新しいCisco IOS®リリースでのFNDでのPNPの 使用に関する問題

内容

<u>概要</u>

<u>問題</u>

<u>解決方法</u>

<u>Windows CAサーバ上のFND/NMSテンプレートを使用した新しい証明書の生成</u> <u>生成された証明書のSANフィールドを確認します。</u> <u>FNDキーストアにインポートする証明書のエクスポート</u> <u>PNPで使用するFNDキーストアの作成</u> FNDで使用する新規/変更されたキーストアのアクティブ化

概要

このドキュメントでは、Field Network Director(FND)のプラグアンドプレイ(PNP)と組み合わせて 使用するために、Windows Private Key Infrastructure(PKI)から正しい証明書を生成してエクスポ ートする方法について説明します。

問題

新しいCisco IOS®およびCisco IOS®-XEリリースでPNPを使用してZero Touch Deployment(ZTD)を実行しようとすると、次のいずれかのPNPエラーでプロセスが失敗します。

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 Cisco IOS®/Cisco IOS®-XEのPNPコードでは、PNPサーバ/コントローラ(この場合はFND)が 提供する証明書にサブジェクト代替名(SAN)フィールドを入力する必要があります。

PNP Cisco IOS®エージェントは、サーバIDの証明書SANフィールドのみをチェックします。共通名(CN)フィールドはチェックされなくなりました。

これは次のリリースで有効です。

- Cisco IOS®リリース15.2(6)E2以降
- Cisco IOS®リリース15.6(3)M4以降
- Cisco IOS®リリース15.7(3)M2以降
- Cisco IOS® XE Denali 16.3.6以降
- Cisco IOS® XE Everest 16.5.3以降
- Cisco IOS® Everest 16.6.3以降
- ・16.7.1以降のすべてのCisco IOS®リリース

詳細については、次のサイトを参照してください<u>。</u> <u>https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-</u> <u>Play/solution/guidexml/b_pnp-solution-guide.html#id_70663</u>

解決方法

FNDに関するガイドやドキュメントのほとんどは、SANフィールドにデータを入力する必要があることを言及していません。

PNPで使用する正しい証明書を作成してエクスポートし、キーストアに追加するには、次の手順 を実行します。

Windows CAサーバ上のFND/NMSテンプレートを使用した新しい証明書の生成

[Start] > [Run] > [mmc] > [File] > [Add/Remove Snap-in...] > [Certificates] > [Add] > [Computer Account] > [Local Computer] > [OK] に移動し、証明書MMCスナップインを開きます。

[Certificates (Local Computer)] > [Personal] > [Certificates]を展開します

図に示すように、[Certificates]を右クリックし、[All Tasks] > [Request New Certificate...] を選択 します。



図に示すように、[Next] をクリックし、[Active Directory Enrollment Policy] を選択します。



[Next] をクリックし、NMS/FND-server用に作成したテンプレートを選択し(後でTelePresence Server(TPS)に対して繰り返します)、図に示すように[More Information] リンクをクリックします

rtificate Enrollment		
Request Certificates		
You can request the following types of certifica	ates. Select the certificates you want to reque	est, and then click Enroll.
Active Directory Enrollment Polic	×y	
Directory Email Replication	i) STATUS: Available	Details 🛞
Domain Controller	i) STATUS: Available	Details 🛞
Domain Controller Authentication	i) STATUS: Available	Details 🛞
	(i) STATUS: Available	Details 🛞
More information is required to en	roll for this certificate. Click here to configure	settings.

証明書のプロパティで、次の情報を入力します。

Subject Name:

0

• 組織: 組織名

 ・一般名:FNDサーバの完全修飾ドメイン名(FQDN)(該当する場合はTPS)

 別名(SANフィールド):

ドメインネームシステム(DNS)を使用してFNDサーバのPNP部分に接続する場合は、
 FQDNのDNSエントリを追加します

• IPを使用してFNDサーバのPNP部分に接続する場合は、IPのIPv4エントリを追加します 検出方法が異なる場合に備えて、証明書に複数のSAN値を含めることを推奨します。たとえば、 SANフィールドにコントローラのFQDNとIPアドレス(またはNAT IPアドレス)の両方を含める ことができます。両方を含める場合は、最初のSAN値としてFQDNを設定し、その後にIPアドレ スを設定します。

設定例:

Certificate 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 receiv	ving 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					

完了したら、[Certificate Properties]ウィンドウで[OK] をクリックし、[Enroll] をクリックして証明 書を生成し、生成が完了したら[Finish] をクリックします。

生成された証明書のSANフィールドを確認します。

生成された証明書に正しい情報が含まれているかどうかを確認するには、次のように確認します。

Microsoft管理コンソール(MMC)で証明書スナップインを開き、[Certificates (Local Computer)] > [Personal] > [Certificates] を展開します。

