SSL Certificate Service

Troubleshooting

Product Documentation

Copyright Notice

Trademark Notice

Tencent Cloud

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.

Contents

Troubleshooting
- Domain Validation Failed
- Domain Security Review Failed
- Website Inaccessible After an SSL Certificate is Deployed
- 404 Error After the SSL Certificate is Deployed on IIS
- “Your Connection is Not Secure” is Displayed After the SSL Certificate is Installed
- Message Indicating Parsing Failure Is Displayed When a Certificate Is Uploaded
- Automatic DNS Validation Failed for a Domain Hosted with www.west.cn
- Host Name Field Cannot Be Edited in IIS Manager When Type Is Set to https
- Message Indicating Intermediate Certificates Missing in Chain Is Displayed When a Free SSL Certificate Is Deployed on IIS

Troubleshooting

Domain Validation Failed

Last updated：2024-03-06 17:56:24

Symptom

When you apply for an SSL certificate for domain validation and has added the corresponding operation, an error indicating a validation failure is reported after you click **View Domain Validation Status** on the certificate domain validation details page.

Possible Causes

Click **View Domain Validation Status** and troubleshoot based on the error message.

Using DNS validation

Cause 1: Specified DNS record value not detected. Please make sure you have added a specified DNS record for this domain or wait for the DNS record value to take effect

The domain is in unresolvable status.
The DNS record hasn't taken effect.

Cause 2: Incorrect DNS record value. Check whether the record value is correct or wait for the DNS cache to update

The host, record value, or other information in the DNS record is incorrect.
After the information is corrected, the DNS cache hasn't been updated.

Cause 3: A record value has been detected for your domain. Please wait for the certificate authority to review

The DNS cache or validation address limits CA from overseas accessing.

Cause 4: The certificate authority has approved your domain. Please wait for the status to change

The system has noticed the validation value but has not issued the certificate.

Cause 5: Too frequent operations. Please try again in 5 minutes

View Domain Validation Status is clicked too many times and thus limited by the CA.

Note:

If a CAA record for a non-Tencent Cloud CA is configured for the domain, an SSL certificate cannot be issued for the domain properly. Before domain validation, check whether a CAA record is added for the domain and remove it if any.

Using file validation

Cause 1: Specified record value not detected. Please check if you have added the specified record value for this domain or wait for the certificate authority to review

The validation file is not uploaded to the root directory of the website.

The website validation file cannot be accessed or the path is incorrect.

The website uses multi-level redirection.

Cause 2: The certificate authority has approved your domain. Please wait for the status to change

CA has approved but hasn't updated the status.

Solutions

Using DNS validation

The DNS record hasn't taken effect

It takes 0–72 hours for the DNS record to take effect globally. Please wait patiently.

The host, record value, or other information in the DNS record is incorrect

Check whether the record value on the **Validate Domain** page and that added to the DNS record is the same. If not, modify it.

After the information is corrected, the DNS cache hasn't been updated

It takes 0–72 hours for a modified DNS record to take effect globally. Please wait patiently.

The DNS cache or validation address limits CA from overseas accessing

Please wait for the DNS cache to update, or check the website can be accessed through an overseas IP address. If not, open the website for the address.

The system has noticed the validation value but has not issued the certificate

The system has noticed the validation value and will issue the certificate in 15 minutes.

View Domain Validation Status is clicked too many times and thus limited by the CA

Do not repeatedly validate your domain. You can retry every 5 minutes.

Using file validation

The validation file is not uploaded to the root directory of the website

Upload the validation file provided on the **Validate Domain** page to the root directory of the website.

The website validation file cannot be accessed or the path is incorrect

Check whether the validation file is accessible and is store in the root directory of the website so that the file content can be viewed when the website is browsed. For example, if the certificate is applied for the domain `cloud.tencent.com` , then, the validation content in the validation file fileauth.txt should be `tencxxxent` . When you browse `cloud.tencent.com/.well-known/pki-validation/fileauth.txt` over HTTPS or HTTP, the browser displays the validation content `tencxxxent` .

The website uses multi-level redirection

File validation requires the website to return the status code of 200 directly and does not support redirection. Therefore, you are advised to set the website to directly return 200 first and add redirection after the domain is validated.

The CA has approved the application but has not updated the status

You can wait for CA to update the status, or refresh the browser to see whether the certificate is issued.

Domain Security Review Failed

Last updated：2024-03-06 17:56:24

Issue Description

When you apply for a free DV SSL certificate, the domain verification fails and the following message is reported:

```
The domain did not pass the CA security verification. Domain certificate applicatio
```

Common Causes

Due to CA's anti-phishing mechanism, sensitive words contained in domain names, such as "bank" and "pay", can cause security review failure. Some less commonly used root domain names may also result in review failure. For example, root domain names suffixed with .pw, such as `www.qq.pw` and `www.qcloud.pw` , will not pass the review. The following are sensitive words that may cause domain names to fail the security review. They are only examples, and the specific sensitive words are defined by CA.

