在较新的Cisco IOS®版本上将PNP用于FND的问题

目录

简介

本文档介绍如何从Windows私钥基础结构(PKI)生成和导出正确的证书，以便与Field Network Director(FND)上的即插即用(PNP)结合使用。

问题

当您尝试使用PNP在较新的Cisco IOS®和Cisco IOS®-XE版本上执行零接触部署(ZTD)时，此过程会因以下PNP错误之一而失败：

```
Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3341,
errorMessage: SSL Server ID check failed after cert-install
Error while creating FND trustpoint on the device. errorCode: PnP Service Error 3337,
errorMessage: Cant get PnP Hello Response after cert-install
```

一段时间后，Cisco IOS®/Cisco IOS®-XE中的PNP代码要求在PNP服务器/控制器（本例中为FND）提供的证书中填充Subject Alternative Name(SAN)字段。

PNP Cisco IOS®代理只检查证书SAN字段中的服务器身份。它不再检查公用名(CN)字段。

这适用于以下版本：

- 思科IOS®版本15.2(6)E2及更高版本
- 思科IOS®版本15.6(3)M4及以上版本
- 思科IOS®版本15.7(3)M2及以上版本
- Cisco IOS® XE Denali 16.3.6及更高版本
- Cisco IOS® XE Everest 16.5.3及更高版本
- Cisco IOS® Everest 16.6.3及更高版本
- 16.7.1及更高版本的所有Cisco IOS®

