Cisco IoT Field Network Director リリース 4.0.x インストール ガイド

初版発行日：2017 年 8 月

Contents

Cisco IoT FND のインストール

この章では、Cisco IoT Field Network Director（Cisco IoT FND）をネットワークにインストールするために必要な手順について概説します。

（注）アプリケーションの機能の概要や、機能の構成方法およびインストールした Cisco IoT Field Network Director の管理方法については、「Cisco IoT Field Network Director User Guide, Release 4.0.x」を参照してください。

IoT FND および関連ソフトウェアのインストール方法

- IoT FND をインストールする前に
- IoT FND データベースのインストールと設定
- IoT FND のインストールおよびセットアップ
- IoT FND TPS プロキシのインストールと設定
- Dual-PHY 用の IoT FND の設定
- IoT FND データベースのバックアップと復元
- ESX 5.x での IoT FND/Oracle/TPS 仮想マシンの展開

IoT FND をインストールする前に

次の項の手順を使用して、IoT FND インストールの準備を行います。

- IoT FND マップ ビューの要件
- システム要件
- IoT FND および CNR のライセンスの取得
- Oracle のインストールに必要な Linux パッケージのインストール
- IoT FND RPM パッケージの取得
- NTP サービスの設定
- IoT FND のインストールの概要

IoT FND マップ ビューの要件

任意のデバイス タブで、メイン ペインの [Map] ボタンをクリックして、デバイス ロケーションの GIS マップを表示します。その [Map View] ペインで、IoT FND は、GIS マップを使用してデバイスの場所を表示します。ただし、この機能を使用するには、すべての IoT FND オペレータ システムがシスコが提供する GIS マップ タイル サーバにアクセスできるように、事前にファイアウォールを設定する必要があります。GIS マップ タイル サーバへのアクセスが許可されているのは、IoT FND オペレータ ブラウザだけです。

（注）オペレータ ブラウザは他の Google サイトにアクセスできません。IoT FND アプリケーション サーバにはインターネット アクセスは必要ありません。

また、完全修飾ドメイン名（FQDN）を各 IoT FND サーバのインストールに割り当て、ask-fnd-pm-external@cisco.com でシスコに以下を提供する必要があります。

- IoT FND インストール環境（テストおよび実稼働）の数
- IoT FND サーバの FQDN
- クラスタ展開の場合、展開での任意のロード バランサの FQDN

（注）FQDN は、プロビジョニングと、ライセンス付与された Cisco IoT FND インストールへのアクセスを認証して、Enterprise Google Map への API コールを行ってマップ タイルをダウンロードするためにのみ使用されます。Google マップ タイルを取得するために、ユーティリティ運用データまたは資産情報が使用（つまり、インターネットを介して送信）されることはありません。マップ タイルは、地理的な位置情報だけを使用して取得されます。

FQDN 情報の例

たとえば、非クラスタのインストールのドメイン名が UtilityA.com でホスト名が cgnms1、FQDN が cgms1.UtilityA.com とします。ask-cgnms-pm@cisco.com に電子メールを送信する際には、FQDN、cgms1.UtilityA.com を含めます。

1 つ以上の IoT FND サーバと loadbalancer-vip という FQDN を持つロード バランサがあるクラスタ展開では、トラフィックを cgnms-main または cnms-dr クラスタに向けます（DR インストール）。ask-cgnms-pm@cisco.com に電子メールを送信する際には、FQDN、loadbalancer-vip.UtilityA.com を含めます。

システム要件

表 1 に、このリリースに関連付けられている必要なハードウェアとソフトウェアのバージョンを示します。

（注）大規模なシステムについては、表 2 と表 3 のスケール要件を参照してください。

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco IoT FND アプリケーション サーバ（またはハードウェアとソフトウェアの最小要件を満たす同等のシステム）	■ プロセッサ – Intel Xeon x5680 2.27 GHz（64 ビット） – 4 個の CPU – RAM：16 GB ■ ディスク領域：100 GB ■ ハードウェア セキュリティ モジュール（HSM）または ソフトウェア セキュリティ モジュール（SSM）	■ すべてのパッケージ（ソフトウェア開発と Web サーバ）がインストールされた Red Hat Enterprise Linux 6.4 以降（64 ビット版） 推奨されるアプリケーション サーバのリソース割り当てプロファイルについては、表 3（12 ページ）を参照してください。 ■ インターネット接続 クライアントのブラウザから IoT FND にアクセスすると、ブラウザはインターネットに接続して、GIS マップ プロバイダーから必要なデータ ファイルをダウンロードします。 ■ メッシュ エンドポイント セキュリティに SafeNet を使用するためのライセンス （注）IoT FND ソフトウェア バンドルには、必要な Java のバージョンが含まれています。

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム（続き）

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco IoT FND TPS プロキシ	■ プロセッサ – Intel Xeon x5680 2.27 GHz（64 ビット） – 2 個の CPU ■ RAM：4 GB ■ ディスク領域：25 GB	■ すべてのパッケージ（ソフトウェア開発と Web サーバ）がインストールされた Red Hat Enterprise Linux 6.4 以降 ■ インターネット接続 (注) IoT FND ソフトウェア バンドルには、必要な Java のバージョンが含まれています。
IoT FND のデータベース サーバ ハードウェアの最小要件で 25 ルータ/10,000 エンドポイントに拡張できます。追加で拡張可能なサイズについては、「リソース管理の注意事項」を参照してください。	■ プロセッサ – Intel Xeon x5680 3.33 GHz（64 ビット） ■ 2 個の CPU ■ RAM：16 GB ■ ディスク領域：100 GB（Oracle 12c のインストール時には 120 GB）	(注) IoT FND 3.2.x は、次に示す Oracle リリースの両方をサポートします。 ■ Oracle Database 12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production（パッチ 20830993） ■ Oracle 11g Enterprise Edition（11.2.0.3 64 ビット バージョンのみ） (注) Oracle をインストールする前に、「Oracle のインストールに必要な Linux パッケージのインストール」に記載されている Linux パッケージをインストールします。 推奨される Oracle データベース サーバのリソース割り当てプロファイルについては、表 2（12 ページ）を参照してください。 ■ すべてのパッケージ（ソフトウェア開発と Web サーバ）がインストールされた Red Hat Linux 6.4 以降（64 ビット版）
Cisco IoT FND クライアント	クライアントが IoT FND アプリケーション サーバに接続して IoT FND を表示するには、次の最小要件を満たしている必要があります。 ■ Windows 7 または Win2000 R2 サーバ ■ RAM：8 GB ■ プロセッサ：2 GHz ■ 解像度：1024 x 768	■ Adobe Flash バージョン 9.0.115 以降（チャートを表示するために必要） ■ サポートされるブラウザ： – Internet Explorer（IE）：11.0 – Mozilla Firefox：3.5 以降 – IE 11.0 が機能する Windows 7

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム（続き）

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco Network Registrar（CNR）（DHCP サーバとして使用）	サーバは、次の最小要件を満たしている必要があります。 ■ ディスクの空き容量：146 GB ■ RAM：4 GB（小規模ネットワーク）、8 GB（平均的なネットワーク）、16 GB（大規模なネットワーク） ■ ハード ドライブ： – SATA ドライブ（7500 RPM ドライブ、500 リース/秒以上） *または* – SAS ドライブ（15K RPM ドライブ、1000 リース/秒以上）	Cisco Network Registrar、ソフトウェア リリース 8.2 をサーバにインストールする前に、次のソフトウェア環境が存在している必要があります。 ■ オペレーティング システム：Windows Server 2000 ■ Development Kit（JDK）Java SE Runtime Environment（JRE）8.0（1.8.0_65-b17）または同等の Java Development Kit（JDK）。 ■ ユーザ インターフェイス：Web ブラウザと、コマンドライン インターフェイス（CLI）（次に示すブラウザ バージョン）： – Internet Explorer（IE）11.0、Mozilla Firefox 3.0 以降 ■ CNR ライセンス。必要なライセンスについては、シスコ パートナーにお問い合わせください。
IoT Device Manager（IoT-DM または Device Manager）	Device Manager を実行しているラップトップには、以下が必要です。 ■ Microsoft Windows 7 Enterprise または Windows 10 ■ 2 GHz 以上のプロセッサ ■ 1 GB 以上の RAM（大きくなる可能性のあるログ ファイル処理用） ■ Wi-Fi またはイーサネット インターフェイス ■ 4 GB のディスク ストレージ領域 ■ Windows ログインが有効になっていること ■ ユーティリティにより署名された認証局（CA）とルータの認証用のクライアント証明書（IT 部門から入手） ■ Device Manager のラップトップ セキュリティを強化するための顧客固有の IT セキュリティ	■ バージョン 5.0.0.16
Cisco 1000 シリーズ Connected Grid ルータ	–	■ Cisco IOS Release 15.7(3)M ■ Cisco CG-OS Release CG4(5)
Cisco ISR 800 シリーズ サービス統合型ルータ（C800）	–	■ Cisco IOS Release 15.7(3)M

表 1　Cisco IoT FND のハードウェアとソフトウェアの最小要件とサポートされるシステム（続き）

コンポーネント	ハードウェアの最小要件	最小ソフトウェア リリース
Cisco 800 シリーズ アクセス ポイント（AP800）	-	■ AP802：ap802-k9w7-tar.153-3.JBB.tar ■ AP803：ap1g3-k9w7-tar.153-3.JBB2.tar
Cisco 800 シリーズ産業用サービス統合型ルータ（IR800）	-	■ Cisco IOS Release 15.7(3)M
Cisco 3900 シリーズ サービス統合型ルータ（ISR）	-	■ Cisco IOS Release 15.4(3)M ■ Cisco IOS Release 15.4(2)T
Cisco ASR 1001 または 1002 アグリゲーション サービス ルータ（ASR）はヘッドエンド ルータとして機能します。	-	■ Cisco IOS XE Release 3.17.02.S Flex トンネル用（IOS） ■ Cisco IOS XE Release 3.11S ポイントツーポイント トンネル用（CG-OS）
Cisco 500 シリーズ Wireless Personal Area Network（WPAN）産業用ルータ（IR500）	-	■ Cisco IR509、DA ゲートウェイ デバイス：ファームウェア バージョン 5.6.10 ■ Cisco IR529、Range Extender：ファームウェア バージョン 5.6.10
（注）異なるリリースの ASR と ISR はネットワーク上に共存できます。		
Cisco Connected Grid CG-Mesh Module とサポートされるエンドポイント	-	■ ファームウェア バージョン 5.6.10 以下と通信する場合 CGR 1000 または Cisco ASR、およびこれらのリリース ノートでこれらのルータに推奨されている Cisco IOS ソフトウェアの最小バージョン
Cisco Connected Grid RF メッシュ エンドポイント		■ ファームウェア バージョン 5.6.10（IR500 と通信する場合）
Cisco 800 シリーズ産業用サービス統合型ルータ（IR800）用に LoRAWAN（Long Range Wide Area Network）インターフェイス モジュール	-	■ Cisco IOS 15.6(3)M1b
ハードウェア セキュリティ モジュール（HSM）	クライアント ソフトウェアが IoT FND アプリケーション サーバにインストールされた Luna SA アプライアンス	Luna SA アプライアンス： ■ リリース 6.10.2 ファームウェア （注）上位のバージョンを実行できるかどうかは、SafeNet にお問い合わせください。 ■ リリース 5.4.7-1 ソフトウェアとセキュリティ パッチ Luna SA クライアント ソフトウェア： ■ リリース 5.4.7-1 ソフトウェア
ソフトウェア セキュリティ モジュール（SSM）	■ RAM：8 GB ■ プロセッサ：2 GHz ■ 2 個の CPU	■ すべてのパッケージ（ソフトウェア開発と Web サーバ）がインストールされた Red Hat Enterprise Linux 6.4 または 7.1（64 ビット版）

(注) IoT FND サーバ クラスタを展開している場合、クラスタ内のすべてのノードを同じようなハードウェアで実行する必要があります。さらに、すべてのノードで同じバージョンの IoT FND を実行する必要があります。

リソース管理の注意事項

仮想マシン設定のワークロード特性は重要です。同じ物理ホスト上で複数の VM を使用する場合、個々の VM が他の VM のパフォーマンスに影響を及ぼさないようにリソースを割り当てます。たとえば、8 CPU のホストで 4 つの VM を割り当てるには、1 つ(以上)の VM がすべてのリソースを使用しないように、8 つの CPU すべてを割り当てないようにします。

表 2(12 ページ)では、CPU、メモリ、ディスク領域などの重要なリソース パラメータの Oracle データベース サーバの使用プロファイルの例がリストされています。

(注) 表 2 に関しては、次の点に注意してください。Oracle が仮想マシン(VM)にバンドルされている IOTFND SKU (R-IOTFND-V-K9)をインストールする場合、サポートされるルータの最大数は 1000 で、サポートされるエンドポイントの最大数は 250,000 です。

表 2　Oracle DB サーバ ハードウェア要件のプロファイル例

ノード (ルータ/エンドポイント)	CPU (仮想コア)	メモリ (RAM GB)	ディスク領域(GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	8	32	500
1,000/1,000,000	12	48	1000
2,000/2,000,000	16	64	1000
5,000/5,000,000	20	96	1000

表 3(12 ページ)には、CPU、メモリ、ディスク領域といった重要なリソース パラメータについて、IoT FND アプリケーション サーバにおける使用プロファイルの例がリストされています。

表 3　アプリケーション サーバのハードウェア要件のプロファイル例

ノード (ルータ/エンドポイント)	CPU (仮想コア)	メモリ (RAM GB)	ディスク領域(GB)
25/10,000	2	16	100
50/50,000	4	16	200
500/500,000	4	16	250
1,000/1,000,000	8	16	250
2,000/2,000,000[1]	8	16	500
5,000/5,000,000[1]	8	16	500

1. クラスタ構成のインストール。

(注) 2 百万以上のエンドポイントを持つ展開には、RAID 10 を強く推奨します。

ルータのみの展開の場合

表 4 と表 5 の情報は、ルータのみの展開に適用されます。

表 4　ルータおよび LoRa モジュールのアプリケーション サーバのハードウェア要件のプロファイル例

ノード（IR800/LoRa モジュール）	CPU（仮想コア）	メモリ（RAM GB）	ディスク領域（GB）
10,000/30,000	4	24	100

表 5　ルータおよび LoRa モジュールのデータベース サーバのハードウェア要件のプロファイル例

ノード（IR800/LoRa モジュール）	CPU（仮想コア）	メモリ（RAM GB）	ディスク領域（GB）
10,000/30,000	6	32	500

IoT FND および CNR のライセンスの取得

- IoT FND および CNR を使用するために必要なライセンスを取得するには、シスコ パートナーにお問い合わせください。
- メッシュ エンドポイント セキュリティの HSM として SafeNet を使用するため、ライセンスを取得します。

Oracle のインストールに必要な Linux パッケージのインストール

(注) 以下に示す Linux パッケージは、Red Hat に直接連絡して入手してください。

Oracle データベースをインストールする前に、次のパッケージをこの順序でインストールします。

1. libaio-devel-0.3.106-5.i386.rpm
2. libaio-devel-0.3.106-5.x86_64.rpm
3. sysstat-7.0.2-11.el5.x86_64.rpm
4. unixODBC-libs-2.2.11-10.el5.i386.rpm
5. unixODBC-libs-2.2.11-10.el5.x86_64.rpm
6. unixODBC-2.2.11-10.el5.i386.rpm
7. unixODBC-2.2.11-10.el5.x86_64.rpm
8. unixODBC-devel-2.2.11-10.el5.i386.rpm
9. unixODBC-devel-2.2.11-10.el5.x86_64.rpm

IoT FND RPM パッケージの取得

Cisco またはシスコ パートナーから IoT FND を購入すると、次の 5 つの RPM パッケージを含んだ ISO ファイルのダウンロード リンクを受け取ります。IoT FND システムをインストールして設定する前に、次の 5 つの RPM パッケージがあることを確認します。

RPM パッケージ	説明
cgms-*version_number*.x86_64.rpm	これが IoT FND アプリケーション サーバそのものを含むメインの RPM です。IoT FND アプリケーション サーバにこのパッケージをインストールします。
cgms-oracle-*version_number*.x86_64.rpm	IoT FND Oracle データベースを作成するためのスクリプトとツールが含まれています。このパッケージには、Oracle データベース テンプレートと、管理スクリプトが含まれています。IoT FND データベース サーバ システムにこのパッケージをインストールします。
cgms-tools-*version_number*.x86_64.rpm	オプションのコマンドライン ツールがいくつか含まれています。必要に応じて、IoT FND アプリケーション サーバが動作しているシステムにこのパッケージをインストールします。
cgms-ssm-*version_number*.x86_64.rpm	ソフトウェア セキュリティ モジュール（SSM）が含まれています。IoT FND アプリケーション サーバが動作しているシステムにこのパッケージをインストールします。
cgms-tpsproxy-*version_number*.x86_64.rpm	TPS プロキシ アプリケーションが含まれます。IoT FND TPS プロキシ システムにこのパッケージをインストールします。

NTP サービスの設定

IoT FND の展開のすべての Red Hat Enterprise Linux（RHEL）サーバ（IoT FND を実行するすべてのサーバを含む）の NTP サービスを有効にし、システムの他のサーバと同じタイム サーバを使用するように設定します。

注意：証明書が生成される前に、すべてのシステム コンポーネントのクロックを同期します。

RHEL サーバで NTP を設定するには、次の手順を実行します。

1. /etc/ntp.conf ファイルを設定します。

   次に例を示します。

   ```
   cat /etc/ntp.conf
   ...
   # Use the same NTP servers on all our Connected Grid systems.
   server 0.ntp.example.com
   server 1.ntp.example.com
   server 2.ntp.example.com
   ...
   ```

2. NTP デーモンを再起動して、ブート時に実行されるように設定されていることを確認します。

   ```
   service ntpd restart
   chkconfig ntpd on
   ```

3. NTP デーモンのステータスを確認して、設定の変更を確認します。

この例では、192.0.2.1 でシステムがローカル NTP サーバになるように設定されていることを示しています。このサーバは、10.0.0.0 で NTP サーバを使用して時刻を同期します。

```
# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.0.2.1       198.51.100.1     3 u    309 1024  377    0.694    0.899   0.435
 LOCAL(0)        .LOCL.          10 l   36   64  377    0.000    0.000   0.001
```

RHEL サーバでの NTP の設定については、RHEL のマニュアルを参照してください。

IoT FND のインストールの概要

IoT FND をインストールするには、次の手順を実行します。

1. IoT FND データベースのインストールと設定。
2. IoT FND のインストールおよびセットアップ。
3. IoT FND TPS プロキシのインストールと設定。

IoT FND データベースのインストールと設定

次の手順を実行して、IoT FND のインストールを完了します。

- インストールと設定の概要
- Oracle データベースのダウンロードと解凍
- Oracle データベース インストーラの実行
- IoT FND データベースの設定
- IoT FND データベースのその他のトピック

インストールと設定の概要

ここでは、IoT FND の展開の概要について説明します。

- シングルサーバの展開
- ハイ アベイラビリティ展開

シングルサーバの展開

シングルサーバ データベースの展開に IoT FND データベースをインストールして設定するには、次の手順を実行します。

1. データベース サーバにログインします。
2. Oracle データベースのダウンロードと解凍。
3. Oracle データベース インストーラの実行。
4. IoT FND データベースの設定。

ハイ アベイラビリティ展開

HA 用に IoT FND データベースをインストールして設定するには、次の手順を実行します。

1. プライマリ IoT FND データベース サーバにログインします。
2. Oracle データベースのダウンロードと解凍。
3. Oracle データベース インストーラの実行。
4. スタンバイ データベース サーバにログインします。
5. Oracle データベースのダウンロードと解凍。
6. Oracle データベース インストーラの実行。
7. HA 用の IoT FND データベースの設定。

Oracle データベースのダウンロードと解凍

Oracle データベースをダウンロードするには、次の手順を実行します。

1. root としてサーバにログインします。
2. Oracle 11g Enterprise Edition（11.2.0.3 64 ビット）または Oracle12c Enterprise Edition Release 12.1.0.2.0 - 64bit Production（パッチ 20830993）をダウンロードします。
3. Oracle データベース ソフトウェアのインストール時に表示関連のエラーを回避するには、root として次のコマンドを実行します。

```
# xhost + local:oracle
```

4. **oracle** ユーザと **dba** グループを作成します。

```
# groupadd dba
# adduser -d /home/oracle -g dba -s /bin/bash oracle
```

5. Oracle データベースの zip アーカイブを解凍します。

```
p10404530_112030_Linux-x86-64_1of7.zip
p10404530_112030_Linux-x86-64_2of7.zip
p10404530_112030_Linux-x86-64_3of7.zip
p10404530_112030_Linux-x86-64_4of7.zip
p10404530_112030_Linux-x86-64_5of7.zip
p10404530_112030_Linux-x86-64_6of7.zip
p10404530_112030_Linux-x86-64_7of7.zip
```

Oracle データベース インストーラの実行

(注) Oracle インストーラを実行する前に、ファイアウォールを無効にします。

Oracle データベースをインストールするには、次の手順を実行します。

1. ユーザ **oracle** に切り替え、Oracle データベースのインストーラを実行します。

```
# su - oracle
# setenv DISPLAY <desktop>
# path_to_DB_installation_folder/database/runInstaller
```

2. [Yes] をクリックし、[Next] をクリックします。

3. [Install database software only] をクリックし、[Next] をクリックします。
4. [Single instance database installation] をクリックし、[Next] をクリックします。
5. データベースを実行する言語として [English] を選択し、[Next] をクリックします。
6. [Enterprise Edition (4.29GB (Oracle 11g)] または [6.4GB (Oracle12c)] をクリックし、[Next] をクリックします。
7. 次の 2 つのデフォルトのインストール値、Oracle ベースおよびソフトウェアの場所（**11.2.0** または **12.1.0**）を選択し、[Next] をクリックします。
   - Oracle ベース：**/home/oracle/app/oracle**
   - ソフトウェアの場所：**/home/oracle/app/oracle/product/11.2.0/dbhome_1**
   - ソフトウェアの場所：**/home/oracle/app/oracle/product/12.1.0/dbhome_1**

   後で Oracle ベースとソフトウェアの場所のプロパティの値に基づいて環境変数 ORACLE_BASE と ORACLE_HOME を作成します。
8. [Create Inventory] ページで、デフォルト値を維持し、[Next] をクリックします。
   - インベントリ ディレクトリ：**/home/oracle/app/oraInventory**
   - oraInventory_Group 名：**dba**
9. [Privileged Operating System Groups] ページで、デフォルト値を維持し、[Next] をクリックします。
   - データベース管理者（OSDBA）グループ：**dba**
   - データベース オペレータ（OSOPER）グループ：**dba**

   データベースのバックアップとリカバリ（OSBACKUPDBA）グループ：**dba**（12c のみ）
   - データ ガード管理（OSDGDBA）グループ：**dba**（12c のみ）
   - 暗号化キー管理の管理（OSKMDBA）グループ：**dba**（12c のみ）
10. （オプション）[Perform Prerequisite Checks] ページで、必要なソフトウェアをインストールするか、提供されるスクリプトを実行します。

    システム カーネルの設定に基づいて、インストーラによって追加のソフトウェアのインストールが求められる場合があります。また、スクリプトを実行してシステムを設定し、データベースのインストールを完了するように指示される場合があります。

    (注) 不足しているパッケージが示されない場合、または「This is a prerequisite condition to test whether the package “ksh” is available on the system」というメッセージが表示された場合は、[Ignore All] ボックスをオンにします。
11. 不足しているパッケージをインストールした後、[Fix & Check Again] をクリックします。

    すべての要件を満たすまでこれを続けます。

    注意： このページのエラーは無視しないでください。データベースのインストール中にエラーが発生すると、IoT FND が適切に機能しない可能性があります。
12. [Next] をクリックします。
13. [Summary] ページで、データベース設定を確認し [Finish]（11g）または [Install]（12c）をクリックして、インストール プロセスを開始します。

14. プロンプトで、提供される構成スクリプトを実行します。

    インストーラはユーザ ***oracle*** で実行するため、ルート権限を必要とする特定のインストール操作は実行できません。これらの操作を実行するため、インストール プロセスを完了するためのスクリプトを実行するように求められます。プロンプトが表示されたら、ターミナル ウィンドウを開き、**root** としてスクリプトを実行します。

15. 正常にインストールされたら、[Finish] ページで [Close] をクリックします。

    (注) Oracle 12c の新規インストールまたは Oracle 11g からのアップグレードを実行する場合には、Oracle 12c パッチ 20830993 をインストールする**必要**があります。(必須) 12c パッチのインストールに進みます。

(必須) 12c パッチのインストール

Oracle 12c データベースの新規インストールと Oracle 11g からのアップグレードにはすべて、12c パッチをインストールする必要があります。

パッチをインストールするには、次の手順を実行します。

1. IoT FND アプリケーションが実行されている場合は停止します。
2. Oracle サービスが実行されている場合は停止します。
3. 次のコマンドを実行して、インストール済みの Oracle ソフトウェア コンポーネントとパッチのインベントリを確認します。この段階ではパッチは適用されていません。最後に「*There are no interim patches installed in this Oracle Home*」が表示されます。

```
/home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch lsinventory -details

Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory   from           :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location
:/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/opatch2016-02-25_10-37-50AM_1.log

Lsinventory Output file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/lsinv/lsinventory2016-02-25_10-37-50
AM.txt
--------------------------------------------------------------------------------

Installed Top-level Products (1):
Oracle Database 12c                                                  12.1.0.2.0
There are 1 products installed in this Oracle Home.
Installed Products (135):
Assistant Common Files                                               12.1.0.2.0
Buildtools Common Files                                              12.1.0.2.0
Cluster Verification Utility Common Files                            12.1.0.2.0
Database Configuration and Upgrade Assistants                        12.1.0.2.0
Database Migration Assistant for Unicode                             12.1.0.2.0
Database SQL Scripts                                                 12.1.0.2.0
Database Workspace Manager                                           12.1.0.2.0
DB TOOLS Listener                                                    12.1.0.2.0
Deinstallation Tool                                                  12.1.0.2.0
Enterprise Edition Options                                           12.1.0.2.0
Expat libraries                                                       2.0.1.0.2
Generic Connectivity Common Files                                    12.1.0.2.0
Hadoopcore Component                                                 12.1.0.2.0
HAS Common Files                                                     12.1.0.2.0
HAS Files for DB                                                     12.1.0.2.0
```

```
Installation Common Files                                       12.1.0.2.0
Installation Plugin Files                                       12.1.0.2.0
Installer SDK Component                                         12.1.0.2.0J
Accelerator (COMPANION)                                         12.1.0.2.0
Java Development Kit                                            1.6.0.75.0
LDAP Required Support Files                                     12.1.0.2.0
OLAP SQL Scripts                                                12.1.0.2.0
Oracle Advanced Security                                        12.1.0.2.0
Oracle Application Express                                      12.1.0.2.0
Oracle Bali Share                                               11.1.1.6.0
Oracle Call Interface (OCI)                                     12.1.0.2.0
Oracle Clusterware RDBMS Files                                  12.1.0.2.0
Oracle Configuration Manager                                    10.3.8.1.1
Oracle Configuration Manager Client                             10.3.2.1.0
Oracle Configuration Manager Deconfiguration                    10.3.1.0.0
Oracle Containers for Java                                      12.1.0.2.0
Oracle Context Companion                                        12.1.0.2.0
Oracle Core Required Support Files                              12.1.0.2.0
Oracle Core Required Support Files for Core DB                  12.1.0.2.0
Oracle Core XML Development Kit                                 12.1.0.2.0
Oracle Data Mining RDBMS Files                                  12.1.0.2.0
Oracle Database 12c                                             12.1.0.2.0
Oracle Database 12c                                             12.1.0.2.0
Oracle Database 12c Multimedia Files                            12.1.0.2.0
Oracle Database Deconfiguration                                 12.1.0.2.0
Oracle Database Gateway for ODBC                                12.1.0.2.0
Oracle Database Plugin for Oracle Virtual Assembly Builder      12.1.0.2.0
Oracle Database User Interface                                  11.0.0.0.0
Oracle Database Utilities                                       12.1.0.2.0
Oracle Database Vault option                                    12.1.0.2.0
Oracle DBCA Deconfiguration                                     12.1.0.2.0
Oracle Extended Windowing Toolkit                               11.1.1.6.0
Oracle Globalization Support                                    12.1.0.2.0
Oracle Globalization Support                                    12.1.0.2.0
Oracle Globalization Support For Core                           12.1.0.2.0
Oracle Help for Java                                            11.1.1.7.0
Oracle Help Share Library                                       11.1.1.7.0
Oracle Ice Browser                                              11.1.1.7.0
Oracle Internet Directory Client                                12.1.0.2.0
Oracle Java Client                                              12.1.0.2.0
Oracle Java Layout Engine                                       11.0.0.0.0
Oracle JDBC Server Support Package                              12.1.0.2.0
Oracle JDBC/OCI Instant Client                                  12.1.0.2.0
Oracle JDBC/THIN Interfaces                                     12.1.0.2.0
Oracle JFC Extended Windowing Toolkit                           11.1.1.6.0
Oracle JVM                                                      12.1.0.2.0
Oracle JVM For Core                                             12.1.0.2.0
Oracle Label Security                                           12.1.0.2.0
Oracle LDAP administration                                      12.1.0.2.0
Oracle Locale Builder                                           12.1.0.2.0
Oracle Message Gateway Common Files                             12.1.0.2.0
Oracle Multimedia                                               12.1.0.2.0
Oracle Multimedia Client Option                                 12.1.0.2.0
Oracle Multimedia Java Advanced Imaging                         12.1.0.2.0
Oracle Multimedia Locator                                       12.1.0.2.0
Oracle Multimedia Locator Java Required Support Files           12.1.0.2.0
Oracle Multimedia Locator RDBMS Files                           12.1.0.2.0
Oracle Net                                                      12.1.0.2.0
Oracle Net Java Required Support Files                          12.1.0.2.0
Oracle Net Listener                                             12.1.0.2.0
Oracle Net Required Support Files                               12.1.0.2.0
Oracle Net Services                                             12.1.0.2.0
Oracle Netca Client                                             12.1.0.2.0
```

```
Oracle Notification Service                                          12.1.0.2.0
Oracle Notification Service (eONS)                                   12.1.0.2.0
Oracle Notification Service for Instant Client                       12.1.0.2.0
Oracle ODBC Driver                                                   12.1.0.2.0
Oracle ODBC Driverfor Instant Client                                 12.1.0.2.0
Oracle OLAP                                                          12.1.0.2.0
Oracle OLAP API                                                      12.1.0.2.0
Oracle OLAP RDBMS Files                                              12.1.0.2.0
Oracle One-Off Patch Installer                                       12.1.0.1.2
Oracle Partitioning                                                  12.1.0.2.0
Oracle Programmer                                                    12.1.0.2.0
Oracle Quality of Service Management (Client)                        12.1.0.2.0
Oracle R Enterprise Server Files                                     12.1.0.2.0
Oracle RAC Deconfiguration                                           12.1.0.2.0
Oracle RAC Required Support Files-HAS                                12.1.0.2.0
Oracle Real Application Testing                                      12.1.0.2.0
Oracle Recovery Manager                                              12.1.0.2.0
Oracle Security Developer Tools                                      12.1.0.2.0
Oracle Spatial and Graph                                             12.1.0.2.0
Oracle SQL Developer                                                 12.1.0.2.0
Oracle Starter Database                                              12.1.0.2.0
Oracle Text                                                          12.1.0.2.0
Oracle Text ATG Language Support Files                               12.1.0.2.0
Oracle Text for Core                                                 12.1.0.2.0
Oracle Text Required Support Files                                   12.1.0.2.0
Oracle Universal Connection Pool                                     12.1.0.2.0
Oracle Universal Installer                                           12.1.0.2.0
Oracle USM Deconfiguration                                           12.1.0.2.0
Oracle Wallet Manager                                                12.1.0.2.0
Oracle XML Development Kit                                           12.1.0.2.0
Oracle XML Query                                                     12.1.0.2.0
oracle.swd.oui.core.min                                              12.1.0.2.0
Parser Generator Required Support Files                              12.1.0.2.0
Perl Interpreter                                                     5.14.1.0.0
Perl Modules                                                         5.14.1.0.0
PL/SQL                                                               12.1.0.2.0
PL/SQL Embedded Gateway                                              12.1.0.2.0
Platform Required Support Files                                      12.1.0.2.0
Precompiler Common Files                                             12.1.0.2.0
Precompiler Common Files for Core                                    12.1.0.2.0
Precompiler Required Support Files                                   12.1.0.2.0
Precompilers                                                         12.1.0.2.0
RDBMS Required Support Files                                         12.1.0.2.0
RDBMS Required Support Files for Instant Client                      12.1.0.2.0
RDBMS Required Support Files Runtime                                 12.1.0.2.0
Required Support Files                                               12.1.0.2.0
Sample Schema Data                                                   12.1.0.2.0
Secure Socket Layer                                                  12.1.0.2.0
SQL*Plus                                                             12.1.0.2.0
SQL*Plus Files for Instant Client                                    12.1.0.2.0
SQL*Plus Required Support Files                                      12.1.0.2.0
SQLJ Runtime                                                         12.1.0.2.0
SSL Required Support Files for InstantClient                         12.1.0.2.0
Tracle File Analyzer                                                 12.1.0.2.0
XDK Required Support Files                                           12.1.0.2.0
XML Parser for Java                                                  12.1.0.2.0
XML Parser for Oracle JVM                                            12.1.0.2.0
There are 135 products installed in this Oracle Home.

There are no Interim patches installed in this Oracle Home.
```

