自动执行CVP证书命令

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[命令说明](#)
[命令](#)
[别名备份](#)
[导出密钥库](#)
[删除别名](#)
[创建新的自签名证书](#)
[导出自签名证书](#)
[生成证书签名请求 (CSR)](#)
[导入CA签名证书](#)
[验证](#)
[故障排除](#)

简介

本文档介绍一种自动执行与CVP证书一起使用的各种命令的方法。这还提供了使证书符合RFC的选项。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科语音门户(CVP)
- Java键工具
- 公钥基础设施(PKI)证书

使用的组件

本文档中的信息基于以下软件版本：

- 思科语音门户(CVP)12.5(1)
- 统一联络中心企业版(UCCE)
- 套装联络中心企业版(PCCE)
- 运营和管理管理门户(OAMP)

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。

配置

命令说明

这些命令旨在通过CVP在很大程度上自动执行管理证书中使用的命令。这些不受官方支持，但需经过测试。

security.properties输出示例：

```
Security.keystorePW = xt_PXM-*4Z!!ZQID7YX*6K(3iii
```

使这些命令能够自动执行的部分是第一部分。本部分显示该行，然后说明其工作原理。

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO <command>
```

命令部分：

命令部分	解释
FOR /f	这是DOS FOR命令，带有用于处理特定匹配文件内容的交换机。
"令牌=3"	这表示我们需要第3个令牌或单词。 使用本部分所示的security.properties文件示例，3个令牌为： 令牌1:Security.keystorePW 令牌2:= 令牌3:xt_PXM-*4Z!!ZQID7YX*6K(3iii)
%i	这是存储与FOR参数匹配的IN命令值的变量。
输入(“更多%CVP_HOME%\conf\security.properties”)	执行命令“more %CVP_HOME%\conf\security.properties”，并将内容传递到FO令。
DO <command>	执行命令并传递%i的值。

本文档中显示的命令读取security.properties中的口令，并自动输入keystore命令。这可确保最终用户无需键入或复制/粘贴此密码，并消除可能导致的错误。

命令

示例命令全部与名为cvp_certificate的别名配合使用。确保根据需要替换别名。

别名备份

此命令通常不使用，但有助于备份旧证书和私钥。

该示例将cvp_certificate重命名为cvp_certificate_back。

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -changealias -alias cvp_certificate -destalias cvp_certificate_back
```

导出密钥库

此命令将整个密钥库导出到文本文件。这允许用户检查密钥库的内容。

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -list -v > %CVP_HOME%\conf\security\cvp_keystore.txt
```

删除别名

此命令删除当前别名和证书。此过程不可撤销，强烈建议您备份密钥库。

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -delete -alias cvp_certificate
```

创建新的自签名证书

此命令会创建新的自签名证书。即使您选择由证书颁发机构(CA)签名证书，也需要此命令，因为这样会创建证书所需的私钥。

对于没有SAN的RSA证书（典型）：

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -genkeypair -alias cvp_certificate -keysize 2048 -keyalg RSA -validity 1825
```

对于带SAN的RSA证书：

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -genkeypair -alias cvp_certificate -keysize 2048 -keyalg RSA -validity 1825 -ext
san=dns:mycvp.mydomain.com,dns:localhost
```

主题备用名称

-ext参数允许用户访问特定分机。所示示例添加了主题备用名称(SAN)，其中包含服务器的完全限定域名(FQDN)以及本地主机。可以将其他SAN字段添加为逗号分隔值。

有效的SAN类型包括：

```
ip:192.168.0.1
dns:myserver.mydomain.com
email:name@mydomain.com
```

每个命令都需要提供6个值。按顺序排列：公用名、组织单位、组织、城市、州和国家/地区。复制答案并更新它们以符合您的特定要求。然后，可根据需要将其粘贴到命令提示符中。

```
myserver.mydomain.com
My Organizational Unit
My Company
City
My State
US
```

导出自签名证书

此命令导出自签名证书。这允许证书导入到其他组件（如OAMP或PCCE管理数据服务器）。

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -export -alias cvp_certificate -file %CVP_HOME%\conf\security\cvp.crt
```

生成证书签名请求 (CSR)

此命令创建CSR，以便您可以让CA对请求进行签名。对于不带SAN的证书：

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -certreq -alias cvp_certificate -file %CVP_HOME%\conf\security\cvp.csr
```

对于带SAN的证书：

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -certreq -alias cvp_certificate -file %CVP_HOME%\conf\security\cvp.csr -ext
san=dns:mycvp.mydomain.com,dns:localhost
```

注意：您必须在CSR请求中包含SAN扩展，才能使证书包含SAN。

导入CA签名证书

这些命令依次导入CA根、中间和服务器证书。

将证书复制到%CVP_HOME%\conf\security\ directory。

确保根据需要更新别名和证书名称。

```
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -import -v -trustcacerts -alias myrootca -file %CVP_HOME%\conf\security\root.crt
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -import -v -trustcacerts -alias myintermediate -file
%CVP_HOME%\conf\security\intermediate.crt
FOR /f "tokens=3" %i IN ('more %CVP_HOME%\conf\security.properties') DO
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
storepass %i -import -v -trustcacerts -alias cvp_certificate -file
%CVP_HOME%\conf\security\cvp.crt
```

验证

没有步骤可验证此过程。

故障排除

没有排除此过程故障的步骤。

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）。