Cloud Certificate Manager

Best Practices

Issue	01
Date	2021-03-01

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Pushing Certificates to WAF

1.1 Scenario

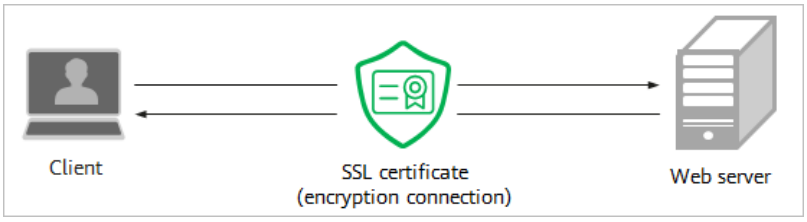
This document provides guidance for you to implement HTTPS on websites, monitor HTTPS service traffic, identify and block attacks, such as SQL injection and CC attacks, and protect web services.

Assume that you have a website with the domain name www.example.com, and that you need to apply for an SSL certificate and use the purchased WAF to monitor HTTPS service traffic. This document describes how to apply for a certificate and enable WAF to monitor HTTPS service traffic in this scenario.

Working Principles of an SSL Certificate

An SSL certificate is used in establishing encryption channels between the web server and browser and between the web server and client. The HTTPS protocol is enabled by configuring and applying SSL certificates to ensure the security of data transmission over Internet.

Figure 1-1 Working principles of an SSL certificate

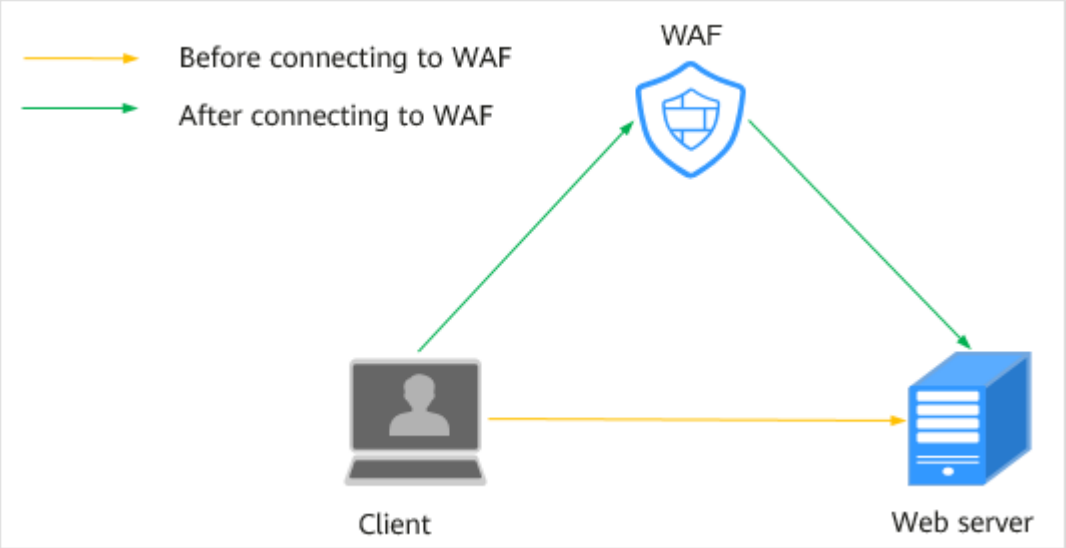


WAF Configuration Principles

WAF is designed to keep web applications stable and secure. It examines all HTTPS requests to detect and block attacks, such as Structure Query Language (SQL) injections, cross-site scripting (XSS), webshell upload, command or code injections, file inclusion, sensitive file access, third-party vulnerability exploits, CC attacks, malicious crawlers, and cross-site request forgery (CSRF).

This section describes how to perform the configuration when no proxy is used between the client and WAF. If a proxy is used between the client and WAF, perform the configuration based on the **WAF documentation**.