4. パッチを適用します。

   a. データベース マシンで、パッチ ファイル "p20830993_121020_Linux-x86-64.zip" をコピーします。

   b. 要件のチェックを実行します。これにパスする必要があります。

```
$ cd /home/oracle/patches/20830993/
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch prereq
CheckConflictAgainstOHWithDetail -ph ./
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

PREREQ session

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory
   from           : /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location :/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtool
logs/opatch/opatch2016-02-25_10-48-48AM_1.log

Invoking prereq "checkconflictagainstohwithdetail"

Prereq "checkConflictAgainstOHWithDetail" passed.

OPatch succeeded.
```

   c. パッチを適用します。

```
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch apply
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory   from           :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location:
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/20830993_Feb_25_2016_10_53_25/ap
ply2016-02-25_10-53-25AM_1.log

Applying interim patch '20830993' to OH '/home/oracle/app/oracle/product/12.1.0/dbhome_1'
Verifying environment and performing prerequisite checks...
All checks passed.

Please shutdown Oracle instances running out of this ORACLE_HOME on the local system.
(Oracle Home = '/home/oracle/app/oracle/product/12.1.0/dbhome_1')

Is the local system ready for patching? [y|n]
y
User Responded with: Y
Backing up files...

Patching component oracle.rdbms, 12.1.0.2.0...

Verifying the update...
Patch 20830993 successfully applied
Log file location:/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/
20830993_Feb_25_2016_10_53_25/apply2016-02-25_10-53-25AM_1.log

OPatch succeeded.
```

d. Opatch ユーティリティを実行して、パッチが現在認識されていることを確認します。次の出力の最後に「Interim Patch」があることに注目してください。

```
$ /home/oracle/app/oracle/product/12.1.0/dbhome_1/OPatch/opatch lsinventory -details
Oracle Interim Patch Installer version 12.1.0.1.3
Copyright (c) 2016, Oracle Corporation.  All rights reserved.

Oracle Home       : /home/oracle/app/oracle/product/12.1.0/dbhome_1
Central Inventory : /home/oracle/app/oraInventory
   from           : /home/oracle/app/oracle/product/12.1.0/dbhome_1/oraInst.loc
OPatch version    : 12.1.0.1.3
OUI version       : 12.1.0.2.0
Log file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/opatch2016-02-25_11-05-19AM_1.lo
g
Lsinventory Output file location :
/home/oracle/app/oracle/product/12.1.0/dbhome_1/cfgtoollogs/opatch/lsinv/lsinventory2016-02-25_11-0
5-19AM.txt

--------------------------------------------------------------------------------
Installed Top-level Products (1):
Oracle Database 12c                                                  12.1.0.2.0
There are 1 products installed in this Oracle Home.

Installed Products (135):

Assistant Common Files                                               12.1.0.2.0
Buildtools Common Files                                              12.1.0.2.0
Cluster Verification Utility Common Files                            12.1.0.2.0
Database Configuration and Upgrade Assistants                        12.1.0.2.0
Database Migration Assistant for Unicode                             12.1.0.2.0
Database SQL Scripts                                                 12.1.0.2.0
Database Workspace Manager                                           12.1.0.2.0
DB TOOLS Listener                                                    12.1.0.2.0
Deinstallation Tool                                                  12.1.0.2.0
Enterprise Edition Options                                           12.1.0.2.0
Expat libraries                                                       2.0.1.0.2
Generic Connectivity Common Files                                    12.1.0.2.0
Hadoopcore Component                                                 12.1.0.2.0
HAS Common Files                                                     12.1.0.2.0
HAS Files for DB                                                     12.1.0.2.0
Installation Common Files                                            12.1.0.2.0
Installation Plugin Files                                            12.1.0.2.0
Installer SDK Component                                              12.1.0.2.0
JAccelerator (COMPANION)                                             12.1.0.2.0
Java Development Kit                                                 1.6.0.75.0
LDAP Required Support Files                                          12.1.0.2.0
LAP SQL Scripts                                                      12.1.0.2.0
Oracle Advanced Security                                             12.1.0.2.0
Oracle Application Express                                           12.1.0.2.0
Oracle Bali Share                                                    11.1.1.6.0
Oracle Call Interface (OCI)                                          12.1.0.2.0
Oracle Clusterware RDBMS Files                                       12.1.0.2.0
Oracle Configuration Manager                                         10.3.8.1.1
Oracle Configuration Manager Client                                  10.3.2.1.0
Oracle Configuration Manager Deconfiguration                         10.3.1.0.0
Oracle Containers for Java                                           12.1.0.2.0
Oracle Context Companion                                             12.1.0.2.0
Oracle Core Required Support Files                                   12.1.0.2.0
Oracle Core Required Support Files for Core DB                       12.1.0.2.0
Oracle Core XML Development Kit                                      12.1.0.2.0
Oracle Data Mining RDBMS Files                                       12.1.0.2.0
Oracle Database 12c                                                  12.1.0.2.0
Oracle Database 12c                                                  12.1.0.2.0
```

```
Oracle Database 12c Multimedia Files                              12.1.0.2.0
Oracle Database Deconfiguration                                   12.1.0.2.0
Oracle Database Gateway for ODBC                                  12.1.0.2.0
Oracle Database Plugin for Oracle Virtual Assembly Builder        12.1.0.2.0
Oracle Database User Interface                                    11.0.0.0.0
Oracle Database Utilities                                         12.1.0.2.0
Oracle Database Vault option                                      12.1.0.2.0
Oracle DBCA Deconfiguration                                       12.1.0.2.0
Oracle Extended Windowing Toolkit                                 11.1.1.6.0
Oracle Globalization Support                                      12.1.0.2.0
Oracle Globalization Support                                      12.1.0.2.0
Oracle Globalization Support For Core                             12.1.0.2.0
Oracle Help for Java                                              11.1.1.7.0
Oracle Help Share Library                                         11.1.1.7.0
Oracle Ice Browser                                                11.1.1.7.0
Oracle Internet Directory Client                                  12.1.0.2.0
Oracle Java Client                                                12.1.0.2.0
Oracle Java Layout Engine                                         11.0.0.0.0
Oracle JDBC Server Support Package                                12.1.0.2.0
Oracle JDBC/OCI Instant Client                                    12.1.0.2.0
Oracle JDBC/THIN Interfaces                                       12.1.0.2.0
Oracle JFC Extended Windowing Toolkit                             11.1.1.6.0
Oracle JVM                                                        12.1.0.2.0
Oracle JVM For Core                                               12.1.0.2.0
Oracle Label Security                                             12.1.0.2.0
Oracle LDAP administration                                        12.1.0.2.0
Oracle Locale Builder                                             12.1.0.2.0
Oracle Message Gateway Common Files                               12.1.0.2.0
Oracle Multimedia                                                 12.1.0.2.0
Oracle Multimedia Client Option                                   12.1.0.2.0
Oracle Multimedia Java Advanced Imaging                           12.1.0.2.0
Oracle Multimedia Locator                                         12.1.0.2.0
Oracle Multimedia Locator Java Required Support Files             12.1.0.2.0
Oracle Multimedia Locator RDBMS Files                             12.1.0.2.0
Oracle Net                                                        12.1.0.2.0
Oracle Net Java Required Support Files                            12.1.0.2.0
Oracle Net Listener                                               12.1.0.2.0
Oracle Net Required Support Files                                 12.1.0.2.0
Oracle Net Services                                               12.1.0.2.0
Oracle Netca Client                                               12.1.0.2.0
Oracle Notification Service                                       12.1.0.2.0
Oracle Notification Service (eONS)                                12.1.0.2.0
Oracle Notification Service for Instant Client                    12.1.0.2.0
Oracle ODBC Driver                                                12.1.0.2.0
Oracle ODBC Driverfor Instant Client                              12.1.0.2.0
Oracle OLAP                                                       12.1.0.2.0
Oracle OLAP API                                                   12.1.0.2.0
Oracle OLAP RDBMS Files                                           12.1.0.2.0
Oracle One-Off Patch Installer                                    12.1.0.1.2
Oracle Partitioning                                               12.1.0.2.0
Oracle Programmer                                                 12.1.0.2.0
Oracle Quality of Service Management (Client)                     12.1.0.2.0
Oracle R Enterprise Server Files                                  12.1.0.2.0
Oracle RAC Deconfiguration                                        12.1.0.2.0
Oracle RAC Required Support Files-HAS                             12.1.0.2.0
Oracle Real Application Testing                                   12.1.0.2.0
Oracle Recovery Manager                                           12.1.0.2.0
Oracle Security Developer Tools                                   12.1.0.2.0
Oracle Spatial and Graph                                          12.1.0.2.0
Oracle SQL Developer                                              12.1.0.2.0
Oracle Starter Database                                           12.1.0.2.0
Oracle Text                                                       12.1.0.2.0
Oracle Text ATG Language Support Files                            12.1.0.2.0
```

```
Oracle Text for Core                                                 12.1.0.2.0
Oracle Text Required Support Files                                   12.1.0.2.0
Oracle Universal Connection Pool                                     12.1.0.2.0
Oracle Universal Installer                                           12.1.0.2.0
Oracle USM Deconfiguration                                           12.1.0.2.0
Oracle Wallet Manager                                                12.1.0.2.0
Oracle XML Development Kit                                           12.1.0.2.0
Oracle XML Query                                                     12.1.0.2.0
oracle.swd.oui.core.min                                              12.1.0.2.0
Parser Generator Required Support Files                              12.1.0.2.0
Perl Interpreter                                                     5.14.1.0.0
Perl Modules                                                         5.14.1.0.0
PL/SQL                                                               12.1.0.2.0
PL/SQL Embedded Gateway                                              12.1.0.2.0
Platform Required Support Files                                      12.1.0.2.0
Precompiler Common Files                                             12.1.0.2.0
Precompiler Common Files for Core                                    12.1.0.2.0
Precompiler Required Support Files                                   12.1.0.2.0
Precompilers                                                         12.1.0.2.0
RDBMS Required Support Files                                         12.1.0.2.0
RDBMS Required Support Files for Instant Client                      12.1.0.2.0
RDBMS Required Support Files Runtime                                 12.1.0.2.0
Required Support Files                                               12.1.0.2.0
Sample Schema Data                                                   12.1.0.2.0
Secure Socket Layer                                                  12.1.0.2.0
SQL*Plus                                                             12.1.0.2.0
SQL*Plus Files for Instant Client                                    12.1.0.2.0
SQL*Plus Required Support Files                                      12.1.0.2.0
SQLJ Runtime                                                         12.1.0.2.0
SSL Required Support Files for InstantClient                         12.1.0.2.0
Tracle File Analyzer                                                 12.1.0.2.0
XDK Required Support Files                                           12.1.0.2.0
XML Parser for Java                                                  12.1.0.2.0
XML Parser for Oracle JVM                                            12.1.0.2.0
There are 135 products installed in this Oracle Home.

Interim patches (1) :

Patch  20830993      : applied on Thu Feb 25 10:53:50 PST 2016
Unique Patch ID:  18912657
Created on 13 May 2015, 00:37:38 hrs PST8PDT
   Bugs fixed:     20830993
Files Touched:
 /qksvc.o --> ORACLE_HOME/lib/libserver12.a
 ins_rdbms.mk --> ORACLE_HOME/rdbms/lib/ioracle
Patch Location in Inventory:
 /home/oracle/app/oracle/product/12.1.0/dbhome_1/inventory/oneoffs/20830993
Patch Location in Storage area:
 /home/oracle/app/oracle/product/12.1.0/dbhome_1/.patch_storage/20830993_May_13_2015_00_37_38
--------------------------------------------------------------------------------
```

プロセスを完了します。

「IoT FND データベースの設定」に進みます。

IoT FND データベースの設定

次の手順を実行して、IoT FND データベースを設定します。

- IoT FND データベースの設定の概要
- Oracle データベース環境変数の定義
- IoT FND Oracle データベース スクリプトのインストール
- IoT FND Oracle データベースの作成
- IoT FND Oracle データベースの起動

IoT FND データベースの設定の概要

IoT FND データベースを設定するには、次の手順を実行します。

1. Oracle データベース環境変数の定義。
2. IoT FND Oracle データベース スクリプトのインストール。
3. IoT FND Oracle データベースの作成。
4. IoT FND Oracle データベースの起動。

Oracle データベース環境変数の定義

IoT FND Oracle データベースをインストールする前に、**oracle** ユーザ アカウントに切り替え、次の Oracle データベースの環境変数を定義します。

表 6　Oracle データベースの環境変数

変数	説明
ORACLE_BASE	システムの Oracle ルート ディレクトリへのパスを定義します。次に例を示します。 `$ export ORACLE_BASE=/home/oracle/app/oracle` この変数を設定しないと、IoT FND のセットアップ スクリプトでエラーが表示されます。
ORACLE_HOME	IoT FND データベースの Oracle ホームへのパスを定義します。次に例を示します。 `$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/dbhome_1` (注) ORACLE_HOME 環境変数には、連続バックスラッシュを使用しないでください。
PATH	Oracle バイナリへのパスを定義します。次に例を示します。 `$ export PATH=$PATH:$ORACLE_HOME/bin`
LD_LIBRARY_PATH	ライブラリへのパスを定義します。次に例を示します。 `$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`

表 6　Oracle データベースの環境変数（続き）

変数	説明

ORACLE_SID	Oracle システム ID（SID）を定義します。
	
	1 つのデータベース サーバだけを使用している場合、または HA 展開をインストールしている場合は、*プライマリ* データベース サーバでこの変数を **cgms** に設定します。
	
	`$ export ORACLE_SID=cgms`
	
	スタンバイ データベース サーバを展開している場合は、*スタンバイ* データベース サーバでこの変数を **cgms_s** に設定します。
	
	`$ export ORACLE_SID=cgms_s`
	
	この変数を設定しないと、IoT FND のセットアップ スクリプトでエラーが表示されます。

次の例に示すように、これらの変数を手動で設定できます。

シングルまたはプライマリ データベース サーバ	スタンバイ データベース サーバ

`$ su - oracle`
`$ export ORACLE_BASE=/home/oracle/app/oracle`
`$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db home_1`
`$ export PATH=$PATH:$ORACLE_HOME/bin`
`$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`
`$ export ORACLE_SID=cgms`
	`$ su - oracle`
	`$ export ORACLE_BASE=/home/oracle/app/oracle`
	`$ export ORACLE_HOME=/home/oracle/app/oracle/product/11.2.0/db home_1`
	`$ export PATH=$PATH:$ORACLE_HOME/bin`
	`$ export LD_LIBRARY_PATH=$ORACLE_HOME/lib:$LD_LIBRARY_PATH`
	`$ export ORACLE_SID=cgms_s`

.bashrc ファイルを使用しても、これらの変数を定義できます。

IoT FND Oracle データベース スクリプトのインストール

IoT FND は、スクリプトおよび Oracle データベースのテンプレートとともにパッケージ化されています。

Oracle スクリプトを Oracle サーバにインストールするには、次の手順を実行します。

1. root ユーザとしてログインします。
2. IoT FND Oracle スクリプト RPM を Oracle サーバに安全にコピーします。

```
$ scp cgms-oracle-version_number.x86_64.rpm root@oracle-machine:~
$ rpm -ivh cgms-oracle-version_number.x86_64.rpm
```

3. cgms ディレクトリを作成し、ここにスクリプトとテンプレートをダウンロードします。

```
$ cd $ORACLE_BASE/app/oracle
$ mkdir cgms
$ cd cgms
$ cp -R /opt/cgms-oracle/scripts .
$ cp -R /opt/cgms-oracle/templates .
$ cp -R /opt/cgms-oracle/tools .
$ cd ..
$ chown -R oracle:dba cgms
```

IoT FND Oracle データベースの作成

シングル データベース サーバの展開で IoT FND Oracle データベースを作成するには、ユーザ *oracle* として setupCgmsDb.sh スクリプトを実行します。このスクリプトは、Oracle データベースを起動して、IoT FND データベースを作成します。

このスクリプトは、IoT FND がデータベースにアクセスするために使用するユーザ **cgms_dev** を作成します。このユーザ アカウントのデフォルト パスワードは **cgms123** です。

sys DBA アカウントのデフォルト パスワードは **cgmsDba123** です。

(注)デフォルト パスワードはすべて変更することを強く推奨します。encryption_util.sh スクリプトを使用する場合には、特殊文字(@、#、!、+ など)は使用しないでください。このスクリプトは特殊文字を暗号化することはできません。

(注)このスクリプトの実行には数分かかる場合があります。設定の進捗を確認するには、次のコマンドを実行します。

```
$ tail -f /tmp/cgmsdb_setup.log
```

```
$ su - oracle
$ export DISPLAY=localhost:0
$ cd $ORACLE_BASE/cgms/scripts
$ ./setupCgmsDb.sh
09-13-2012 10:38:07 PDT: INFO: ======== CGMS Database Setup Started ==========
09-13-2012 10:38:07 PDT: INFO: Log file: /tmp/cgmsdb_setup.log

Are you sure you want to setup CG-NMS database (y/n)? y

09-13-2012 10:38:08 PDT: INFO: User response: y
09-13-2012 10:38:08 PDT: INFO: CGMS database does not exist.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:38:14 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:38:18 PDT: INFO: User entered CG-NMS DB password.
09-13-2012 10:38:18 PDT: INFO: Stopping listener ...
09-13-2012 10:38:18 PDT: INFO: Listener already stopped.
09-13-2012 10:38:18 PDT: INFO: Deleting database files ...
09-13-2012 10:38:18 PDT: INFO: Creating listener ...
09-13-2012 10:38:19 PDT: INFO: Listener creation completed successfully.
09-13-2012 10:38:19 PDT: INFO: Configuring listener ...
09-13-2012 10:38:19 PDT: INFO: Listener successfully configured.
09-13-2012 10:38:19 PDT: INFO: Creating database. This may take a while. Please be patient ...
09-13-2012 10:42:55 PDT: INFO: Database creation completed successfully.
09-13-2012 10:42:55 PDT: INFO: Updating /etc/oratab ...
09-13-2012 10:42:55 PDT: INFO: /etc/oratab updated.
09-13-2012 10:42:55 PDT: INFO: Configuring database ...
09-13-2012 10:42:56 PDT: INFO: Starting listener ...
09-13-2012 10:42:56 PDT: INFO: Listener start completed successfully.
09-13-2012 10:42:56 PDT: INFO: Starting database configuration ...
09-13-2012 10:43:17 PDT: INFO: Database configuration completed successfully.
09-13-2012 10:43:17 PDT: INFO: Starting Oracle ...
09-13-2012 10:43:17 PDT: INFO: Starting Oracle in mount state ...
ORACLE instance started.

Total System Global Area 1.6836E+10 bytes
Fixed Size    2220032 bytes
Variable Size 8589934592 bytes
Database Buffers 8187281408 bytes
Redo Buffers   56487936 bytes
Database mounted.
09-13-2012 10:43:26 PDT: INFO: Opening database for read/write ...

Database altered.

09-13-2012 10:43:29 PDT: INFO: ========== CGMS Database Setup Completed Successfully ==========
```

IoT FND Oracle データベースの起動

IoT FND Oracle データベースを起動するには、次の手順を実行します。

1. 次のスクリプトを実行します。

```
$ su - oracle
$ cd $ORACLE_BASE/cgms/scripts
$ ./startOracle.sh
```

2. このスクリプトを実行して、ブートアップで IoT FND データベースを起動する cron ジョブを設定します。

```
./installOracleJob.sh
```

IoT FND データベースのその他のトピック

次の手順では、データベース管理について説明します。

- IoT FND Oracle データベースの停止
- IoT FND データベースの削除
- IoT FND データベースのアップグレード
- SYS DBA と IoT FND データベースのパスワードの変更
- IoT FND データベースのヘルパー スクリプト

IoT FND Oracle データベースの停止

通常、インストール手順で、Oracle データベースを停止する必要はありません。ただし、Oracle データベースの停止が必要になった場合には、scripts ディレクトリ内の停止スクリプトを使用します。

```
su - oracle
cd $ORACLE_BASE/cgms/scripts
./stopOracle.sh
...
SQL> Database closed.
Database dismounted.
ORACLE instance shut down.
...
```

IoT FND データベースの削除

注意: 次のスクリプトは破壊的です。このスクリプトは通常の操作では使用しないでください。

IoT FND データベースを削除するには、このスクリプトを実行します。

```
cd $ORACLE_BASE/cgms/scripts
./deleteCgmsDb.sh
```

IoT FND データベースのアップグレード

IoT FND データベースをアップグレードするには、次の手順を実行します。

1. データベース ファイル（合計 15 ファイル）を追加します。

```
ALTER TABLESPACE USERS ADD DATAFILE '&oracle_base/oradata/&sid_caps/users<02 to 15>.dbf'
SIZE 5M AUTOEXTEND ON;
```

これはシステムのスケーリングに必要です。

2. ブロック変更の追跡を有効化します(増分バックアップに必要)。

```
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
'&oracle_base/oradata/&sid_caps/rman_change_track.f' REUSE;
```

3. 並列実行を無効にします。

```
set parallel_max_servers = 0 scope=both
```

注意:IoT FND の増分バックアップ スクリプトは、Oracle のブロック変更の追跡機能を有効にして、バックアップのパフォーマンスを向上させます。この機能を利用するには、IoT FND データベースを削除して、setupCgmsDb.sh スクリプトを実行してから、最初の増分バックアップを実行します。データの損失を回避するには、次のコマンドを実行します。

```
sqlplus sys/password@cgms as sysdba
ALTER DATABASE ENABLE BLOCK CHANGE TRACKING USING FILE
'/home/oracle/app/oracle/oradata/CGMS/rman_change_track.f' REUSE;
exit;
```

SYS DBA と IoT FND データベースのパスワードの変更

cgms_dba ユーザの IoT FND データベースのデフォルト パスワードを変更するには、次の手順を実行します。

1. IoT FND サーバで、setupCgms.sh スクリプトを実行し、cgms_dba ユーザのパスワードを変更します。

注意:IoT FND データベースのパスワードと cgnms_dba ユーザのパスワードは一致している必要があります。一致していない場合、IoT FND はデータベースにアクセスできません。

```
# cd /opt/cgms/bin
# ./setupCgms.sh
...
Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y
Enter database password:
Re-enter database password:
09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait
...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
...
```

setupCgms.sh スクリプトの実行については、「IoT FND のセットアップ」を参照してください。

2. Oracle サーバで、change_password.sh スクリプトを実行し、cgms_dba ユーザのパスワードを変更します。

```
$ ./change_password.sh
09-13-2012 10:48:32 PDT: INFO: ======== Database Password Util Started ==========
09-13-2012 10:48:32 PDT: INFO: Log file: /tmp/cgms_oracle.log

Are you sure you want to change CG-NMS database password (y/n)? y
09-13-2012 10:48:33 PDT: INFO: User response: y

Enter current password for SYS DBA:
Re-enter current password for SYS DBA:
09-13-2012 10:48:41 PDT: INFO: User entered current SYS DBA password.
Enter new password for SYS DBA:
Re-enter new password for SYS DBA:
09-13-2012 10:48:54 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-13-2012 10:49:03 PDT: INFO: User entered CG-NMS DB password.
User altered.
...
```

(注)root としてこのスクリプトを使用すると、sys ユーザ(SYS DBA)のパスワードを変更することもできます。

3. IoT FND サーバで cgms_status.sh スクリプトを実行して、IoT FND と IoT FND データベース間の接続を確認します。

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

IoT FND データベースのヘルパー スクリプト

表 7 に、$ORACLE_BASE/cgms/scripts/ ディレクトリ内の使用可能な IoT FND データベースのヘルパー スクリプトを示します。

表 7　IoT FND データベースのヘルパー スクリプト

スクリプト	説明
change_password.sh	データベース管理と IoT FND データベース ユーザ アカウントのパスワードを変更するには、このスクリプトを使用します。IoT FND データベース ユーザ アカウントは、IoT FND がデータベースにアクセスするために使用されます。
backup_archive_log.sh	アーカイブ ログをバックアップするには、このスクリプトを使用します。
backupCgmsDb.sh	IoT FND データベースをバックアップするには、このスクリプトを使用します。このスクリプトは完全バックアップと増分バックアップをサポートします。
restoreCgmsDb.sh	バックアップから IoT FND データベースを復元するには、このスクリプトを使用します。
setupCgmsDb.sh	IoT FND データベースを設定するには、このスクリプトを使用します。
startOracle.sh	IoT FND データベースを起動するには、このスクリプトを使用します。
stopOracle.sh	IoT FND データベースを停止するには、このスクリプトを使用します。
setupStandbyDb.sh	(IoT FND データベース HA のインストールのみ) スタンバイ データベース サーバを設定するには、このスクリプトを使用します。
setupHaForPrimary.sh	(IoT FND データベース HA のインストールのみ) プライマリ データベース サーバを設定するには、このスクリプトを使用します。
getHaStatus.sh	データベースが HA 用に設定されていることを確認するには、このスクリプトを実行します。

SSM のインストールと設定

ソフトウェア セキュリティ モジュール (SSM) は、ハードウェア セキュリティ モジュール (HSM) の低コストの代替策です。IoT FND は CSMP プロトコルを使用して、メーター、DA ゲートウェイ (IR500 デバイス)、および Range Extender と通信します。SSM は CiscoJ を使用して、CSMP メッセージの署名や確認などの暗号化サービス、およびを CSMP キーストア管理を提供します。SSM は連邦情報処理標準 (FIPS) を順守しつつ、サービスを提供します。SSM は IoT FND アプリケーション サーバまたはその他のリモート サーバにインストールします。SSM のリモート コンピュータのインストールでは、IoT FND と安全に通信するため、HTTPS を使用します。

ここでは、SSM のインストールと設定について説明します。具体的な内容は次のとおりです。

- SSM サーバのインストールまたはアップグレード
- SSM サーバのアンインストール
- SSM と IoT FND の統合

SSM サーバをインストール、設定、起動し、SSM 用に IoT FND を設定すると、[Admin] > [Certificates] > [Certificate for CSMP] で CSMP の証明書を確認できます。