有关详细信息，请访问：https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

解决方案

大多数FND指南和文档都没有提到SAN字段需要填充。

要创建并导出用于PNP的正确证书并将其添加到密钥库，请执行以下步骤。

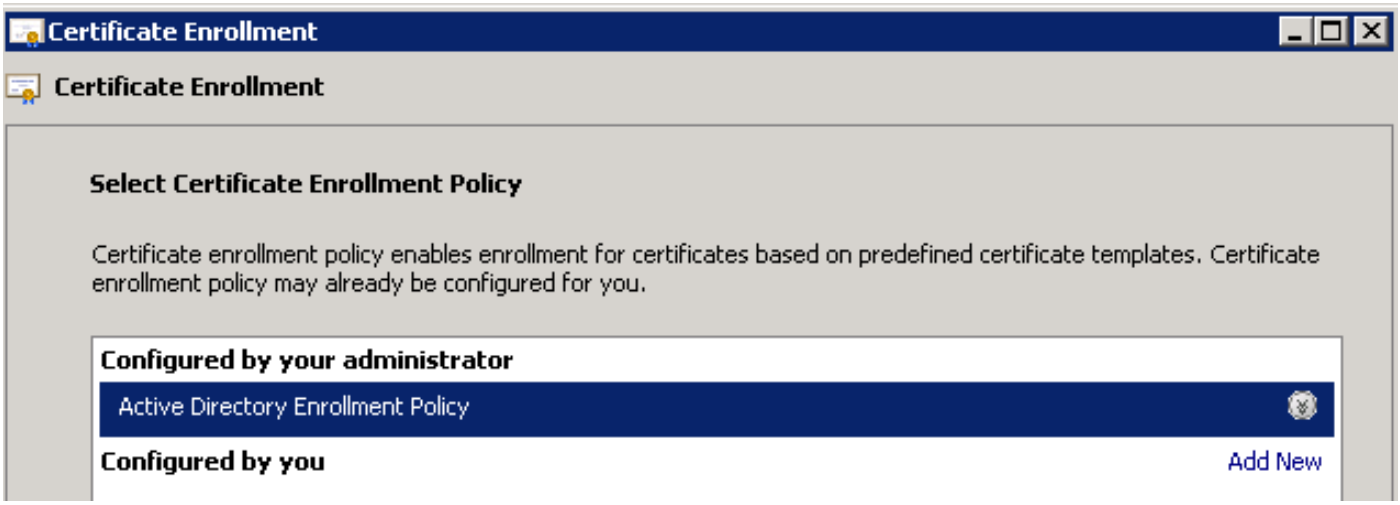
使用Windows CA服务器上的FND/NMS模板生成新证书

导航到**开始>运行> mmc >文件>添加/删除管理单元..... >证书>添加>计算机帐户>本地计算机>确定**，然后打开证书MMC管理单元。

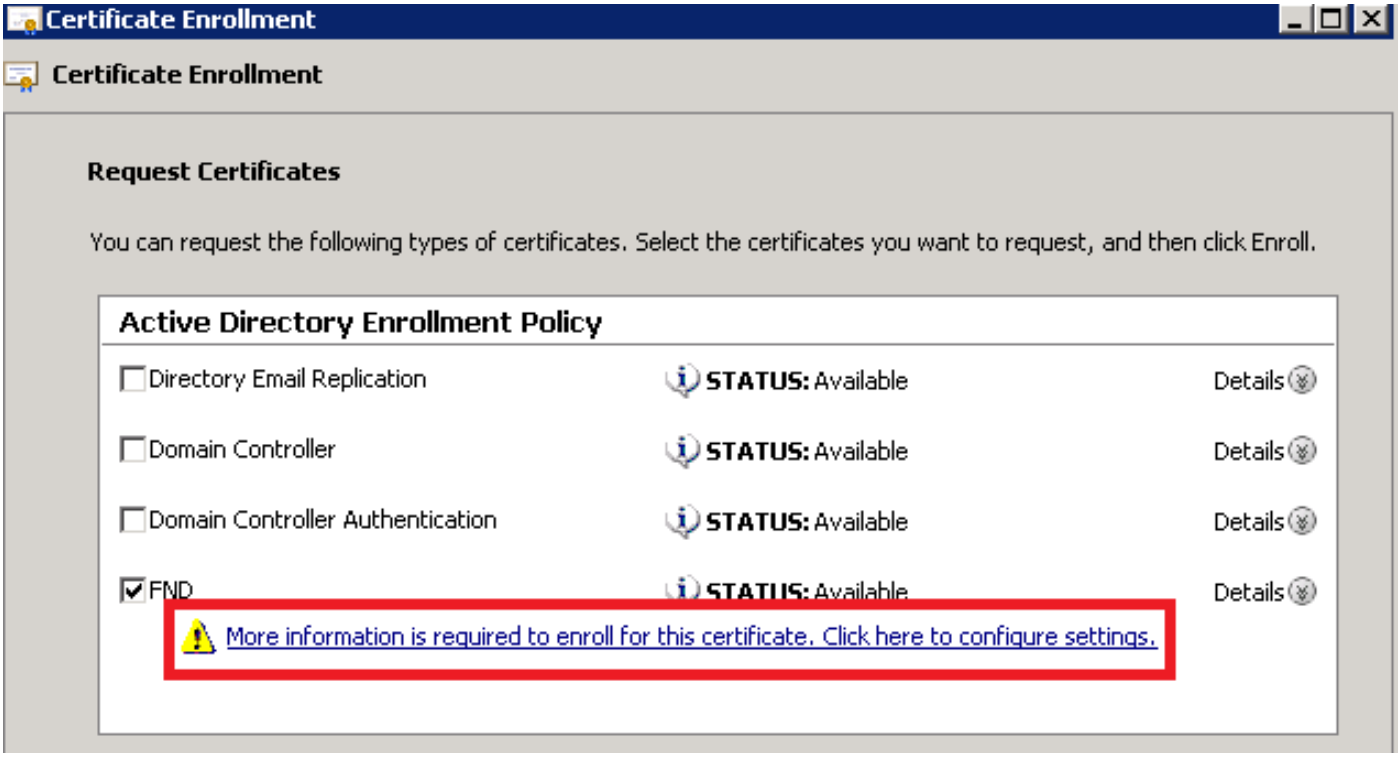
展开证书（本地计算机）>个人>证书

右键单击Certificates并选择**All Tasks > Request New Certificate...**，如图所示。

单击**下一步**，然后选择**Active Directory注册策略**，如图所示。



单击**Next**，选择为NMS/FND-server创建的模板(稍后为TelePresence Server(TPS)重复)，然后单击More Information链接（如图所示）。



在证书属性中，提供以下信息：

主题名称:

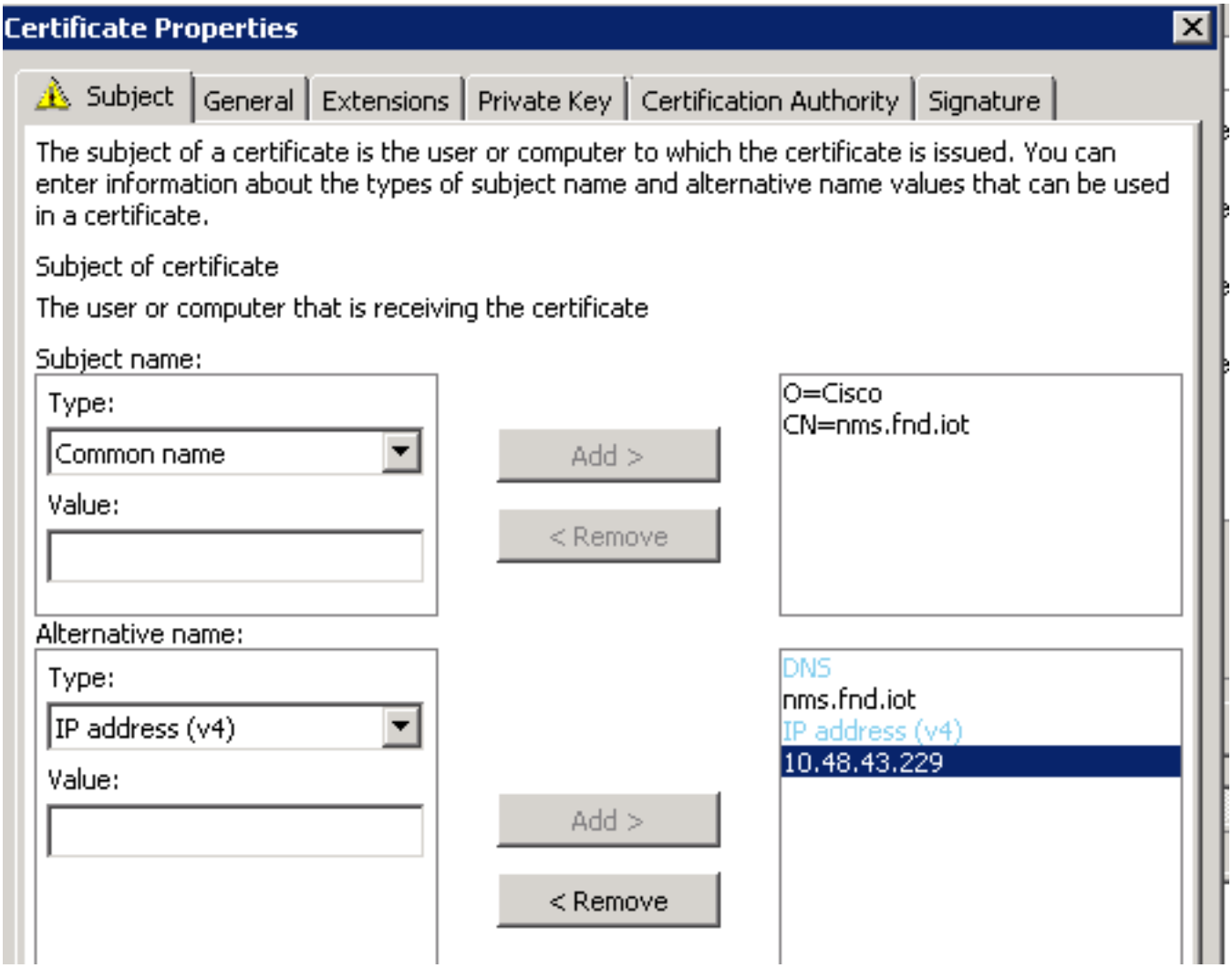
- 组织：您的组织名称
- 公用名：fnd-server（或TPS，如果适用）的完全限定域名(FQDN)

备用名称（SAN字段）：

- 如果使用域名系统(DNS)联系FND服务器的PNP部分，请为FQDN添加DNS条目
- 如果使用IP联系FND服务器的PNP部分，请为IP添加一个IPv4条目