Figure 1-2 No proxy used



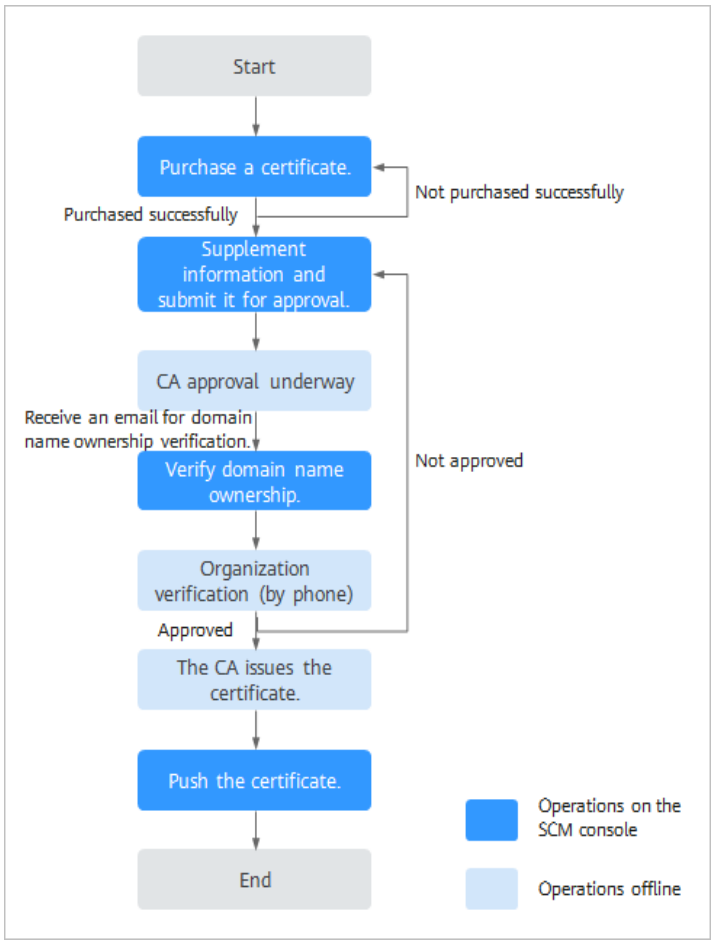
- DNS resolves your domain name to the origin server IP address before your website is connected to WAF. Therefore, web visitors can directly access the server.
- After your website is connected to WAF, DNS resolves your domain name to the CNAME record of WAF. In this way, the traffic passes through WAF. WAF then filters out illegitimate traffic and only routes legitimate traffic back to the origin server.

1.2 Applying for and Pushing a Certificate

You need to apply for a certificate on the SCM console and push the certificate to WAF after the certificate application is complete.

Figure 1-3 shows the process of applying for and pushing a certificate.

Figure 1-3 Applying for and pushing a certificate



NOTE

- Verification of the domain name ownership
  - If you are managing your domain name on HUAWEI CLOUD, verify the domain name ownership using Domain Name Service (DNS) on HUAWEI CLOUD.
  - If you are managing your domain name on another domain management platform, verify the domain name ownership on the corresponding platform.
- Organization verification (required only for OV and EV certificates)

  The CA will contact the public phone number of the organization to check whether the organization has initiated the certificate application.

This section describes how to verify domain names on the HUAWEI CLOUD management platform.

Procedure

This section describes only the operations that need to be performed on the HUAWEI CLOUD console.

1. Purchasing a certificate: You need to purchase a certificate based on your domain name type. For details, see **Purchasing a Certificate**.

2. Applying for a certificate: After a certificate is purchased, you need to apply for the certificate and submit it for approval. For details, see **Applying for a Certificate**.
3. Verifying a domain name: After the certificate application is submitted, the CA sends an email to your mailbox. You need to verify the domain name. For details, see **Verifying the Domain Name**.
4. Verifying an organization: If you apply for an OV or EV certificate, the CA sends an organization verification email to your email address after domain name verification is complete. The CA contacts the enterprise or organization based on the selected verification method to check whether the enterprise or organization has initiated the certificate application. For details, see **Verifying the Organization**.
5. **Pushing the Certificate**.