(注) ハードウェア セキュリティ モジュール (HSM) の詳細については、「HSM クライアントの設定」を参照してください。

はじめる前に

インストールが表 1 にリストしたハードウェアとソフトウェアの要件を満たしていることを確認します。

SSM サーバのインストールまたはアップグレード

SSM サーバをインストールするには、次の手順を実行します。

1. rpm スクリプト cgms-ssm-<version>-<release>.<architecture>.rpm を実行します。

```
[root@VMNMS demossm]# rpm -Uvh cgms-ssm-<version>.x86_64.rpm
Preparing...                ########################################### [100%]
   1:cgms-ssm               ########################################### [100%]
```

2. SSM に対する IoT FND の設定の詳細を取得します。SSM には次のデフォルトのクレデンシャルが同梱されています。

   - ssm_csmp_keystore パスワード:**ciscossm**
   - csmp のエイリアス名:**ssm_csmp**
   - キー パスワード:**ciscossm**
   - ssm_web_keystore パスワード:**ssmweb**

```
[root@VMNMS demossm]# cd /opt/cgms-ssm/bin/
[root@VMNMS bin]# ./ssm_setup.sh

Software Security Module Server
1. Generate a new keyalias with self signed certificate for CSMP
2. Generate a new keypair & certificate signing request for CSMP
3. Import a trusted certificate
4. Change CSMP keystore password
5. Print CG-NMS configuration for SSM
6. Change SSM server port
7. Change SSM-Web keystore password
Select available options.Press any other key to exit
Enter your choice :
```

3. プロンプトが表示されたら「5」を入力し、次を実行します。

```
Enter current ssm_csmp_keystore password :ciscossm
Enter alias name : ssm_csmp
Enter key password :ciscossm

security-module=ssm
ssm-host=<Replace with IPv4 address of SSM server>
ssm-port=8445
ssm-keystore-alias=ssm_csmp
ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
```

4. この SSM サーバに接続するには、3 からの出力をコピーして cgms.properties ファイルに貼り付けます。

   (注)SSM サーバに接続するために使用する IoT FND のインターフェイスの IPv4 アドレスを含める必要があります。

5. (オプション)以下を行うには、ssm_setup.sh スクリプトを実行します。

   - CSMP の新しいキー エイリアスと自己署名証明書を生成する
   - SSM キーストアのパスワードを変更する
   - SSM サーバ ポートを変更する
   - SSM-Web キーストアのパスワードを変更する

   (注) 上記のいずれかの操作を実行する場合、SSM セットアップ スクリプトを実行し、[Print CG-NMS configuration for SSM] を選択し、すべての詳細をコピーして cgms.properties ファイルに貼り付ける必要があります。

6. SSM サーバを起動します。

```
[root@VMNMS ~]# service ssm start
Starting Software Security Module Server:                  [  OK  ]
```

SSM ログ ファイルのモニタリング

SSM のログは、/opt/cgms-ssm/log/ssm.log でモニタできます。

レポート間隔のデフォルトのメトリックは、最小有効値の 900 秒（15 分）です。サービスのメトリックのみが記録されます。レポートするメトリックがない場合、ログにメッセージは記録されません。

レポート間隔のメトリックは、/opt/cgms-ssm/conf/ssm.properties ファイルで [ssm-metrics-report-interval] フィールド（秒）を設定することで変更できます。

(注) IoT FND サーバを起動する前に、SSM サーバが起動され実行されている必要があります。

SSM サーバのアンインストール

ここでは、SSM サーバを完全にアンインストールする手順を示します。これには新規インストールの手順も含まれます。

(注) この手順はアップグレードには使用しないでください。SSM サーバのインストールまたはアップグレードで説明されている手順を使用します。

SSM サーバをアンインストールするには、次の手順を実行します。

1. SSM サーバを停止します。

```
service ssm stop
```

2. /opt/cgms-ssm/conf ディレクトリとコンテンツを /opt/cgms-ssm の以外のディレクトリにコピーして移動します。
3. cgms ssm rpm をアンインストールします。

```
rpm -e cgms-ssm
```

新規インストールのみ

4. 新しい SSM サーバをインストールします。
5. 2 で移動したコンテンツを /opt/cgms-ssm/conf ディレクトリにコピーして上書きします。

SSM と IoT FND の統合

(注) SSM に切り替える前に、SSM サーバをインストールして起動する必要があります。

CSMP ベースのメッセージングに、ハードウェア セキュリティ モジュール（HSM）の使用から SSM の使用に切り替えるには、次の手順を実行します。

1. IoT FND を停止します。

```
service cgms stop
```

2. SSM サーバで ssm_setup.sh スクリプトを実行します。
3. オプション 3 を選択し、IoT FND SSM 設定を印刷します。

4. 詳細を cgms.properties にコピー アンド ペーストして、SSM サーバに接続します。

   例

   ```
   security-module=ssm
   ssm-host=127.107.155.85
   ssm-port=8445
   ssm-keystore-alias=ssm_csmp
   ssm-keystore-password=NQ1/zokip4gtUeUyQnUuNw==
   ssm-key-password=NQ1/zokip4gtUeUyQnUuNw==
   ```

5. HSM を設定するには、cgms.properties ファイルで次のプロパティを指定します(「HSM クライアントの設定」も参照)。

   ```
   security-module=ssm/hsm (required; hsm : Hardware Security Module default.)
   hsm-keystore-name=testGroup1 (optional; hsm partition name; testGroup1 default)
   hsm-keystore-password=TestPart1 (optional; encrypted hsm partition password; TestPart1 default)
   ```

6. SSM が起動して動作しており、接続できることを確認します。

7. IoT FND を起動します。

IoT FND のインストールおよびセットアップ

次の手順を実行して、IoT FND のインストールを完了します。

- インストールと設定の概要
- IoT FND のインストール
- 証明書の生成およびインストール
- IoT FND のセットアップ
- IoT FND の起動
- IoT FND ステータスのチェック
- IoT FND データベース移行スクリプトの実行
- IoT FND Web GUI へのアクセス

はじめる前に

IoT FND をインストールするには、最初に IoT FND のインストール RPM を取得します。

`cgms-version_number.x86_64.rpm`

(注) /etc/hosts ファイルと /etc/resolv.conf ファイルが IoT FND サーバで正しく設定されていることを確認します。

インストールと設定の概要

ここでは、2 つのタイプの IoT FND のインストールの概要を提供します。

- シングルサーバの展開
- クラスタ展開(HA)

シングルサーバの展開

シングルサーバの展開に IoT FND をインストールして設定するには、次の手順を実行します。

1. IoT FND をホストする RHEL サーバにログインします。
2. IoT FND のインストール。
3. IoT FND のセットアップ。
4. IoT FND データベース移行スクリプトの実行。
5. IoT FND ステータスのチェック。
6. IoT FND Web GUI へのアクセス

クラスタ展開(HA)

HA 展開に IoT FND をインストールして設定するには、「シングルサーバの展開」のステップを繰り返します。ただし、IoT FND データベースの移行スクリプトは 1 回だけ実行します。

IoT FND のインストール

IoT FND アプリケーションをインストールするには、次の手順を実行します。

1. IoT FND インストール RPM を実行します。

```
$ rpm -ivh cgms-version.x86_64.rpm
```

2. インストールを確認し、RPM バージョンを確認します。

```
$ rpm -qa | grep -i cgms
cgms-1.0
```

IoT FND のセットアップ

IoT FND を設定するには、setupCgms.sh スクリプトを実行します。

(注) IoT FND サーバ クラスタを展開している場合、クラスタ内のすべてのノードで setupCgms.sh スクリプトを実行する必要があります。

注意:IoT FND 証明書はデータベースのデータを暗号化します。setupCgms.sh スクリプトは、データベースの移行を実行します。これには、キーストア内の IoT FND 証明書へのアクセスが必要です。setupCgms.sh を実行する前に証明書を設定する必要があります。データベースを移行し、証明書にアクセスできない場合、スクリプトはエラーになります(「証明書の生成およびインストール」を参照)。

注意:setupCgms.sh スクリプトの実行時に、入力したデータベース パスワードが有効であることを確認します。無効なパスワードを複数回入力すると、Oracle によってユーザ アカウントがロックされる場合があります。アカウントのロック解除はデータベース サーバでできます。パスワードのロック解除の詳細については、「IoT Field Network Director User Guide, Release 4.0.x.」のトラブルシューティングの章で、『Unlocking the IoT FND Database Password』を参照してください。

この例では、setupCgms.sh スクリプトを使用して、1 つのデータベースを使用するシングルサーバの IoT FND システムを設定します。

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ========== CG-NMS Setup Started - 2012-09-13-17-10-00 ==========
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log
```

```
Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms

Do you wish to configure another database server for this CG-NMS ? (y/n)? n

09-13-2012 17:11:18 PDT: INFO: User response: n
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y
09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n
09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ========== CG-NMS Setup Completed Successfully ==========
```

setupCgms.sh スクリプトでは、これらの設定を行うことができます。

- データベース設定の構成
- データベース HA の構成
- IoT FND データベース パスワードの設定
- キーストア パスワードの設定
- Web root ユーザ パスワードの設定
- FTPS 設定の構成

データベース設定の構成

データベース設定を構成するため、setupCgms.sh スクリプトによって次の情報の入力が求められます。

- プライマリ IoT FND データベース サーバの IP アドレス
- IoT FND データベース サーバのポート番号

  デフォルトのポート番号（1522）を受け入れるには、Enter キーを押します。
- データベース システム ID（SID）。これはプライマリ データベース サーバの cgms です。

  デフォルトの SID（cgms）を受け入れるには、Enter キーを押します。この SID はサーバをプライマリ データベース サーバと見なします。

```
Do you want to change the database settings (y/n)? y
09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [example.com]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522

Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms
```

データベース HA の構成

スタンバイ データベース設定を構成するため、setupCgms.sh スクリプトによって次の情報の入力が求められます。

- スタンバイ IoT FND データベース サーバの IP アドレス
- スタンバイ IoT FND データベース サーバのポート番号

  1522 と入力します。
- データベース システム ID（SID）。これはプライマリ データベース サーバの cgms です。

  cgms_s を入力します。この SID はサーバをスタンバイ データベース サーバと見なします。

```
Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait ...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.
```

データベース HA の設定については、「HA 用の IoT FND データベースの設定」を参照してください。

IoT FND データベース パスワードの設定

IoT FND データベースのパスワードを変更するよう求められたら、データベース サーバで cgms_dba ユーザ アカウントのパスワードを入力します。デフォルトのパスワードを使用している場合、データベース パスワードをここで変更しないでください。

```
Do you want to change the database password (y/n)? y

09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait ...
09-13-2012 17:15:34 PDT: INFO: Database password configured.
```

キーストア パスワードの設定

キーストア パスワードを設定します。

```
Do you want to change the keystore password (y/n)? y
09-13-2012 10:21:52 PDT: INFO: User response: y

Enter keystore password: keystore_password
Re-enter keystore password: keystore_password

09-13-2012 10:21:59 PDT: INFO: Configuring keystore password. This may take a while. Please wait ...
09-13-2012 10:22:00 PDT: INFO: Keystore password configured.
```

Web root ユーザ パスワードの設定

ブラウザベースの IoT FND インターフェイスへのアクセスを可能にする root ユーザ アカウントのパスワードを変更するには、**y** を入力し、パスワードを入力します。

```
Do you want to change the web application 'root' user password (y/n)? n
09-13-2012 17:16:34 PDT: INFO: User response: n
```

FTPS 設定の構成

クラスタを展開している場合は、ログのダウンロードに必要な FTPS 設定を提供します。FTPS は、クラスタ ノード間で安全にファイルを転送します。FTPS 設定が構成されていない場合、現在ログインしている IoT FND ノードからログだけをダウンロードできます。

```
Do you want to change the FTP settings (y/n)? y
09-13-2012 17:16:45 PDT: INFO: User response: y

Enter FTP user password:
Re-enter FTP user password:

09-13-2012 17:16:49 PDT: INFO: Configuring FTP settings. This may take a while. Please wait ...
09-13-2012 17:16:57 PDT: INFO: FTP settings configuration completed successfully
```

IoT FND ステータスのチェック

IoT FND を起動する前に、このコマンドを実行して IoT FND データベースへの接続を確認します。

```
# service cgms status
09-06-2012 18:51:20 PDT: INFO: CG-NMS database server: localhost
09-06-2012 18:51:21 PDT: INFO: CG-NMS database connection verified.
```

このコマンドにより、IoT FND データベースの IP アドレスまたはホスト名およびステータスが提供され、IoT FND データベースへの接続も確認されます。接続が確認されない場合、IoT FND を起動することはできません。

IoT FND データベース移行スクリプトの実行

IoT FND はデータベースのダンプと復元を行わずに、IoT FND データベースをすばやく移行できる特別なデータベースの移行システムを使用しています。データベースを移行するたび、IoT FND がすでに実行された移行のレコードを維持できるように、IoT FND データベースの一部のテーブルが作成または変更されます。

最初に IoT FND を起動する前に、データベース移行スクリプトを実行して、データベースの IoT FND テーブルを設定します。

```
# cd /opt/cgms/bin
# ./db-migrate
```

(注) IoT FND を初めて起動する前にこのスクリプトを実行すると、数分かかります。IoT FND の新しいバージョンへのアップグレード後にこのスクリプトを実行すると、IoT FND データベースのデータ量によってはさらに時間がかかります。

(注) IoT FND サーバ クラスタを展開している場合、1 つのクラスタ ノードでのみ db-migrate スクリプトを実行します。

db-migrate コマンドでは、データベース パスワードが要求されます。デフォルト パスワードは **cgms123** です。

注意：db-migrate スクリプトの実行時に入力したパスワードが正しいことを確認します。間違ったパスワードを複数回入力すると、Oracle によってユーザ アカウントがロックされる場合があります。この場合、データベース サーバでアカウントのロック解除をする必要があります。パスワードのロックは、以下の手順で解除できます。

- 不正な IoT FND データベース パスワードが複数回入力されると、Oracle はユーザ アカウントをロックします。Oracle ソフトウェアを次の例のように使用して、パスワードをロック解除してください。

```
# su - oracle
# sqlplus sys/<database_password>@cgms as sysdba
alter user cgms_dev account unlock;
exit;.
```

IoT FND Web GUI へのアクセス

IoT FND にはその Web GUI の自己署名証明書が含まれています。IoT FND GUI にアクセスするには、ブラウザにセキュリティ例外を追加する必要があります。IoT FND を起動すると、その Web GUI にアクセスできます。

https://*nms_machine_IP_address*/

デフォルトの初期ユーザ名は root で、パスワードは **root123** です。

セットアップ スクリプトの実行時にパスワードを変更した場合を除き、IoT FND はデフォルトのパスワード **root123** を使用します。

セットアップ スクリプトの詳細については、「IoT FND のセットアップ」を参照してください。

(注) IoT FND にハードウェア セキュリティ モジュール（HSM）が含まれている場合、Firefox ブラウザは IoT FND に接続しません。この問題に対処するには、Firefox の [Preferences] を開き、[Advanced] に移動して [Encryption] タブをクリックします。[Protocols] の下の [Use TLS 1.0] チェック ボックスをオフにします。IoT FND に再接続し、ページが正常にロードされたことを確認します。

HTTPS 接続

IoT FND は TLSv1.2 ベースの HTTPS 接続のみを受け入れます。IoT FND GUI にアクセスするには、TLSv1.2 プロトコルを有効にして、IoT FND との HTTPS 接続を確立する必要があります。

(注) IoT FND リリース 2.1.1-54 以降では、TLSv1.0 または TLSv1.1 ベースの接続をサポートしていません。

初めてのログイン アクション

パスワードの変更

初めて IoT FND にログインすると、パスワードの変更を求めるポップアップ ウィンドウが表示されます。

(注) IoT FND では、最大 32 文字のパスワード長をサポートしています。

1. 新しいパスワードを入力します。
2. 新しいパスワードを [Confirm Password] フィールドにも入力します。
3. [Change Password] をクリックします。

タイム ゾーンの設定

タイム ゾーンを設定するには、以下のステップに従います。

1. [username] ドロップダウン メニュー(右上)から、[Time Zone] を選択します。
2. 時間帯を選択します。
3. [Update Time Zone] をクリックします。
4. [OK] をクリックします。

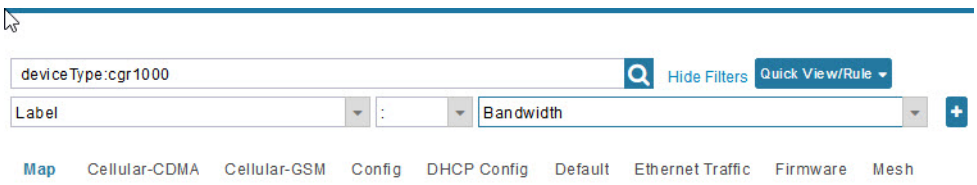
列のソート順序の変更

列見出しの下にリスト(ルータのリストなど)が表示されるページでは、列見出しにある三角形のアイコンを切り替えることで、ソート順(昇順または降順)を変更できます。

リストのフィルタリング

IoT FND では、[DEVICES] ページと [OPERATIONS] ページでフィルタを定義できます。

- フィルタを定義するには、検索フィールドの右側にある [Show Filters] をクリックして、フィルタ定義パネル(以下に表示)を開きます。フィールドで検索パラメーターを定義したら、虫めがねアイコンをクリックして検索を開始します。結果は、フィルタ フィールドの下に表示されます。



- [Hide Filters] をクリックして検索フィールドを閉じます。

次の例では、[Search Devices] フィールドに検索文字列「**deviceType:cgmesh status:up**」を入力することで、Up ステータスのメッシュ エンドポイント デバイスをリストします。

ユーザ インターフェイスのユーザ設定

<ユーザ名> ドロップダウン メニュー（右上）の下にある [Preferences] オプションを選択すると、ユーザ インターフェイスに表示される項目を定義できます。

表示される [User Preferences] パネルでは、オプションの横にあるチェックボックスをオンにして、表示する項目（以下にリスト）を選択できます。[Apply] をクリックして保存します。

以下のような [User Preference] オプションがあります。

- イベント ページにグラフを表示
- イベントまたは問題ページにサマリー カウントを表示
- MAP の有効化：
- デフォルトでマップ ビューを表示
- デバイス ページにデバイス タイプおよび機能（ルータ、エンドポイント、ヘッドエンド ルータ、サーバ）を表示

ログアウト

<ユーザ名> ドロップダウン メニュー（右上）の [Log Out] をクリックします。

IoT FND CLI

このセクションでは、IoT FND の管理に使用する主要なコマンドライン インターフェイス（CLI）について説明します。

- IoT FND の起動
- IoT FND ステータスのチェック
- IoT FND の停止
- IoT FND ログ ファイルの場所
- IoT FND ヘルパー スクリプト
- IoT FND のアップグレード
- IoT FND のアンインストール

IoT FND の起動

IoT FND を起動するには、このコマンドを実行します。

```
service cgms start
```

IoT FND がブート時に自動的に動作するように設定するには、このコマンドを実行します。

```
chkconfig cgms on
```

IoT FND ステータスのチェック

IoT FND のステータスを確認するには、このコマンドを実行します。

```
service cgms status
```

IoT FND の停止

IoT FND を停止するには、このコマンドを実行します。

```
service cgms stop
```

(注)アプリケーションが停止するには、通常、約 10 秒かかります。Java プロセスが実行されていないことを確認するには、**ps | grep java** を実行します。

IoT FND ログ ファイルの場所

IoT FND ログ ファイル(server.log)は /opt/cgms/server/cgms/log ディレクトリにあります。

IoT FND ヘルパー スクリプト

表 8 で、/opt/cgms/bin/ ディレクトリ内の IoT FND ヘルパー スクリプトについて説明します。

表 8　IoT FND ヘルパー スクリプト

スクリプト	説明
deinstall_cgms_watchdog.sh	ウォッチドッグ スクリプトをアンインストールします。
install_cgms_watchdog.sh	ウォッチドッグ スクリプトをインストールします。
mcast_test.sh	クラスタ メンバー間の通信をテストします。
password_admin.sh	IoT FND へのアクセスに使用するユーザ パスワードを変更またはリセットします。
print_cluster_view.sh	クラスタ メンバーを印刷します。

IoT FND のアップグレード

(注)通常のアップグレード時には、データベースを停止する必要はありません。すべてのアップグレードはインプレースです。

(注)カスタム セキュリティ証明書を使用した仮想 IoT FND のインストールについては、このアップグレードを実行する前に「カスタム証明書の管理」を参照してください。

注意:次の手順を順に実行します。

IoT FND アップグレードするには、次の手順を実行します。

1. 新しい IoT FND RPM を取得します。
2. IoT FND を停止します。

   ```
   service cgms stop
   ```

   (注)アプリケーションが停止するには、通常、約 10 秒かかります。Java プロセスが実行されていないことを確認するには、**ps | grep java** を実行します。
3. IoT FND RPM をアップグレードします。

   ```
   rpm -Uvh new_cgms_rpm_filename
   ```

   (注)これらのファイルは、/opt/cgms 内のファイルを上書きします。
4. データベースの移行を実行し、/opt/cgms ディレクトリからデータベースをアップグレードします。

   ```
   cd /opt/cgms
   bin/db-migrate
   ```

   (注)db-migrate スクリプトは、アップグレードが終了するたびに実行する必要があります。

5. プロンプトが表示されたら、データベースのパスワードを入力します。デフォルト パスワードは **cgms123** です。
6. IoT FND を起動します。

```
# service cgms start
```

RHEL（Red Hat Enterprise Linux）GUI を使用して IoT FND サービスを開始することもできます（[ADMIN] > [System Management] > [Server Settings] > [Services]）。詳細については、RHEL のマニュアルを参照してください。

IoT FND のアンインストール

(注) これは、すべての IoT FND のローカル インストールの設定とインストール ファイル（証明書を含むキーストアなど）を削除します。

ヒント：IoT FND を再インストールする予定がある場合は、現在のキーストアと証明書ファイルをコピーして、インストール パッケージに含まれるキーストアと証明書ファイルを上書きするのに使用します。

IoT FND アプリケーションを削除するには、次のコマンドを実行します。

```
# rpm -e cgms
# rm -rf /opt/cgms
```

IoT FND データベースのクリーンアップ

IoT FND データベースをクリーンアップするには、次の手順を実行します。

1. （HA データベース設定）オブザーバ サーバを停止します。
2. （HA データベース設定）$ORACLE_BASE/cgms/scripts/ha/deleteStandbyDb.sh スクリプトを実行して、スタンバイ データベースを削除します。
3. （HA データベース設定）$ORACLE_BASE/cgms/scripts/ha/deletePrimaryDbHa.sh スクリプトを実行して、プライマリ データベースから HA 設定を削除します。
4. $ORACLE_BASE/cgms/scripts/deleteCgmsDb.sh スクリプトを実行して、プライマリ データベースを削除します。

IoT FND TPS プロキシのインストールと設定

通常、オプション TPS プロキシを初めて使用するのは、IoT FND が処理する Zero Touch Deployment（ZTD）の部分を初期化するインバウンド要求を CGR が送信するときです。IoT FND はファイアウォールの背後で稼働しており、パブリックで到達可能な IP アドレスがありません。フィールド エリア ルータ（CGR）は、IoT FND に初めてコンタクトするときに、IoT FND から TPS プロキシを使用するよう求められます。このサーバは、これらのルータが IoT FND アプリケーション サーバにコンタクトして、トンネル プロビジョニングを要求できるようにします（「トンネルのプロビジョニングの管理」を参照）。

TPS プロキシには独自の GUI はありません。HTTPS アウトバウンド トンネル プロビジョニング要求が、IoT FND で TPS プロキシからの要求として認識されるように、**cgnms.properties** ファイルと **tpsproxy.properties-template** ファイルでプロパティを編集する必要があります。

トンネルをプロビジョニングすると、フィールド エリア ルータは TPS プロキシを使用せずに IoT FND に直接コンタクトすることができます。IoT FND にプロキシの証明書から正確な証明書の件名が通知され、TPS プロキシからの HTTPS インバウンド要求が認証されます。

TPS プロキシの設定

cgms-tpsproxy RPM パッケージ Java アプリケーションを、ファイアウォールの外側の IoT FND のステートレス拡張として機能するように、別の（TPS プロキシ）サーバにインストールします。TPS プロキシは Red Hat Enterprise Linux（RHEL）サーバ（表 1 の TPS プロキシのシステム要件を参照）が可能です。cgnms-tpsproxy アプリケーションはサーバでデーモンとして実行され、次の設定パラメータを必要とします。

- IoT FND サーバの URL（インバウンド要求を転送するため）。
- アウトバウンド要求を転送するためのホワイトリスト（認定リスト）の一部としての IoT FND サーバの IP アドレス。

TPS プロキシをインストールする前に、TPS プロキシのインストール パッケージを取得します。

`cgms-tpsproxy-version_number.x86_64.rpm`

プロキシサーバの設定を構成するには、次の手順を実行します。

1. TPS プロキシとして使用するように RHEL サーバを設定します。
2. この RHEL サーバをファイアウォールの外側で到達できるように接続します。
3. テンプレート ファイルを使用して TPS プロキシを設定します。

```
ssh root@tps_proxy_server
cd /opt/cgms-tpsproxy/conf
cp tpsproxy.properties-template tpsproxy.properties
```

(注) IoT FND TPS プロキシの登録時に encryption_util.sh スクリプトを実行した後、cgnms.properties ファイルと tpsproxy.properties ファイルを編集します。

4. tpsproxy.properties ファイルを編集して、IoT FND アプリケーション サーバのインバウンド アドレスとアウトバウンド アドレスを定義する次の行を追加します。

```
[root@cgr-centos57 conf]# cat tpsproxy.properties-template
inbound-proxy-destination=https://nms_domain_name:9120
outbound-proxy-allowed-addresses=nms_ip_address
cgms-keystore-password-hidden=<obfuscated password>
```

(注) HTTPS アウトバウンド トンネル プロビジョニング要求が、IoT FND で TPS プロキシからの要求として認識されるように、cgnms.properties ファイルと tpsproxy.properties-template ファイルでプロパティを編集する必要があります。

TPS プロキシ ファイアウォールの設定

TPS プロキシ ファイアウォールを設定するには、次の手順を実行します。

- ポート 9120 で TPS プロキシから IoT FND サーバへの HTTPS 接続を許可するファイアウォール ルールを設定します（HTTPS インバウンド要求）。
- ポート 9122 で IoT FND サーバから TPS プロキシへの HTTPS 接続を許可するファイアウォール ルールを設定します（HTTPS アウトバウンド要求）。

IoT FND TPS プロキシの登録

TPS プロキシの登録プロセスは、IoT FND の登録プロセスと同じです。IoT FND アプリケーション サーバの証明書に署名する認証局（CA）は、TPS プロキシの証明書にも署名する必要があります。TPS プロキシの証明書は Java キーストアに保存され、IoT FND 証明書に似ています。

登録プロセスについては、次のシナリオを検討してください。

- 新規インストール
  - キーストアのパスワードがデフォルト パスワードと同じ場合は、デフォルト パスワードを変更します。

    (注) デフォルト パスワードはすべて変更することを**強く推奨します**。encryption_util.sh スクリプトは特殊文字を暗号化できないため、@、#、!、+ などの特殊文字は使用しないでください。
  - キーストア パスワードがデフォルト パスワードとは異なっている場合、encryption_util.sh スクリプトを実行して、暗号化されたパスワードを properties ファイルにコピーします。

    (注) encryption_util.sh スクリプトを実行した後、cgnms.properties ファイルと tpsproxy.properties ファイルを編集します。
- アップグレード

  デフォルト パスワードまたはカスタム パスワードを使用しているかどうかに関わらず、アップグレード プロセスでは /opt/cgms-tpsproxy/conf/tpsproxy.properties ファイルのパスワードが暗号化されます。

IoT FND の登録の詳細については、「*Generating and Exporting Certificates*」を参照してください。

端末 TPS プロキシを登録するには、次の手順を実行します。

1. **cgms_keystore** ファイルを作成します。
2. このファイルに証明書を追加します。
3. **/opt/cgms-tpsproxy/conf** ディレクトリにファイルをコピーします。

TPS プロキシを使用するための IoT FND の設定

HTTPS アウトバウンド トンネル プロビジョニング要求が、IoT FND で TPS プロキシからの要求として認識されるように、cgnms.properties ファイルと tpsproxy.properties-template ファイルでプロパティを編集する必要があります。TPS プロキシは、すべてのインバウンドおよびアウトバウンド要求をログに記録します。

(注) cgnms.properties ファイルと tpsproxy.properties-template ファイルでプロパティを設定しないと、IoT FND は TPS プロキシを認識せず、転送された要求をドロップし、不明なデバイスからの要求と見なします。

(注) 次の例では、必須の値でない変数を使用しています。これらは例としてのみ提示しています。

TPS プロキシを使用するように IoT FND を設定するには、次の手順を実行します。

1. IoT FND サーバへの SSH 接続を開きます。

   ```
   ssh root@nms_machine
   cd /opt/cgms/server/cgms/conf/
   ```

   (注) IoT FND TPS プロキシの登録時に encryption_util.sh スクリプトを実行した後、cgnms.properties ファイルと tpsproxy.properties ファイルを編集します。
2. **cgdm tpsproxy** ファイルを編集して、cgdm-tpsproxy-subject プロパティに TPS プロキシの IP アドレス、ドメイン名、ユーザの情報カテゴリを特定する行を追加します。

   (注) cgdm-tpsproxy-subject プロパティは、インストールされた TPS プロキシの証明書と一致する必要があります。

   ```
   cgdm-tpsproxy-addr=proxy_server_IP_address
   cgdm-tpsproxy-subject=CN="common_name", OU="organizational_unit", O="organization", L="location",
   ST="state", C="country"
   ```

   (注) カンマ区切りの文字列を引用符で囲みます。

IoT FND TPS プロキシの起動

インストール、設定、登録を行ったら、TPS プロキシを起動します。

TPS プロキシを起動するには、起動スクリプトを実行します。

