生成CSR并将证书应用于CMS

目录

简介

本文档介绍如何生成证书签名请求(CSR)并将签名证书上传到思科Meeting Server (CMS)。

先决条件

要求

Cisco 建议您了解以下主题：

- CMS服务器基础知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Putty或类似软件
- CMS 2.9或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

生成CSR

有两种生成CSR的方法，一种是从具有管理员访问权限的命令行界面(CLI)直接在CMS服务器上生成

CSR，另一种是通过外部第三方证书颁发机构(CA)（例如Open SSL）生成CSR。

在这两种情况下，必须使用正确的语法生成CSR，CMS服务才能正常工作。

步骤1:语法结构

```
pki csr <key/cert basename> <CN:value> [OU:<value>] [O:<value>] [ST:<-value>] [C:<value>] [subjectAltNa
```

- <key/cert basename>是标识新密钥和CSR名称的字符串。它可以包含字母数字、连字符或下划线字符。这是必填字段。
- <CN：value>是公用名。这是完全限定域名(FQDN)，指定服务器在域名系统(DNS)中的确切位置。这是必填字段。
- [OU：<value>]是组织单位或部门名称。例如，支持、IT、工程师、财务。这是可选字段。
- [O：<value>]是组织或企业名称。 通常为公司合法注册的名称。这是可选字段。
- [ST：<value>]是省、地区、县或州。 例如，白金汉郡California。 这是可选字段。
- [C：<value>]是国家/地区。贵组织所在国家/地区的两个字母的国际标准化组织(ISO)代码。例如，US、GB、FR。这是可选字段。
- [subjectAltName：<value>]是主题备用名称(SAN)。 从X509版本3 (RFC 2459)开始，允许安全套接字层(SSL)证书指定证书必须匹配的多个名称。此字段使生成的证书涵盖多个域。它可以包含IP地址、域名、邮件地址、常规DNS主机名等，用逗号分隔。如果已指定，则还必须在此列表中包含CN。虽然这是可选字段，但必须填写SAN字段才能使可扩展消息传送和网真协议(XMPP)客户端接受证书，否则XMPP客户端将显示证书错误。

第二步：生成Callbridge、Smpp、Webadmin和Webbridge CSR

1. 使用Putty访问CMS CLI并使用管理员帐户登录。
2. 运行以下命令，以便为CMS上所需的每项服务创建CSR。也可以创建具有通配符(*.com)或集群FQDN作为CN、每个CMS服务器的FQDN并且在必要时加入URL的单个证书。

服务	命令
Webadmin	pki csr <cert name> CN:<server FQDN>
Webbridge	pki csr <cert name> CN:<Server FQDN> subjectAltName:<Join Url>,<XMPP domain>
Callbridge TURN 负载均衡器	pki csr <cert name> CN:<Server FQDN's>

3. 如果CMS是集群的，请运行以下命令。

服务	命令
Callbridge TURN 负载均衡器	pki csr <cert name> CN:<cluster FQDN> subjectAltName:<Peer FQDN's>
XMPP	pki csr <cert name> CN:<Cluster FQDN> subjectAltName:<XMPP Domain>,<Peer FQDN's>

第三步：生成数据库集群CSR并使用内置CA对其进行签名

从CMS 2.7开始，您需要拥有数据库集群的证书。 在2.7中，我们包含一个可用于签署数据库证书的内置CA。

1. 在所有核心上运行database cluster remove。
2. 在主上，运行pki selfsigned dbca CN。示例：Pki selfsigned dbca CN：tplab.local
3. 在主上，运行pki csr dbserver CN：cmscore1.example.com subjectAltName。 示例：cmscore2.example.com，cmscore3.example.com。
4. 在主要上，为数据库clientpki csr dbclient CN：postgres创建证书。
5. 在主上，使用dbca签署dbserver certpki签署dbserver dbca。
6. 在主上，使用dbca签署dbclient证书pki签署dbclient dbca。
7. 将dbclient.crt复制到需要连接到数据库节点的所有服务器
8. 将dbserver.crt文件复制到已加入数据库的所有服务器（构成数据库集群的节点）。
9. 将dbca.crt文件复制到所有服务器。
10. 在主DB服务器上，运行数据库集群证书dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt。 这将使用dbca.crt作为根ca证书。
11. 在主DB服务器上，运行数据库集群localnode a。
12. 在主DB服务器上，运行数据库群集初始化。
13. 在主DB服务器上，运行数据库群集状态。 必须看到节点：(me)：已连接的主节点。
14. 在已加入数据库集群的所有其他内核上，运行数据库集群证书dbserver.key dbserver.crt dbclient.key dbclient.crt dbca.crt。
15. 在连接到数据库集群（而不是与数据库共置）的所有内核上，运行database cluster certs dbclient.key cbclient.crt dbca.crt.

    - 在已连接的核心上（与数据库共置）：

        - 运行**database cluster localnode a**。

        - 运行**database cluster join**。

- 在已连接（不与数据库共置）的内核上：
    - 运行数据库集群**localnode a**.
        - 运行**database cluster connect**.