Pushing the Certificate

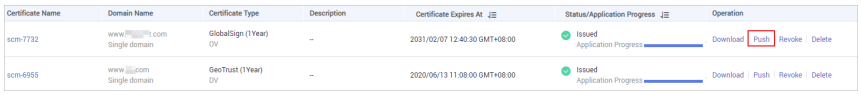
Step 1 Log in to the **management console**.

Step 2 In the navigation pane on the left, click ☰ and choose **Cloud Certificate Management Service** under **Security & Compliance**.

Step 3 In the navigation pane on the left, choose **Certificate Manager** > **SSL Certificate**.

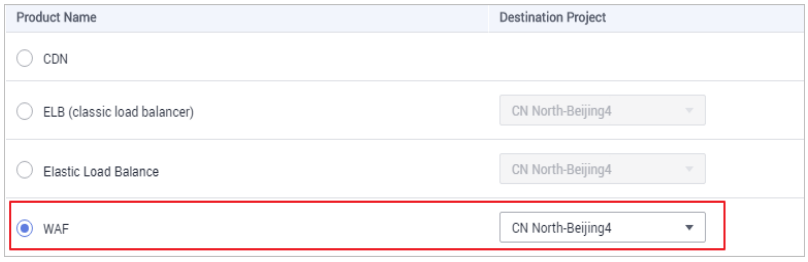
Step 4 In the **Operation** column of the certificate to be pushed, click **Push** to go to the certificate push details page.

Figure 1-4 Pushing a certificate



Step 5 Select WAF and click ▼ on the right of the target project and select the target region.

Figure 1-5 Selecting a region



Step 6 Click **Push Certificate** at the lower right corner of the page.

If a message indicating that the certificate is successfully pushed is displayed, the SSL certificate is successfully pushed to the target service.

You need to further configure the certificate on the console of the service to enable HTTPS for it.

Step 7 In the displayed dialog box, click **Configure Now**. The WAF management page is displayed.

You can also click **Continue Pushing** or ✕ in the upper right corner of the page. The certificate push page or SSL certificate management page is displayed. You can then access the WAF page to perform the configuration.

----End

1.3 Adding a Domain Name to be Protected or Updating a Certificate

After the certificate is successfully pushed, you need to select HTTPS in WAF and select the pushed certificate.

This section describes how to add a domain name or update a certificate in WAF.

Guide descriptions:

- **Adding a Domain Name**: If your domain name has not been added to WAF, perform the operations in this topic. For details, see **Adding a Domain Name**.
- **Updating a Certificate**: If your domain names have been added to WAF (the added domain names correspond to the domain names associated with the certificate) and **Client Protocol** is set to **HTTPS**, you can replace the certificate with the pushed certificate based on the instructions in this topic.

Adding a Domain Name

If you have not added your domain name to WAF, perform the operations in this topic.

Prerequisites

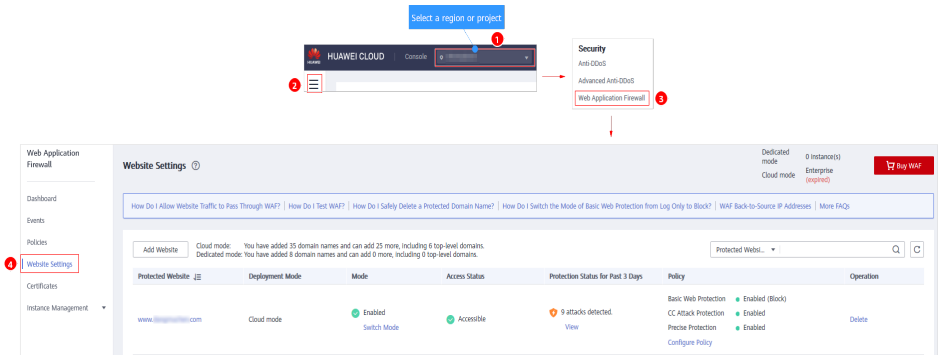
- You have obtained an account and its password for logging in to the management console.
- The certificate has been pushed.
- You have purchased WAF. If you have not purchased WAF, purchase it based on the instructions in **Buying WAF**.

Procedure

Step 1 (Optional) **Log in to the management console**.

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 1-6**.