```
service tpsproxy start
```

TPS プロキシのログ ファイルは次の場所にあります。

```
/opt/cgms-tpsproxy/log/tpsproxy.log
```

(注)詳細については、「TPS プロキシの検証」を参照してください。

TPS プロキシの検証

TPS プロキシはインバウンドおよびアウトバウンドのすべての HTTPS 要求を、/opt/cgms-tpsproxy/log/tpsproxy.log にある TPS ログ ファイルに記録します。

TPS プロキシの tpsproxy.log ファイルの次のエントリは、CGR のインバウンド要求を定義します。

```
73: cgr-centos57: May 21 2014 01:05:20.513 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][eid=CGR1240/K9+JAF1732ARCJ][ip=192.168.201.5][sev=INFO][tid=qtp46675819-
29]: Inbound proxy request from [192.168.201.5] with client certificate subject
[CN=CGRJAF1732ARCJ.example.com, SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

TPS プロキシの tpsproxy.log ファイルのこのメッセージ エントリは、TPS が正常にメッセージを IoT FND に転送したことを示します。

```
74: cgr-centos57: May 21 2014 01:05:20.564 -0700: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyServlet-49dc423f][sev=INFO][tid=com.cisco.cgms.tpsproxy.TpsProxyServlet-49dc423f-22]:
Completed inbound proxy request from [192.168.201.5] with client certificate subject
[CN=CGRJAF1732ARCJ.example.com, SERIALNUMBER=PID:CGR1240/K9 SN:JAF1732ARCJ]
```

IoT FND サーバのログ ファイル内の次のエントリは、TPS プロキシを特定します。

```
Request came from proxy
Using forwarded client subject (CN=cg-cgr-1, SERIALNUMBER=PID:CGR1240/K9 SN:JSJ15220047) for 認証
```

TPS プロキシの tpsproxy.log ファイルの次のエントリは、アウトバウンド要求を定義します。

```
%CGMS-6-UNSPECIFIED: %[ch=TpsProxyOutboundHandler][ip=192.168.205.5][sev=INFO][tid=qtp257798932-15]:
Outbound proxy request from [192.168.205.5] to [192.168.201.5:8443]
```

IoT FND サーバのログ ファイル内の次のエントリは、HTTPS 接続を特定します。

```
Using proxy at 192.168.201.6:9122 to send to https://192.168.201.4:8443/cgdm/mgmt commands:
```

Dual-PHY 用の IoT FND の設定

Dual-PHY CGR では、Dual-PHY WPAN プロパティを設定することにより、すべての Dual-PHY WPAN モジュール(マスターおよびスレーブ)を構成する必要があります(「IoT FND 4.0 User Guide」の『*Managing Devices*』の章で表 13 を参照してください)。適切なデバイス追加ファイルで設定するパラメータは、**masterWpanInterface** と **slaveWpanInterface** です。スレーブ Dual-PHY WPAN デバイスでは、**slave-mode** パラメータも設定する必要があります。

(注)Dual-PHY CGR の設定情報については、『*Connected Grid WPAN Module for CGR 1000 Series Installation and CG-Mesh Configuration Guide (Cisco IOS)*』を参照してください。

例

次の例は、設定のプッシュ時にどの WPAN デバイスをマスター インターフェイスとスレーブ インターフェイスとして割り当てるかを IoT FND に指示します。

```
deviceType,eid,ip,meshPrefixConfig,meshPrefixLengthConfig,meshPanidConfig,meshAddressConfig,
dhcpV4LoopbackLink,dhcpV4TunnelLink,dhcpV6LoopbackLink,dhcpV6TunnelLink,tunnelSrcInterface1,
tunnelHerEid,adminUsername,adminPassword,certIssuerCommonName,ipsecTunnelDestAddr1,
masterWpanInterface,slaveWpanInterface,lat,lng
cgr1000,CGR1240/K9+JAF1741BFQS,2.2.56.253,2319:EXTRA:BEEF:CAFE::,64,1233,
2319:EXTRA:BEEF:CAFE::,20.211.0.1,20.211.0.1,2001:420:7bf:7e8::1,
2001:420:7bf:7e8::1,GigabitEthernet2/1,cg-isr900,cg-nms-administrator,
0ERIF+cKsLwyT0YTFd0k+NpVAAPxcIvFfoX1sogAXVkSOAczUFT8TG0U58ccJuhds52KXL4dtu5iljZsQNH+
pEQ1aIQvIGuIas9wp9MKUARYpNErXRiHEnpeH044Rfa4uSgsWXEyrVNxHyuvSefB5j6H0uA7tIQwEHDXOiq
/d0yxvfd4IYos7NzPXlJNiR+Cp6bwx7dG+d9Jo+JuNxLXpi8Fo5n88usjMoXPNbyrqvgn7SS4f+VYgXx1iyDNP0k
+7OEE8uSTVeUJXe7UXkndz5CaU17yk94UxOxamv2i1KEQxTFgw/UvrkCwPQoDMijPstDBXpFv8dqtA0xDGKuaRg
==,cenbursaca-cenbu-sub-ca,2.2.55.198,Wpan3/1,Wpan5/1,41.413324,-120.920315
```

以下は、CGR WPAN モジュールでのマスター/スレーブ インターフェイスを設定するための標準的なテンプレートです。

```
interface ${device.masterWpanInterface}
  no shut
  ipv6 address ${device.meshAddressConfig}/${device.meshPrefixLengthConfig}
  ieee154  panid ${device.meshPanidConfig}
  outage-server ${device.relayDest}
exit

interface ${device.slaveWpanInterface}
  no ip address
ip broadcast-address 0.0.0.0
no ip route-cache
ieee154 beacon-async min-interval 10 max-interval 10 suppression-coefficient 0
ieee154 ssid cisco_muruga_dual
ieee154 txpower 21
slave-mode 3
rpl dag-lifetime 240
rpl dio-min 21
rpl version-incr-time 240
authentication host-mode multi-auth
authentication port-control auto
ipv6 dhcp relay destination global  2001:420:7BF:5F::705
dot1x pae authenticator
  ieee154 panid ${device.meshPanidConfig}
exit
end
```

Dual-PHY デバイスのメッシュ セキュリティ キー

(注) スレーブ WPAN デバイスにはメッシュ セキュリティ キーを設定しないでください。

IoT FND でマスター/スレーブ モードが正しく設定されていると、IoT FND は自動的にマスター WPAN を検出し、そのメッシュ セキュリティ キーを設定します。既存の CGR を設定し、別の WPAN インターフェイスを追加すると、すべてのメッシュ セキュリティ キーが両方のインターフェイスから削除され、IoT FND によりマスター/スレーブ モードが設定されます。CGR が接続されると、すべてのメーターが再認証を経由します。

次のコマンドを使用して、メッシュ キーを削除できます。

```
mesh-security expire mesh-key interface wpan <slot>/<slot number>
```

設定例

次の例では、現在の Dual-PHY WPAN デバイスの RPL スロット ツリー、RPL スロット テーブル、RPL IP ルート情報テーブル、スロット 4/1 と 3/1 の設定情報を取得します。

```
cisco-NXT-FAR5#show wpan 4/1 rpl stree

---------------------------- WPAN RPL SLOT TREE [4] -----------------------------

  [2001:RTE:RTE:64::4]
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1800    // SY RF nodes
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1801
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A00
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1802
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1803
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1804
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1805
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A03
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A07
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1806
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1807
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1808
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1809
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180A
           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:180B
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A01
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C05
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C06
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C07
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A02
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A04
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A05
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C03
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C08
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C09
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0A
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A06
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C02
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C04
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A08
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A09
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0A
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C00
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C01
                           \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1C0B
                   \--(RF )-- 2001:RTE:RTE:64:207:8108:3C:1A0B
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E00    // CY PLC nodes
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E01
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E02
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E03
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E04
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E05
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E06
           \--(PLC)-- 2001:RTE:RTE:64:217:3BCD:26:4E07

RPL SLOT TREE: Num.DataEntries 44, Num.GraphNodes 45 (external 0) (RF 36) (PLC 8)


cisco-NXT-FAR5#ping 2001:RTE:RTE:64:217:3BCD:26:4E01
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:217:3BCD:26:4E01, timeout is 2 seconds:
!!!!!
```

```
Success rate is 100 percent (5/5), round-trip min/avg/max = 254/266/294 ms

cisco-NXT-FAR5#ping 2001:RTE:RTE:64:207:8108:3C:1C00
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:RTE:RTE:64:207:8108:3C:1C00, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 272/441/636 ms
cisco-NXT-FAR5#

cisco-NXT-FAR5#show wpan 4/1 rpl stable

------------------------------ WPAN RPL ROUTE SLOT TABLE [4] ------------------------------
NODE_IPADDR                    NEXTHOP_IP                     SSLOT LAST_HEARD
2001:RTE:RTE:64:207:8108:3C:1800        2001:RTE:RTE:64::4                       3      17:49:12
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801        2001:RTE:RTE:64::4                       3      18:14:05
2001:RTE:RTE:64:207:8108:3C:1802        2001:RTE:RTE:64::4                       3      18:14:37
2001:RTE:RTE:64:207:8108:3C:1803        2001:RTE:RTE:64::4                       3      17:56:56
2001:RTE:RTE:64:207:8108:3C:1804        2001:RTE:RTE:64::4                       3      17:48:53
2001:RTE:RTE:64:207:8108:3C:1805        2001:RTE:RTE:64::4                       3      17:47:52
2001:RTE:RTE:64:207:8108:3C:1806        2001:RTE:RTE:64::4                       3      17:49:54
2001:RTE:RTE:64:207:8108:3C:1807        2001:RTE:RTE:64::4                       3      17:46:38
2001:RTE:RTE:64:207:8108:3C:1808        2001:RTE:RTE:64::4                       3      18:22:01
2001:RTE:RTE:64:207:8108:3C:1809        2001:RTE:RTE:64::4                       3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180A        2001:RTE:RTE:64::4                       3      17:50:02
2001:RTE:RTE:64:207:8108:3C:180B        2001:RTE:RTE:64::4                       3      18:24:00
2001:RTE:RTE:64:207:8108:3C:1A00        2001:RTE:RTE:64:207:8108:3C:1801         3      17:56:34
2001:RTE:RTE:64:207:8108:3C:1A01        2001:RTE:RTE:64:207:8108:3C:180B         3      18:27:34
2001:RTE:RTE:64:207:8108:3C:1A02        2001:RTE:RTE:64:207:8108:3C:180B         3      18:03:06
2001:RTE:RTE:64:207:8108:3C:1A03        2001:RTE:RTE:64:207:8108:3C:1805         3      18:25:18
2001:RTE:RTE:64:207:8108:3C:1A04        2001:RTE:RTE:64:207:8108:3C:180B         3      17:57:15
2001:RTE:RTE:64:207:8108:3C:1A05        2001:RTE:RTE:64:207:8108:3C:180B         3      18:23:39
2001:RTE:RTE:64:207:8108:3C:1A06        2001:RTE:RTE:64:207:8108:3C:180B         3      18:04:16
2001:RTE:RTE:64:207:8108:3C:1A07        2001:RTE:RTE:64:207:8108:3C:1805         3      17:55:00
2001:RTE:RTE:64:207:8108:3C:1A08        2001:RTE:RTE:64:207:8108:3C:180B         3      18:19:35
2001:RTE:RTE:64:207:8108:3C:1A09        2001:RTE:RTE:64:207:8108:3C:180B         3      18:02:02
2001:RTE:RTE:64:207:8108:3C:1A0A        2001:RTE:RTE:64:207:8108:3C:180B         3      18:18:00
2001:RTE:RTE:64:207:8108:3C:1A0B        2001:RTE:RTE:64:207:8108:3C:180B         3      18:02:46
2001:RTE:RTE:64:207:8108:3C:1C00        2001:RTE:RTE:64:207:8108:3C:1A0A         3      18:22:03
2001:RTE:RTE:64:207:8108:3C:1C01        2001:RTE:RTE:64:207:8108:3C:1A0A         3      18:24:03
2001:RTE:RTE:64:207:8108:3C:1C02        2001:RTE:RTE:64:207:8108:3C:1A06         3      18:25:03
2001:RTE:RTE:64:207:8108:3C:1C03        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C04        2001:RTE:RTE:64:207:8108:3C:1A06         3      18:24:05
2001:RTE:RTE:64:207:8108:3C:1C05        2001:RTE:RTE:64:207:8108:3C:1A01         3      18:10:02
2001:RTE:RTE:64:207:8108:3C:1C06        2001:RTE:RTE:64:207:8108:3C:1A01         3      18:05:03
2001:RTE:RTE:64:207:8108:3C:1C07        2001:RTE:RTE:64:207:8108:3C:1A01         3      18:11:03
2001:RTE:RTE:64:207:8108:3C:1C08        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:05
2001:RTE:RTE:64:207:8108:3C:1C09        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0A        2001:RTE:RTE:64:207:8108:3C:1A05         3      18:15:04
2001:RTE:RTE:64:207:8108:3C:1C0B        2001:RTE:RTE:64:207:8108:3C:1A0A         3      18:24:03
2001:RTE:RTE:64:217:3BCD:26:4E00        2001:RTE:RTE:64::4                       4      18:21:40

// CY PLC nodes
2001:RTE:RTE:64:217:3BCD:26:4E01        2001:RTE:RTE:64::4                       4      17:47:23
2001:RTE:RTE:64:217:3BCD:26:4E02        2001:RTE:RTE:64::4                       4      18:20:16
2001:RTE:RTE:64:217:3BCD:26:4E03        2001:RTE:RTE:64::4                       4      17:49:07
2001:RTE:RTE:64:217:3BCD:26:4E04        2001:RTE:RTE:64::4                       4      18:21:49
2001:RTE:RTE:64:217:3BCD:26:4E05        2001:RTE:RTE:64::4                       4      18:22:06
2001:RTE:RTE:64:217:3BCD:26:4E06        2001:RTE:RTE:64::4                       4      18:22:51
2001:RTE:RTE:64:217:3BCD:26:4E07        2001:RTE:RTE:64::4                       4      18:24:04

Number of Entries in WPAN RPL ROUTE SLOT TABLE: 44 (external 0)

cisco-NXT-FAR5#show wpan 4/1 rpl itable
```

```
        ------------------------------ WPAN RPL IPROUTE INFO TABLE [4] ------------------------------
NODE_IPADDR                    RANK  VERSION     NEXTHOP_IP                      ETX_P      ETX_LRSSIR  RSSIF HOPS  PARENTS      SSLOT
2001:RTE:RTE:64:207:8108:3C:1800        835   1     2001:RTE:RTE:64::4                        0     762   -67   -71   1     1      3
// SY RF nodes
2001:RTE:RTE:64:207:8108:3C:1801        692   2     2001:RTE:RTE:64::4                        0     547   -68   -67   1     1      3
2001:RTE:RTE:64:207:8108:3C:1802        776   2     2001:RTE:RTE:64::4                        0     711   -82   -83   1     1      3
2001:RTE:RTE:64:207:8108:3C:1803        968   2     2001:RTE:RTE:64::4                        0     968   -72   -63   1     1      3
2001:RTE:RTE:64:207:8108:3C:1804        699   1     2001:RTE:RTE:64::4                        0     643   -71   -66   1     1      3
2001:RTE:RTE:64:207:8108:3C:1805        681   1     2001:RTE:RTE:64::4                        0     627   -70   -64   1     1      3
2001:RTE:RTE:64:207:8108:3C:1806        744   1     2001:RTE:RTE:64::4                        0     683   -69   -68   1     1      3
2001:RTE:RTE:64:207:8108:3C:1807        705   1     2001:RTE:RTE:64::4                        0     648   -76   -63   1     1      3
2001:RTE:RTE:64:207:8108:3C:1808        811   2     2001:RTE:RTE:64::4                        0     811   -68   -69   1     2      3
2001:RTE:RTE:64:207:8108:3C:1809        730   1     2001:RTE:RTE:64::4                        0     692   -68   -70   1     1      3
2001:RTE:RTE:64:207:8108:3C:180A        926   1     2001:RTE:RTE:64::4                        0     926   -66   -68   1     1      3
2001:RTE:RTE:64:207:8108:3C:180B        602   2     2001:RTE:RTE:64::4                        0     314   -74   -69   1     1      3
2001:RTE:RTE:64:207:8108:3C:1A00        948   1     2001:RTE:RTE:64:207:8108:3C:1801        692   256   -73   -75   2     1      3
2001:RTE:RTE:64:207:8108:3C:1A01        646   2     2001:RTE:RTE:64:207:8108:3C:180B        323   256   -73   -75   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A02        948   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -73   -75   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A03        803   2     2001:RTE:RTE:64:207:8108:3C:1805        503   256   -68   -78   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A04        858   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -65   -69   2     1      3
2001:RTE:RTE:64:207:8108:3C:1A05        646   2     2001:RTE:RTE:64:207:8108:3C:180B        323   256   -71   -69   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A06        858   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -73   -75   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A07        979   1     2001:RTE:RTE:64:207:8108:3C:1805        627   352   -71   -73   2     1      3
2001:RTE:RTE:64:207:8108:3C:1A08        646   2     2001:RTE:RTE:64:207:8108:3C:180B        390   256   -75   -70   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A09        948   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -70   -69   2     3      3
2001:RTE:RTE:64:207:8108:3C:1A0A        646   2     2001:RTE:RTE:64:207:8108:3C:180B        390   256   -75   -71   2     2      3
2001:RTE:RTE:64:207:8108:3C:1A0B        858   1     2001:RTE:RTE:64:207:8108:3C:180B        602   256   -68   -68   2     2      3
2001:RTE:RTE:64:207:8108:3C:1C00        902   2     2001:RTE:RTE:64:207:8108:3C:1A0A        646   256   -70   -74   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C01        902   2     2001:RTE:RTE:64:207:8108:3C:1A0A        646   256   -71   -72   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C02        1114  1     2001:RTE:RTE:64:207:8108:3C:1A06        858   256   -74   -73   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C03        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -76   -77   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C04        902   2     2001:RTE:RTE:64:207:8108:3C:1A06        646   256   -75   -68   3     2      3
2001:RTE:RTE:64:207:8108:3C:1C05        1114  1     2001:RTE:RTE:64:207:8108:3C:1A01        858   256   -66   -74   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C06        1114  1     2001:RTE:RTE:64:207:8108:3C:1A01        858   256   -74   -72   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C07        1114  1     2001:RTE:RTE:64:207:8108:3C:1A01        858   256   -70   -75   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C08        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -74   -70   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C09        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -70   -74   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C0A        1114  1     2001:RTE:RTE:64:207:8108:3C:1A05        858   256   -70   -69   3     1      3
2001:RTE:RTE:64:207:8108:3C:1C0B        902   2     2001:RTE:RTE:64:207:8108:3C:1A0A        646   256   -76   -74   3     1      3
2001:RTE:RTE:64:217:3BCD:26:4E00        616   2     2001:RTE:RTE:64::4                        0     616   118   118   1     1      4     // CY PLC
nodes
2001:RTE:RTE:64:217:3BCD:26:4E01        702   1     2001:RTE:RTE:64::4                        0     646   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E02        557   2     2001:RTE:RTE:64::4                        0     557   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E03        626   1     2001:RTE:RTE:64::4                        0     579   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E04        609   2     2001:RTE:RTE:64::4                        0     609   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E05        602   2     2001:RTE:RTE:64::4                        0     602   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E06        594   2     2001:RTE:RTE:64::4                        0     594   118   118   1     1      4
2001:RTE:RTE:64:217:3BCD:26:4E07        584   2     2001:RTE:RTE:64::4                        0     584   118   118   1     1      4

        Number of Entries in WPAN RPL IPROUTE INFO TABLE: 44

        cisco-NXT-FAR5#

        cisco-NXT-FAR5#show run int wpan 4/1
        Building configuration...
        Current configuration : 320 bytes
        !
        interface Wpan4/1
         no ip address
         ip broadcast-address 0.0.0.0
         no ip route-cache
         ieee154 beacon-async min-interval 100 max-interval 600 suppression-coefficient 1
         ieee154 panid 5552
         ieee154 ssid ios_far5_plc
         ipv6 address 2001:RTE:RTE:64::4/64
         ipv6 enable
         ipv6 dhcp relay destination  2001:420:7BF:5F::500
        end

        cisco-NXT-FAR5#show run int wpan 3/1
        Building configuration...
        Current configuration : 333 bytes
        !
        interface Wpan3/1
         no ip address
         ip broadcast-address 0.0.0.0
         no ip route-cache
```

```
 ieee154 beacon-async min-interval 120 max-interval 600 suppression-coefficient 1
 ieee154 panid 5551
 ieee154 ssid ios_far5_rf
 slave-mode 4
 ipv6 address 2001:RTE:RTE:65::5/64
 ipv6 enable
 ipv6 dhcp relay destination  2001:420:7BF:5F::500
end
```

IoT FND データベースのバックアップと復元

ここでは、IoT FND がデータベースの完全バックアップと増分バックアップをどのようにサポートしているかを説明します。

はじめる前に

IoT FND データベースをバックアップする前に、次の手順を実行します。

1. 最新の cgms-oracle-*version_number*.x86_64.rpm パッケージをダウンロードしてインストールします。
2. スクリプト、テンプレート、ツール フォルダを /opt/cgms-oracle フォルダから $ORACLE_BASE/cgms フォルダにコピーします。
3. oracle:dba にコピーしたファイルとフォルダの所有権を設定します。

IoT FND データベースの完全バックアップの作成

完全バックアップは、データ ファイルからすべてのブロックをバックアップします。完全バックアップは時間がかかり、部分バックアップより多くのディスク領域とシステム リソースを消費します。

IoT FND では、IoT FND データベースの完全なホット バックアップを実行できます。ホット バックアップでは、IoT FND および IoT FND データベースはバックアップ中も動作します。

(注) バックアップ先のディレクトリは、oracle ユーザによる書き込みが可能で、IoT FND データ用に十分な領域が必要です。

IoT FND ソフトウェアのバックアップ ファイルを作成するには、次の手順を実行します。

1. IoT FND データベース サーバで、CLI ウィンドウを開きます。
2. ユーザ oracle に切り替えます。

   su - oracle

3. ディレクトリを IoT FND バックアップ スクリプト（backupCgmsDb.sh）の場所に変更します。

   cd /home/oracle/app/oracle/cgms/scripts

4. バックアップ スクリプトを実行し、バックアップ先フォルダを指定します。たとえば、/home/oracle/bkp フォルダにバックアップ データを保存するには、次のコマンドを入力します。

```
./backupCgmsDb.sh full /home/oracle/bkp
08-03-2012 15:54:10 PST: INFO: ========== CGMS Database Backup Started ==========
08-03-2012 15:54:10 PST: INFO: Log file: /tmp/cgms_backup_restore.log
Are you sure you want to backup CG-NMS database (y/n)? y
```

5. バックアップ プロセスを開始するには、「y」を入力します。

IoT FND の完全バックアップのスケジュール設定

IoT FND の完全バックアップを毎日 1:00 AM（デフォルト設定）に実行するようにスケジュール設定するには、次の手順を実行します。

(注) バックアップ先のディレクトリは、oracle ユーザによる書き込みが可能で、IoT FND データ用に十分な領域が必要です。

1. IoT FND データベース サーバで、CLI ウィンドウを開きます。
2. ユーザ *oracle* に切り替えます。

   ```
   su - oracle
   ```

3. ディレクトリを IoT FND バックアップ スクリプト（backupCgmsDb.sh）の場所に変更します。

   ```
   cd /home/oracle/app/oracle/cgms/scripts
   ```

4. バックアップ スクリプトを実行し、バックアップ先フォルダを指定します。

バックアップのスケジュール間隔を変更するには、installCgmsBackupJob.sh スクリプトを編集してから実行します。たとえば、バックアップ データを /home/oracle/bkp に保存するには、次のコマンドを入力します。

```
./installCgmsBackupJob.sh /home/oracle/bkp
```

バックアップ ジョブを削除するには、次のコマンドを入力します。

```
cd /home/oracle/app/oracle/cgms/scripts
./deinstallCgmsBackupJob.sh
```

IoT FND データベースの増分バックアップ

増分バックアップは、前回指定したバックアップから変更されたデータ ファイル ブロックのみをバックアップします。IoT FND は 2 つのレベルの増分バックアップと、毎時のログ バックアップをサポートしています。

- incr0：増分バックアップ後のベース バックアップ。これは完全バックアップに似ています。大規模展開（数百万のメッシュ エンドポイント、数千のルータ（CGR1000 や IR800 など））の場合。週に 2 回 incr0 バックアップを実行します。
- incr1：前回の増分バックアップ以降に変更されたすべてのブロックの差分バックアップ。大規模展開（数百万のメッシュ エンドポイントと数千のルータ）の場合、1 日に 1 回 incr1 バックアップを実行します。

(注) incr1 差分バックアップのベースを確立するため、incr0 バックアップを incr1 バックアップの前に実行する必要があります。

- 毎時のアーカイブ ログのバックアップ：Oracle データベースは、アーカイブ ログを使用してデータベースへのすべての変更を記録します。これらのファイルは徐々に増え、大量のディスク領域を消費する可能性があります。1 時間ごとに backup_archive_log.sh スクリプトを実行するようにスケジュール設定します。このスクリプトはデータベースのアーカイブ（.arc）ログ ファイルをバックアップし、それらを別のサーバに保存し、元のアーカイブ ログ ファイルを削除してデータベース サーバの領域を解放します。

  ヒント：IoT FND データベースに多くの変更を及ぼす重大な操作（百万のメッシュ エンドポイントをインポートしたり、メッシュ エンドポイントにファームウェア イメージをアップロードするなど）を実行する前に、incr0 バックアップを実行します。操作が完了したら、別の incr0 バックアップを実行してから、スケジュール設定された増分バックアップを再開します。

増分バックアップの実行

(注)バックアップ先のディレクトリは、oracle ユーザによる書き込みが可能で、IoT FND データ用に十分な領域が必要です。

増分バックアップを実行するには、次の手順を実行します。

1. IoT FND データベース サーバで、CLI ウィンドウを開きます。
2. ユーザ *oracle* に切り替え、IoT FND バックアップ スクリプトの場所にディレクトリを変更します。

```
su - oracle
cd /home/oracle/app/oracle/cgms/scripts
```

3. バックアップ スクリプトを実行し、増分バックアップのレベルとバックアップ データを保存する保存先フォルダ(/home/oracle/bkp など)を指定します。たとえば、/home/oracle/bkp への incr0 バックアップを実行するには、次のコマンドを入力します。

```
./backupCgmsDb.sh incr0 /home/oracle/bkp
```

incr1 バックアップを実行するには、次のコマンドを入力します。

```
./backupCgmsDb.sh incr1 /home/oracle/bkp
```

IoT FND バックアップの復元

cgms-oracle.rpm パッケージで提供されるスクリプトを使用して、データベースのバックアップと復元を実行します。提供されたスクリプトを使用している場合、バックアップと復元は Oracle データベースの同じバージョンで実行された場合にのみ機能します。

(注)提供されたスクリプトを使用している場合、Oracle バージョン 11.2.0.1 からのバックアップは、v11.2.0.1 でのみ復元できます。Oracle の異なるバージョン間でのバックアップは機能しません。たとえば、11.2.0.1 で作成されたバックアップは、提供されたスクリプトを使用して 11.2.0.3 で復元することはできません。データベースを 11.2.0.1 から 11.2.0.3 にアップグレードする必要がある場合は、Oracle のアップグレード手順に従います。Oracle のアップグレード マニュアルおよび Web サイトを参照してください。

IoT FND は同じホストまたは別のホストでの IoT FND バックアップの復元をサポートしています。IoT FND バックアップを別のホストに復元する場合は、そのホストで Oracle データベース ソフトウェアの同じかそれ以降のバージョンが実行され、復元先のホストで IoT FND データベースが setupCgmsDb.sh スクリプトを使用して作成されていることを確認します。

(注)IoT FND ではクロスプラットフォーム バックアップはサポートしていません。

IoT FND バックアップを復元するには、次の手順を実行します。

1. IoT FND を停止します。

```
service cgms stop
```

2. ユーザ oracle に切り替え、スクリプトの場所にディレクトリを変更し、Oracle を停止します。

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./stopOracle.sh
```

3. IoT FND データベースを復元するには、次のコマンドを実行します。

```
./restoreCgmsDb.sh full-backup-file
```

ヒント:完全バックアップからの復元の実行には時間がかかる場合があります。大規模展開では、増分バックアップからのデータベースを復元することを推奨します。

増分バックアップから IoT FND データベースを復元するには、次のコマンドを実行して、前回の増分バックアップ ファイルへのパスを指定します。

```
su -oracle
cd /home/oracle/app/oracle/cgms/scripts
./restoreCgmsDb.sh last-incr1-backup-file
```

復元スクリプトで次のエラーが表示される場合があります。

```
06-08-2012 13:12:56 PDT: INFO: Import completed successfully
06-08-2012 13:12:56 PDT: INFO: Shared memory file system. Required (1K-blocks): 6084456,
Available (1K-blocks): 4083180
06-08-2012 13:12:56 PDT: ERROR: Insufficient shared memory file system. Increase your
shared memory file system before restoring this database.
06-08-2012 13:12:56 PDT: ERROR: ========== CGMS Database Restore Failed ==========
06-08-2012 13:12:56 PDT: ERROR: Check log file for more information.
```

これらのエラーを避けるには、共有メモリ ファイル システムのサイズを増やします。

```
###### as "root" user
###### Following command allocates 6G to shm. Adjust size as needed.
# umount tmpfs
# mount -t tmpfs tmpfs -o size=6G /dev/shm

###### Edit /etc/fstab and replace defaults as shown below
tmpfs                   /dev/shm                tmpfs   size=6G        0 0
```

4. Oracle を起動します。

