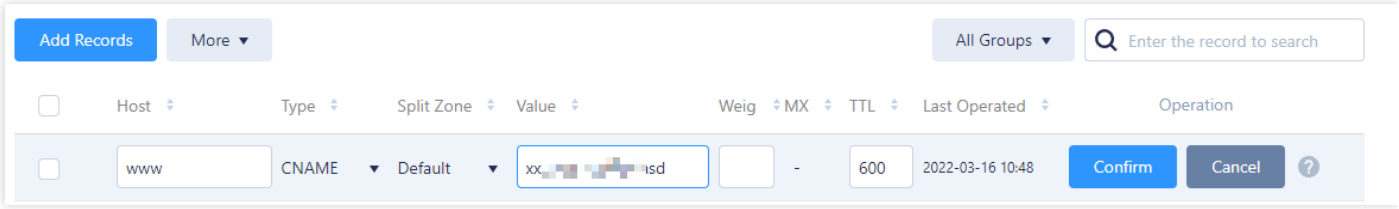


3. Click **Add Record** and add a DNS record depending on the certificate type.

Note：
Only the CNAME and TXT types of DNS records are supported, and they are applicable for certificates of different brands. Please select the DNS record type as needed.

- TrustAsia and WoTrus Certificates
- Certificates of Other Brands

For TrustAsia and WoTrus certificates, enter a DNS record of the CNAME type. See the figure below:



- **Host**: enter the host record obtained in step 1.
- **Type**: select **CNAME**.
- **Split Zone**: select **Default**. Otherwise, the corresponding CA will not be able to review the DNS record.
- **Value**: enter the record value obtained in step 1.
- **MX Priority**: leave it empty.
- **TTL**: it refers to the time to live. The smaller the value is, the less the time cost for record changes to take effect globally. The default value is 600 seconds.

4. Click **Save**.
5. After the record is added, the system periodically checks for the record value. If the record value is detected and matches the specified value, the domain ownership verification will be completed. Please wait for the CA's review.

Note：

- DNS usually takes effect within **10 minutes to 24 hours**. The actual time depends on the ISP refresh time.
- After the certificate is issued or the domain name information is approved, you can manually clear the DNS record.

File Validation

Last updated：2022-09-14 17:27:10

Overview

This document describes how to validate a domain when you apply for a certificate or add a domain in the SSL Certificate Service console and the domain validation mode is file validation.

Validation Rules

Domain validation rules

During file validation, pay attention to the following:

Note：

- Due to changes of the policies for SSL certificate domain validation, Tencent Cloud discontinued the file validation mode for wildcard certificates on **November 21, 2021**. For more information, see Domain Ownership Validation Policy Update.
- If the domain that you apply for is a primary domain, **www** must also be validated. For example, if the domain applied for is `tencent.com`, `www.tencent.com` must also be validated.
- If the domain that you apply for contains **www**, the domain name following **www** must also be validated, regardless of the domain levels. For example, if the target domain is `www.a.tencent.com`, `a.tencent.com` must also be validated.
- If the domain that you apply for does not contain **www** and is not a primary domain, only the current domain needs to be validated. For example, if the target domain is `cloud.tencent.com`, only `cloud.tencent.com` needs to be validated.

CA validation rules

- During DNS query, you must recursively query the authoritative NS server of each domain on the authoritative root server, and then query the corresponding A, AAAA, or CNAME records from the NS server.
- If the DNS service supports DNSSEC, you must verify the signing information of the response data.
- If the queried domain is an IP address, verify the content via IP access.
- The standard HTTP/HTTPS default port must be adopted for access.

- Up to two 301/302 redirections are supported. The redirection destination IP and the validated domain must be in the same primary domain.
- In the final validation result, the status code 200 must be returned.
- For HTTPS access, certificate errors can be ignored.

Directions

Step 1. View validation information

1. Log in to the SSL Certificate Service console.
2. Select a certificate in the **Validating** state. On the **Validate Domain** page displayed, follow instructions on the page to complete validation within a specific period of time.

Step 2. Add a file record

1. Log in to the server and make sure that the domain name points to the server and the corresponding website is enabled.

> Note：
> If your **DNS Service Provider** is Tencent Cloud, for how to point the domain to your server, see A Record.

2. Create the specified file in the root directory of the website, including the file directory, name, and content.

> Note：
> - The website root directory refers to the folder where you store the website programs on the server. Its name may be `wwwroot`, `htdocs`, `public_html`, or `webroot`.
> - Ensure that the website port is set to 80 or 443.