如果发现方法不同，建议在证书中包含多个SAN值。例如，可以在SAN字段中同时包含控制器FQDN和IP地址（或NAT IP地址）。如果确实包括这两者，请将FQDN设置为第一个SAN值，后跟IP地址。

配置示例:



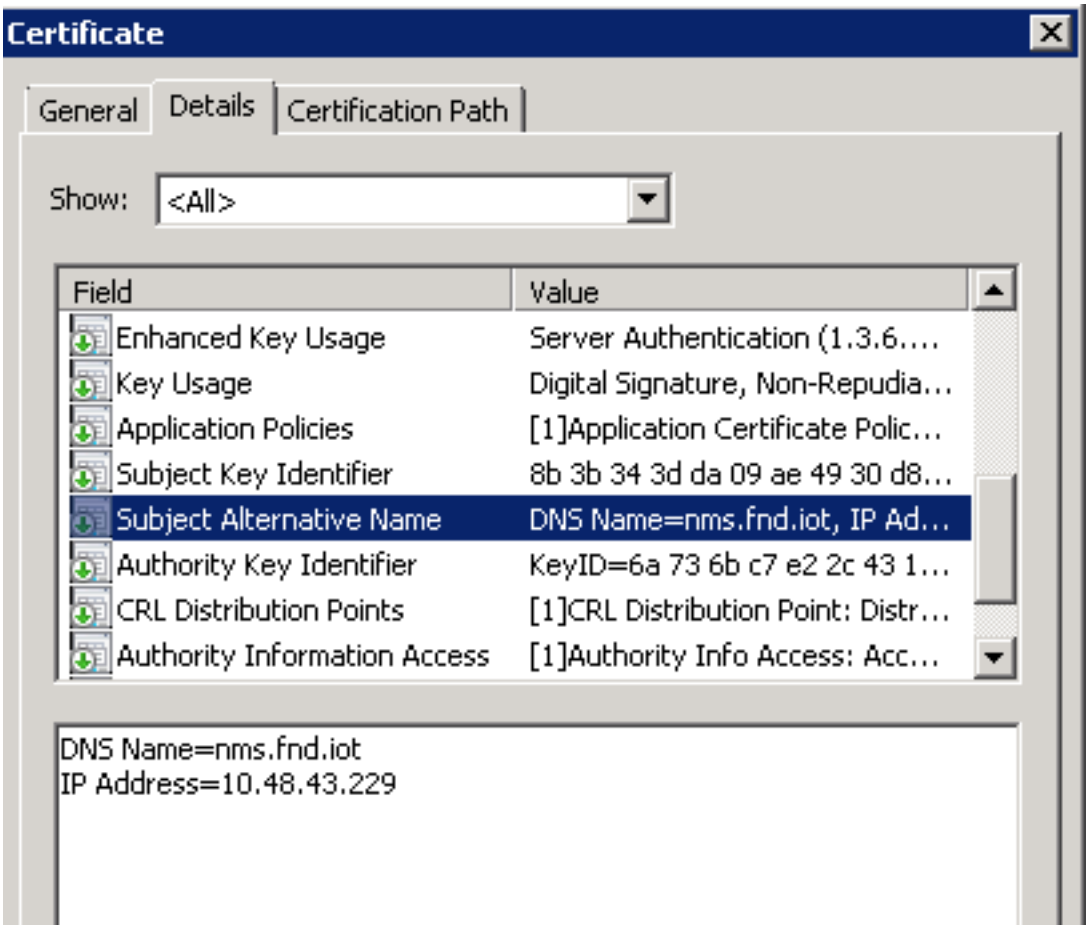
完成后，单击Certificate Properties窗口中的**OK**，然后单击**Enroll**以生成证书，并在生成完成后单击**Finish**。

