Alibaba Cloud Certificates Service

Best Practices

Issue: 20190730

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. **You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.**
2. **No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.**
3. **The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.**
4. **This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use**

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `cd / d C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich {stand | slave}`

Contents

1 Deploy SSL certificate on Ubuntu Apache2

This manual describes how to install the Alibaba Cloud SSL certificate in Apache2 on Ubuntu.

Environment

OS: Ubuntu

Web server: Apache2

Prerequisites

- The Apache server certificate is downloaded from the Alibaba Cloud SSL certificate services console.
- Open SSL is installed.

Steps

1. In *apache2* directory, execute the following command to create `ssl` directory.

```
mkdir / etc / apache2 / ssl
```

2. Execute the following command to copy the downloaded Alibaba Cloud certificate file to `ssl` directory.

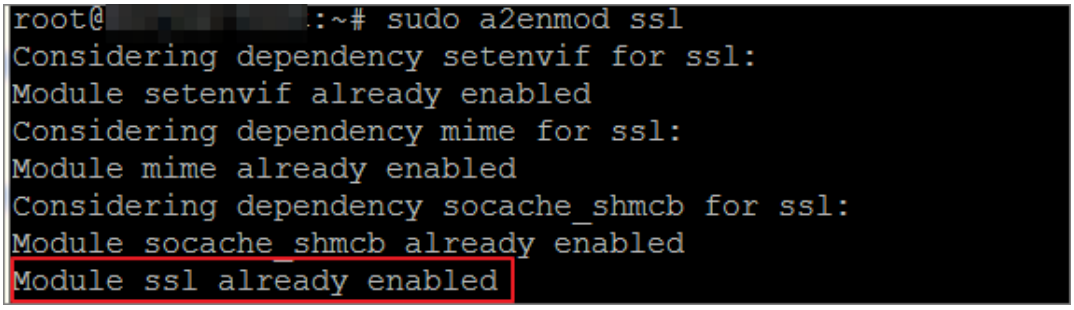
```
cp - r YourDomain Name_publi c . crt / etc / apache2 / ssl

cp - r YourDomain Name_chain . crt / etc / apache2 / ssl

cp - r YourDomain Name . key / etc / apache2 / ssl
```

3. Execute the following command to enable the SSL module.

```
sudo a2enmod ssl
```



After the SSL module is enabled, you can execute `ls / etc / apache2 / sites - available` and view the *default - ssl . conf* file created in the directory.

> **Note:**
> Port 443 is a network browsing port that is used primarily for HTTPS services. After the SSL module is enabled, port 443 is automatically released. If port 443 is not automatically released, you can execute `vi / etc / apache2 / ports . conf` and add `Listen 443` to manually release it.

4. Execute the following command to modify the configuration file *default - ssl . conf* for certificate installation.

```
vi / etc / apache2 / sites - available / default - ssl . conf
```

In *default - ssl . conf* file, find the following parameters and modify the parameters. After modification is complete, click `: wq` to save and exit.

```
< IfModules mod_ssl . c >
< VirtualHos t *: 443 >
 ServerName # change to the domain as www . YourDomain
 Name . com bound by the certificat e .
 SSLCertifi cateFile / etc / apache2 / ssl / www . YourDomain
 Name_publi c . crt # replace / etc / apache2 / ssl / www .
 YourDomain Name . com_public . crt with certificat e file
 path + certificat e file name .
 SSLCertifi cateKeyFil e / etc / apache2 / ssl / www .
 YourDomain Name . com . key # replace / etc / apache2 / ssl /
 www . YourDomain Name . com . key with certificat e key
 file path + certificat e key file name .
 SSLCertifi cateChainF ile / etc / apache2 / ssl / www .
 YourDomain Name . com_chain . crt # replace / etc / apache2 /
 ssl / www . YourDomain Name . com_chain . crt with certificat
 e chain file path + certificat e chain file name .
```

```
root@ ~
<IfModule mod_ssl.c>
        <VirtualHost *:443>
                ServerAdmin webmaster@localhost
                ServerName www.                                    .com

                DocumentRoot /var/www/html

                ErrorLog ${APACHE_LOG_DIR}/error.log
                CustomLog ${APACHE_LOG_DIR}/access.log combined
                SSLEngine on
                SSLCertificateFile      /etc/apache2/ssl/                                    s.com_public.crt
                SSLCertificateKeyFile /etc/apache2/ssl/                                    .com.key

                SSLCertificateChainFile /etc/apache2/ssl/                                    _chain.crt
```