第四步：验证签名证书

- 证书有效性（到期日期）可以通过证书检查进行验证，请运行**pki inspect <filename>**命令。
- 您可以验证证书是否与私有密钥匹配，请运行**pki match <keyfile> <certificate file>**命令。
- 要验证证书是否由CA签署，以及证书捆绑是否可用于声明证书，请运行**pki verify <cert> <certificate bundle/Root CA>**命令。

第五步：将签名证书应用于CMS服务器上的组件

- 要将证书应用到Webadmin，请运行以下命令：

webadmin disable webadmin certs <keyfile> <certificate file> <certificate bundle/Root CA> webadmin enable

- 要将证书应用于Callbridge，请运行以下命令：

callbridge certs <keyfile> <certificate file> <certificate bundle/Root CA> callbridge restart

- 要将证书应用到Webbridge，请运行以下命令：

webbridge disable webbridge certs <keyfile> <certificate file> <certificate bundle/Root CA> webbridge enable

- 要将证书应用于XMPP，请运行以下命令：

xmpp disable xmpp certs <keyfile> <certificate file> <certificate bundle/Root CA> xmpp enable

- 要将证书应用于数据库或替换当前数据库群集上的过期证书，请运行以下命令：

database cluster remove (on all servers, noting who was primary before beginning) database cluster certs <server_key> <server_certificate> <client_key> <
database cluster initialize (only on primary node)
database cluster join <FQDN or IP of primary> (only on slave node)
database cluster connect <FQDN or IP of primary> (only on nodes that are not part of the database cluster)

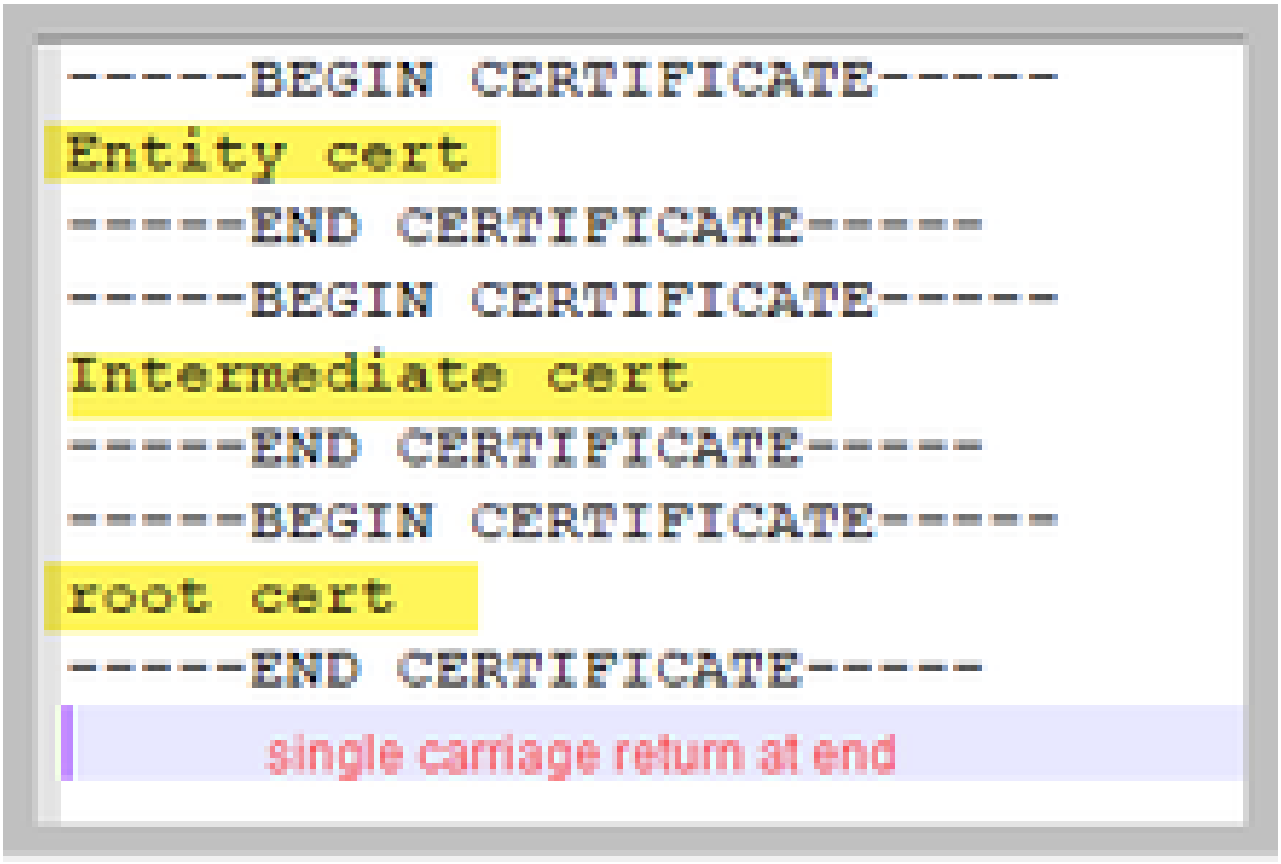
- 要将证书应用到TURN，请运行以下命令：

turn disable turn certs <keyfile> <certificate file> <certificate bundle/Root CA> turn enable

