

V4.0.1+

# 使用 OpenSSL 生成自签名证书

OpenSSL 是 SSL 和 TLS 协议的开放式源代码实现。它在标准通信层上提供了加密传输层，允许其与诸多网络应用程序和服务相结合。Cloud Management Console 中的缺省 SSL 概要文件具有通用公共名称。将 SSL 概要文件关联至网关集群时，如果使用缺省 SSL 概要文件，那么发出 API 调用的应用程序可能无法根据提供的证书验证其所连接到的主机名。在这种情况下，您可以生成一个新的自签名证书，以表示应用程序可以验证的公共名称。该主题告诉您如何使用 OpenSSL 工具箱生成自签名 SSL 证书，以启用 HTTPS 连接。

## 过程

要使用 OpenSSL 生成自签名 SSL 证书，请完成以下步骤：

1. 写下您的 SSL 证书的公共名称 (CN)。该公共名称 (CN) 是使用该证书的系统的标准名称。如果您使用的是动态 DNS，那么 CN 应该具有通配符，例如： `*.api.com.`。否则，使用网关集群中设置的主机名或 IP 地址（例如，`192.16.183.131` 或 `dp1.acme.com`）。

2. 运行以下 OpenSSL 命令来生成您的专用密钥和公用证书。回答问题并在出现提示时输入公共名称。

```
openssl req -newkey rsa:2048 -nodes -keyout key.pem -x509 -days 365 -out certificate.pem
```

3. 检查已创建的证书：


```
openssl x509 -text -noout -in certificate.pem
```

4. 将密钥和证书组合在 PKCS#12 (P12) 捆绑软件中：

```
openssl pkcs12 -inkey key.pem -in certificate.pem -export -out certificate.p12
```

5. 验证您的 P12 文件。

```
openssl pkcs12 -in certificate.p12 -noout -info
```

6. 在 Cloud Management Console 的导航部分中，单击 **SSL 概要文件** 图标 。这样会打开“SSL 概要文件”页面。

7. 在“SSL 概要文件”页面中，单击添加 **SSL 概要文件**。

8. 在名称文本字段中，输入新 SSL 概要文件的名称。

9. 在“现有证书”部分中，单击**选择文件**，然后浏览以查找 `certificate.p12`，并选择该文件。

注：

- P12 文件必须包含专用密钥、来自认证中心的公用证书，以及用于签名的所有中间证书。
- P12 文件最多可包含 10 个中间证书。

10. 在**密码**文本字段中，输入证书文件的密码。

**注：**

现有证书**必须**用密码加以保护。

11. 单击**上载证书**。这样会填充该证书。

12. 要验证证书，请将针对信任库中提供的 **CA**，**请求并验证证书**滑块滑至打开位置。

13. 在**信任库**窗口部分中，单击**选择文件**，然后浏览以查找“信任库”证书。


14. 在**密码**文本字段中，输入证书文件的密码。

15. 单击**上载证书**。这样会填充该证书。

16. 展开“协议”部分，以显示 SSL 和 TLS 版本。

17. 使用复选框来指示 SSL 或 TLS 版本。

18. 单击**保存**。这样会上载证书并保存 SSL 或 TLS 版本。

19. 在 Cloud Management Console 的导航部分中，单击**集群**图标 ( )。

20. 在“网关集群”窗口区域中，单击**设置**。这样会显示“网关集群”窗口。

21. 在“网关集群”窗口中，单击**选择文件**，然后浏览以查找要与网关集群关联的 SSL 概要文件。

22. 单击**保存**。

## 结果

已实施您的 SSL 活动。

父主题：

➔ [SSL 概要文件](#)

相关任务：

➔ [SSL 概要文件](#)

➔ [生成认证中心的 PKCS#12 文件。](#)

更多 **IBM API Management** 信息位于：

对于社区支持，请访问：**dW Answers**