Figure 1-6 Access to the Website Settings page

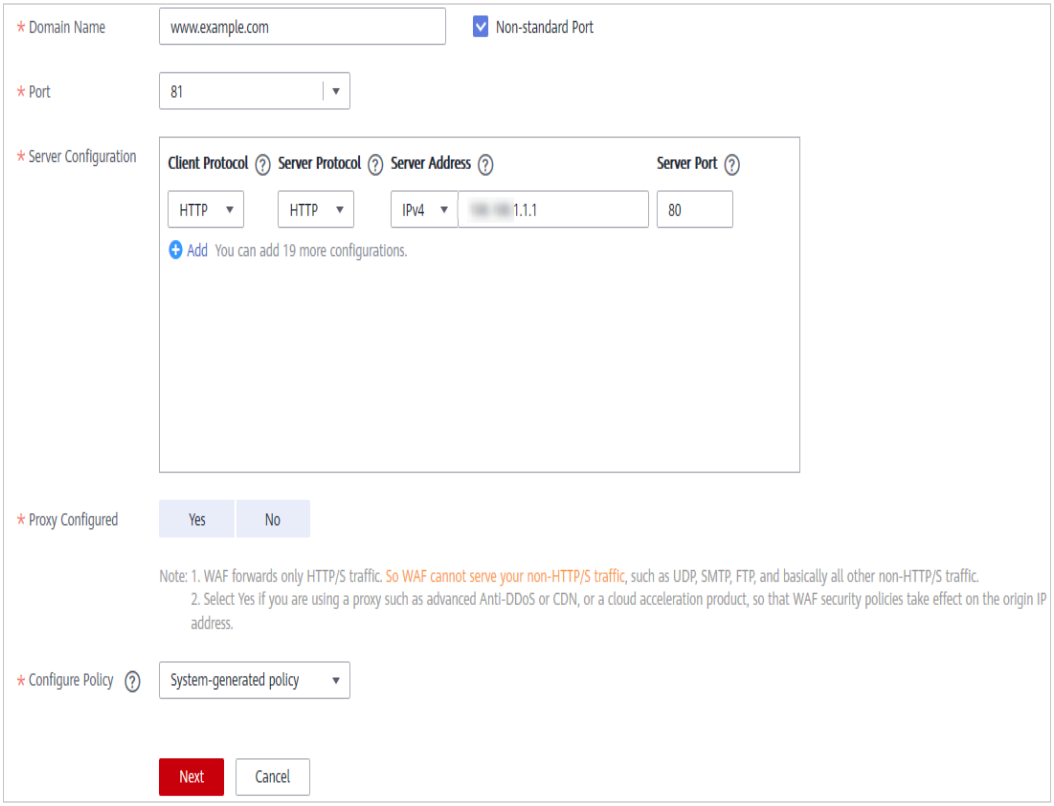


Step 3 In the navigation pane, choose **Website Settings**.

Step 4 In the upper left corner of the website list, click **Add Website**.

Step 5 Select **Cloud mode** and configure basic domain name information. **Figure 1-7** shows an example.

Figure 1-7 Configuring basic settings



- **Domain Name**: Enter the domain name associated with the certificate.
- **Port**: Set this parameter only if **Non-standard Port** is selected.

  If **Client Protocol** is set to **HTTPS**, WAF protects services of the standard port 443 by default.

  To configure a port other than port 443, select **Non-standard Port** and select a non-standard port from the **Port** drop-down list.
- **Server Configuration**: configuration of a web server address. The configuration contains the client protocol, server protocol, server address, and server port.

  Set **Client Protocol** to **HTTPS**.
- **Certificate Name**: Click and select a pushed certificate.
- **Proxy Configured**: A website that accessed WAF has used proxies, such as CDN and cloud acceleration.

  The default value is **No**.
- **Configure Policy**: **System-generated policy** is selected by default.

For details, see **Adding a Domain Name**.

Step 6 Click **Next**.

You are advised to click **Next** and then click **Finish** to skip this step. You can connect the domain name to WAF later by referring to **Testing WAF** and **Connecting a Domain Name to WAF**

Step 7 Click **Next** and then **Finish**.