- **Example**
  The root directory of your website is `C:/inetpub/wwwroot`. You can create a file as shown in the following table in the `wwwroot` folder.

File Directory	File Name	File Content
/.well-known/pki-validation	The file content shown on the validation page. Example: A32CF****7EEtrust-provider.comTT**bu6	201908060**alzeo

- **Note**
  - The above is for reference only, and both the filename and content are random values. The values shown on your validation page shall prevail.
  - On Windows, you need to create a file and folder that begin with a dot by running commands.
    For example, to create a `.well-known` folder, open a command prompt window and execute the command `mkdir .well-known` to create it. See the following figure.

3. On the **Validate Domain** page, you can click **View Domain Ownership Validation Status** to check whether the configuration is successful.

> Note：
>
> - Both HTTP and HTTPS are supported, and either can be accessed.
> - File verification does not support any redirection. Instead, it directly returns the status code 200 and file content.
> - For a domain name starting with "www", such as `www.a.tencent.com`, file validation is required for the domain name itself as well as `a.tencent.com`.

4. Wait for the CA's review. After the certificate is issued or the domain name information is approved, the file and directory can be cleared.

Automatic File Validation

Last updated：2021-12-27 12:30:04

Overview

This document describes how to validate a domain when you apply for a certificate or add a domain in the certificate management console and the domain validation mode is automatic file validation.

Note：
Automatic file validation applies only to multi-year international standard certificates and non-wildcard certificates.

Validation Rules

Domain name validation rules

During automatic file validation, pay attention to the following:

Note：

- Due to SSL certificate domain validation policy changes, Tencent Cloud discontinued the file validation mode for wildcard certificates on **November 21, 2021**. For more information, please see Domain Validation Policy Update.
- If the domain that you apply for is a primary domain, **www** must also be validated. For example, if the domain applied for is `tencent.com`, `www.tencent.com` must also be validated.
- If the domain that you apply for contains **www**, the domain name following **www** must also be validated, regardless of the domain levels. For example, if the domain applied for is `www.a.tencent.com`, `a.tencent.com` must also be validated.
- If the domain that you apply for does not contain **www** and is not a primary domain, only the current domain needs to be validated. For example, if the domain applied for is `cloud.tencent.com`, only `cloud.tencent.com` needs to be validated.

CA validation rules

- During DNS query, you must recursively query the authoritative NS server of each domain on the authoritative root server, and then query the corresponding A, AAAA, or CNAME records from the NS server.
- If the DNS service supports DNSSEC, you must verify the signing information of the response data.
- If the queried domain is an IP address, verify the content via IP access.
- The standard HTTP/HTTPS default port must be adopted for access.
- Up to two 301/302 redirections are supported. The redirection destination IP and the validated domain must be in the same primary domain.
- In the final validation result, the status code 200 must be returned.
- For HTTPS access, certificate errors can be ignored.

Directions

Step 1. View validation information

1. Log in to the SSL Certificate Service console. In the left sidebar, click **My Profile** to go to the **My Profile** page.

2. On the **My Profile** page, click the name of the organization for which domain information is to be validated. Then you can view the information of administrators that have been applied for.

3. Click the name of the administrator whose domain information is to be validated. The **Review Information** page is displayed.

4. Click the **Domain Information* tab, select the domain to be validated, and click **View Validation**.

5. On the **Validate Domain** page, follow the instructions on the page to complete validation within a specific period of time.

Step 2. Add file validation

1. Log in to the server and ensure that the A record is added for your domain and the A record points to the server.

> Note：
> If your domain name is hosted with Tencent Cloud, point the domain name to your server. For more information, please see **A Record**.

2. Start a web service on the server (or use the web service where the business is running), listen on port 80 or 443, and set the reverse proxy address of the file validation path to the reverse proxy address provided in **Step 1: View**

validation information (as shown in the figure in substep 5 in step 1).

Tencent Cloud provides the following web service configuration guidelines for your reference:

- NGINX reverse proxy configuration
- Apache reverse proxy configuration

Note：

- Both HTTP and HTTPS are supported, and either can be accessed.
- A configured reverse proxy cannot be deleted or modified. After being deleted or modified, a reverse proxy becomes invalid.
- Up to two 301/302 redirections are supported. The redirection destination IP and the validated domain must be in the same primary domain. For a domain name starting with "www", such as `www.a.tencent.com`, file validation is required for the domain name itself as well as `a.tencent.com`.

3. After configuring the reverse proxy, wait for the CA to complete the file validation. After the file validation is passed, the domain is approved.
4. On the **Validate Domain** page, you can click **Validate** to validate the domain configuration.