```
./startOracle.sh
```

5. ディレクトリを /opt/cgms に変更し、db-migrate スクリプトを実行します。

```
$ cd /opt/cgms
$ bin/db-migrate
```

IoT FND データベースを復元すると、復元スクリプトによってデータベースはデータベースが使用していた IoT FND のバージョンに復元されます。古いデータベースを IoT FND の新しいバージョンに復元するとエラーが返されます。移行スクリプトを実行して、データベースが IoT FND の現在のバージョンで実行されていることを確認します。

6. IoT FND を起動します。

```
service cgms start
```

ディザスタ リカバリについては、クリーンな復元を実行します。スクリプトは最初に現在の IoT FND データベースを削除します。

```
$ su -oracle
$ cd /home/oracle/app/oracle/cgms/scripts
$ ./deleteCgmsDb.sh
INFO: ======== CGMS Database Deletion Started - 2011-10-16-07-24-09 ==========
INFO: Log file: /tmp/cgmsdb_setup.log
INFO: Deleting database. This may take a while. Please be patient ...
INFO: Delete database completed successfully
INFO: ========== CGMS Database Deletion Completed Successfully - 2011-10-16-07-25-01 ==========
```

クリーンな復元が必要ない場合は、Oracle ツールを使用してデータベースを復元します。

ESX 5.x での IoT FND/Oracle/TPS 仮想マシンの展開

VMware vSphere Client を使用して、OVA ファイルを ESXi 5.x. にインポートします。

はじめる前に

- ESXi 5.x サーバ用の VMware vSphere Client をインストールします。
- VMware ESXi 5.x のクレデンシャルを見つけて ESXi 5.x で仮想マシンを作成します。
- VMware サーバ マシンの要件を満たしていることを確認します。

  以下は小規模展開の VM CPU とメモリの要件です。

  NMS OVA

  - 16 GB のメモリ
  - 1 つのコアと 4 つの仮想ソケット
  - 150 GB の仮想ストレージ

  Oracle OVA

  - 24 GB のメモリ
  - 2 つの仮想ソケットとソケットあたり 2 つのコア
  - 300 GB の仮想ストレージ

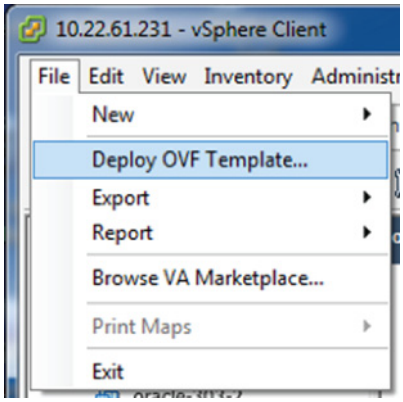
  TPS OVA

  - 4 GB のメモリ
  - 1 つの仮想ソケットと 1 つのコア
  - 50 GB の仮想ストレージ

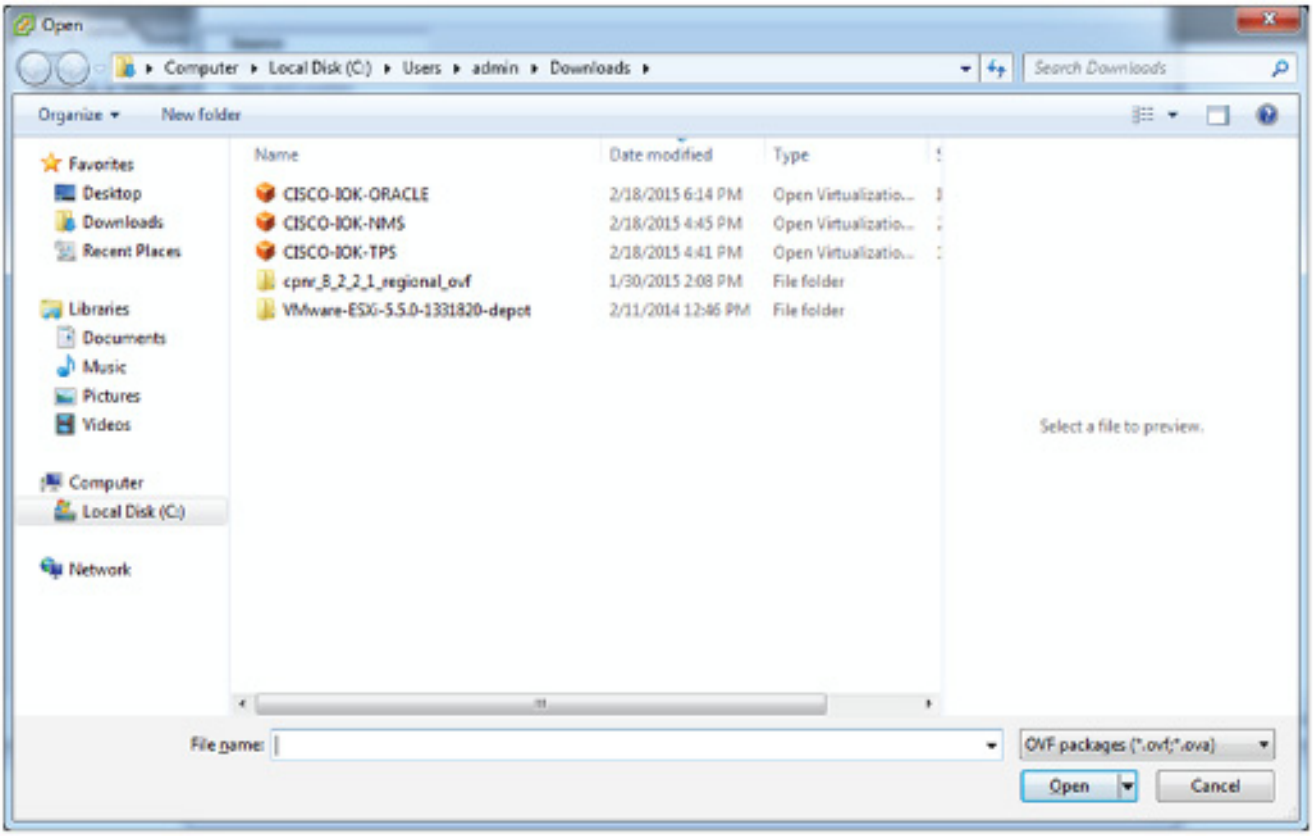
手順の詳細

VMware vSphere Client 5.x を使用して、IoT FND、Oracle、および TPS 仮想アプライアンスを ESXi 5.x にインポートするには、次の手順を実行します。

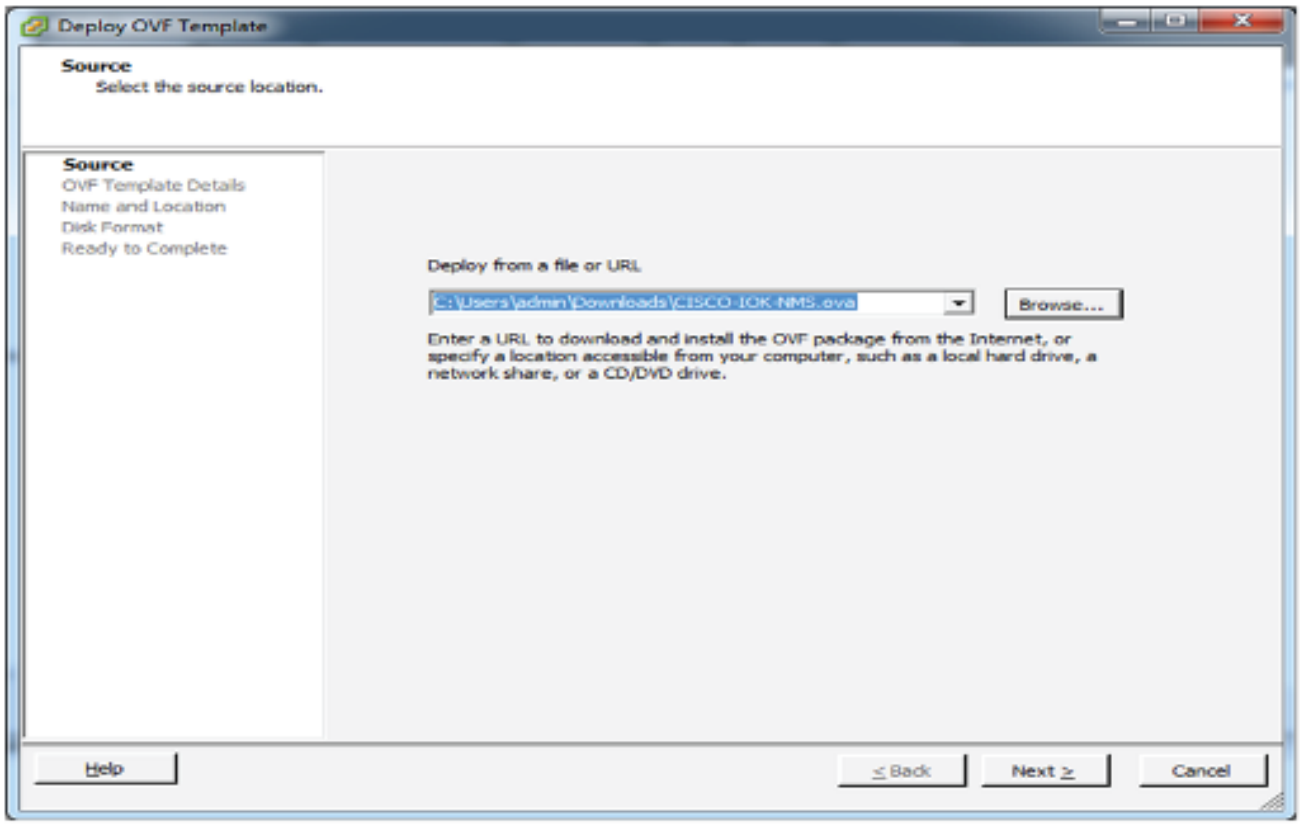
1. VMware vSphere Client にログインします。
2. [File] > [Deploy OVF Template...] の順に選択します。



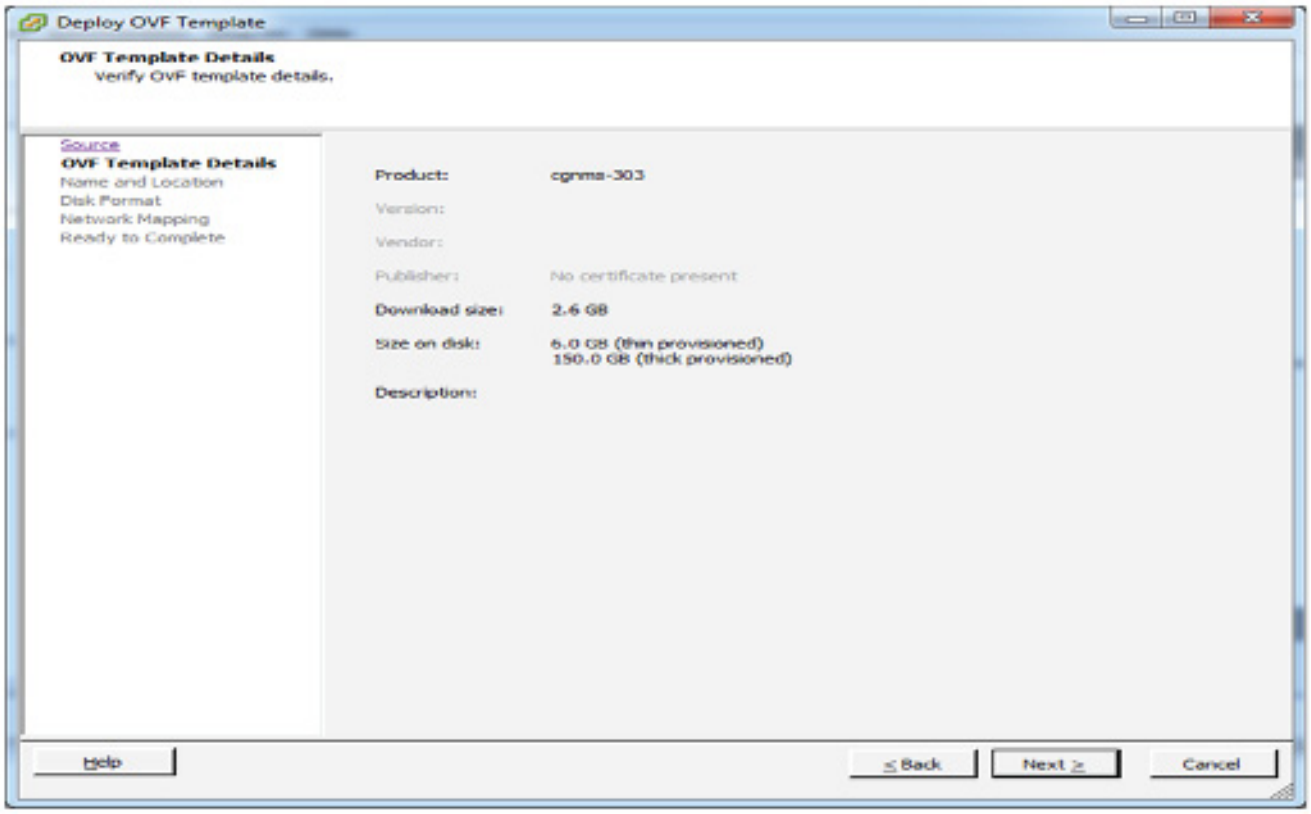
3. CISCO-IOK-NMS.ova ファイルを参照し、[Open] をクリックします。



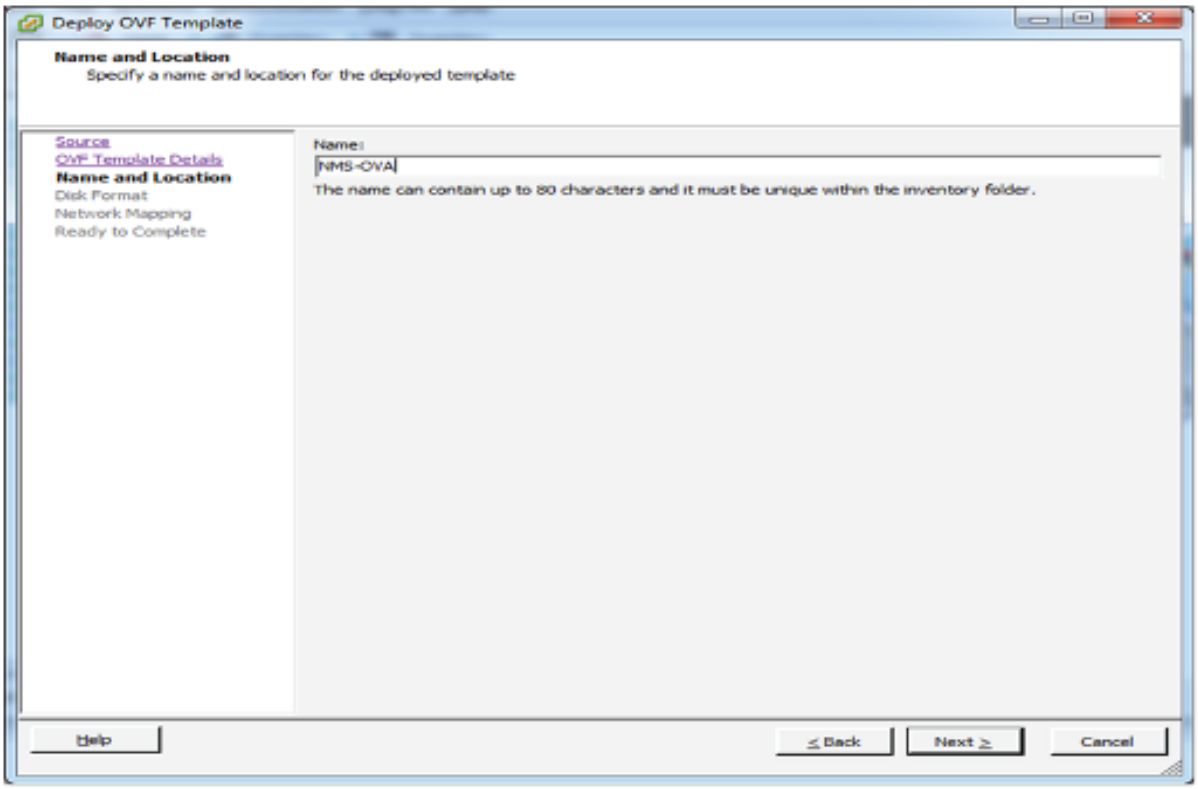
4. [Source] ウィンドウに正しい OVA ファイルが表示されていることを確認し、[Next] をクリックします。



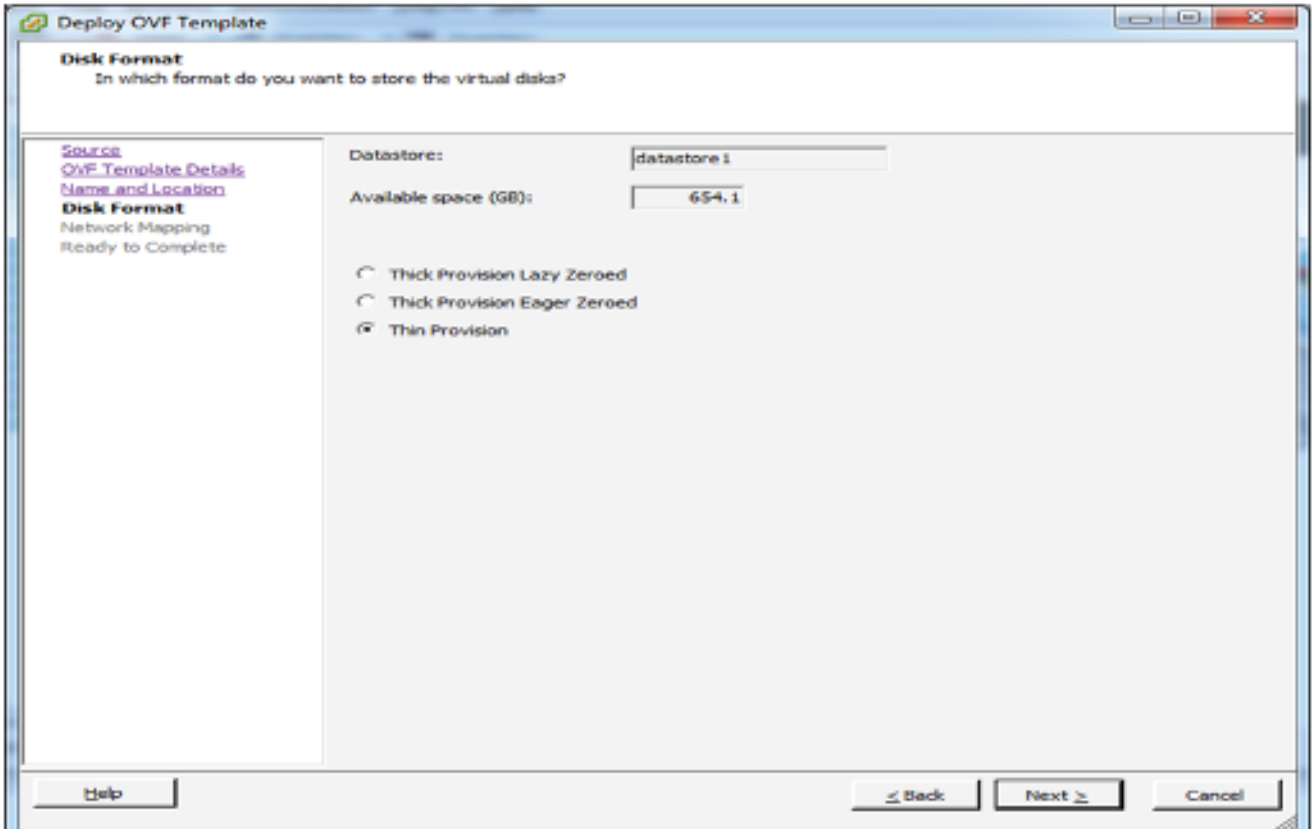
5. [OVF Template Details] ウィンドウで、情報を確認して [Next] をクリックします。



6. [Name and Location] ウィンドウで、この仮想アプライアンスの名前を入力し、[Next] をクリックします。

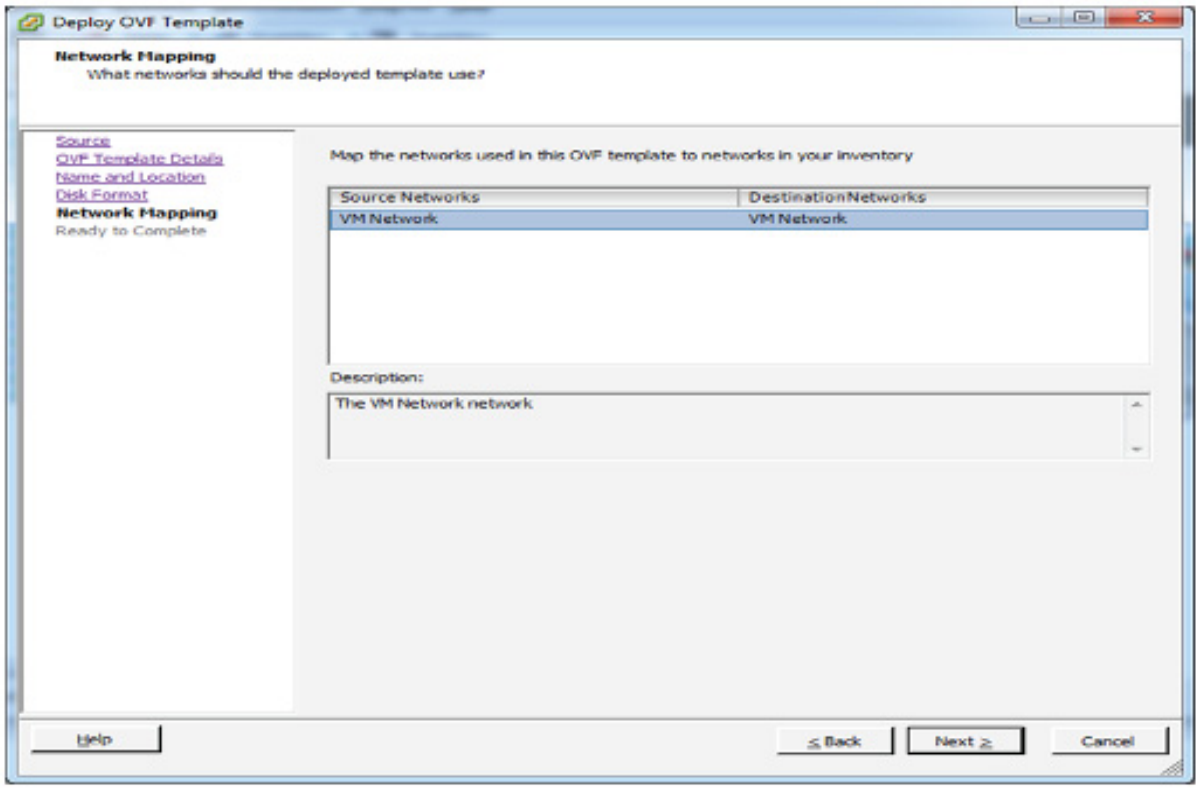


7. [Disk Format] ウィンドウで、[Thin Provision] を選択し、[Next] をクリックします。

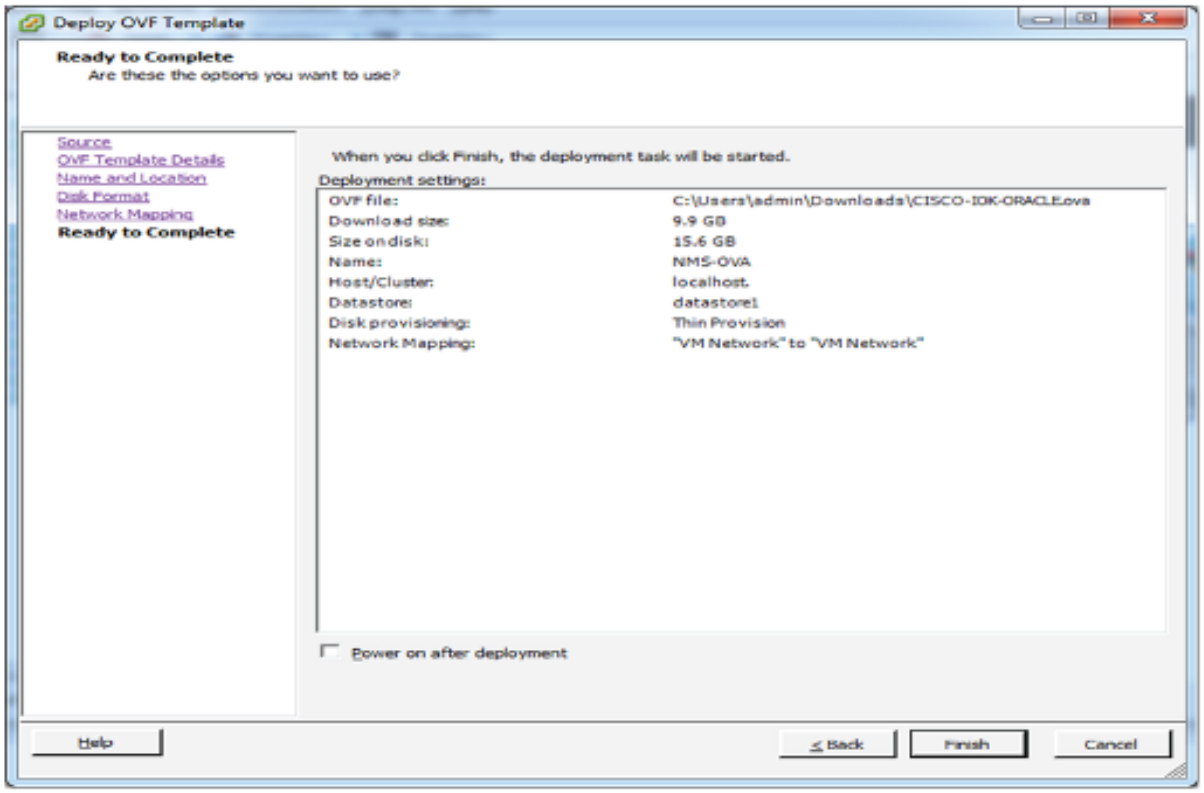


シン プロビジョニングでは、VM ディスクを必要に応じて大きくすることができます。

8. [Network Mapping] ウィンドウで、[Source Network] を選択し、[Next] をクリックします。



9. [Ready to Complete] ウィンドウで、展開設定を確認し、[Finish] をクリックします。

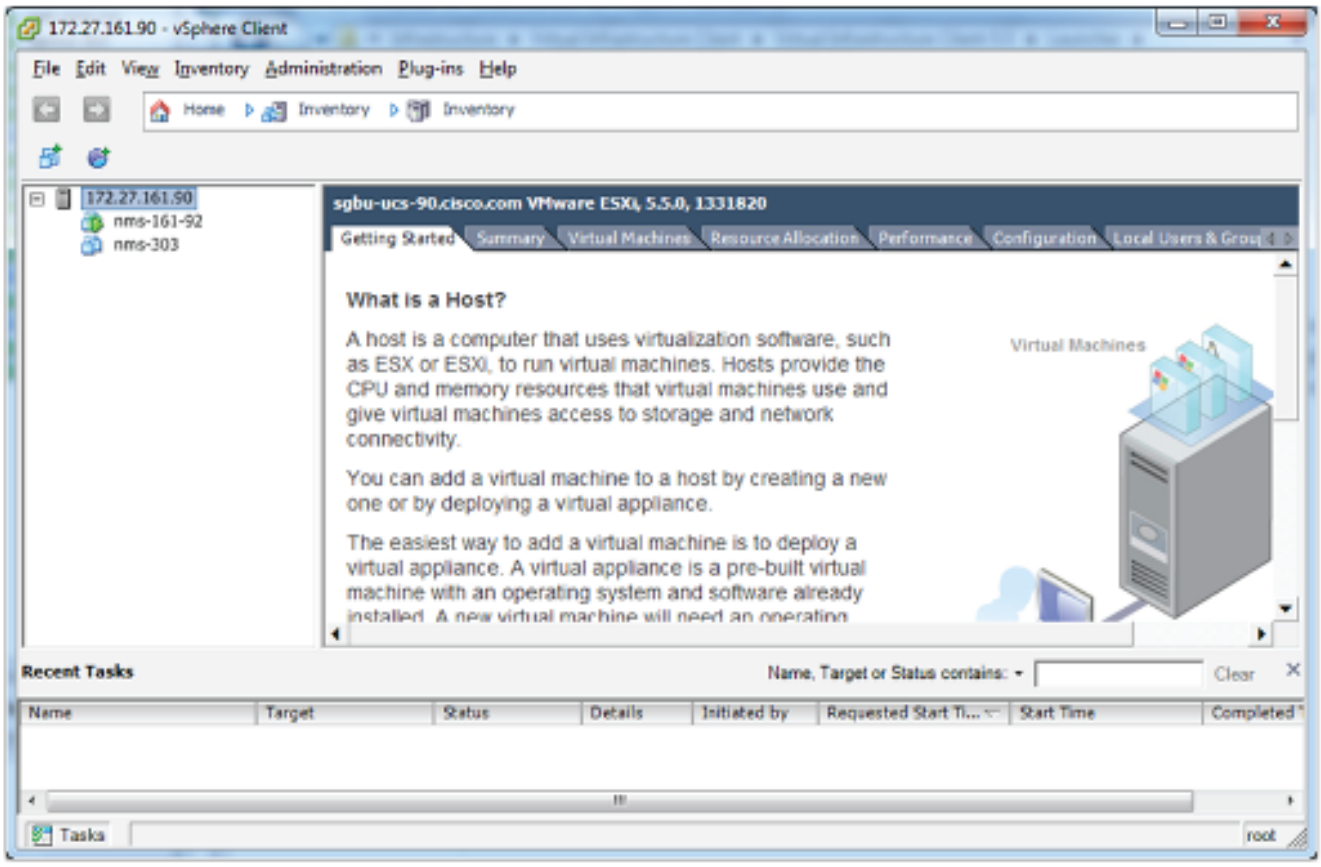


VM は現在、データストアにあります。

10. vSphere Client にログインしている間、上記の手順を繰り返して CISCO-IOK-ORACLE ファイルと CISCO-IOK-TPS OVA ファイルを展開します。

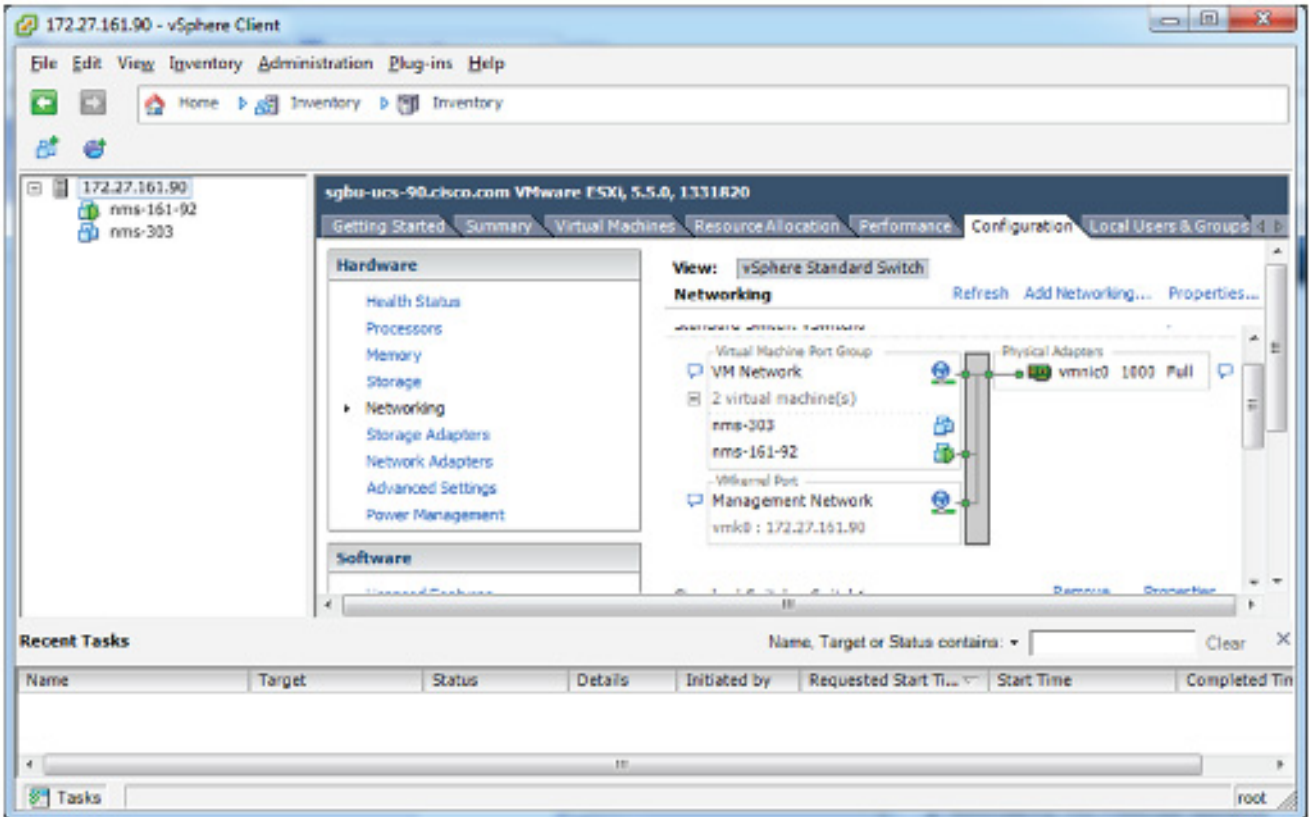
11. すべての新しい OVA アプライアンスを VM ネットワークに追加します。

次の vSphere Client のホーム画面には、nms アプライアンスが示されています。



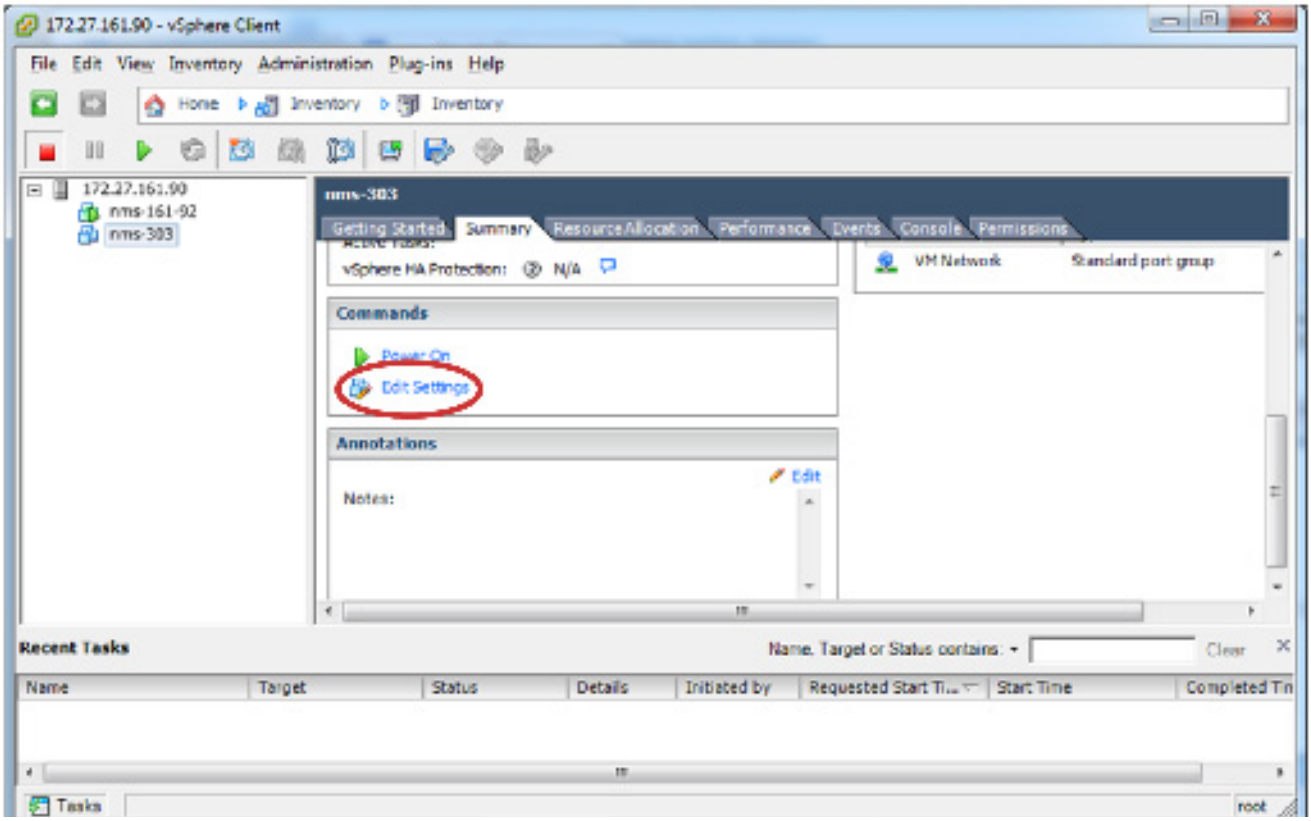
12. [Configuration] タブを選択して、この選択した ESXi サーバのネットワーク プロパティを表示します。

    ネットワーク プロパティは、サーバの要件によって異なります。以下は、管理ネットワーク接続用の vSphere Standard Network Switch と VM Network ラベルを示しています。



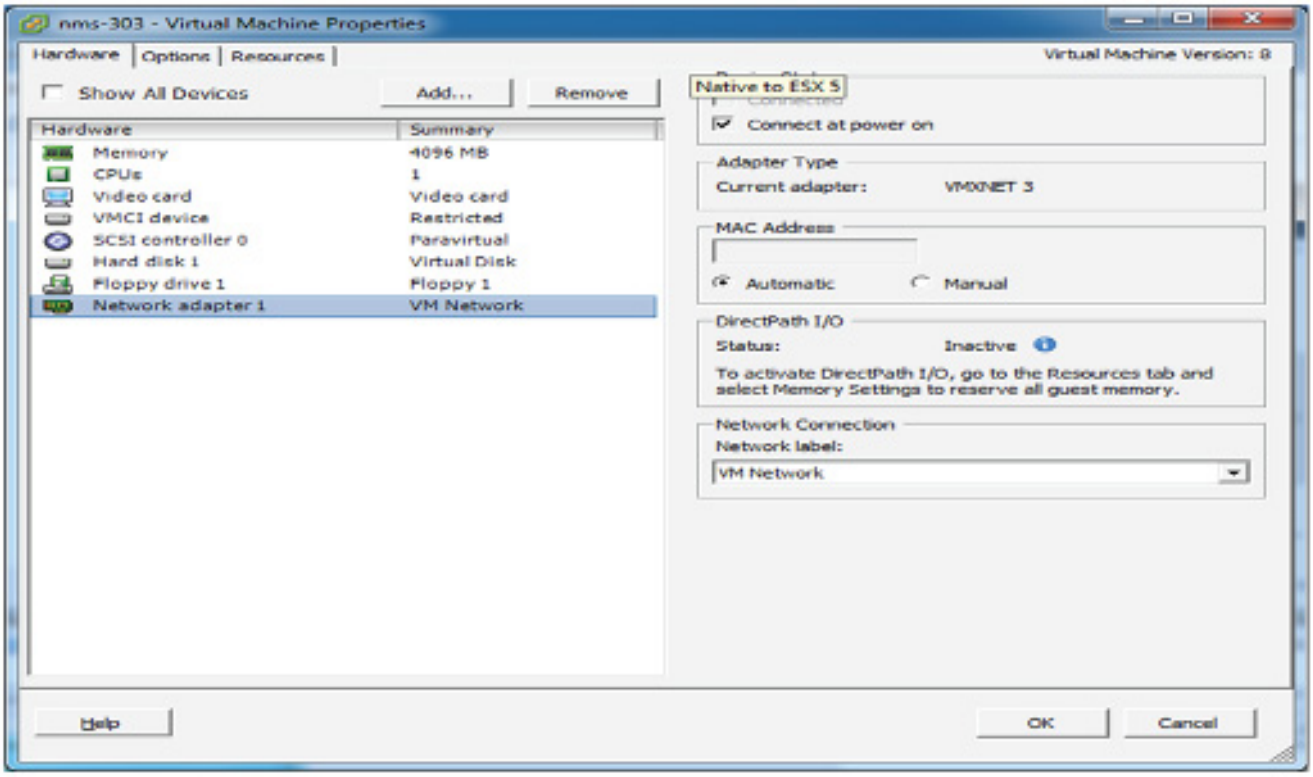
13. 左側のパネルで、[nms 303] アプライアンスを選択し、[Summary] タブを選択します。

14. [Command] セクションまでスクロールし、[Edit Settings] をクリックします。



[Virtual Machine Properties] ページが表示されます。

15. [Hardware] タブの [Network Connection] セクションで、ネットワーク アダプタを選択し、[Network label] ドロップダウン メニューから [VM Network] ラベル（または作成したネットワーク ラベル）を選択します。



16. [OK] をクリックします。

    ネットワーク ラベルはユーザ設定に保存されます。

17. nms インスタンスを右クリックして、コンテキスト メニューから [Open Console] を選択します。

18. 緑色の [Play] ボタンをクリックします。

    Linux VM を開始して起動します。

    Linux のブート メッセージが表示され、ログイン画面が表示されます。

    VM コンソールを終了するには、Ctrl キーを押した状態で Alt キーを押します。

19. 画面の中央をクリックしてログインし、IP アドレスの設定を調整します。

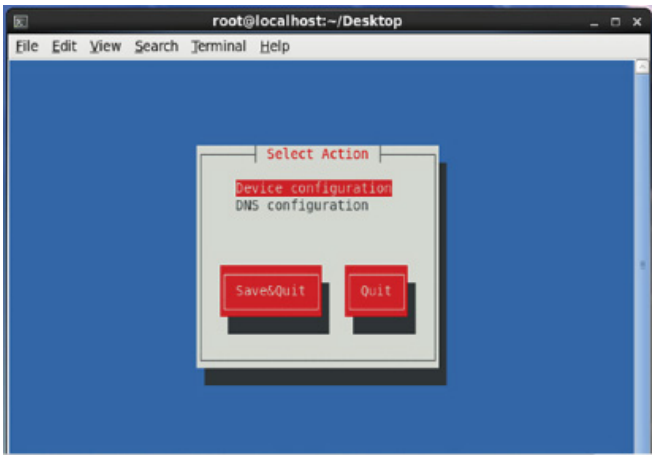
    これは他の RedHat 6.4 Enterprise System と同じです。

20. Oracle と TPS アプライアンスに対して、ステップ 12 ～ 19 を繰り返します。

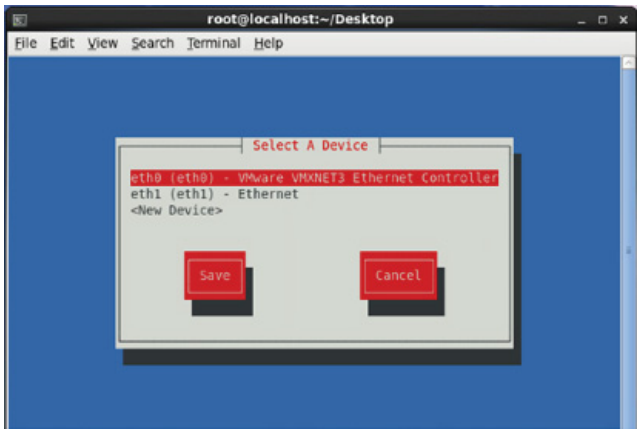
VM 内でのネットワーク構成ファイルの編集

1. デスクトップを右クリックし、[Open in Terminal] をクリックします。
2. コマンド プロンプトで、「**system-config-network**」を入力します。

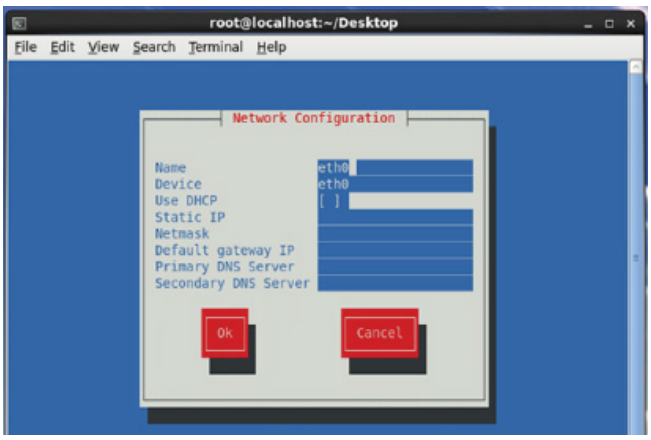
   [Device configuration] ウィンドウが表示されます。



3. [Select Action] ウィンドウで、[Device configuration] が選択されていることを確認し、**Enter** キーを押します。
4. [Select A Device] ウィンドウで、方向キーを使用してインターフェイスを選択し、Enter キーを押します。



次の例では、[Network Configuration] ウィンドウで [DHCP] が選択されています。



5. ネットワーク管理者によって割り当てられたネットワーク設定を入力します。
6. [OK] をクリックします。
7. アプライアンスごとにステップ 1 ～ 5 を繰り返して IP アドレスを割り当てます。

証明書の生成およびインストール

この項では、デジタル証明書を生成してインストールする方法について説明します。次の項目を取り上げます。

証明書について

ここでは、証明書について説明します。

証明書の役割

Cisco 1000 シリーズ Connected Grid ルータ（CGR 1000 または単に CGR）と Cisco Connected IoT Field Network Director（IoT FND）との間のすべての通信は、両方向とも相互認証により認証される必要があります。相互認証が行われる前に、Cisco IoT FND および CGR は、それぞれ同じ認証局（CA）により署名される必要があります。ルート CA またはや下位 CA（subCA）のいずれかを採用できます。

CGR の証明書の生成について詳しくは、『Certificate Enrollment Guide for the Cisco 1000 Series Connected Grid Routers』を参照してください。

IoT FND の証明書の生成には、IoT FND TPS プロキシ（tpsproxy）の証明書の生成と読み込みも関係しています。証明書を生成したら、それらを TPS プロキシとキーストアとして知られている IoT FND 上のストレージ場所にインポートします。

キーストア

Keystore により、特定のシステム（IoT FND や TPS プロキシなど）の詳細が提供され、それには次の項目が含まれています。

- そのシステムの証明書（IoT FND 証明書または TPS プロキシ証明書など）
- システムの秘密キー
- 証明書チェーン（CA または subCA へのパス）

IoT FND キーおよび証明書は、IoT FND サーバ上の /opt/cgms/server/cgms/conf/ ディレクトリ内の cgms_keystore ファイルに格納されます。

証明書の生成およびエクスポート

(注) IoT FND 証明書は、データベースのデータを暗号化します。**この証明書は決して消失させないでください。**この証明書を消失すると、一部のデータベース データが復号できなくなります。

証明書を生成してエクスポートするには、次の手順を実行します。

- IoT FND および TPS プロキシの証明書テンプレートの設定IoT FND
- 証明書テンプレートの有効化
- IoT FND および IoT FND TPS プロキシの証明書の生成
- コマンド認可サポート
- HSM のカスタム CA の設定
- SSM のカスタム CA の設定
- CA 証明書のエクスポート

IoT FND および TPS プロキシの証明書テンプレートの設定IoT FND

CA（または subCA）上で、IoT FND と TPS プロキシの証明書を生成する証明書テンプレートを作成する必要があります。

証明書テンプレートを作成するには、次の手順を実行します。

1. Windows Server 2008 R2 Enterprise エディションを稼働するシステム上で、認証局アプリケーションを開きます。

認証局アプリケーションは、上記の Windows Server バージョン上では標準です。

2. メニューを展開して、証明書テンプレート フォルダを表示します。
3. [Certificate Templates] を右クリックし、コンテキスト メニューから [Manage] を選択します。
4. 右ペインで [Computer] を右クリックし、コンテキスト メニューから [Duplicate Template] を選択し、[NMS] を入力します。
5. [Duplicate Template] ペインで、[Windows Server 2008 Enterprise] を選択します。
6. [OK] をクリックします。
7. [NMS Properties] > [General] タブをクリックし、次の手順を実行します。
   a. [Template display name] と [Template name] フィールドに、**NMS** を入力します。
   b. 適切な [Validity] を入力します。これは証明書の存続期間を定義します。