----End

Updating a Certificate

If your domain names have been added to WAF (the added domain names correspond to the domain names associated with the certificate) and **Client Protocol** is set to **HTTPS**, you can replace the certificate with the pushed certificate based on the instructions in this topic.

Prerequisites

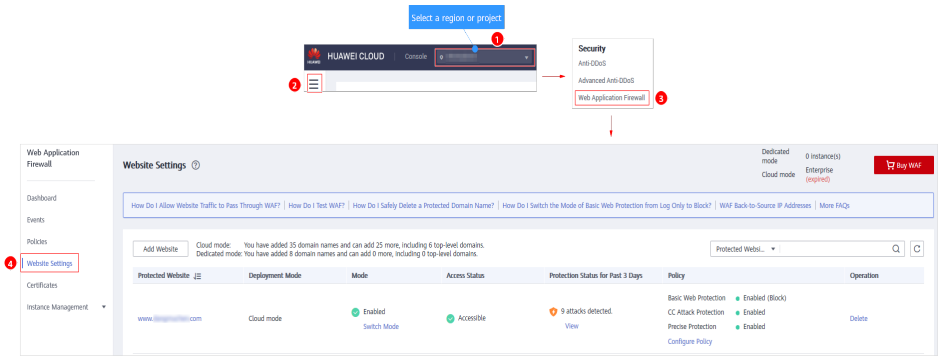
- You have obtained an account and its password for logging in to the management console.
- The certificate has been pushed.
- You have purchased WAF. If you have not purchased WAF, purchase it based on the instructions in **Buying WAF**.
- The protected domain names have been added to WAF, and the protected domain names correspond to the certificate domain names.
- **Client Protocol** is set to **HTTPS**.

Procedure

Step 1 (Optional) **Log in to the management console**.

Step 2 Go to the **Website Settings** page by following the steps shown in **Figure 1-8**.

Figure 1-8 Access to the Website Settings page



Step 3 In the **Protected Website** column, click the domain name of the website to go to the basic information page.

Step 4 Click next to the target certificate name. In the displayed dialog box, select the pushed certificate.

Step 5 Click **OK**. Your certificate is updated.

----End

2 Verifying Domain Ownership by Resolving the DNS TXT Record - SCM

After applying for an SSL certificate, you need to perform domain name verification. This topic describes how to verify your domain name ownership by DNS.

Background

After you apply for an SSL certificate from a CA, you are required to verify the domain name ownership. You need to work with the CA to complete the domain name ownership verification. After your ownership of the domain name is verified by you and approved by the CA, the status of your certificate will change.

If you do not complete the domain ownership verification, your certificate will remain in the **Pending domain name verification** state.

Domain name ownership verification by DNS is to verify domain ownership by resolving a specific DNS record on the platform hosting the domain name. When you apply for a certificate and select **DNS** for **Domain Name Verification Method**, follow the instructions in this part to complete the verification.

Procedure

Step 1 Obtain the host record and record value of a certificate. For details, see **Obtaining the Host Record and Record Value of a Certificate**.

Step 2 Perform domain name ownership verification by DNS.

Domain name ownership verification by DNS is to resolve DNS records, which can be performed only on the domain name management platform that hosts your domain name. The following examples are for your reference.

- If your domain name is hosted in the DNS service on HUAWEI CLOUD, complete the TXT resolution by following the instructions in **HUAWEI CLOUD DNS TXT Resolution**.
- If your domain name is hosted in the DNS service on Tencent Cloud, complete the TXT resolution by following the instructions in **Tencent Cloud DNS TXT Resolution**.

- If your domain name is hosted in the DNS service on Alibaba Cloud, complete the TXT resolution by following the instructions in **Alibaba Cloud DNS TXT Resolution**.

Step 3 Check whether the ownership verification takes effect. For details, see **Verifying DNS Configurations**.