Private/Public IP	Host name	live (excluding the .live top-level domain name)	bank
banc	alpha	test	example
credit	pw (excluding the .pw top-level domain name)	apple	ebay
trust	root	amazon	android
visa	google	discover	financial
wordpress	pal	hp	lv
free	scp		-

Solution

You can:

Purchase a non-DV SSL certificate to bind to your domain.

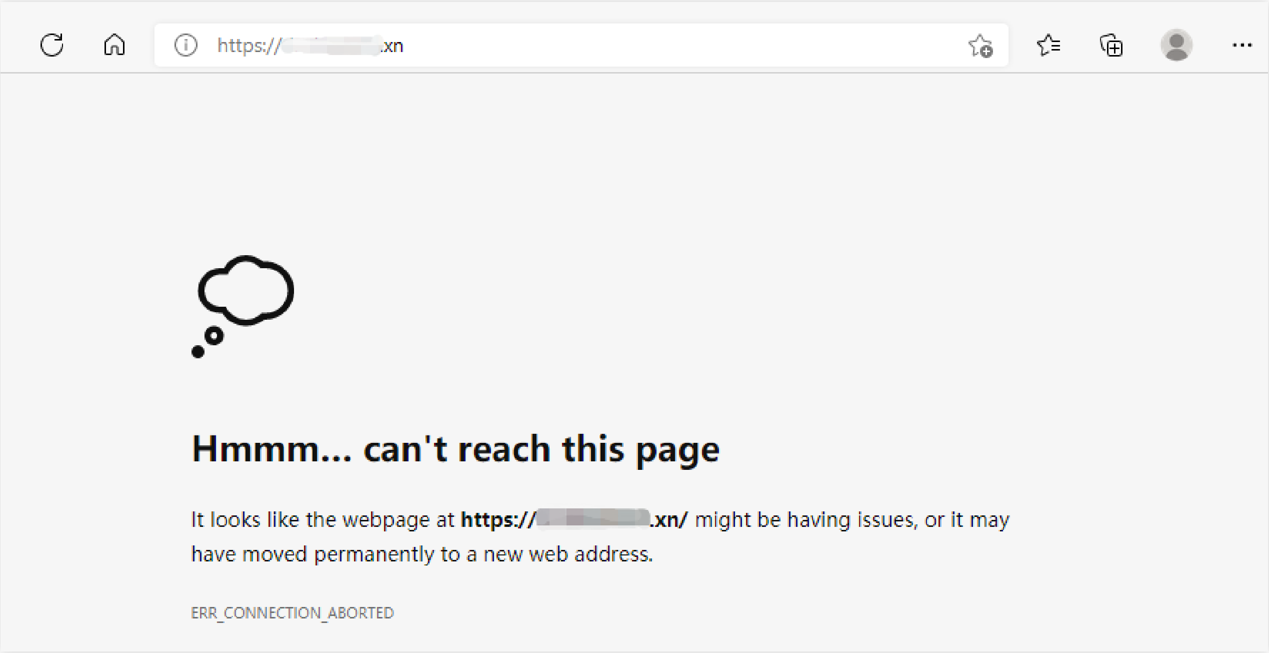
Apply for a domain that does not contain sensitive words.

Website Inaccessible After an SSL Certificate is Deployed

Last updated：2024-03-06 17:56:24

Symptoms

After the SSL certificate is deployed on the server, using HTTPS to access pages is slow, the page is blank, or “This page can’t be reached” is displayed, as shown in the following figure:



https://[redacted].xn

Hmmm... can't reach this page

It looks like the webpage at **https://[redacted].xn/** might be having issues, or it may have moved permanently to a new web address.

ERR_CONNECTION_ABORTED

Possible Causes

Port 443 is closed on the server firewall: If port 443 is closed, you may not be able to access pages over HTTPS normally. In this case, please open port 443 on the server and then retry.

Disabled security group: A security group is a virtual firewall that features stateful data packet filtering. It is used for vendors to configure the network access control of CVM, Cloud Load Balancer, TencentDB, and other instances while controlling their outbound and inbound traffic. It is an important means of network security isolation. The security group is disabled by default. You can enable the security group on your server and then retry.

Browser cache pollution: Browser cache speeds up the loading and allows you to make better use of network resources. In most cases, the browser caches recently requested resources and returns these resources when they are requested again.

Incorrect configuration file: If the configuration file of the server's web service is incorrect, requests may not be handled correctly and thus the website cannot be accessed.

Solutions

Opening port 443 on the server firewall

If you use Tencent Cloud's Cloud Virtual Machine (CVM) service, you can skip this step as port 443 is open on CVM instances by default. Therefore, you can proceed with Disabled security group.