   c. [Publish certificate in Active Directory] チェックボックスをオンにします。
   d. [OK] をクリックします。
8. [NMS Properties] > [Extensions] タブをクリックし、次の手順を実行します。
   a. [Extensions] ペインで、[Application Policies] を選択します。
   b. [Application Policies] ペインで、クライアント認証とサーバ認証が下部のペインに表示されていることを確認します。
   c. 上部の [Extensions] ペインで [Key Usage] を選択し、[Edit] をクリックします。
   d. [Edit Key Usage Extension] ペインで、[Make this extension critical] チェックボックスをクリアします。
   e. [OK] をクリックします。

9. [NMS Properties] > [Request Handling] タブをクリックし、次の手順を実行します。
   a. [Purpose] ドロップダウン メニューから [Signature and encryption] を選択します。
   b. [Allow private key to be exported] チェックボックスをオンにします。
   c. [OK] をクリックします。
10. [NMS Properties] > [Security] タブをクリックし、次の手順を実行します。
    a. [Group] または [User Names] ペインで [Administrator] を選択します。
    b. リストされている各グループまたはユーザ名項目（認証されたユーザ、管理者、ドメイン管理者、エンタープライズ管理者など）に対して、すべての権限（フル コントロール、読み取り、書き込み、登録、自動登録）の、[Allow] チェックボックスをオンにします。
    c. [OK] をクリックします。
11. [NMS Properties] > [Cryptography] タブで、次のデフォルト設定を保持します。

- Algorithm name：RSA
- Minimum key site：2048
- Cryptographic provider：要求には、対象コンピュータ上の任意のプロバイダを使用できます
- Request hash：SHA256

12. [OK] をクリックします。
13. [NMS Properties] > [Subject Name] タブで、次のデフォルト設定を保持します。

- [Supply in the request radio button] のラジオボタンをオン
- [Use subject information from existing certificates for autoenrollment renewal requests] のチェックボックスをオン

14. [OK] をクリックします。

(注) 残りのタブ（[Superseded Templates]、[Server]、および [Issuance Requirements]）は、デフォルトの設定のままにしておきます。

証明書テンプレートの有効化

証明書を作成するには、まず証明書テンプレートを有効にする必要があります。

証明書テンプレートを有効にするには、次の手順を実行します。

1. 証明書テンプレートを設定します（証明書の生成およびエクスポートを参照）。
2. Windows Server 上で認証局アプリケーションを開きます。
3. メニューを展開して、証明書テンプレート フォルダを表示します。
4. [Certificate Templates] を右クリックし、[New] > [Certificate Template to Issue] をコンテキスト メニューから選択します。
5. [Enable Certificate Templates] ウィンドウで、[NMS] テンプレートを強調表示します。
6. [OK] をクリックします。

IoT FND および IoT FND TPS プロキシの証明書の生成

前に作成した設定テンプレートを使用して、IoT FND と TPS プロキシの証明書を生成するための同じ手順を実行します。

この項の手順を 2 回実行します。1 回は IoT FND の証明書を生成するため、もう 1 回は TPS プロキシの証明書を生成するためです。

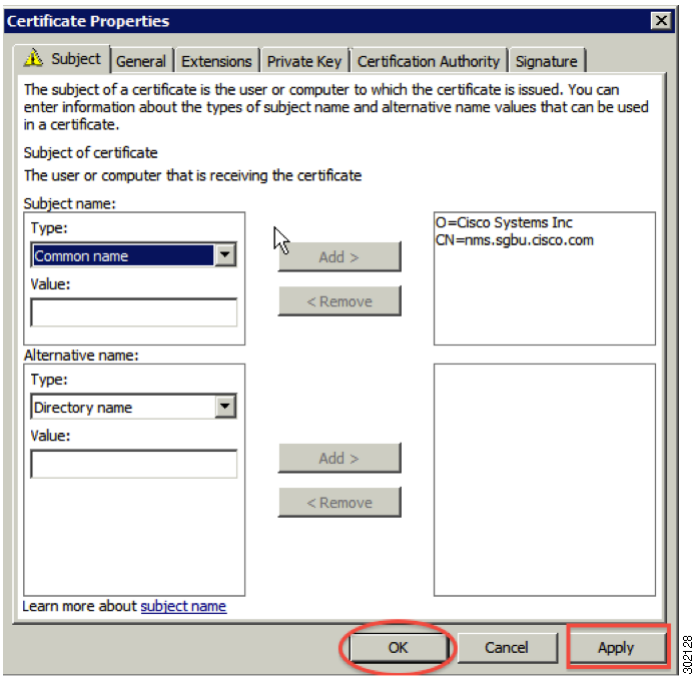
ヒント：9.b で、入力する値は、IoT FND または TPS プロキシの証明書を作成するかどうかによって異なります。

これら 2 つの証明書を作成したら、IoT FND 証明書を IoT FND アプリケーション サーバに安全に転送したり、TPS プロキシ証明書を TPS プロキシ サーバに安全にコピーしたりできます。

証明書を生成するには、次の手順に従います。

1. 証明書テンプレートを設定します（証明書の生成およびエクスポートを参照）。
2. 証明書テンプレートを有効にします（証明書テンプレートの有効化を参照）。
3. Windows Server 2008 を実行するサーバから、[Start] > [Run] を選択し、**mmc** を入力して MMC コンソールを開きます。
4. [Console 1] ウィンドウで、[Certificates] > [Personal] フォルダを展開します。
5. [Certificates] を右クリックして、コンテキスト メニューから [All Tasks] > [Request New Certificate] を選択します。
6. [Before You Begin] ウィンドウで、[Next] をクリックします。
7. [Select Certificate Enrollment Policy] ウィンドウで、[Active Directory Enrollment Policy] を選択します。[Next] をクリックします。
8. [Request Certificates] ウィンドウで、次の手順を実行します。
   a. [NMS] チェックボックスをオンにします。
   b. [More information...] リンクをクリックします。
9. [Certificate Properties] ウィンドウで、[Subject] タブをクリックし、次の手順を実行します。
   a. [Type] ドロップダウン メニューから、[Common name (CN)] を選択します。
   b. [Value] フィールドに、次のようにして完全修飾ドメイン名（FQDN）を追加します。
      - IoT FND 証明書の場合、導入システムの IoT FND サーバの FQDN を入力します（例：CN=nms.sgbu.cisco.com）。
      - TPS プロキシ証明書の場合、導入システムの TPS プロキシの FQDN を入力します（例：CN= tps.sgbu.cisco.com）。
   c. [Add] をクリックすると、右ペインに共通名が表示されます。
   d. [Type] ドロップダウン メニューから、[Organization (O)] を選択します。
   e. [Value] フィールドに、IoT FND または TPS プロキシの会社名または設定を追加します。
   f. [Add] をクリックすると、組織が右ペインに表示されます。

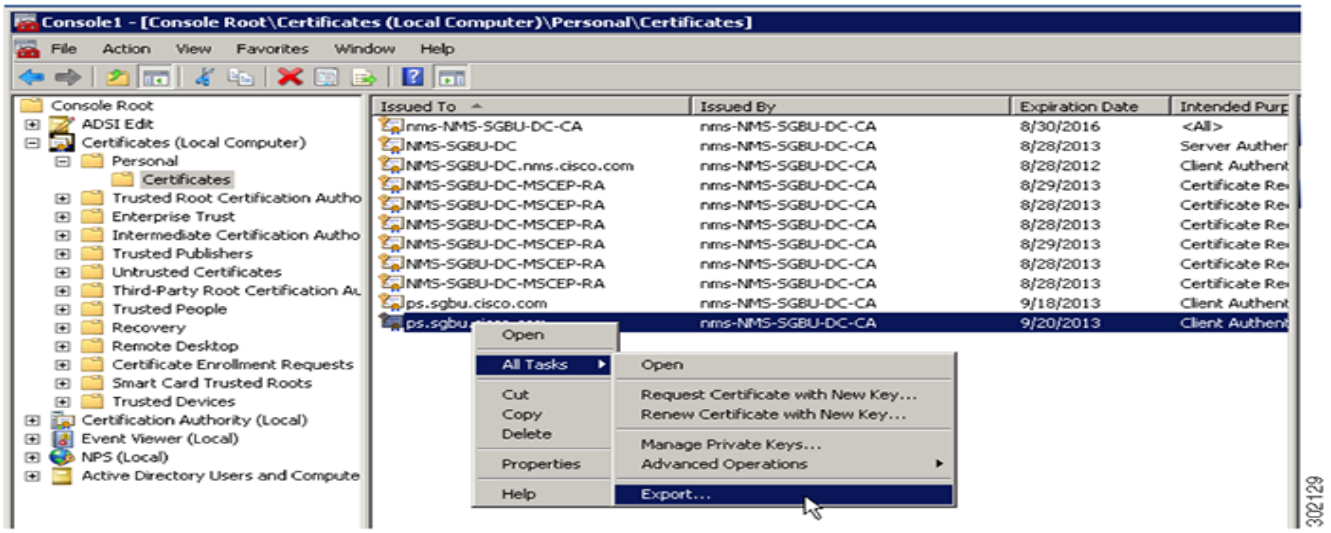
図 1　IoT FND の共通名および組織の定義



10. [Apply] をクリックします。[OK] をクリックします。
11. [Certificate Enrollment] ウィンドウで、[NMS] チェックボックスをオンにし、[Enroll] をクリックします。
12. 登録が完了したら、[Finish] をクリックします。
13. MMC コンソール（コンソール 1）で、[Certificates] を展開します。
14. [Personal] > [Certificates] を選択します。
15. [Issued To] ペインで、新しい証明書を右クリックして、コンテキスト メニューから [All Tasks] > [Export] を選択します。

    [Export Wizard] ウィンドウが表示されます。

図 2　サポートされる証明書を表示する [Issued To] ペイン



16. [Export Wizard] を開始します。
17. [Export Private Key] ウィンドウで、[Yes, export the private key] ラジオ ボタンを選択します。[Next] をクリックします。
18. [Export File Format] ウィンドウで、次の手順を実行します。
    a. [Personal Information Exchange] ラジオ ボタンをクリックします。
    b. [Include all certificates in the certification path if possible] チェックボックスをオンにします。

    このオプションには、証明書内のすべての証明書チェーンが含まれています。

    c. [Next] をクリックします。
19. パスワード ウィンドウで、**keystore** と入力し、確認のために再入力します。

    このパスワードは、IoT FND と TPS プロキシがこのファイルを読み取るために使用するデフォルトのパスワードです。
20. [Next] をクリックします。
21. [File to Export] ウィンドウに、ファイル名（*nms_cert* または *tps_cert* など）を入力し、[Next] をクリックします。
22. [Completing the Certificate Export Wizard] で、[Finish] をクリックします。

    *.pfx 拡張子を持つファイルは、デスクトップに自動的に保存されます。PFX とは、Personal Information Exchange 形式のことであり、PKCS_#12 形式とも呼ばれます。PFX は、コンピュータ間で証明書と秘密キーを転送（エクスポート）可能にするための、業界標準形式です。
23. 2 つの証明書ファイル（*nms_cert.pfx* および *tps_cert.pfx*）は、Windows デスクトップから IoT FND（*nms_cert.pfx*）および TPS プロキシ（*tps_cert.pfx*）にそれぞれ安全に転送されます。

    (注)セキュリティを向上させるには、転送が正常に実行されたら、*.pfx ファイルを Windows デスクトップから削除して、ごみ箱を空にします。

コマンド認可サポート

Cisco Connected Grid ルータ（CGR）は、3G、4G、または WiMAX などの WAN バックホール接続を介して IoT FND により管理されます。CG-OS CGR の場合、IoT FND に対する管理権限を有効にするには、OID 値を定義します。

このポリシーの OID は、1.3.6.1.4.1.9.21.3.3.1 です。IoT FND が管理権限で管理コマンドを CGR に対して発行することが許可されている場合に、この要素は表示されます。IoT FND は TLS などのセキュア セッションを介して CGR と通信し、CGR はそれらのコマンドを、ネットワーク管理者が発行したかのように実行できます。

ここでは、次の内容について説明します。

- NMS/TPS 証明書を使用したコマンド認可の有効化
- CA 証明書への OID 値の追加
- 証明書の更新

NMS/TPS 証明書を使用したコマンド認可の有効化

ルータのコマンド認可（CA）機能を承認するための手順に従い、IoT FND への登録を実行します。

1. 新しい NMS/TPS 証明書を生成するか（IoT FND および IoT FND TPS プロキシの証明書の生成を参照）、既存の NMS/TPS 証明書を更新します（証明書の更新を参照）。
2. OID 値を CA 証明書に追加します（CA 証明書への OID 値の追加を参照）。
3. NMS/TPS 証明書の新しい .pfx ファイルを生成します（IoT FND および IoT FND TPS プロキシの証明書の生成を参照）。
4. IoT FND を停止します（IoT FND の停止を参照）。
5. 既存の cgms_keystore ファイルの名前を変更します（たとえば、cgms_keystore_no_oid）。
6. .pfx ファイルを IoT FND にエクスポートし、新しい cgms_keystore ファイルを作成します（キーツールを使用した cgms_keystore ファイルの作成を参照）。
7. 新しい証明書をインストールします（証明書のインストールを参照）。
8. 新しい cgms_keystore ファイルを IoT FND に追加します（cgms_keystore ファイルの IoT FND へのコピーを参照）。
9. IoT FND を開始します（IoT FND の起動を参照）。
10. ルータを IoT FND に登録します。

CA 証明書への OID 値の追加

IoT FND がルータ上でのコマンド認可に管理者役割を使用できるようにするには、OID 値を CA 証明書に追加する必要があります。

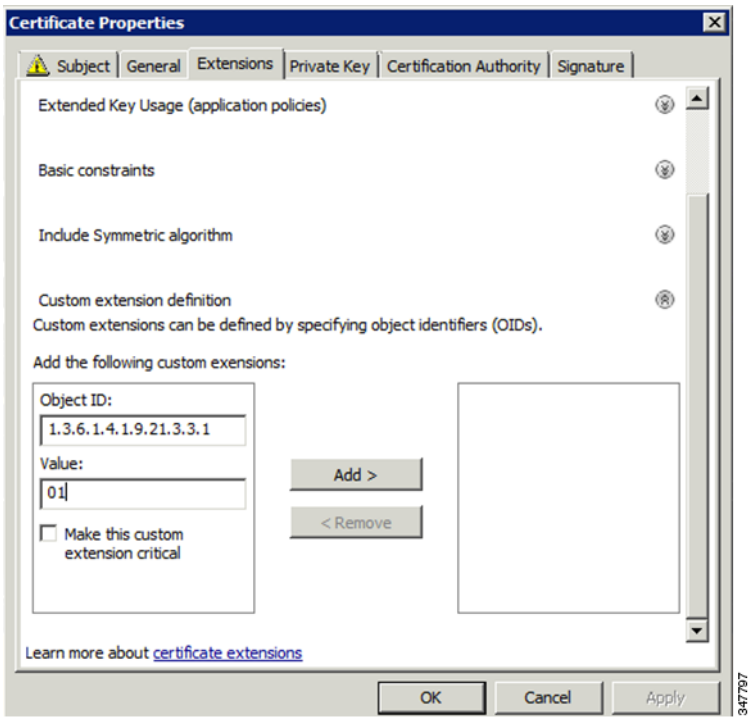
OID 値を CA 証明書に追加するには、次の手順を実行します。

1. CA サーバ上で、cmd コンソールを開き、次のように入力します。