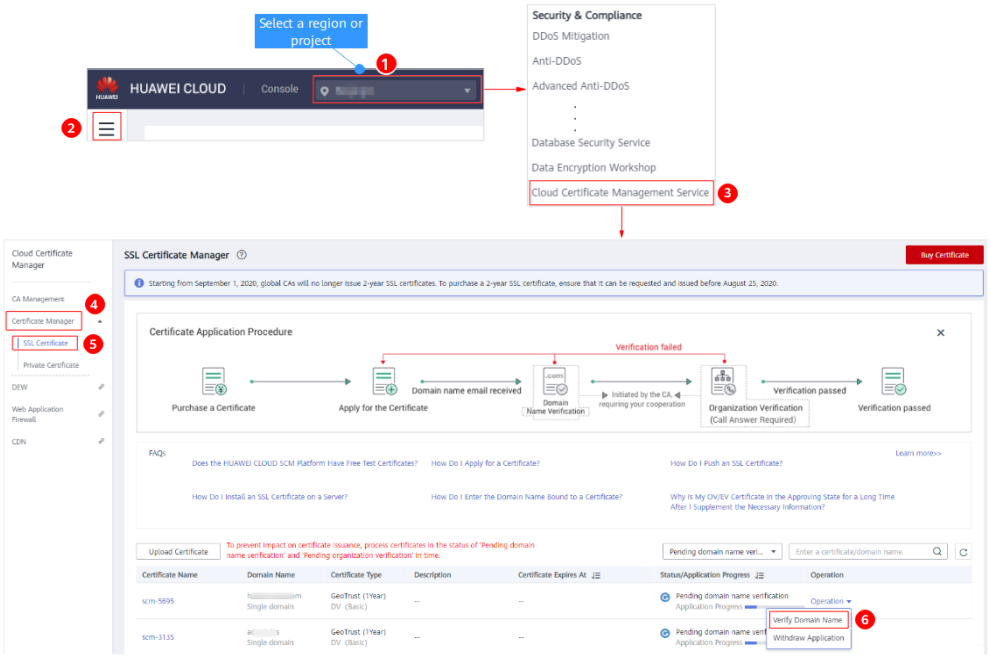
----End

Obtaining the Host Record and Record Value of a Certificate

Step 1 Log in to the **management console**.

Step 2 Go to the domain name verification page by following the steps in **Figure 2-1**.

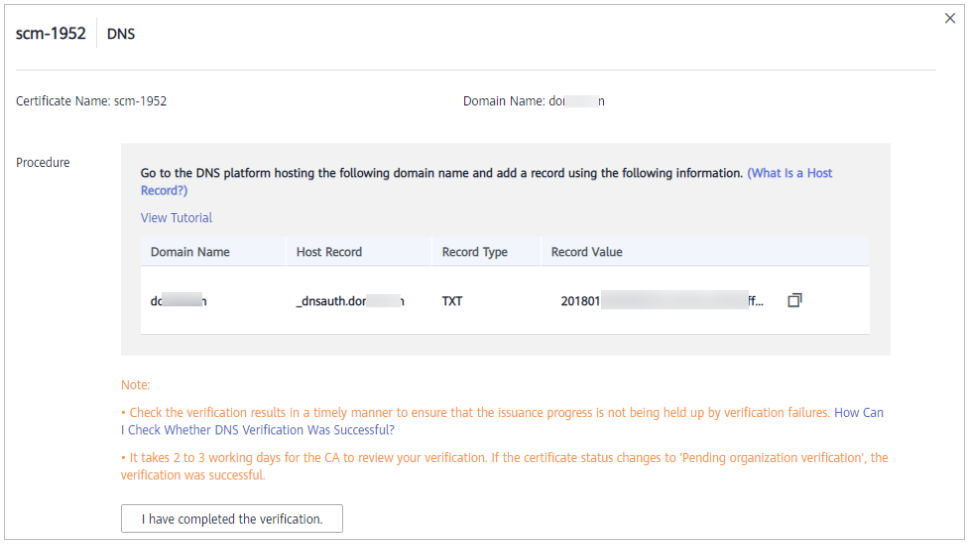
Figure 2-1 Accessing the domain name verification page



Step 3 On the **Verify Domain Name** page, view the values for **Host Record**, **Record Type**, and **Record Value**. **Figure 2-2** shows an example.

If **Host Record**, **Record Type**, and **Record Value** are not displayed, log in to the mailbox to view. The mailbox is the one you provide during certificate application.

