在較新Cisco IOS®版本上將PNP用於FND的問題

目錄

<u>簡介</u>

問題 解決方案 使用Windows CA伺服器上的FND/NMS模板生成新證書 檢查生成的證書中的SAN欄位 匯出證書以匯入到FND金鑰庫 建立與PNP一起使用的FND金鑰庫 啟用新/修改金鑰庫以用於FND

簡介

本檔案介紹如何從Windows私密金鑰基礎架構(PKI)產生和匯出正確憑證,以與Field Network Director(FND)上的即插即用(PNP)結合使用。

問題

嘗試使用PNP在較新的Cisco IOS®和Cisco IOS®-XE版本上執行零接觸部署(ZTD)時,此程式會失 敗,並出現以下PNP錯誤之一:

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

一段時間以來,Cisco IOS®/Cisco IOS®-XE中的PNP代碼要求在PNP伺服器/控制器(本例中為 FND)提供的證書中填寫「使用者替代名稱(SAN)」欄位。

PNP Cisco IOS®代理只檢查證書SAN欄位中的伺服器標識。它不再檢查公用名(CN)欄位。

此版本對以下版本有效:

- Cisco IOS®版本15.2(6)E2及更新版本
- Cisco IOS®版本15.6(3)M4及更新版本
- Cisco IOS®版本15.7(3)M2及更新版本
- Cisco IOS® XE Denali 16.3.6及更新版本
- Cisco IOS® XE Everest 16.5.3及更高版本
- Cisco IOS® Everest 16.6.3及更高版本
- 所有Cisco IOS®版本(16.7.1及更高版本)

有關詳細資訊,請訪問:<u>https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-</u> Play/solution/guidexml/b_pnp-solution-guide.html#id_70663

解決方案

FND的大部分指南和文檔都未提及SAN欄位需要填充。

要建立並匯出用於PNP的正確證書並將其新增到金鑰庫,請執行以下步驟。

使用Windows CA伺服器上的FND/NMS模板生成新證書

導航到「開始」>「運行」>「mmc」>「檔案」>「新增/刪除管理單元……」>「證書」>「新增>電 腦帳戶」>「本地電腦」>「確定」,然後開啟證書MMC管理單元。

展開Certificates(Local Computer)> Personal > Certificates

按一下右鍵「Certificates」,然後選擇**「All Tasks」>「Request New Certificate...」**,如下圖所示 。



按一下「Next」,然後選擇「Active Directory Enrollment Policy」,如下圖所示。

ling Ce	ertificate Enrollment	
🗐 C	ertificate Enrollment	
	Select Certificate Enrollment Policy Certificate enrollment policy enables enrollment for certificates based on predefined certificate templates. Ce enrollment policy may already be configured for you.	rtificate
	Configured by your administrator	
	Active Directory Enrollment Policy	8
	Configured by you	vdd New

按一下「**Next**」,然後選擇為NMS/FND-server建立的模板(稍後為TelePresence Server(TPS)重複),然後按一下「More Information」連結,如下圖所示。

ates. Select the certificates you want to reque	est, and then click Enroll.
×y	
i) STATUS: Available	Details 🛞
i) STATUS: Available	Details 🛞
i) STATUS: Available	Details 🛞
i) STATUS: Available	Details 🛞
roll for this certificate. Click here to configure	settings.
	ates. Select the certificates you want to reque Y STATUS: Available STATUS: Available STATUS: Available STATUS: Available STATUS: Available Model of this certificate. Click here to configure

在證書屬性中,提供以下資訊:

使用者名稱:

• 組織:您的組織名稱

• 公用名:fnd伺服器的完全限定域名(FQDN)(如果適用,則為TPS) 備用名稱(SAN欄位):

•如果使用域名系統(DNS)來聯絡FND伺服器的PNP部分,請為FQDN新增DNS條目

•如果使用IP連線至FND伺服器的PNP部分,請為IP新增IPv4專案 建議證書中包括多個SAN值,以防發現方法不同。例如,可以在SAN欄位中同時包含控制器 FQDN和IP地址(或NAT IP地址)。如果包含這兩個引數,請將FQDN設定為第一個SAN值,後跟 IP地址。

配置示例:

ertificate Properties 🛛 🔀			
🔥 Subject General Extension	s Private Key Certificatio	n Authority Signature	
The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.			
Subject of certificate The user or computer that is receiving the certificate			
Subject name:			
Туре:		O=Cisco	
Common name	Add >		
Value:			
	< Remove		
Alternative name:	1	DMC	
Type:		nms.fnd.iot	
IP address (v4)		IP address (v4)	
Value:		10.48.43.229	
	Add >		
	< Remove		

完成後,在「Certificate Properties(證書屬性)」視窗中按一下OK,然後按一下Enroll以生成證書 ,並在生成完成後按一下Finish。

檢查生成的證書中的SAN欄位

只是為了檢查生成的證書是否包含正確的資訊,您可以按如下方式檢查它:

在Microsoft管理控制檯(MMC)中開啟證書管理單元,然後展開證書(本地電腦)>個人>證書。

按兩下生成的證書並開啟Details頁籤。向下滾動以查詢SAN欄位,如下圖所示。

ertificate General Details Certification Path]	×
Show: <a>All>	•	
Field	Value	
 Enhanced Key Usage Key Usage Application Policies Subject Key Identifier Subject Alternative Name Authority Key Identifier CRL Distribution Points Authority Information Access 	Server Authentication (1.3.6 Digital Signature, Non-Repudia [1]Application Certificate Polic 8b 3b 34 3d da 09 ae 49 30 d8 DNS Name=nms.fnd.iot, IP Ad KeyID=6a 73 6b c7 e2 2c 43 1 [1]CRL Distribution Point: Distr [1]Authority Info Access: Acc	
DNS Name=nms.fnd.iot IP Address=10.48.43.229		