生成された証明書をダブルクリックし、[Details] タブを開きます。下にスクロールして、図のように[SAN]フィールドを探します。

tificate eneral Details Certification Path]	E
ihow: <all></all>	•	
Field	Value	
🛐 Enhanced Key Usage	Server Authentication (1.3.6	
🛐 Key Usage	Digital Signature, Non-Repudia	
🛐 Application Policies	[1]Application Certificate Polic	
🛐 Subject Key Identifier	8b 3b 34 3d da 09 ae 49 30 d8	
🐻 Subject Alternative Name	DNS Name=nms.fnd.iot, IP Ad	
🛐 Authority Key Identifier	KeyID=6a 73 6b c7 e2 2c 43 1	
🛐 CRL Distribution Points	[1]CRL Distribution Point: Distr	
Authority Information Access	[1]Authority Info Access: Acc	•
DNS Name=nms.fnd.iot IP Address=10.48.43.229		٦

FNDキーストアにインポートする証明書のエクスポート

FNDキーストアに存在する証明書をインポートまたは置き換える前に、.pfdファイルにエクスポートする必要があります。

MMCの証明書スナップインで、[証明書(ローカルコンピューター)] > [個人] > [証明書] の順に 展開します

生成された証明書を右クリックし、図に示すように[All Tasks] > [Export...]を選択します。

🚾 consolet – Econsole kooc/cercii	icaces (cocar con	ipacer)/rersona	arcerancaces	
🚠 File Action View Favorites	Window Help			
🗢 🔿 🖄 📅 🖌 👫 🗱	3 🗟 🛛 🖬			
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	🔄 🖾 ra	Open	rootca	4/03
표 🚞 Trusted Root Certification A	🖾 ra	All Tasks 🔹 🕨	Open	4/03
표 🚞 Enterprise Trust	🤹 ra			4/03
표 🚞 Intermediate Certification A		Cut	Request Certificate with New Key	4/03
표 🧮 Trusted Publishers		Сору	Renew Certificate with New Key	4/02
표 🚞 Untrusted Certificates	iana iana	Delete		4/03
표 🚞 Third-Party Root Certificati			Manage Private Keys	4/03
🛨 🚞 Trusted People	Salrootca	Properties	Advanced Operations	5/03
표 🚞 Remote Desktop	Salrootca.fnd.iot	Help	Export	4/03
표 🚞 Certificate Enrollment Requ		Tiop	exportin	1
l 🖂 🖂 e de de da da d	1			

Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

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

図に示すように、すべての証明書を認証パスに含めるために選択します。

попле за селинстве и си селинствиот рай на роззиле.

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)

Nextをクリックし、エクスポート用のパスワードを選択して、.pfxを既知の場所に保存します。

PNPで使用するFNDキーストアの作成

証明書をエクスポートしたので、FNDに必要なキーストアを構築できます。

前の手順で生成した**.pfx**を、SCPなどを使用して、FNDサーバ(Network Management Systems(NMS)マシンまたはOVAホスト)に安全に転送します。

.pfxの内容をリストして、エクスポートで自動生成されたエイリアスを確認します。

[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 次のコマンドを使用して、新しいキーストアを作成します。 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".

コマンドで、nms.pfxを正しいファイル(Windows CAからエクスポートされたファイル)に置き 換え、srcalias値が前のコマンド(keytool -list)の出力と一致することを確認します。

生成した後で、次に示すように新しい形式に変換します。

[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".

先ほどエクスポートしたCA証明書をキーストアに追加します。

[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

最後に、キーストアにSUDI証明書を追加します。この証明書は、PNPを使用するときにFARのシ リアルによるIDを確認するために使用されます。

RPMインストールの場合、SUDI証明書はパッケージにバンドルされており、 /opt/cgms/server/cgms/conf/ciscosudi/cisco-sudi-ca.pemにあります。

OVAをインストールする場合は、最初にSUDI証明書をホストにコピーします。

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

次に、これをエイリアスSUDIで信頼できるキーストアに追加します。

[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 この時点で、キーストアはFNDで使用できる状態になります。

FNDで使用する新規/変更されたキーストアのアクティブ化

キーストアを使用する前に、以前のバージョンを置き換え、オプションでcgms.propertiesファイ ルのパスワードを更新します。

まず、既存のキーストアのバックアップを取ります。

RPMインストールの場合:

[root@fndnms ~]# cp /opt/cgms/server/cgms/conf/cgms_keystore cgms_keystore_backup OVAインストールの場合:

[root@iot-fnd ~]# cp /opt/fnd/data/cgms_keystore cgms_keystore_backup 既存のものを新しいものと置き換えます。

RPMインストールの場合:

[root@fndnms ~]# cp cgms_keystore_new /opt/cgms/server/cgms/conf/cgms_keystore OVAインストールの場合:

[root@iot-fnd ~]# cp cgms_keystore_new /opt/fnd/data/cgms_keystore 必要に応じて、cgms.propertiesファイルのキーストアのパスワードを更新します。

まず、新しい暗号化されたパスワード文字列を生成します。

RPMインストールの場合:

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

OVAインストールの場合:

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

7jlXPniVpMvat+TrDWqh1w==

キーストアをキーストアの正しいパスワードに置き換えてください。

新しい暗号化パスワードを含めるには、RPMベースのインストールの場合は

/opt/cgms/server/cgms/conf/cgms.propertiesでcgms.propertiesを変更し、OVAベースのインスト ールの場合は/opt/fnd/data/cgms.propertiesで変更します。

最後に、FNDを再起動して、新しいキーストアとパスワードの使用を開始します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。