证书信任链和捆绑包

从CMS 3.0开始，您需要使用证书信任链或完整链信任。 此外，对于您了解如何在制作捆绑包时构建证书的任何服务而言，这一点也非常重要。

当按照Web网桥3的要求构建证书信任链时，必须构建如图所示的证书信任链，其中实体证书位于顶部，中间证书位于中间，根CA位于底部，然后返回一个回车。



无论何时创建捆绑，证书的末尾都必须只有一个回车符。

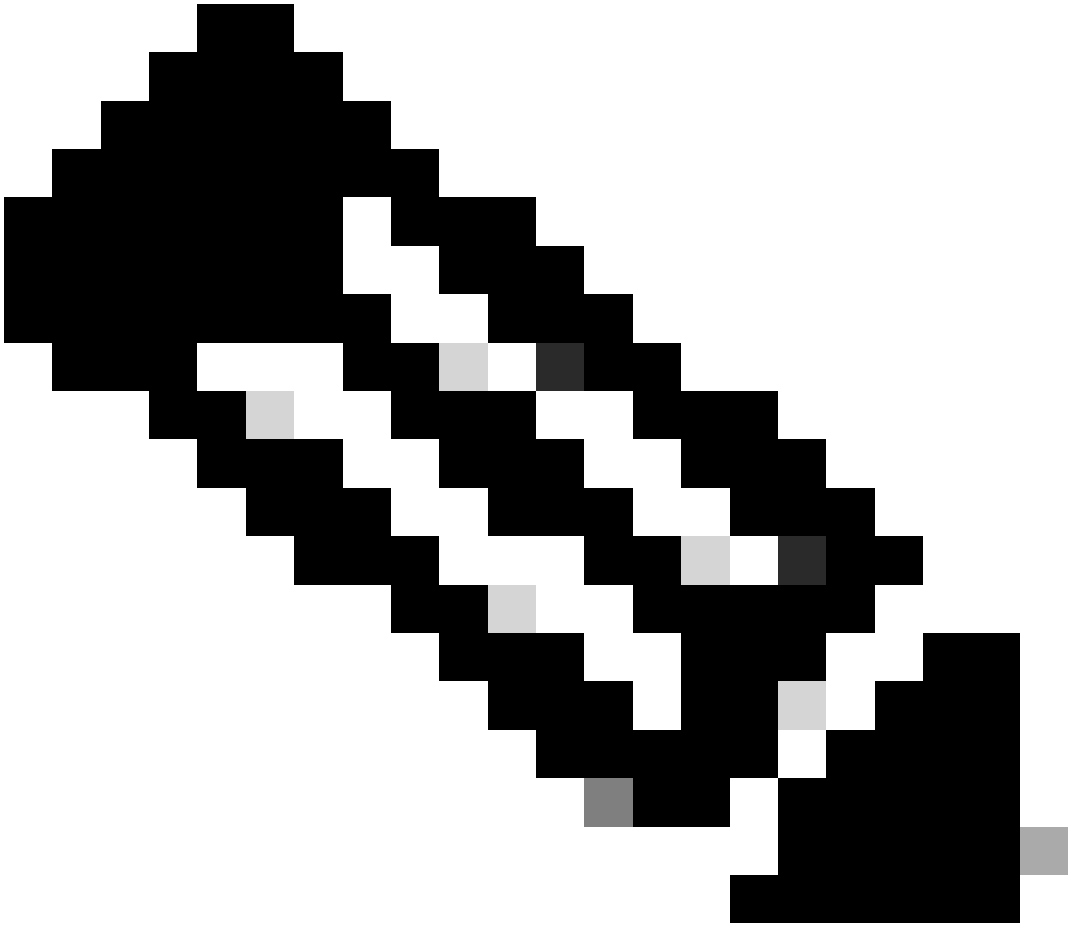
CA捆绑包与图中所示相同，当然，没有实体证书。

故障排除

如果需要替换除数据库证书之外的所有服务的过期证书，最简单的方法是上传与旧证书同名的新证书。如果执行此操作，只需重新启动服务，而无需重新配置服务。

如果您执行**pki csr ...**且证书名称与当前密钥匹配，则会立即中断服务。 如果生产现场且您主动创建了新的CSR和密钥，请使用新名称。 在将新证书上传到服务器之前，可以重命名当前活动名称。

如果数据库证书已过期，您需要查看数据库集群状态谁是数据库主节点，并在所有节点上运行**database cluster remove**命令。 然后可以使用步骤3中的说明。生成数据库集群CSR并使用内置CA对其进行签名。



注意：如果需要更新思科会议管理器(CMM)证书，请参阅下一个视频：更新思科会议管理SSL证书。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。