检查生成的证书中的SAN字段

要检查生成的证书是否包含正确的信息，您可以按如下方式检查它：

在Microsoft管理控制台(MMC)中打开证书管理单元，然后展开**证书（本地计算机）>个人>证书**。

双击生成的证书并打开**Details**选项卡。向下滚动以查找SAN字段，如图所示。

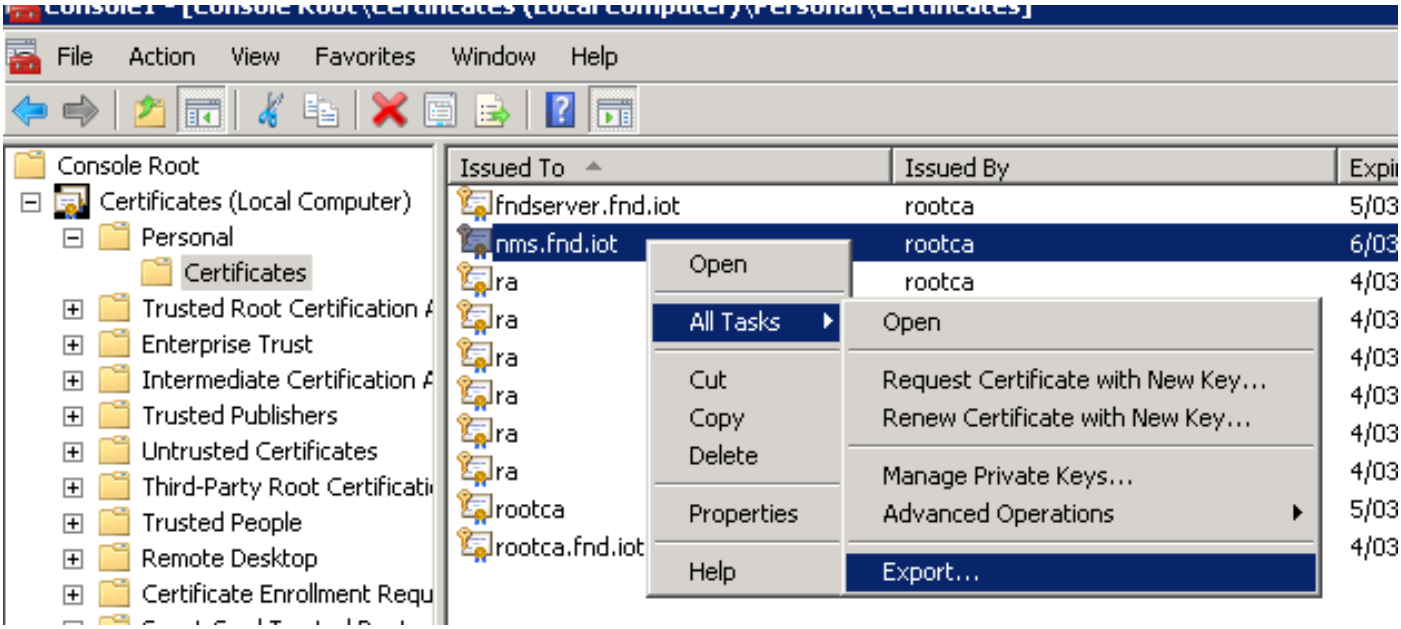


导出证书以导入到FND密钥库

在导入或替换FND密钥库中存在的证书之前，需要将其导出到.pfd文件。

在MMC中的证书管理单元中，展开**证书（本地计算机）>个人>证书**

右键单击生成的证书，然后选择**All Tasks > Export...**（如图所示）。



单击**下一步**，选择以导出私钥，如图所示。

选择以包括证书路径中的所有证书，如图所示。

单击**下一步**，选择导出密码并将**.pfx**保存在已知位置。

创建与PNP一起使用的FND密钥库

现在已导出证书，您可以构建FND所需的密钥库。

将上一步生成的**.pfx**安全地传输到FND服务器(网络管理系统(NMS)计算机或OVA主机)，例如使用SCP。

列出**.pfx**的内容，以便了解导出中自动生成的别名：

```
[root@iot-fnd ~]# keytool -list -v -keystore nms.pfx -srcstoretype pkcs12 | grep Alias
Enter keystore password:  keystore
Alias name: le-fnd-8f0908aa-dc8d-4101-a526-93b4eaad9481
```