/ sites - available : This directory stores available virtual machine host; */ sites - enabled* : This directory stores enabled virtual machine host.

Note:

default - ssl . conf This file may be stored at */ etc / apache2 / sites - available* or */ etc / apache2 / sites - enabled* .

5. Map *default - ssl . conf* to */ etc / apache2 / sites - enabled* folder, create soft links in order to automatically link the two folders.

```
sudo   ln   - s   / etc / apache2 / sites - available / default - ssl
. conf   / etc / apache2 / sites - enabled / 001 - ssl . conf
```

6. Reload the Apache2 configuration file.

```
sudo   / etc / init . d / apache2    force - reload
```

```
root@                    :~# sudo /etc/init.d/apache2 force-reload
[ ok ] Reloading apache2 configuration (via systemctl): apache2.serv
```

7. Execute the following command to restart the Apache2 service.

```
sudo   / etc / init . d / apache2    restart
```

```
root@                    :~# sudo /etc/init.d/apache2 restart
[ ok ] Restarting apache2 (via systemctl): apache2.service.
```

What to do next

Apache2 service is reloaded successfully. You can enter *https :// www . YourDomain Name . com* in your explorer to validate certificate installation result.

2 Deploy SSL certificates on Tomcat 8.5 or Tomcat 9.0 running CentOS

This topic describes how to deploy SSL certificates on Tomcat 8.5 or Tomcat 9.0 running CentOS.

Test environment

Operating system: CentOS 7.6, 64-bit

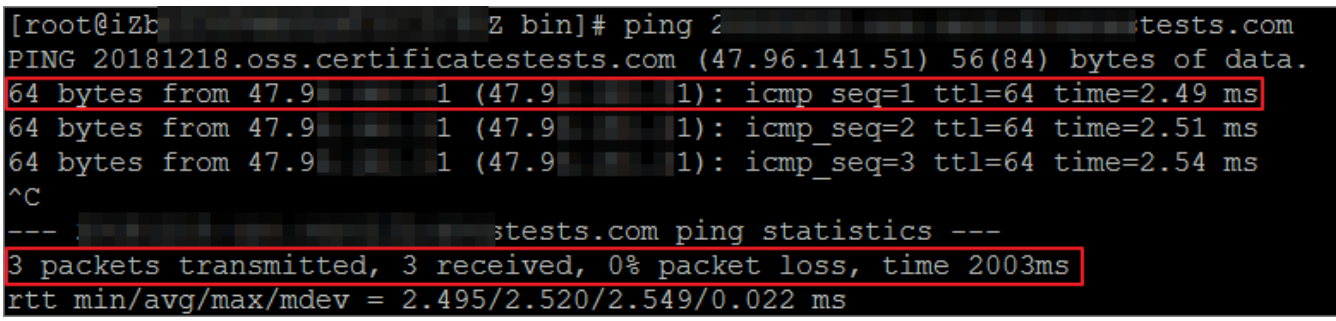
Web server: Tomcat 8.5 or Tomcat 9.0

> Note:
> JDK environment variables must be installed on the Tomcat server first. You can view the recommended JDK compatible configuration on the Tomcat official website.