Figure 2-2 Viewing a host record



----End

HUAWEI CLOUD DNS TXT Resolution

Refer to this part if you are managing your domain name on HUAWEI CLOUD.

Step 1 Log in to the **management console**.

Step 2 Choose **Domain Name Service** under **Network** to go to the **Domain Name Service** page.

Step 3 In the navigation pane on the left, choose **DNS Resolution** > **Public Zones**.

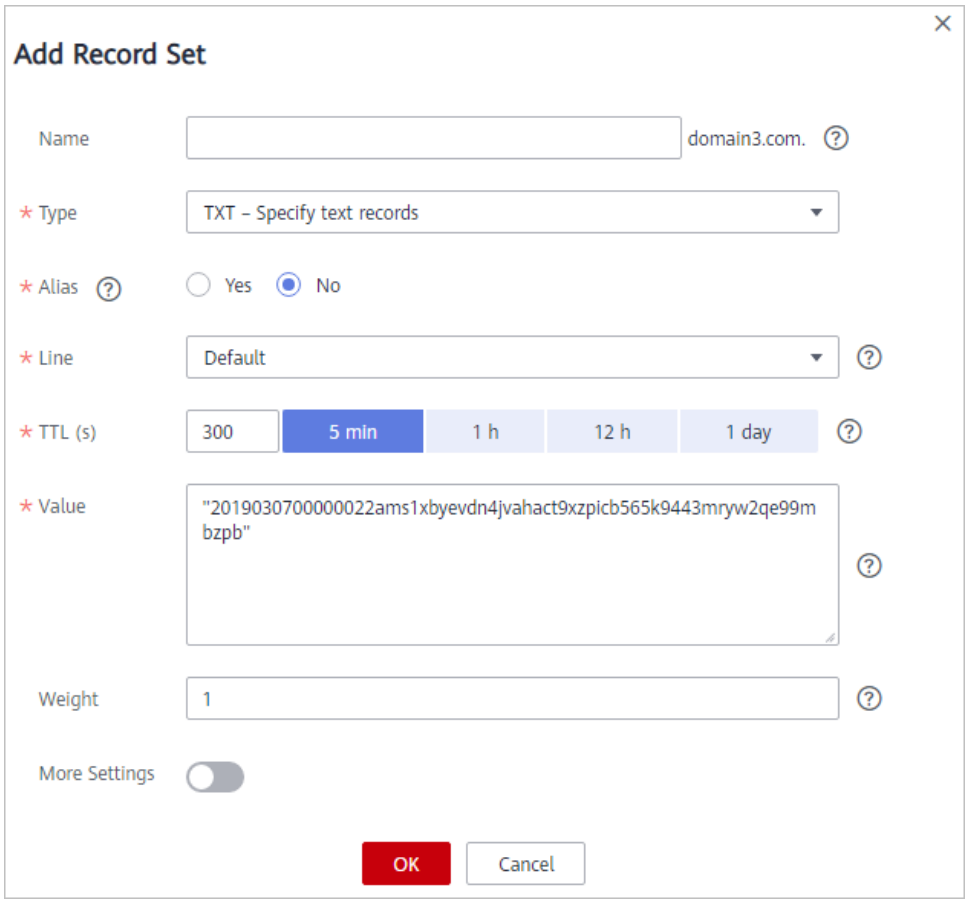
Step 4 In the domain name list on the **Public Zones** page, click the added domain name (or the primary domain name for a multi-domain certificate) to go to the record set page.

Step 5 In the upper right corner of the page, click **Add Record Set**. **Figure 2-3** shows an example.

NOTE

If there is a TXT record of domain name **domain3.com** in the domain name list, click **Modify** in the **Operation** column. Modify the record in the displayed **Modify Record Set** dialog box.

Figure 2-3 Adding a record set



- **Name**: Enter the prefix of the host record returned by the domain name service provider on the domain name verification page.