使用以下命令创建新密钥库：

```
root@iot-fnd ~]# keytool -importkeystore -v -srckeystore nms.pfx -srcstoretype pkcs12 -
destkeystore cgms_keystore_new -deststoretype jks -srcalias le-fnd-8f0908aa-dc8d-4101-a526-
93b4eaad9481 -destalias cgms -destkeypass keystore
Importing keystore nms.pfx to cgms_keystore_new...
Enter destination keystore password:
```

```
Re-enter new password:
Enter source keystore password:
[Storing cgms_keystore_new]

Warning:
The JKS keystore uses a proprietary format. It is recommended to migrate to PKCS12 which is an
industry standard format using "keytool -importkeystore -srckeystore cgms_keystore_new -
destkeystore cgms_keystore_new -deststoretype pkcs12".
```

在该命令中，确保用正确的文件（从Windows CA导出）替换**nms.pfx**，并且srcalias值与上一个命令(**keytool -list)的输出相匹配。**

生成后，将其转换为建议的新格式：

```
[root@iot-fnd ~]# keytool -importkeystore -srckeystore cgms_keystore_new -destkeystore
cgms_keystore_new -deststoretype pkcs12 Enter source keystore password: Entry for alias cgms
successfully imported. Import command completed: 1 entries successfully imported, 0 entries
failed or cancelled Warning: Migrated "cgms_keystore_new" to Non JKS/JCEKS. The JKS keystore is
backed up as
"cgms_keystore_new.old".
```

将之前导出的CA证书添加到密钥库：

```
[root@iot-fnd ~]# keytool -import -trustcacerts -alias root -keystore cgms_keystore_
new -file rootca.cer Enter keystore password: Owner: CN=rootca, DC=fnd, DC=iot Issuer:
CN=rootca, DC=fnd, DC=iot ... Trust this certificate? [no]: yes Certificate was added to
keystore
```

最后，将用于在使用PNP时通过FAR的序列验证身份的SUDI证书添加到密钥库。

对于RPM安装，SUDI证书与软件包捆绑在一起，可在以下位置找到：**/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem**

对于OVA安装，首先将SUDI证书复制到主机：

```
[root@iot-fnd ~]# docker cp fnd-container:/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem
.
```

然后将其添加为别名SUDI的可信密钥库：

```
[root@iot-fnd ~]# keytool -import -trustcacerts -alias sudi -keystore cgms_keystore_new -file
cisco-sudi-ca.pem
Enter keystore password:
Owner: CN=ACT2 SUDI CA, O=Cisco
Issuer: CN=Cisco Root CA 2048, O=Cisco Systems
...
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

此时，密钥库已准备好与FND一起使用。

激活新/修改密钥库以用于FND

使用密钥库之前，请替换以前的版本，或者更新cgms.properties文件中的密码。

首先，备份已经存在的密钥库：

对于RPM安装：

```
[root@fndnms ~]# cp /opt/cgms/server/cgms/conf/cgms_keystore cgms_keystore_backup
```

对于OVA安装：

```
[root@iot-fnd ~]# cp /opt/fnd/data/cgms_keystore cgms_keystore_backup
```

将现有的替换为新替换：

对于RPM安装：

```
[root@fndnms ~]# cp cgms_keystore_new /opt/cgms/server/cgms/conf/cgms_keystore
```

对于OVA安装：

```
[root@iot-fnd ~]# cp cgms_keystore_new /opt/fnd/data/cgms_keystore
```

或者，更新cgms.properties文件中密钥库的密码：

首先，生成一个新的加密密码字符串。

对于RPM安装：

```
[root@fndnms ~]# /opt/cgms/bin/encryption_util.sh encrypt keystore
7jlXPniVpMvat+TrDWqh1w==
```

对于OVA安装：

```
[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh encrypt
keystore
7jlXPniVpMvat+TrDWqh1w==
```

确保使用正确的密钥库密码替换密钥库。

对于基于RPM的安装，请在/opt/cgms/server/cgms/conf/cgms.properties中更改cgms.properties，对于基于OVA的安装更改/opt/fnd/data/cgms.properties，以便包含新的加密密码。

最后，重新启动FND以开始使用新的密钥库和密码。

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）。