

服务器证书安装配置指南

F5

二〇二一年一月



### 第一步:生成证书请求文件(CSR)

如果你已经生成了CSR,并且证书已经颁发了,请从第三步开始阅读,如果没有请从第

一步开始阅读。

进入OpenSSL安装目录下的Bin目录,运行如下命令生成私钥(KEY):

openssl genrsa -out server.key 2048 Generating RSA private key, 2048 bit long modulus

e is 65537 (0x10001)

运行如下命令生成证书请求文件(CSR)

openssl req -new -key server.key -out server.csr

如是Windows系统,请使用下面命令生成证书请求文件(CSR)

set OPENSSL\_CONF=C:\Program Files\OpenSSL-Win64\bin\openssl.cfg openssl req -new -key server.key -out server.csr

#### 接下来提示输入私钥密码和申请证书的详细信息

Enter pass phrase for server.key: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. Country Name (2 letter code) []:CN State or Province Name (full name) []:Shanghai Locality Name (eg, city) []:Shanghai Organization Name (eg, company) []:GlobalSign China Co., Ltd. Organizational Unit Name (eg, section) []:IT Dept. Common Name (eg, your websites domain name) []:cn.globalsign.com Email Address []: Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:



从Email地址开始,下面的信息都不需要,请保留为空,直接回车即可。

需要输入的信息说明请见下表:

| 字段                       | 说明             | 示例                      |
|--------------------------|----------------|-------------------------|
| Country Name             | ISO 国家代码(两位字符) | CN                      |
| State or Province Name   | 所在省份           | Shanghai                |
| Locality Name            | 所在城市           | Shanghai                |
| Organization Name        | 公司名称           | GlobalSign CN Co., Ltd. |
| Organizational Unit Name | 部门名称           | IT Dept.                |
| Common Name              | 申请证书的域名        | Cn.globalsign.com       |
| Email Address            | 不需要输入          |                         |
| A challenge password     | 不需要输入          |                         |

完成以上的操作后会在对应的目录下生成server.key 和 server.csr , 请妥善保存这两个 文件。

### 第二步:提交CSR,申请证书

递交证书申请表及相关资料,并同时把证书请求文件(CSR)提交给GlobalSign销售。

#### 第三步:获取服务器和中级证书

1.获取服务器证书,也就是 Globalsign 给你颁发的证书,绑定了你的域名或公网IP 的 SSL 证书,从收到的证书邮件中复制第一段代码,此证书由GlobalSign系统通过 Email 方式发送给用户,证书文件的内容为(从"-----BEGIN CERTIFICATE-----"开始,并 到"-----END CERTIFICATE-----"结束的所有内容),请把此内容在文本编辑器中保 存为 server.cer。

2.如果你申请的是域名型 SSL 证书,请获取域名型(DV)中级证书从收到的证书邮件 中复制第二段代码(包含中级证书及交叉证书),此证书由 GlobalSign 系统通过 Email方式发送给用户,证书文件的内容为(从"-----BEGIN CERTIFICATE-----"开 始,并到"-----END CERTIFICATE-----"结束的所有内容),请把此内容在文本编辑 器中保存为域名型(DV)中级证书,文件名为dvroot.cer

或

如果你申请的是企业型 SSL 证书,请获取企业型(OV)中级证书 从收到的证书邮件中 复制第二段代码(包含中级证书及交叉证书),此证书由 GlobalSign 系统通过 Email 方式发送给用户,证书文件的内容为(从"-----BEGINCERTIFICATE-----"开始,到



"----ENDENCERTIFICATE-----"结束的所有内容),请把此内容在文本编辑器中保存为企业型(OV)中级证书,文件名为 ovroot.cer 或如果你申请的是增强型(EV)SSL 证书,获取增强型(EV)中级证书,从收到的证书邮件中复制第二段代码(包含中级证书及交叉证书),此证书由 GlobalSign 系统通过 Email方式发送给用户,证书文件的内容为(从"-----BEGINCERTIFICATE-----"开始,到"-----ENDCERTIFICATE-------"结束的所有内容),请把此内容在文本编辑器保存为增强型(EV)中级证书,文件名为 evroot.cer