  The returned host record varies depending on the domain name service provider. The following are two examples:

  Example:

  - If the host record returned by the domain name service provider is **_dnsauth.domain3.com**, set **Name** to **_dnsauth**.
  - If the host record returned by the domain name service provider is **domain3.com**, leave **Name** empty.
- **Type**: Select **TXT – Specify text records**.
- **Line**: Select **Default**.
- **TTL (s)**: The recommended value is **5 min**. A larger TTL value will make it slower for synchronization and update of DNS records.
- **Value**: Enter the record value returned by the domain name service provider on the domain ownership verification page.

  NOTE

  Record values must be quoted with quotation marks and then pasted in the text box.
- Keep other settings unchanged.

Step 6 Click **OK**.

If the status of the record set is **Normal**, the record set is added successfully.

NOTE

- DNS configuration records can be deleted only after the certificate is issued or revoked.
- Check whether the DNS record is correctly configured. If not, the certificate cannot be issued.

Step 7 After the verification is complete, additional time is required for the CA to verify your domain name. During this period, the certificate is in the **Pending domain name verification** state.

The certificate enters the **Pending organization verification** state only after the CA has confirmed your domain ownership.

----End

Tencent Cloud DNS TXT Resolution

If your domain name is hosted in Tencent Cloud, you need to add a TXT record through the Tencent Cloud DNS console to complete the verification.

Step 1 Log in to the Tencent Cloud DNS console.

Step 2 In the zone list, locate the zone for which you want to configure a TXT record and click **Resolve** in the **Operation** column.

Step 3 Click **Add Record** and provide the following information:

- **Host**: Enter the prefix of the host record obtained in **Obtaining the Host Record and Record Value of a Certificate**.

  The returned host record varies depending on the domain name service provider. The following are two examples:

  Example:

  - If the host record returned by the domain name service provider is **_dnsauth.domain.com**, set **Host** to **_dnsauth**.
  - If the host record returned by the domain name service provider is **domain.com**, set **Host** to **@**.
- **Type**: Select **TXT**.
- **Line**: Select **Default**. You must specify an ISP line. Otherwise, your domain name may become inaccessible to some users.
- **Value**: TXT record from the SCM console. To obtain the record, refer to **Obtaining the Host Record and Record Value of a Certificate**.
- **MX Priority**: You do not need to set this parameter.
- **TTL**: cache time. The smaller the value, the faster the modification takes effect. The default value is 600 seconds.

Step 4 Click **OK**.

----End

Alibaba Cloud DNS TXT Resolution

If your domain name is hosted in Alibaba Cloud, you need to add a TXT record through the Alibaba Cloud DNS console to complete the verification.

Step 1 Log in to the Alibaba Cloud DNS console.

Step 2 On the **Manage DNS** page, click the **Domains** tab and click the name of the domain name for which you want to configure a TXT record.

Step 3 Click **Add Record** and provide the following information:

- **Type**: Select **TXT**.
- **Host**: Enter the prefix of the host record obtained in **Obtaining the Host Record and Record Value of a Certificate**.

  The returned host record varies depending on the domain name service provider. The following are two examples:

  Example:

  – If the host record returned by the domain name service provider is **_dnsauth.domain.com**, set **Host** to **_dnsauth**.

  – If the host record returned by the domain name service provider is **domain.com**, set **Host** to **@**.
- **ISP line**: Select **Default**. You must specify an ISP line. Otherwise, your domain name may become inaccessible to some users.
- **Value**: TXT record from the SCM console. To obtain the record, refer to **Obtaining the Host Record and Record Value of a Certificate**.
- **TTL**: cache time. The smaller the value, the faster the modification takes effect. The default value is 600 seconds.

Step 4 Click **OK**.

----End

Verifying DNS Configurations

Select a command based on your operating system and check whether the DNS configuration takes effect.

Use TXT record **_dnsauth.domain.com** as an example.

- For Windows OSs:
  ```
  nslookup -q=TXT _dnsauth.domain.com
  ```
- For Linux OSs:
  ```
  dig TXT _dnsauth.domain.com
  ```
- For macOS OSs:
  ```
  dig TXT _dnsauth.domain.com
  ```

If the value recorded in the command output (value of **text**) is the same as that returned by the domain name service provider, the configuration of domain name ownership verification has taken effect.

A Change History

Released On	Description
2021-03-01	This issue is the first official release.

