3. 安装证书

        在开发过程中，有一个简单的方法创建新的证书（也可以使用其他方式制作证书，只要符合Ice要求的证书格式都可以）。OpenSSL包括所有必要的基础设施来设立自己的证书颁发机构（CA），但是我们必须对OpenSSL非常的熟悉。为了简化这个过程，Ice提供了一系列Python脚本（对应Ice-3.1.1版本的Python版本为2.7.5），位于Ice安装目录下的config/ca子目录，这些Python脚本隐藏了复杂的OpenSSL操作过程，并允许我们快速执行必要的任务：

        l 初始化一张新的根证书

        l 生成新的证书请求

        l 给证书请求签名，创建一个有效的证书链

        l 转换证书，以匹配特定的平台需求

        首先需要在系统中安装Python-2.7.5版本，才能够顺利执行Python脚本。

        设置环境变量ICE\_CA\_HOME，指定一个目录，制作证书的过程中，运行Python脚本生成的文件，将存放在该目录中。

3.1. 初始化root CA

        通过以下的命令初始化一个根证书

        python initca.py [--no-password] [--overwrite]

        --overwrite操作会覆盖一个已经存在的根证书，如果对CA的私钥不做加密处理可以使用--no-password操作。

         假设ICE\_CA\_HOME环境变量设置为c:\iceca,则会在该目录下生产两个文件，req.cnf和ca\_cert.pem。ca\_cert.pem文件包含根证书，我们的IceSSL配置文件必须指定该根证书作为我们的信任证书，C++程序通过IceSSL.CertAuthFile=C:\iceca\ca\_cert.pem 指定，在java中，我们需要添加该证书到信任域中，使用如下的命令：

        keytool -import -trustcacerts -file ca\_cert.pem -keystore ca.jks

         ca.jks是java支持的密钥库文件格式，Java中通过IceSSL.Truststore属性指定该根证书。

3.2. 生成证书请求

        生成证书请求使用如下命令：

        python req.py [--overwrite] [--no-password] [--node|--registry|--server|--user]

        此脚本会查找req.cnf和ca\_cert.pem文件，在ICE\_CA\_HOME 环境变量指定的目录下，然后生成两个文件:一个私钥和一个文件包含证书请求。请求文件必须被传送到证书颁发机构签名，产生一个有效的证书链。

         --node，--registry代表IceGrid 的节点和注册器，--server表示Ice 的服务器，--user表示一个人或者一个客户端，这些操作只是影响着生成文件的名称，如服务器需要一个证书，可以使用命令python req.py --server，执行完脚本之后生成的文件名字为server\_key.pem和server\_req.pem。节点证书请求、应用程序证书请求、注册器证书请求、客户端证书请求，都需要分别执行这一条命令。server\_key.pem文件为服务器生成的新的私钥，这个文件必须被安全保存，server\_req.pem为服务器证书请求文件。

3.3. 签名证书请求

        使用如下命令：

        sign.py --in <req> --out <cert>

        输入文件req为证书请求文件，输出文件cert是证书链，如给节点证书请求签名，使用如下命令：

        python sign.py --in node\_req.pem --out node\_cert.pem

3.4. 转换证书格式

        对于java用户来说，私钥和证书链必须被转换成合适的格式，使用如下命令：

        python import.py [--overwrite] [--java alias cert key keystore]

        如从节点的证书链文件中导出节点的私钥和节点证书到一个java密钥库中，使用如下命令：

        python import.py --java mycert node\_cert.pem node\_key.pem cert.jks

        在密钥库cert.jks文件中，Mycert为一个节点证书条目的别名，IceSSL配置文件通过属性IceSSL.Keystore来指定这个密钥库。

---------------------

作者：骑在木马上的黑客

来源：CSDN

原文：https://blog.csdn.net/KnightOnHourse/article/details/80643761

版权声明：本文为博主原创文章，转载请附上博文链接！