Prerequisites

- You have downloaded the Tomcat server certificate from the Alibaba Cloud SSL Certificates console. The Tomcat server certificate includes the PFX format certificate file and TXT format password file.
- You have added DNS records for the domain name that is bound to your SSL certificate, pointing the domain name to the IP address of the Tomcat server.

  Run the `ping www.yourdomain.com` command after the domain name resolution is configured. If the IP address of the Tomcat server is returned, the resolution is successful.



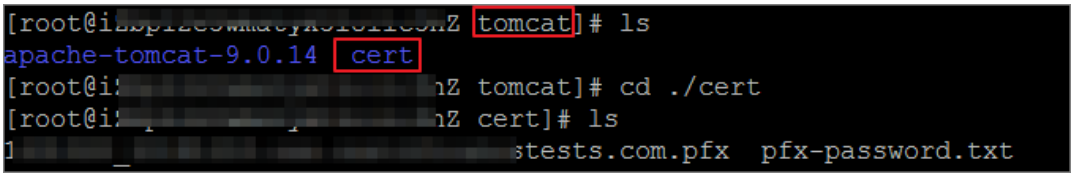
Procedure

1. Decompress the Tomcat server certificate.

   > Note:

A new password file is generated each time you download the certificate. The password is valid only for the downloaded certificate. If you want to update the certificate, you must update the password at the same time.

2. **Create the cert directory under the Tomcat installation directory and copy the downloaded certificate and password files to the cert directory.**



3. **Open** *Tomcat / conf / server . xml* **, locate the following parameters in the** *server . xml* **file, and modify these parameters.**

```
< Connector   port =" 8080 "  protocol =" HTTP / 1 . 1 "
              connection  Timeout =" 20000 "
              redirectPo  rt =" 8443 " />

 # Locate   the   preceding   parameters ,  remove   the  <! - -
 and  - ->  annotation   symbols ,  and   modify   the   parameters
   as   follows :
 < Connector   port =" 80 "  protocol =" HTTP / 1 . 1 "
 # Set   Connector   port   to   80 .
               connection  Timeout =" 20000 "
               redirectPo  rt =" 443 " />
              # Set   redirectPo  rt   to   the   SSL   default
   port   443   to   redirect   HTTP   requests   to   HTTPS
 requests .
```

```
   < Connector   port =" 8443 "
          protocol =" org . apache . coyote . http11 . Http11NioP
 rotocol "
          maxThreads =" 150 "
          SSLEnabled =" true ">
        < SSLHostCon  fig >
            < Certificat  e         certificat  eKeystoreF  ile ="
 cert / keystore . pfx "
             certificat  eKeystoreP  assword =" XXXXXXX "
                         certificat  eKeystoreT  ype =" PKCS12 " />

   # Locate   the   preceding   parameters ,  remove   the  <! - -
 and  - ->  annotation   symbols ,  and   modify   the   parameters
   as   follows :
   < Connector   port =" 443 "
   # Change   the   default   Tomcat   HTTPS   port   Connector
   port   from   8443   to   443 .  Port   8443   cannot   be
 directly   accessed   through   the   domain   name .  Therefore ,
 you   must   append   a   port   number   to   the   domain   name
 .  Port   443   is   the   default   HTTPS   port .  You   can
 directly   access   it   through   the   domain   name   without
 the   need   to   append   a   port   number   to   the   domain
 name .
          protocol =" org . apache . coyote . http11 . Http11NioP
 rotocol "
```

```
          # Connector   port   in   file   server . xml   has   two
  modes :  NIO   and   APR .  In   this   deployment ,  the   NIO
  mode   is   used .  The   protocol =" org . apache . coyote .
http11 . Http11NioP  rotocol "  setting   specifies   the   NIO
mode .
          maxThreads =" 150 "
          SSLEnabled =" true ">
       < SSLHostCon  fig >
          < Certificat  e         certificat  eKeystoreF  ile ="/
usr / local / tomcat / cert / Certificat  e   Domain   Name . pfx "
            # The   certificat  eKeystoreF  ile   parameter
specifies   the   path   of   the   certificat  e   file .  Use
your   certificat  e   path   and   file   name   to   replace
Certificat  e   Domain   Name . pfx ,  for   example ,  certificat
eKeystoreF  ile ="/ usr / local / tomcat / cert / abc . com . pfx
".
            certificat  eKeystoreP  assword =" password "
            # The   certificat  eKeystoreP  assword   parameter
specifies   the   password   for   the   SSL   certificat  e .  Use
  your   certificat  e   password   in   pfx - password . txt   to
  replace   it ,  for   example ,  certificat  eKeystoreP  assword
=" bMNML1Df ".
            certificat  eKeystoreT  ype =" PKCS12 " />
            # When   the   certificat  e   type   is   PFX ,  set
certificat  eKeystoreT  ype   to   PKCS12 .
```

```
< Connector   port =" 8009 "  protocol =" AJP / 1 . 3 "  redirectPo
 rt =" 8443 " />

# Locate   the   preceding   parameters ,  remove   the  <! - -  and
  - ->  annotation   symbols ,  and   modify   the   parameters   as
   follows :
< Connector   port =" 8009 "  protocol =" AJP / 1 . 3 "  redirectPo
 rt =" 443 " />
 # Set   redirectPo  rt   to   443   to   redirect   HTTP   requests
  to   HTTPS   requests .
```