匯出證書以匯入到FND金鑰庫

在可以匯入或替換FND金鑰庫中的證書之前,需要將其匯出到.pfd文件。

在MMC中的證書管理單元中,展開**證書(本地電腦)>個人>證書**

按一下右鍵生成的證書,然後選擇**「所有任務」>「匯出**...」,如下圖所示。

🚾 consolet - Teousole voor/cercii	icaces (cocar con	ipucery\rerson	ar/ceruncaces]	
🚠 File Action View Favorites	Window Help			
(= =) 🖄 📅 🖌 🖬 🗙 🕻	1 🛃 🛛 🖬			
🦰 Console Root	Issued To 🔺		Issued By	Expi
🖃 🔜 Certificates (Local Computer)	🛱 fndserver.fnd.	iot	rootca	5/03
🖃 🧮 Personal	🖏 nms.fnd.iot 🛛	0	rootca	6/03
Certificates	🔄 🖾	Open	rootca	4/03
Trusted Root Certification 4	🔄 🖾	All Tasks 🔹 🕨	Open	4/03
🕀 📃 Enterprise Trust	🤹 ra			4/03
Intermediate Certification A	🖾 ra	Cut	Request Certificate with New Key	4/03
🕀 🚞 Trusted Publishers	1 Ta	Сору	Renew Certificate with New Key	4/03
🕀 🚞 Untrusted Certificates		Delete	Managan Dukusha Kawa	4/03
🕀 🚞 Third-Party Root Certificati			Manage Private Keys	- 703 - 5703
🕀 🚞 Trusted People		Properties	Advanced Operations	5/03
🕀 🚞 Remote Desktop	Arootca.rnd.iot	Help	Export	4/03
🕀 🚞 Certificate Enrollment Requ	l			
l 🖂 🖴 e ne te nite n l				

按一下Next,選擇以匯出私鑰,如下圖所示。

Certificate Export Wizard	×
Export Private Key	ŀ
You can choose to export the private key with the certificate.	ł
Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
Do you want to export the private key with the certificate?	
Yes, export the private key	
O No, do not export the private key	
選擇該選項以在證書路徑中包含所有證書,如下圖所示。	
Personal Information Exchange - PKCS #12 (.PFX)	
Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export all extended properties	
C Microsoft Serialized Certificate Store (.SST)	
按一下 下一步 ,選擇匯出密碼並將 .pfx 儲存到已知位置。	
建立與PNP一起使用的FND金鑰庫	
匯出證書後,即可構建FND所需的金鑰庫。	

將上一步生成的**.pfx**安全地傳輸到FND伺服器(網路管理系統(NMS)電腦或OVA主機),例如使用SCP。

列出.pfx的內容以瞭解匯出中的自動生成的別名:

[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 使用以下命令建立新的金鑰庫:

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".

在命令中,確保將**nms.pfx**替換成正確的檔案(從Windows CA匯出),並且srcalias值將與以前命 令(**keytool -list**)的輸出匹配。

生成後,將其轉換為建議的新格式:

[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".

將之前匯出的CA證書新增到金鑰庫:

[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

最後,將SUDI證書新增到金鑰庫,該證書用於在使用PNP時通過FAR的串列驗證身份。

對於RPM安裝,SUDI證書與軟體包捆綁在一起,可在以下網址找到 :/opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pem

對於OVA安裝,首先將SUDI證書複製到主機:

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

然後將其新增到金鑰庫中,作為別名SUDI的信任:

[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

此時,金鑰庫已準備好用於FND。

啟用新/修改金鑰庫以用於FND

使用keystore之前,請替換先前版本並更新cgms.properties檔案中的密碼(可選)。

首先,對已經存在的金鑰庫進行備份:

對於RPM安裝:

[root@fndnms ~]# cp /opt/cgms/server/cgms/conf/cgms_keystore cgms_keystore_backup 對於OVA安裝:

[root@iot-fnd ~]# cp /opt/fnd/data/cgms_keystore cgms_keystore_backup 將現有的替換為新版本:

對於RPM安裝:

[root@fndnms ~]# cp cgms_keystore_new /opt/cgms/server/cgms/conf/cgms_keystore 對於OVA安裝:

[root@iot-fnd ~]# cp cgms_keystore_new /opt/fnd/data/cgms_keystore 或者,更新cgms.properties檔案中金鑰庫的密碼:

首先,生成一個新的加密密碼字串。

對於RPM安裝:

[root@fndnms ~]# /opt/cgms/bin/encryption_util.sh encrypt keystore 7jlXPniVpMvat+TrDWqhlw== 對於OVA安裝:

[root@iot-fnd ~]# docker exec -it fnd-container /opt/cgms/bin/encryption_util.sh encrypt
keystore

7jlXPniVpMvat+TrDWqh1w==

確保使用正確的金鑰庫密碼替換金鑰庫。

對於基於RPM的安裝,請更改/opt/cgms/server/cgms/conf/cgms.properties中的 cgms.properties,對於基於OVA的安裝,請更改/opt/fnd/data/cgms.properties,以便包括新的加密 密碼。

最後,重新啟動FND以開始使用新的金鑰庫和密碼。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。