If you use Tencent Cloud's Lighthouse service, open port 443 by referring to Firewall Management.

If you use cloud servers of other vendors, please contact your cloud vendor.

Enabling a security group

If you use Tencent Cloud's CVM service, open port 443 by referring to Adding Security Group Rules.

Tencent Cloud's Lighthouse service does not have this feature. Therefore, you can check whether port 443 is opened on the firewall.

If you use cloud servers of other vendors, please check whether your vendor supports this policy. If yes, consult your vendor about how to open port 443. If not, check whether port 443 is opened on the firewall.

Browser cache pollution

Clear your browser cache or try to use another browser to access the page.

Incorrect configuration file

Check whether the configuration file is correct by referring to the corresponding deployment guide, or purchase the certificate deployment service in the Tencent Cloud Market.

Note:

If your SSL certificate was installed and deployed by referring to Tencent Cloud's documentation, please see Selecting an Installation Type for an SSL Certificate.

404 Error After the SSL Certificate is Deployed on IIS

Last updated：2024-03-06 17:56:24

Error Description

After the SSL certificate is deployed in IIS, a 404 error is reported when you access resources.

Possible Causes

The websites bound to HTTP and HTTPS are different.

The website configuration is incorrect.

Solutions

After the certificate is successfully deployed, resources can be accessed over HTTP but not HTTPS (with a 404 error). In this case, if you have configured the SSL certificate in IIS and enabled port 443 in the firewall, you can troubleshoot as follows:

The website's root directory can be set differently for HTTP and HTTPS. On the IIS server, check how port 443 is bound and confirm whether the website bound to port 443 is the same as that bound to HTTP port 80.

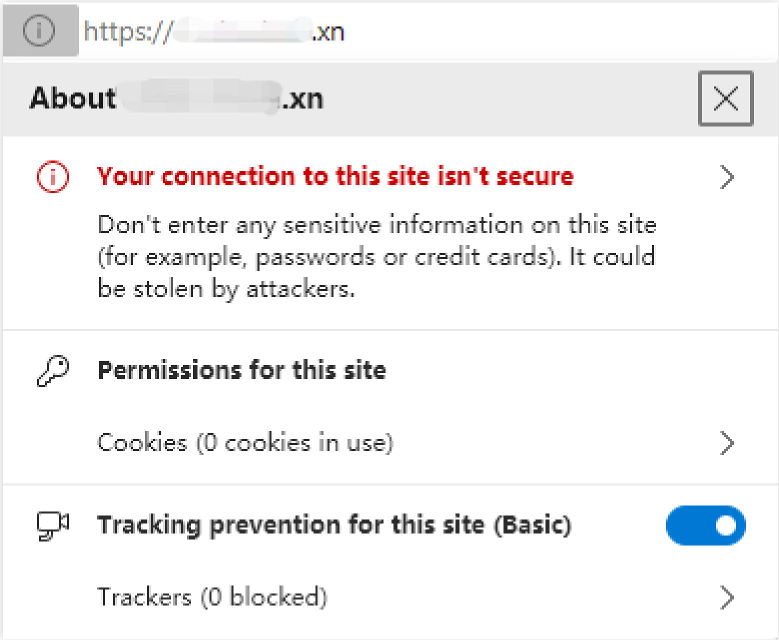
When you check the port binding, check whether the IP address and hostname of the website are correct.

“Your Connection is Not Secure” is Displayed After the SSL Certificate is Installed

Last updated：2024-03-06 17:56:24

Symptoms

After the SSL certificate is deployed, the ⓘ icon and the “Not Secure” warning are displayed in the address bar when you access the website over HTTPS. If you click ⓘ, a warning in red, “Your connection is not secure”, is displayed, as shown in the following figure:



ⓘ https://[redacted].xn

About [redacted].xn ☒

ⓘ Your connection to this site isn't secure

Don't enter any sensitive information on this site (for example, passwords or credit cards). It could be stolen by attackers.

Permissions for this site

Cookies (0 cookies in use)

Tracking prevention for this site (Basic) ●

Trackers (0 blocked)

Possible Causes

Expired SSL certificate: To ensure the security of private keys, SSL certificates are only effective for a period of time. According to the latest international standard, an SSL certificate can be effective for one year at most. If your

SSL certificate has expired but is not replaced in time, the “Not secure” warning in red will be displayed on your website.

Insecure website content: If your website has configured an SSL certificate, but calls external resources such as images and JavaScript files that do not use HTTPS, “Your connection is not secure” may be displayed on your website. If users choose to load the insecure content, the browser will further display the red “Not Secure” warning.