```
certutil -setreg policy\EnableRequestExtensionList +1.3.6.1.4.1.9.21.3.3.1
```

2. CA を再起動します。
3. [Select Certificate Enrollment Policy] ウィンドウで、[Active Directory Enrollment Policy] を選択し、[Next] を選択します。

4. [Request Certificates] ウィンドウで、次の手順を実行します。
   a. [NMS] チェックボックスをオンにします。
   b. [More information...] リンクをクリックします。
5. [Certificate Properties] ウィンドウで、[Subject] タブをクリックし、フィールドに入力します。
6. [Certificate Properties] ウィンドウで、[Extensions] タブをクリックし、[Custom extension definition] ボタンをクリックして、セクションを展開します。



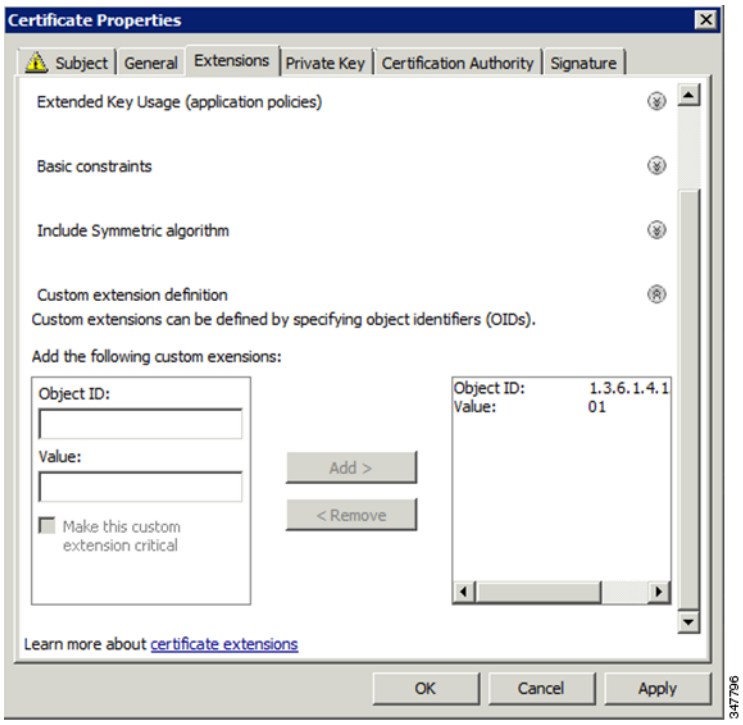
7. [Object ID] フィールドに、次のように入力します。

   ```
   1.3.6.1.4.1.9.21.3.3.1
   ```

8. [Value] フィールドに、次のように入力します。

   ```
   01
   ```

9. [Add] をクリックします。



OID と値は、カスタム拡張機能として右側のフィールドに追加されます。

10. これらの値が正しいことを確認し、[Apply] をクリックします。

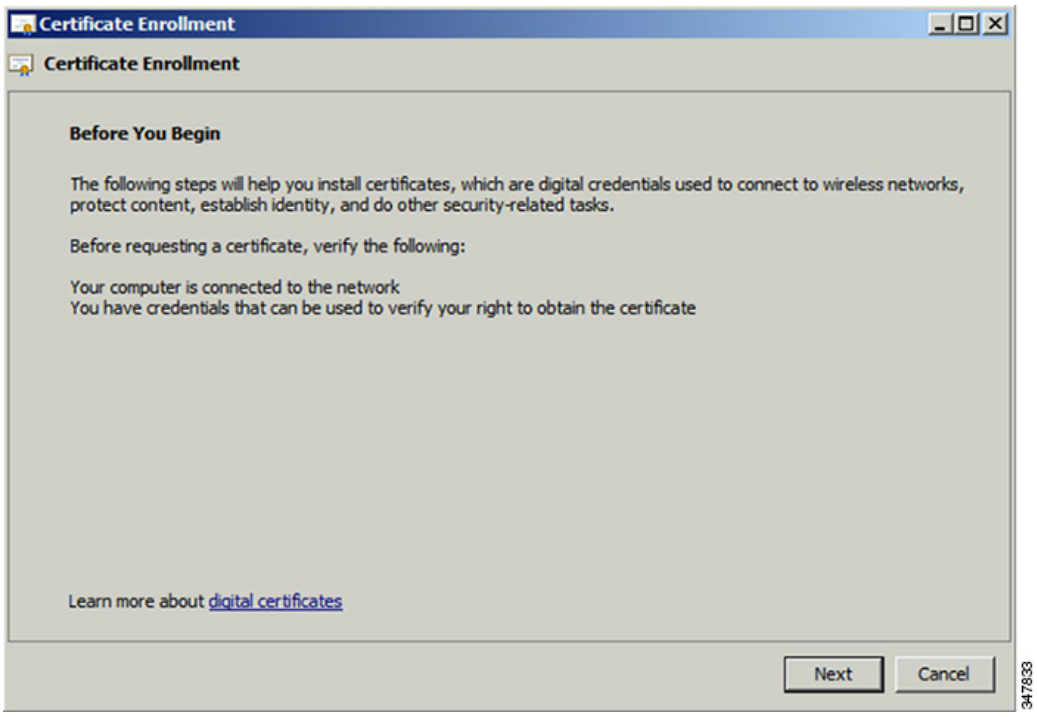
証明書の更新

証明書を更新し、OID 値を追加するには、次のようにします。

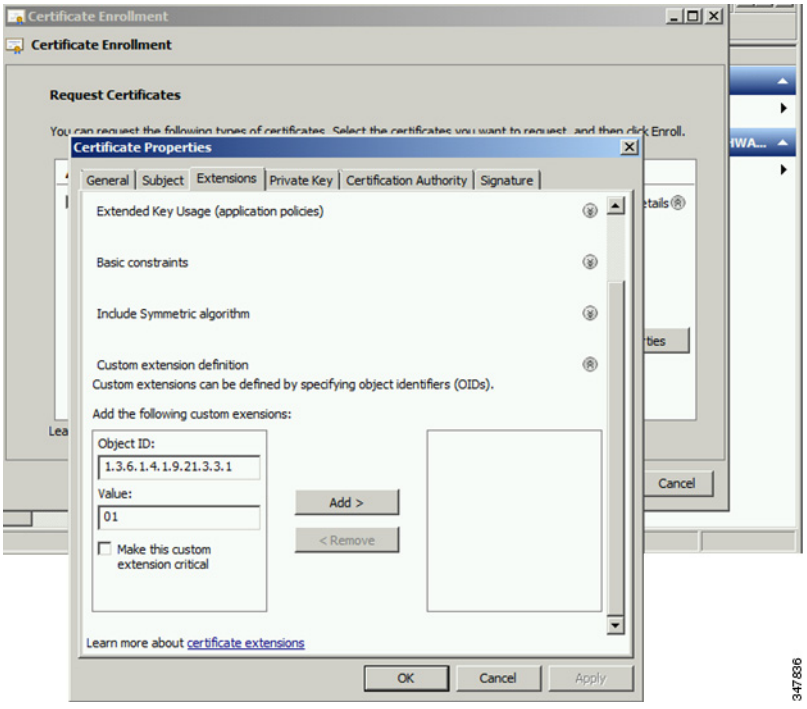
1. 元の NMS/TPS 証明書がある RSA CA サーバから、コマンド プロンプトで次のオープン コマンドを入力します。

   ```
   certutil -setreg policy\EnableRequestExtensionList +1.3.6.1.4.1.9.21.3.3.1
   ```

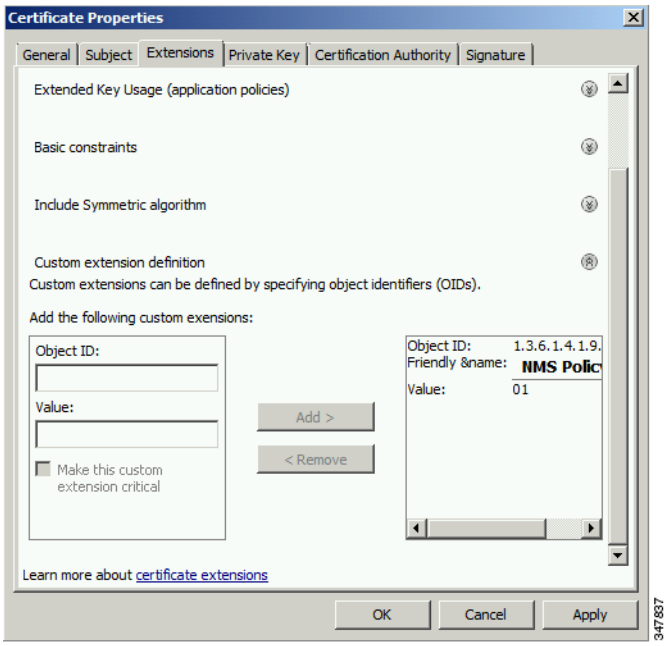
2. CA サーバを再起動します。
3. MMC で証明書のコンソールを開きます。
4. CA サーバ上の Personal フォルダ内から、発行された NMS/TPS 証明書を見つけます。
5. サーバ アイコンを右クリックし、コンテキスト メニューから [All Tasks] > [Advanced Operations] > [Renew This Certificate with the Same Key] オプションを選択します。
6. [Certificate Enrollment] ウィンドウで、[Next] をクリックします。



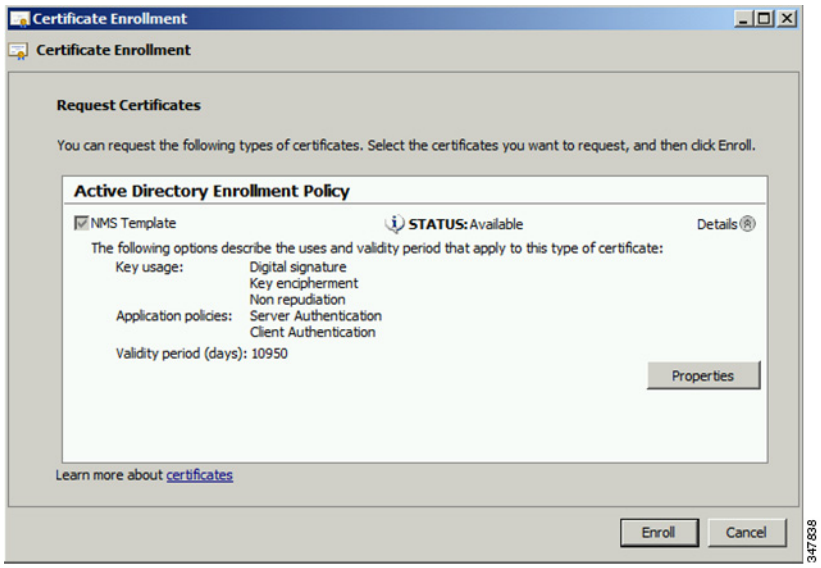
7. [Details] をクリックします。
8. [Properties] をクリックします。
9. OID とその値を入力し、[OK] をクリックします。



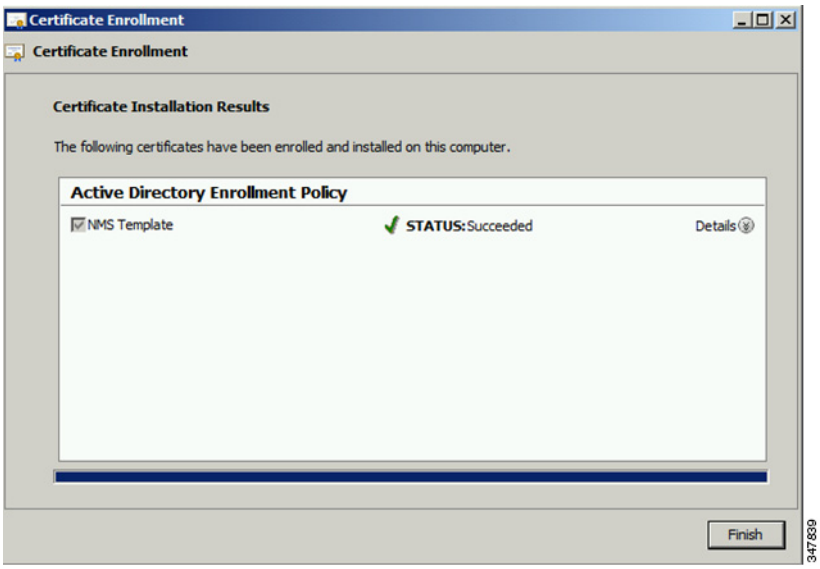
10. [Add>] をクリックし、次に [OK] をクリックします。



11. [Enroll] をクリックします。



12. [Finish] をクリックします。



13. 証明書に OID 値が含まれていることを確認します。

HSM のカスタム CA の設定

この項では、IoT FND からメッシュ デバイスに送信される CSMP メッセージに署名するための、ハードウェア セキュリティ モジュール(HSM)用のカスタム CA の設定について説明します。

はじめる前に

- 表 1(8 ページ)にリストされている SafeNet クライアント ソフトウェア バージョンが、IOT-FND サーバ上にインストールされていることを確認します。
- 独自の CA(たとえば、Microsoft や OpenSSL)を持つ必要があります。

HSM 証明書を生成するためのカスタム CA を設定するには、次の手順を実行します。

1. HSM 上に新しいパーティションを作成し、それを IoT FND クライアントに割り当てます(HSM クライアントの設定を参照)。
2. HSM 上でキーペアを生成し、そのキーペアの CSR をエクスポートします(キーストアを参照)。

   すべてのコマンドは、IoT FND サーバ上の Luna クライアントから実行します。HSM マシンにログインする必要はありません。

```
[root@<user>-scaledb bin]# cd /usr/safenet/lunaclient/bin/

# Generate a Key Pair (a set of private and public keys. You MUST provide explicit labels to the
private and public keys)
[root@<user>-scaledb bin]# ./cmu generatekeypair -sign=T -verify=T -labelpublic="nms_public_key"
-labelprivate="nms_private_key"
Please enter password for token in slot 1 : ********
Enter key type - [1] RSA  [2] DSA [3] ECDSA : 3    <--- Choose option 3
Enter curve type [1] NISTP 192
                 [2] NISTP 224
                 [3] NISTP 256
                 [4] NISTP 384
                 [5] NISTP 521

Enter curve type [1] NISTP 192
                 [2] NISTP 224
                 [3] NISTP 256   <--- Choose option 3
```

```
                [4] NISTP 384
                [5] NISTP 521
 (1 to 5) 3
[root@<user>-scaledb bin]#

# Test if the keypair exists on the HSM partition

[root@<user>-scaledb bin]# ./cmu list
Please enter password for token in slot 1 : ********
handle=2000001    label=nms_public_key
handle=2000002    label=nms_private_key

# Now, export a certificate signing request for this keypair. Note that the specific fields for DN
and handle may be different for your HSM.Fill appropriately.

[root@<user>-scaledb bin]#./cmu requestcertificate
Please enter password for token in slot 1 : ********
Select the private key for the request :

Handler    Label
2000002    nms_private_key
Enter handler (or 0 for exit) : 2000002
Enter Subject 2-letter Country Code (C) : US
Enter Subject State or Province Name (S) : CA
Enter Subject Locality Name (L) : San Jose
Enter Subject Organization Name (O) : Cisco Systems Inc.
Enter Subject Organization Unit Name (OU) : IOTSSG
Enter Subject Common Name (CN) : IOT-FND-HSM
Enter EMAIL Address (E) :
Enter output filename : hsm.csr
[root@<user>-scaledb bin]#

# Verify the file exists and has properly formatted content

[root@<user>-scaledb bin]# ls hsm.csr
hsm.csr

[root@<user>-scaledb bin]# cat hsm.csr
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBKzCB0QIBADBvMQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0ExETAPBgNVBAcT
CFNhbiBKb3NlMRowGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEluYzEPMA0GA1UECxMG
SW9UU1NHMRMwEQYDVQQDEwpDRy1OTVMtSFNNMFkwEwYHKoZIzj0CAQYIKoZIzj0D
AQcDQgAESfdlrrcVtzN3Yexj9trlI5qd0w5Sdu8Vj2s17JAF/vPFUOYIw/uXwD6+
bb8vq3WHlA6tmgRbj+FU6G3Bmt/vCqAAMAsGBYqGSM49BAEFAANIADBFAiEAroJO
qz3dHA2GLrGzBmUO1vYys642Nkb4B4qyEoUZIGsCIFs0iTUyGQreM1BaSDEPHArZ
RvFlrKo/Zi3c8O4gzFZW
-----END NEW CERTIFICATE REQUEST-----
```

3. 生成された CSR を CA に保存して、証明書に署名します。

   (注)証明書は必ず有効期限を 30 年として署名します。メッシュ ノードは、30 年未満の有効期限で署名された証明書はすべて拒否します。ノード アドミッションのための 802.1x 認証に使用されるルート CA を使用できます。

4. 署名付き証明書を IoT FND サーバにコピーして、HSM にインポートします。

```
[root@<user>-scaledb bin]# ./cmu import
Please enter password for token in slot 1 : ********
Enter input filename : <your file name with signed certificate>

# Verify that the certificate was imported
```

```
[root@<user>-scaledb bin]# ./cmu list
Please enter password for token in slot 1 : ********
handle=2000001    label=nms_public_key
handle=2000002    label=nms_private_key
handle=2000003    label=IOT-FND-HSM    <--- This is my certificate with label = CN
```

5. この新しい証明書を使用するように IoT FND を設定します。

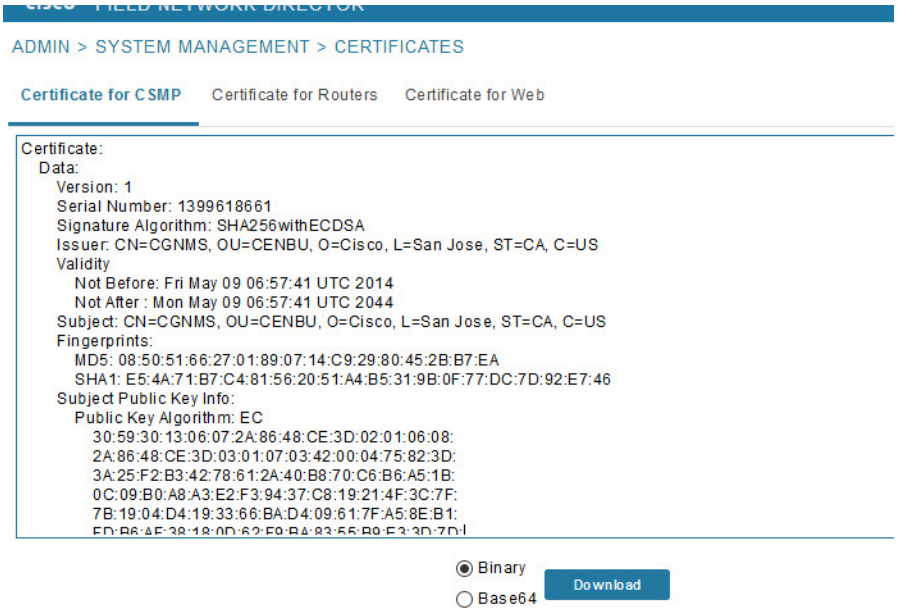
```
[root@kartven2-nms ~]# service cgms stop
[root@kartven2-nms ~]# cd /opt/cgms/server/cgms/conf/

# Add following properties to the cgms.properties file

hsm-private-key-label=nms_private_key     <--- private key label you gave to your public key
hsm-public-key-label=nms_public_key       <--- public key label you gave to your public key
hsm-cert-label=IOT-FND-HSM                <--- label for your signed certificate
hsm-keystore-name=customca-group          <--- your HA partition group
hsm-keystore-password=2bVvZsq+vsq94YxuAKdaag==   <--- encrypted password for the partition

[root@kartven2-nms conf]# service cgms start
[root@kartven2-nms conf]#
```

6. 証明書が [Certificates for CSMP] タブ（[ADMIN] > [System Management Certificates]）に表示されることを確認します



7. 署名にこの証明書を使用するように、メッシュ ノードを設定します。

SSM のカスタム CA の設定

この項では、IoT FND からメッシュ デバイスに送信される CSMP メッセージに署名するための、ソフトウェア セキュリティ モジュール（SSM）用のカスタム CA の設定について説明します。

はじめる前に

- 表 1（8 ページ）にリストされている SafeNet クライアント ソフトウェア バージョンが、IOT-FND サーバ上にインストールされていることを確認します。
- サポート対象は、SSM バージョン 2.2.0-37 以上です。
- 独自の CA（たとえば、Microsoft や OpenSSL）を持つ必要があります。

SSM 証明書を生成するためのカスタム CA を設定するには、次の手順を実行します。

1. ssm サービスを停止します。

```
[root@nms-rhel-6-6 ~]# stop ssm
```

2. ssm_setup.sh スクリプトを使用して、新しいキーペアを特定のエイリアスで設定し、CSR を生成します。

```
[root@nms-rhel-6-6 ~]# cd /opt/cgms-ssm/bin/
[root@nms-rhel-6-6 bin]# ./ssm_setup.sh


Software Security Module Server

1.Generate a new keyalias with self signed certificate for CSMP

2.Generate a new keypair & certificate signing request for CSMP   <--- Choose option 2

3.Import a trusted certificate

4.Change CSMP keystore password

5.Print CG-NMS configuration for SSM

6.Change SSM server port

7.Change SSM-Web keystore password


Select available options.Press any other key to exit


Enter your choice : 2
Warning: This action will modify ssm_csmp_keystore file. Backup the file before performing this
action.
Do you want to proceed (y/n): y

Enter current ssm_csmp_keystore password :
Enter a new key alias name (8-16): ssmcustomca
Enter key password (8-12):

Enter certificate issuer details

Enter common name CN [Unknown]: IOT-FND-SSM

Enter organizational unit name OU [Unknown]: IOTSSG

Enter organization name O [Unknown]: Cisco Systems Inc.