#### 第四步: 配置证书

1.进入F5的System Flie Management: SSL Certificate List目录,点击 import,导

入私钥文件、服务器证书和中级证书。

| Syste | m 💀 File Managemer   | t : SSL Certificate |                          |               |                      |                    |       |                      |         |        |             |
|-------|----------------------|---------------------|--------------------------|---------------|----------------------|--------------------|-------|----------------------|---------|--------|-------------|
| ۰ ه   | Data Group File List | IFile List          | External Monitor Program | File List     | SSL Certificate List | Apache Certificate | List  |                      |         |        |             |
| 1     |                      | S                   | sarch                    |               |                      |                    |       |                      | Im      | port   | Create      |
| -     | Name                 |                     | 0                        | Contents      | Common N             | ame Organiz        | ation | Expiration           |         | 0 Part | tion / Path |
|       | a-bundle             |                     | Ce                       | ertificate Bu | Indie                |                    |       | Aug 13, 2018 - Aug 1 | 3. 2018 | Comm   | on          |

(1)导入私钥文件,此例私钥名称设置为Mykey

| Import Type        | Select                      |
|--------------------|-----------------------------|
|                    | Select                      |
| Free Space on Disk | Key                         |
|                    | Certificate                 |
| Cancel             | PKCS 12 (IIS)               |
|                    | Archive                     |
|                    | Certificate Revocation List |



## (2) 导入中级证书, certificate name此例设置为Entrustchain

| Import Type        | Certificate   |  |
|--------------------|---|--|
| Certificate Name   | Create New      Overwrite Existing     EntrustChain             |  |
| Certificate Source | Upload File     Paste Text     Choose File     ChainBundle1.crt |  |
| Free Space on Disk | 174 MB  |  |

# (3) 返回SSL Certificate List,点击列表里的私钥名称Mykey

| Sys | System » File Management : SSL Certificate List |                    |                       |                |                               |                         |  |  |
|-----|---|--------------------|-----------------------|----------------|-------------------------------|-------------------------|--|--|
| ø   | <ul> <li>Data Group File List</li> </ul>        | iFile List         | External Monitor Pro  | gram File List | SSL Certificate List Apache C | Apache Certificate List |  |  |
| 1   |   | Se                 | arch                  |                |                               | nport Create            |  |  |
| 4   | ▲ Name  | © Contents         | © Common Name         | Organization   | Expiration                    | Partition / Path        |  |  |
|     | EntrustChain                                    | Certificate Bundle |                       |                | Dec 5, 2030 - Dec 5, 2030     | Common                  |  |  |
|     | МуКеу   | Кеу                |                       |                |                               | Common                  |  |  |
|     | ca-bundle                                       | Certificate Bundle |                       |                | Aug 13, 2018 - Aug 13, 2018   | Common                  |  |  |
|     | default   | Certificate        | localhost.localdomain | MyCompany      | Jan 11, 2026                  | Common                  |  |  |
|     | f5-irule  | Certificate        | support.f5.com        | F5 Networks    | Aug 13, 2031                  | Common                  |  |  |
| Arc | hive Delete                                     |                    |                       |                |                               |                         |  |  |

# (4) 点击导入

| System » File Management : SSL Certificate List » MyKey |       |  |  |  |  |
|---|-------|--|--|--|--|
| 🚓 🗸 Certificate   | Кеу   |  |  |  |  |
|   |       |  |  |  |  |
| General Properties                                      |       |  |  |  |  |
| Name  | MyKey |  |  |  |  |
|   |       |  |  |  |  |