4. **Save the configuration in the server.xml file.**

5. Restart the Tomcat service.

   a. Run `./shutdown.sh` in the bin directory of Tomcat to disable the Tomcat service.

```
[root@iZ                    Z bin]# ./shutdown.sh
Using CATALINA_BASE:   /usr/local/tomcat/apache-tomcat-9.0.14
Using CATALINA_HOME:   /usr/local/tomcat/apache-tomcat-9.0.14
Using CATALINA_TMPDIR: /usr/local/tomcat/apache-tomcat-9.0.14/temp
Using JRE_HOME:        /usr/local/java/jdk-11.0.2
Using CLASSPATH:       /usr/local/tomcat/apache-tomcat-9.0.14/bin/bootstrap.jar:/usr/local
ache-tomcat-9.0.14/bin/tomcat-juli.jar
NOTE: Picked up JDK_JAVA_OPTIONS:  --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens
/java.io=ALL-UNNAMED --add-opens=java.rmi/sun.rmi.transport=ALL-UNNAMED
[root@iZ                    nZ bin]# ps -ef|grep java
root       939   843  0 16:37 pts/2    00:00:00 grep --color=auto java
```

   b. Run `./startup.sh` in the bin directory of Tomcat to enable the Tomcat service.

```
[root@iZ                    nZ bin]# ./startup.sh
Using CATALINA_BASE:   /usr/local/tomcat/apache-tomcat-9.0.14
Using CATALINA_HOME:   /usr/local/tomcat/apache-tomcat-9.0.14
Using CATALINA_TMPDIR: /usr/local/tomcat/apache-tomcat-9.0.14/temp
Using JRE_HOME:        /usr/local/java/jdk-11.0.2
Using CLASSPATH:       /usr/local/tomcat/apache-tomcat-9.0.14/bin/bootstrap.jar:/usr/loca
ache-tomcat-9.0.14/bin/tomcat-juli.jar
Tomcat started.
```

Subsequent procedures

After the Tomcat service restarts, enter domain name *https :// www . YourDomain Name . com* into the address bar of your browser, and verify the certificate deployment result. If the green lock icon appears in the address bar of your browser, the certificate is installed.

See also:

- Deploy SSL certificates on Tomcat servers
- Install SSL certificates in Apache servers
- Deploy SSL certificate on Ubuntu Apache2
- How do I deploy the issued certificate in Apache server
- Install SSL certificates in Nginx/Tengine servers
- Install SSL certificates in IIS servers
- An SSL certificate is configured by the jetty server