Solutions

Expired SSL certificate

Replace the expired SSL certificate as soon as possible. Then, reapply for a new certificate and deploy it to the website server. The following documents are for your reference:

1. Selecting an Installation Type for an SSL Certificate

Insecure website content

You can copy the external link to the address bar and append an “s” to the “http” to see whether the external link supports HTTPS access.

If yes, change “http” to “https” in the code directly.

If not, download the resources to the local server, modify the resource path to that on your server, and use a relative path such as `image/button.gif` , or a complete HTTPS URL such as `https://***/image/button.gif` .

Message Indicating Parsing Failure Is Displayed When a Certificate Is Uploaded

Last updated：2024-03-06 17:56:24

Symptom

"DNS query failed. Check whether the certificate conforms to the standard" is prompted when a third-party SSL certificate is uploaded in the SSL Certificate Service console.

Possible Causes

Cause 1: The format of the uploaded certificate is incorrect.
Cause 2: The uploaded certificate chain is incomplete.
Cause 3: Extra spaces are not deleted before certificate format verification.

Solutions

The format of the uploaded certificate is incorrect

Check whether the uploaded certificate is in the correct format.
The certificate file starts with "-----BEGIN CERTIFICATE-----" and ends with "-----END CERTIFICATE-----".
The private key starts with "-----BEGIN (RSA) PRIVATE KEY-----" and ends with "-----END (RSA) PRIVATE KEY-----".

The uploaded certificate chain is incomplete

Check whether the uploaded certificate chain is complete. For more information, see How Can I Combine an SSL Certificate Chain?

Extra spaces are not deleted before certificate format verification

Check whether the uploaded certificate contains extra spaces.

Automatic DNS Validation Failed for a Domain Hosted with www.west.cn

Last updated：2024-03-06 17:56:24

Symptom

The domain hosted with www.west.cn failed the automatic DNS validation.

Solutions

On the DNS server of www.west.cn, the TXT record value added for the domain cannot be validated, and the CNAME validation will not be redirected to automatically. Therefore, the ownership of domains hosted with www.west.cn cannot be verified.

You can solve the issue in either of the following ways:

Point the DNS server address of the domain to the DNSPod server address and perform DNS query in Tencent Cloud.

Note:

Different DNSPod plans correspond to different DNS addresses.

Verify the domain ownership through automatic file validation.

Host Name Field Cannot Be Edited in IIS Manager When Type Is Set to https

Last updated：2024-03-06 17:56:24

Symptom

During certificate installation with IIS Manager, **Host name** is grayed out and cannot be edited if you set **Type** to **https** when adding site binding after importing the PFX certificate file.

Possible causes

Windows Server 2008 does not support the operation, and you need to modify the corresponding file.

Solutions

1. Open the `applicationHost.config` file in the `C:\\Windows\\system32\\inetsrv\\config\\applicationHost.config` directory.
2. Modify the file content as follows:

Note:

Take the `tencent.com` domain as an example.

Change `<binding protocol="https" bindingInformation="*:443:" />` to `<binding protocol="https" bindingInformation="*:443:tencent.com" />`.

If you cannot modify the file directly, modify it with the admin permission, or copy the file to the desktop for modification and replace the original file.

```
<site name="example.tencent.com" id="8">
             <application path="/">
                 <virtualDirectory path="/" physicalPath="D:\\web\\tencent" />
             </application>
             <bindings>
                 <binding protocol="http" bindingInformation="*:80:example.tencent.
                 <binding protocol="http" bindingInformation="*:80:www.tencent.com"
                 <binding protocol="https" bindingInformation="*:443:" />
             </bindings>
         </site>
```

3. Add site binding again after saving the file.

Message Indicating Intermediate Certificates Missing in Chain Is Displayed When a Free SSL Certificate Is Deployed on IIS

Last updated：2024-03-06 17:56:24

Symptom

"One or more intermediate certificates in the certificate chain are missing. To resolve this issue, make sure that all of the intermediate certificates are installed" is prompted when a free SSL certificate is deployed on the IIS web server.

Possible Causes

Intermediate certificates are missing.

Solutions

Step 1. View the encryption algorithm of the certificate

Log in to the SSL Certificate Service console and view the encryption algorithm type of your certificate.

Step 2. Download the intermediate certificate file

Download the intermediate certificate file to your CVM instance based on the encryption algorithm type of your certificate.
RSA encryption algorithm: Download here.
ECC encryption algorithm: Download here.

Step 3. Install the intermediate certificate

1. On the target server, double-click the intermediate certificate file and click **Install Certificate** in the pop-up window.
2. In the certificate import wizard, set **Store Location** to **Local Machine** and click **Next**.
3. In **Certificate Store**, select **Place all certificates in the following store** > **Intermediate Certification Authorities** and click **Next**.
4. Check the location to install the certificate and click **Finish**.
5. If "The import was successful." is displayed, the operation is successful. Then, try deploying your SSL certificate again.