# (5)上传服务器证书文件

| SL Certificate/Key S   | ource  |   |  |  |   |
|--|--|---|--|--|---|
| Import Type  | port Type Certificate  |   |  |  |   |
| certificate Name /Common/MyKey   |  |   |  |  |   |
| Certificate Source  Upload File  Paste Text Choose File ServerCertificate.crt  |  |   |  |  |   |
| Free Space on Disk   | 174 M  | в   |  |  |   |
| ystem » File Mana<br>+ - Data Group Fil  | gement : SSL Certif<br>e List IFile List   | icate List<br>External Monitor Pro                          | gram File List                                   | SL Certificate List  | ertificate List   |
| ystem » File Mana<br>• - Data Group Fil  | gement : SSL Certif<br>e List iFile List   | icate List<br>External Monitor Pro                          | gram File List                                   | SSL Certificate List   | ertificate List   |
| rstem » File Mana<br>Data Group File<br>Name   | gement : SSL Certif<br>e List IFile List<br>© Contents   | icate List<br>External Monitor Pro                          | gram File List S                                 | SL Certificate List Apache C   | ertificate List   |
| vstem » File Mana<br>Data Group Fil<br>Name<br>EntrustChain  | gement : SSL Certif<br>e List IFIIe List   | Icate List<br>External Monitor Pro<br>Search<br>Common Name | gram File List S                                 | SL Certificate List Apache C<br>Ir<br>Expiration<br>Dec 5, 2030 - Dec 5, 2030  | ertificate List   |
| rstem » File Mana<br>Data Group Fil<br>Name<br>EntrustChain<br>MyKey   | gement : SSL Certif<br>e List IFIIe List<br>e Contents<br>Certificate Bundle<br>Certificate & Key                                      | External Monitor Pro  | gram File List S<br>Organization<br>Entrust Inc. | SSL Certificate List Apache C<br>Ir<br>Expiration<br>Dec 5, 2030 - Dec 5, 2030<br>Jan 14, 2017   | ertificate List   |
| <ul> <li>Pile Mana</li> <li>Data Group File</li> <li>Name</li> <li>EntrustChain</li> <li>MyKey</li> <li>ca-bundle</li> </ul> | gement : SSL Certif<br>e List IFile List<br>Contents<br>Certificate Bundle<br>Certificate & Key<br>Certificate Bundle                  | icate List<br>External Monitor Pro                          | gram File List S                                 | SL Certificate List Apache C<br>Ir<br>Expiration<br>Dec 5, 2030 - Dec 5, 2030<br>Jan 14, 2017<br>Aug 13, 2018 - Aug 13, 2018           | ertificate List<br>nport Create<br>Partition / Po<br>Common<br>Common<br>Common |
| ystem >> File Mana   | gement : SSL Certif<br>e List IFIIe List<br>© Contents<br>Certificate Bundle<br>Certificate & Key<br>Certificate Bundle<br>Certificate | Icate List<br>External Monitor Pro                          | gram File List S                                 | SL Certificate List Apache C<br>Expiration<br>Dec 5, 2030 - Dec 5, 2030<br>Jan 14, 2017<br>Aug 13, 2018 - Aug 13, 2018<br>Jan 11, 2026 | ertificate List   |

2.进入Local Traffic Profiles : SSL : Client目录,新建一个client ssl profile,

选择当前Profile所使用的证书(Certificate)、私钥(key),以及在 Chian 处,设置 与该证书相关联的证书链(之前导入的中级证书),完成后,选择"Update"保存。

| Local Traffic » Profiles : | SSL : Client » TestCertificates |          |
|----------------------------|---------------------------------|----------|
| 🔅 🚽 Properties             |                                 |          |
|                            |                                 |          |
| General Properties         |                                 |          |
| Name                       | TestCertificates                |          |
| Partition / Path           | Common                          |          |
| Parent Profile             | clientssl 🔻                     |          |
| Configuration: Advanced    | •                               | Custom 🗹 |
| Certificate                | МуКеу                           | V        |
| Кеу                        | МуКеу                           |          |
| Pass Phrase                |                                 | ×.       |
| Confirm Pass Phrase        |                                 |          |
| Chain                      | EntrustChain V                  | V        |



3.将ssl profile关联到对应的virtual server

完成证书配置后,请备份私钥与公钥文件,便于以后,有需要可以使用备份文件来恢

复。

GlobalSign China Co., Ltd

环玺信息科技 (上海)有限公司

2021年1月