Enter city or locality name L [Unknown]: San Jose

Enter state or province name ST [Unknown]: CA

Enter country code for this unit C [Unknown]: US


Is [CN=IOT-FND-SSM, OU=IOTSSG, O=Cisco Systems Inc., L=San Jose, ST=CA, C=US] correct (y/n)? :y
Certificate Signing Request file name: /opt/ssmcustomca.csr
Succefully generated keypair with alias ssmcustomca. You can use the CSR from /opt/ssmcustomca.csr
for signature by certificate authority
[root@nms-rhel-6-6 bin]#
```

3. 生成された CSR を CA に保存して、証明書に署名します。

   (注)証明書は必ず有効期限を 30 年として署名します。メッシュ ノードは、30 年未満の有効期限で署名された証明書はすべて拒否します。ノード アドミッションのための 802.1x 認証に使用されるルート CA を使用できます。

4. 署名付き証明書を IoT FND サーバにコピーして、SSM にインポートします。

5. ssm_setup.sh スクリプトを使用して、2 つの証明書を SSM キーストアにインポートします。

```
[root@nms-rhel-6-6 bin]# ./ssm_setup.sh


Software Security Module Server

1.Generate a new keyalias with self signed certificate for CSMP

2.Generate a new keypair & certificate signing request for CSMP

3.Import a trusted certificate   <--- Choose option 3

4.Change CSMP keystore password

5.Print CG-NMS configuration for SSM

6.Change SSM server port

7.Change SSM-Web keystore password


Select available options.Press any other key to exit


Enter your choice : 3

Enter current ssm_csmp_keystore password :
Enter the alias for import: root
Certificate file name: /opt/ca.crt
Certificate reply was installed in keystore
Succefully imported certificate into alias root
```

6. ssm_setup.sh スクリプトを使用して、エイリアスの署名付き証明書認証をインポートします。

```
[root@nms-rhel-6-6 bin]# ./ssm_setup.sh


Software Security Module Server

1.Generate a new keyalias with self signed certificate for CSMP

2.Generate a new keypair & certificate signing request for CSMP

3.Import a trusted certificate   <--- Choose option 3

4.Change CSMP keystore password

5.Print CG-NMS configuration for SSM

6.Change SSM server port

7.Change SSM-Web keystore password


Select available options.Press any other key to exit
```

```
Enter your choice : 3

Enter current ssm_csmp_keystore password :
Enter the alias for import: ssmcustomca
Certificate file name: /opt/ssmcustomca.crt
Certificate reply was installed in keystore
Succefully imported certificate into alias ssmcustomca
```

7. cgms.properties ファイルを次のパラメータで更新して、IoT FND がこの証明書を署名のために SSM で使用するように設定します。

```
security-module=ssm
ssm-host=172.27.163.153
ssm-port=8445
ssm-keystore-alias=ssmcustomca
ssm-keystore-password=GgeQJAOk3fSIH97qJARGRA==
ssm-key-password=GgeQJAOk3fSIH97qJARGRA==
```

8. 証明書が [Certificates for CSMP] タブ（[ADMIN] > [System Management Certificates]）に表示されることを確認します。

9. 署名にこの証明書を使用するように、メッシュ ノードを設定します。

CA 証明書のエクスポート

証明書を認証局または下位 CA から IoT FND にエクスポートするには、次の手順を実行します。

1. Windows Server 2008 R2 Enterprise エディションを稼働するシステム上で、認証局アプリケーションを開きます。
2. メニューを展開して、[Certificates (Local Computer)] > [Personal] > [Certificates] フォルダを表示します。
3. フィンガープリントが Cisco CGR 1000 と Cisco ASR により使用されているものと一致する証明書を見つけます。
4. 証明書を右クリックして、コンテキスト メニューから [All Tasks] > [Export] を選択します。
5. [Certificate Export Wizard] ウィンドウで、[Next] をクリックします。
6. [Export Private Key] ウィンドウで、[No, do not export the private key] ラジオ ボタンを選択します。[Next] をクリックします。
7. [Export File Format] ウィンドウで、[Base-64 encoded X.509（.CER）] ラジオ ボタンをオンにします。[Next] をクリックします。
8. [File to Export] ウィンドウで、エクスポートするファイルに名前を割り当てます。[Next] をクリックします。
9. [File to Export] ウィンドウに、ファイル名（*ca_cert* または *subca_cert* など）を入力し、[Next] をクリックします。
10. [Completing the Certificate Export Wizard] で、[Finish] をクリックします。

*.cer 拡張子を持つファイルは、デスクトップに自動的に保存されます。

11. 証明書ファイル（*ca_cert.cer* など）を、Windows デスクトップから IoT FND に安全に転送します。

(注)セキュリティを向上させるには、転送が正常に実行されたら、*.cer ファイルを Windows デスクトップから削除して、ごみ箱を空にします。

証明書のインストール

cgms_keystore ファイルは、IoT FND と IoT FND TPS プロキシを稼働している両方のサーバ上に作成する必要があります。

- **IoT FND**：cgms_keystore ファイルを作成するときは、IoT FND 証明書、秘密キー、および証明書チェーンをインポートする必要があります。cgms_keystore ファイルを作成したら、それをサーバ上の特定のディレクトリにコピーします。
- **IoT FND TPS プロキシ**：cgms_keystore ファイルを作成したら、IoT FND TPS プロキシの証明書、秘密キー、および証明書チェーンをインポートします。cgms_keystore ファイルを作成したら、TPS プロキシ上の特定のディレクトリにそれをコピーします。

TPS プロキシおよび IoT FND 用の cgms_keystore を作成するには、キーツールを使用して、次の手順を実行します。

- はじめる前に
- キーツールを使用した cgms_keystore ファイルの作成
- cgms_keystore ファイルの IoT FND へのコピー
- CA 証明書のインポート
- カスタム ブラウザ証明書のインストール

はじめる前に

- キーストアに使用するパスワードを決定します。

  この章の例では、このパスワードを *keystore_password* としています。

キーツールを使用した cgms_keystore ファイルの作成

IoT FND と TPS プロキシの両方に対して cgms_keystore ファイルを作成するには、次の手順を実行します。

1. root として、.pfx ファイルの内容を、サーバ上（IoT FND および TPS プロキシ）で次のコマンドを入力して表示します。

[root@*tps_server* ~]# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12

（注）.pfx の内容を表示すると、インポート時に必要なエイリアス名を入手できます。

2. プロンプトが表示されたら、キーストアのパスワードを入力します。

これは、.pfx ファイルの作成時に入力したものと同じパスワードです。

表示される情報には（次の例を参照）、3 に必要な alias_name が含まれています。

3. 証明書を cgms_keystore ファイルにインポートするには、次のコマンドを入力します。

```
keytool -importkeystore -v -srckeystore filename.pfx -srcstoretype pkcs12
-destkeystore cgms_keystore -deststoretype jks -srcalias alias_name -destalias cgms
-destkeypass
keystore_password
```

4. プロンプトで、宛先キーストア パスワードを入力します。
5. プロンプトが表示されたら、キーストアのパスワードを再入力します。
6. ソースのキーストア パスワードの入力を求めるプロンプトが表示されたら、.pfx ファイルの作成時に使用したパスワードを入力します（*nms_cert.pfx* または *tps_cert.pfx* のどちらか）。

（注）この例では、**keystore** が *.pfx* ファイルを作成したときのパスワードです。

例

nms_cert.pfx ファイルを表示して別名にアクセスするには、root として以下のコマンドを入力します。

(注) この例は、*nms_cert.pfx* についての手順を示しています。*tps_cert.pfx* に関する詳細を表示して、証明書を TPS プロキシにインポートするには、同じコマンドを使用しますが、*nms_cert.pfx* の部分は *tps_cert.pfx* に置き換え、*tps_cert.pfx* ファイルからの別名を使用します。

```
# keytool -list -v -keystore nms_cert.pfx -srcstoretype pkcs12
Enter keystore password: keystore
Keystore type: PKCS12
Keystone provider: SunJSSE
Your keystore contains 1 entry
Alias name: le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b
Creation date: March 29.2012
Entry type: PrivateKey Entry
Certificate chain length: 3
Certificate[1]:
Owner: CN=nms.sgbu.cisco.com
Issuer: CN=cisco-RSA-SUBCA-CA, DC=cisco, DC=com
...
```

証明書を IoT FND 上の **cgms_keystore** ファイルにインポートするには、root として次のコマンドを入力します。

```
# keytool -importkeystore -v -srckeystore nms_cert.pfx -srcstoretype pkcs12
-destkeystore cgms_keystore -deststoretype jks -srcalias
le-cgnms-75edd1e3-7e65-41b4-97f1-a913ebf21c8b -destalias cgms
-destkeypass
keystore_password

Enter destination keystore password: keystore_password
Re-enter new password: keystore_password
Enter source keystore password: keystore
...Storing cgms_keystore
```

(注) ***cgms*_keystore** テキストが**保存**されたことは正常な完了を示します。

cgms_keystore ファイルの IoT FND へのコピー

cgms_keystore ファイルを次の IoT FND および TPS プロキシのディレクトリにコピーします。

1. IoT FND の場合は、cgms_keystore ファイルをディレクトリ **/opt/cgms/server/cgms/conf/** にコピーします。
2. TPS プロキシの場合、cgms_keystore ファイルをディレクトリ **/opt/cgms-tpsproxy/conf/** にコピーします。

(注) 証明書をアクティブで適用可能なものとするには、正しいディレクトリに入れておく必要があります。

CA 証明書のインポート

NMS 証明書のインポートに加え、CA(または subCA)証明書を cgms_keystore にインポートする必要があります。

CA 証明書を cgms_keystore にインポートするには、次の手順を実行します。

1. IoT FND アプリケーション サーバ上で、root としてログインします。
2. cgms_keystore ファイルが置かれている /opt/cgms/server/cgms/conf ディレクトリに移動します。

```
# cd /opt/cgms/server/cgms/conf
```

3. CA 証明書をインポートします。

```
# keytool -import -trustcacerts -alias root -keystore cgms_keystore -file ca_cert.cer
```

画面にスクリプトが表示されます。

4. プロンプトが表示されたら、キーストアのパスワードを入力します。
5. パスワードを再入力します。
6. 証明書を信頼するかどうかを確認するメッセージが表示されたら、**yes** と入力します。

証明書はキーストアに追加されます。

例

CA 証明書をインポートするには、次のコマンドを root として入力します。

```
# keytool -import -trustcacerts -alias root -keystore cgms_keystore -file ca_cert.cer
Enter keystore password: keystore_password
Owner:  CN=SGBUNMSCA-WIN-4BGS4M94L66-CA,DC=SGBUNMSCA,DC=lab,DC=co
Issuer: CN=SGBUNMSCA-WIN-4BGS4M94L66-CA,DC=SGBUNMSCA,DC=lab,DC=co
Serial number:50adbd57e6b136984f9c1512a0eb7174
Valid from: Wed Jan 11 10:58:09 PDT 2012 until: Wed Jan 11:08:59 PDT 2016
Certificate _fingerprints:
    MD5: AE:5D:F4:0A:2B:E5:C8:D8:4A:F4:18:56:FD:A7:8D:7D
    SHA1: 83:22:12:8C:6A:23:D3:08:2B:00:55:EF:BD:FF:BA:47:97:99:7E:41
    Signature algorithm name: SHA1withRSA
    Version:3

Extensions:
#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
CA:true
PathLen:2147483647
]
#2:ObjectId: 2.5.29.15 Criticality=false
KeyUsage[
DigitalSignature
Key_CertSign
Crl_Sign
]
#3:ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000:C6 AB 38 CC EE 79 B0 51 3B 4D 13 c8 9A 56 F6 73 ..8..y.Q;M...V.s
0010:B9 19 FF 7B                                     ....
]
]
#4: ObjectId:1.3.6.1.4.1.311.21.1 Criticality=false
Trust this certificate [no] yes
Certificate was added to the keystore.
```

IoT FND TPS プロキシ キーストアへの CA 証明書のインポート

CA 証明書のインポートと同じ手順に従って、CA 証明書を IoT FND TPS プロキシ上の cgms_keystore にインポートします。

カスタム ブラウザ証明書のインストール

デフォルトの IoT FND インストール システムは、クライアント Web ブラウザまたは NB API クライアントのいずれかを使用する HTTP(S)通信に、自己署名証明書を使用します。必要であれば、ユーザ自身の CA サーバによって署名された証明書を使用できます。この項では、これらのカスタム証明書のインストール方法を示します。

この項では、次のトピックについて取り上げます。

- ブラウザ クライアントでのカスタム証明書のインストール
- North Bound API クライアント(Windows)を使用している場合のカスタム証明書のインポート
- Window IE を使用している場合のカスタム証明書のインポート
- カスタム証明書の管理
- North Bound API イベントの管理

はじめる前に

- クライアント ブラウザのキャッシュをクリアします。
- クライアント ブラウザで、NMS サーバの既存の証明書を(IP および DNS により)削除します。

  たとえば、Firefox では、[Preferences] > [Advanced] > [Encryption] > [View Certifications] を選択します。それぞれのサーバについてリスト内の証明書を削除します。
- 署名付き証明書で使用する共通名を選択します。

  この名前には、NMS サーバの IP アドレスに解決するための DNS エントリが必要です。
- 新しい証明書を生成し、それを .PFX ファイルにエクスポートします。

  このファイルには、秘密キー、パブリック証明書、および CA サーバ証明書が含まれている必要があります。

  cgms_keystore ファイルの秘密キーと公開キーを生成してそれらを .PFX ファイルにエクスポートする手順については、キーツールを使用した cgms_keystore ファイルの作成を参照してください。

ブラウザ クライアントでのカスタム証明書のインストール

1. NMS サーバで、既存の jbossas.keystore および jbossas.keystore.password ファイルを、/opt/cgms/server/cgms/conf/ ディレクトリから安全な場所にコピーします。
2. 既存の jbossas.keystore および jbossas.keystore.password ファイルを /opt/cgms/server/cgms/conf/ ディレクトリから削除します。
3. jbossas.keystore ファイルにインポートする予定の別名を、.PFX ファイル内で確認します。

   ```
   #keytool -list -v -keystore newcert.pfx -storetype pkcs12
   ```

   次のキーストア パスワードを入力します。***keystore_password_when_pfx_file_was_created***

   ```
   Keystore type: PKCS12
   Keystore provider: SunJSSE

   Your keystore contains 1 entry

   Alias name: le-nms-a88ef13a-a519-457f-a2e1-0540f5453ee0
   Creation date: Feb 23, 2016
   Entry type: PrivateKeyEntry
   Certificate chain length: 2
   Certificate[1]:
   …
   ```

4. .pfx ファイル形式の新しいカスタム証明書を新しい jbossas.keystore ファイルにインポートし、同時にエイリアス名を **jboss** に変更します。プロンプトに従います。

```
# keytool -importkeystore -v -srckeystore newcert.pfx -srcstoretype pkcs12
-destkeystore /opt/cgms/server/cgms/conf/jbossas.keystore -deststoretype jks-
srcalias le-nms-a88ef13a-a519-457f-a2e1-0540f5453ee0 -destalias
jboss -destkeypass your_keystore_password
Enter destination keystore password: your_keystore_password
Enter source keystore password: keystore_password_when_pfx_file_was_created
[Storing /opt/cgms/server/cgms/conf/jbossas.keystore]
```

5. （任意）SALT を定義します。

   （注）SALT を変更しない場合は、この手順をスキップすることができます。

   SALT は暗号化パスワードの強度を定義します。それは少なくとも 8 文字の長さにする必要があります。
   例：A1a1B2b2C3c3D4dE5e5F6f6G7g7H8h8I9i9J10j10K11k11L12l12M13m13N14n14O15

   a. ファイル /opt/cgms/server/cgms/deploy/security-service.xml を安全な場所にコピーします。

   b. /opt/cgms/server/cgms/deploy/security-service.xml ファイル内で SALT を更新します。

（注）実行している NMS リリースに応じて、手順 6 *または*手順 7 *のどちらか*を選択します。

6. **2.1.0 より *前の* CG-NMS リリース**では、キーストア パスワードは、ファイル /opt/cgms/server/cgms/conf/jbossas.keystore.password に保存します。

   この手順では、jbossas.keystore.password ファイルに保存されるパスワードを暗号化します。

   このパスワードは、手順 4 でインポートされた新しいカスタム証明書がある jbossas.keystore を開くために使用されます。

   a. /opt/cgms/bin/encrypt-password.sh スクリプトを、次のパラメータを指定して実行します。

   – 手順 5 で定義した新しい SALT を指定するか、または /opt/cgms/server/cgms/deploy/security-service.xml ファイル内にある既存のものを使用します。

   – count を 1024 に設定します。

   – パスワード ファイルを jbossas.keystore.password に設定します。

   – your_keystore_password を設定します。

```
#./encrypt-password.sh
A1a1B2b2C3c3D4dE5e5F6f6G7g7H8h8I9i9J10j10K11k11L12l12M13m13N14n14O15 1024 jbossas.keystore.password
your_keystore_password
```

   b. jbossas.keystore.password を /opt/cgms/server/cgms/conf ディレクトリに移動させるかまたはコピーします。

   c. ステップ 8 に進みます。

7. **2.1.0 または IoT FND 3.0 *以降の* CG-NMS リリース**では、キーストア パスワードはファイル /opt/cgms/server/cgms/conf/VAULT.dat に保存します。

   続く手順を実行し、パスワードを更新して、手順 4 で入力したもの（***your_keystore_password***）と一致するようにします。

   a. /opt/cgms/server/cgms/conf 内の VAULT.dat と vault.keystore ファイルを安全な場所にバックアップします。

   b. VAULT.dat ファイルを新しいパスワードで更新します。

```
#/opt/cgms/bin/vault.sh -k /opt/cgms/server/cgms/conf/vault.keystore -p cgms123
-e /opt/cgms/server/cgms/conf -i 50 -s 12345678 -v vault -b keystore_pass
-a password -x your_keystore_password
```

ここで、vault.keystore には VAULT.dat への参照が含まれており、VAULT.dat は jboss キーストア パスワードを保存して非表示にします。このコマンドは、新しい jboss.keytsore を含む新しい VAULT.dat ファイルを作成します。vault.keystore を開くデフォルトのパスワードは cgnms123 です。

8. IoT FND を再起動します。

```
# service cgms restart
```

9. ブラウザを使用して、NMS サーバに接続します。
10. 新しい証明書を承認し、追加します。
11. ブラウザを使用して IoT FND にログインします。

North Bound API クライアント（Windows）を使用している場合のカスタム証明書のインポート

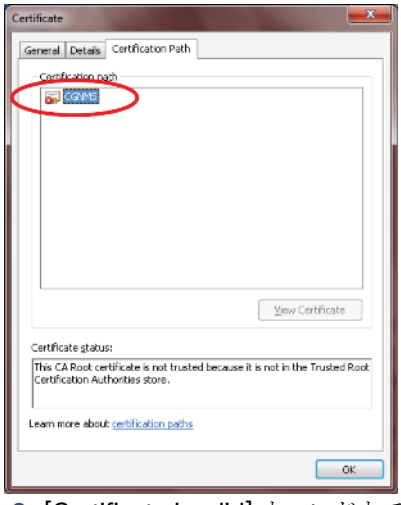
Windows Server 上で実行する NB API クライアントの場合は、CA パブリック証明書をローカル コンピュータ上の証明書ストアにインポートします。一致する CA パブリック証明書により、クライアント マシンは必ず NB API クライアントを使用して IoT FND と通信します。

Window IE を使用している場合のカスタム証明書のインポート

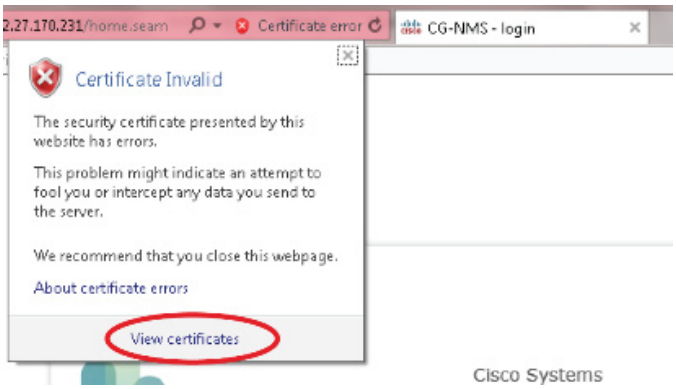
1. IE では、NMS サーバの https URL アドレスを入力します。

   URL 名は、NMS サーバ証明書の共通名と一致している必要があります。

2. [Security Alert] ウィンドウで、[OK] をクリックします。
3. [Security Certificate Warning] ウィンドウで、[Continue to this Website (Not Recommended)] リンクをクリックします。
4. [Security Alert] ウィンドウで、[OK] をクリックします。
5. アドレス バーの [Certificate error] セクションをクリックします。

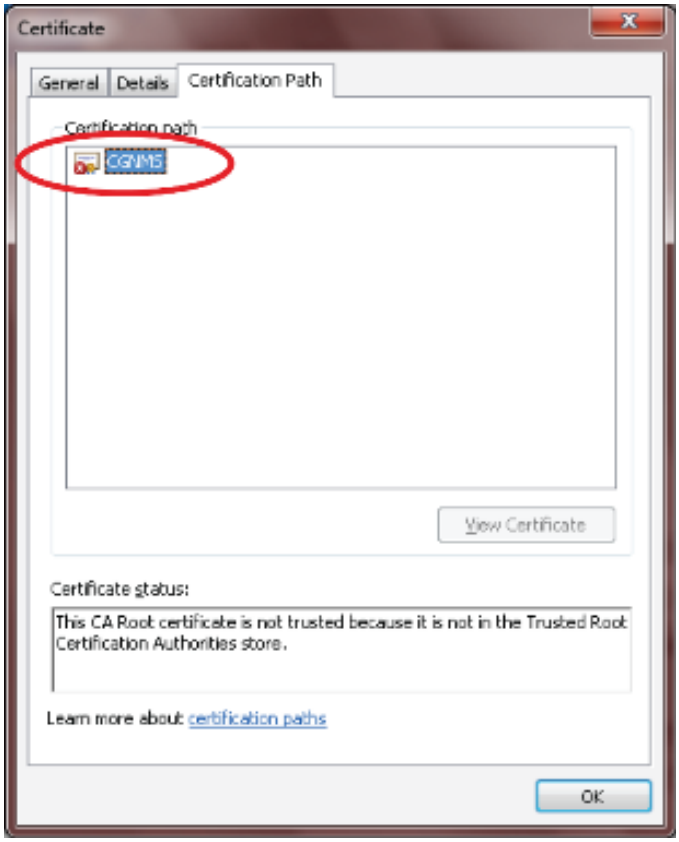


6. [Certificate Invalid] ウィンドウで、[View certificates] をクリックします。

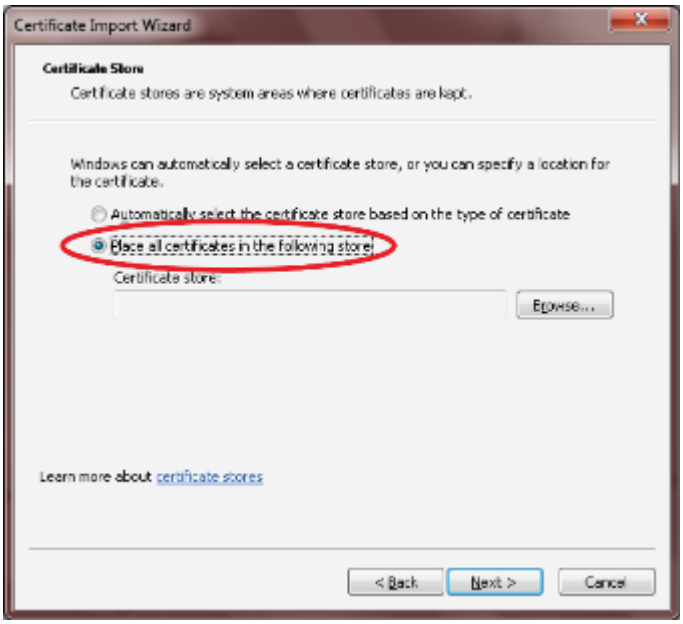


[Certificate] ウィンドウには、NMS サーバに対して発行され、発行元 CA（または下部 CA）サーバによって署名されたデバイス証明書がリストされます。

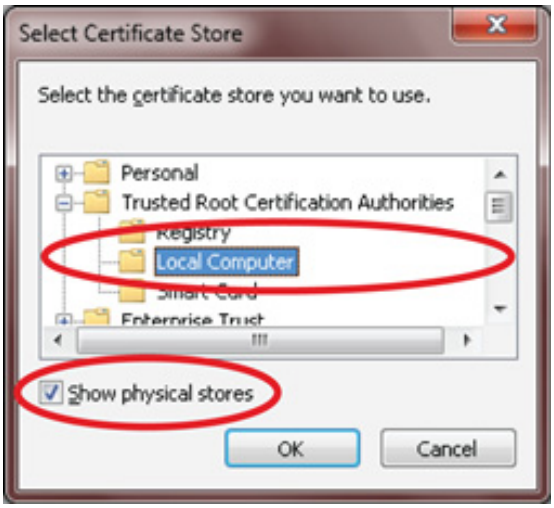
7. [Certification Path] タブを選択し、無効な証明書（つまり赤いバツ印が付いているもの）を探します。



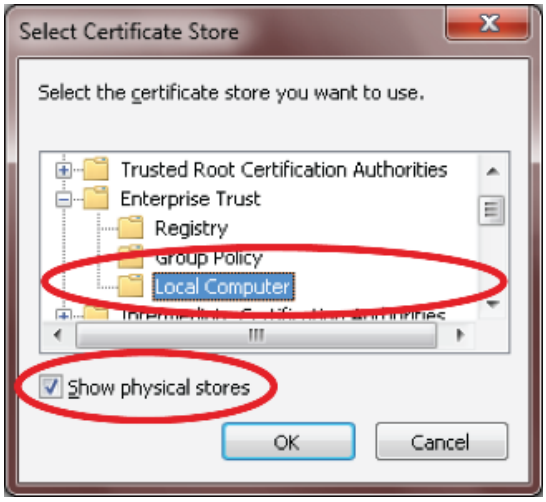
8. 無効な証明書を選択し、[General] タブを選択します。
9. [Install Certificate] をクリックします。
10. [Certificate Install Wizard] ウィンドウで、[Next] をクリックします。
11. [Place all certificates in the Following Store] を選択し、[Browse] をクリックします。



12. [Certificate Store] ウィンドウで、[Show physical stores] チェックボックスをオンにし、Trusted Root Certification Authorities フォルダを開き、[Local Computer] を選択して、[OK] をクリックします。



13. [Next] をクリックします。
14. [Finish] をクリックします。
15. [OK] をクリックします。
16. [Certificate] ウィンドウで、[Install Certificate] をクリックします。
17. [Place all certificates in the Following Store] を選択し、[Browse] をクリックします。
18. [Certificate Store] ウィンドウで、[Show physical stores] チェックボックスをオンにし、Trusted Root Certification Authorities フォルダを開き、[Local Computer] を選択して、[OK] をクリックします。



19. [Next] をクリックします。
20. [Finish] をクリックします。
21. [OK] をクリックします。
22. [Certificate] ウィンドウで、[OK] をクリックします。
23. アドレス バーの [Certificate error] セクションが引き続き表示される場合は、前述の手順を繰り返します。
    - NMS サーバに対して発行され、発行元 CA（または下部 CA）サーバによって署名されたデバイス証明書が、[Certificate] ウィンドウに表示されていることを確認します。
    - [Certification Path] タブを選択し、パス内のすべての証明書が有効である（つまり、証明書の上に赤いバツ印が付いていない）ことを確認します。
24. ブラウザを閉じてから再起動します。
25. アドレス バーに、IoT FND サーバのセキュア URL を入力します。

    IoT FND ログイン ページが表示されます（セキュリティ画面は表示されません）。

カスタム証明書の管理

1. IoT FND を更新するかまたはフレッシュ インストールを実行するときに上書きされる次のファイルをバックアップします。
    - /opt/cgms/server/cgms/conf/ ディレクトリ内の次のファイル：
        - jbossas.keystore.password
        - jbossas.keystore
    - /opt/cgms/server/cgms/deploy/ ディレクトリ内の次のファイル：
        - security-service.xml ファイル

      これは、ブラウザ クライアントでのカスタム証明書のインストールで SALT 値を追加したファイルです。

- /opt/cgms/server/cgms/conf ディレクトリ内の次のファイル:
  - VAULT.dat
  - vault.keystore

2. IoT FND のアップグレードまたは新規インストールを実行します(IoT FND のアップグレードを参照)。
3. 上記のファイルをそれぞれの該当するフォルダにコピーして、IoT FND を再起動します。

North Bound API イベントの管理

North Bound(NB)API クライアントは、HTTPS を使用してイベントを送信できます。NB API クライアントは、IoT FND がイベント送信に使用する有効な URL HTTPS を提供することで、IoT FND をサブスクライブする必要があります。IoT FND は、NB API クライアントがパブリッシュする SSL 証明書とハンドシェイクを受け入れます。

キーストアにアクセスするための IoT FND の設定

cgms_keystore を作成し、NMS と CA 証明書をそれにインポートしたら、IoT FND が cgms_keystore ファイルにアクセスするように設定します。

keystore パスワードを設定するには、次の手順を実行します。

1. IoT FND を停止します。
2. setupCgms.sh スクリプトを実行します。

```
pwd
/opt/cgms/bin
./setupCgms.sh
06-12-2012 10:21:39 PDT: INFO: ========== CG-NMS Setup Started - 2012-06-12-10-21-39 =====
06-12-2012 10:21:39 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log
Are you sure you want to setup CG-NMS (y/n)? y
06-12-2012 10:21:39 PDT: INFO: User response: y
...
Do you want to change the keystore password (y/n)? y
06-12-2012 10:21:52 PDT: INFO: User response: y
Enter keystore password: keystore_password
Re-enter keystore password: keystore_password
06-12-2012 10:21:59 PDT: INFO: Configuring keystore password. This may take a while.
Please wait ...
06-12-2012 10:22:00 PDT: INFO: Keystore password configured.
...
```

このスクリプトは、cgms.properties ファイル内に設定されたパスワードを保存します。

3. IoT FND を起動します。

ヒント:cgms_keystore と cgms.properties ファイルを保護するには、そのアクセス許可を root の読み取り専用に設定します。

注意:システムは必ず保護してください。root でのみ IoT FND サーバにアクセスできることを確認します。ファイアウォールは必ず内部ホストからの SSH アクセスのみを許可するように設定します。

キーストアにアクセスする TPS プロキシの設定

keystore にアクセスするように TPS プロキシを設定するには、次のようにします。

1. tpsproxy bin ディレクトリに移動します。

```
cd /opt/cgms-tpsproxy/bin
```

2. 選択したパスワードを暗号化形式に変換します。

```
./encryptionUtil.sh {your chosen password for cgms_keystore}
7jlXPniVpMvat+TrDWqh1w==
```

3. 暗号化したパスワードを tpsproxy.properties ファイルにコピーします。

   a. 編集のためにファイルを開きます。

   ```
   cd /opt/cgms-tpsproxy/conf
   emacs tpsproxy.properties
   ```

   b. ファイルに次の行を追加します。

   ```
   cgms-keystore-password-hidden=keystore_password
   ```

   この例では、暗号化された *keystore_password* は「7jlXPniVpMvat+TrDWqh1w==」です。

4. TPS プロキシを再起動します。

```
service tpsproxy restart
```

HSM クライアントの設定

HSM クライアントをセットアップするには、次の手順を実行します。

- IoT FND サーバ上への HSM クライアントのインストール
- HSM HA クライアントの設定

(注)インストール システムで CSMP ベースのメッセージングに SSM を使用している場合は、SSM のインストールと設定を参照してください。

IoT FND サーバ上への HSM クライアントのインストール

ハードウェア セキュリティ モジュール(HSM)は、ポート 1792 でリスニングするセキュリティ サーバとして機能します。IoT FND が HSM と通信するようにセットアップするには、次の手順を実行します。

1. HSM クライアントを IoT FND サーバ上にインストールします。
2. HSM クライアントが HSM の証明書を持つように設定します。
3. 証明書を HSM にアップロードします。

この項では、HSM クライアントをインストールして設定する方法を説明していますが、HSM は 172.16.0.1、クライアントは 172.31.255.254 であると想定しています。

HSM クライアントをインストールしてセットアップするには、次の手順を実行します。

1. HSM クライアント パッケージを取得して、アンパックし、インストール スクリプトを実行します。

   sh install.sh

2. /usr/lunasa/bin ディレクトリに移動します。

   cd /usr/safenet/lunaclient/bin/

3. クライアント証明書を作成します。

   ./vtl createCert -n *ip_address_of_hsm_client*

4. HSM サーバから HSM 証明書をダウンロードします。

   scp admin@*ip_address_of_hsm_server***:server.pem .**

5. クライアント証明書を HSM サーバにアップロードします。

   scp ../cert/client/ip_address_of_hsm_client.pem admin@ip_address_of_hsm_server: .

6. HSM 証明書をロードします。

   vtl addServer -n ip_address_of_hsm_server -c server.pem .

7. HSM サーバが追加されていることを確認します。

   vtl listServer

8. HSM クライアントから、SSH を使用して HSM サーバにログインします。

   ```
   ssh admin@ip_address_of_hsm_server
   Last login: Mon Aug 15 15:36:43 2012 from 10.27.164.171
   Luna SA 5.0.1-2 Command Line Shell - Copyright (c) 2001-2010 SafeNet, Inc. All rights reserved.
   [TestLunaSA1] lunash:>
   ```

9. SSH を使用して、HSM サーバ上で次の手順を実行します。

   a. クライアントを HSM サーバに追加します。

   [TestLunaSA1] lunash:>client register -c *hsm_client_name* **-i** *ip_address_of_hsm_client*
   ```
   'client register' successful.     Command Result : 0 (Success)
   ```

   b. 次の手順で、サーバ上で定義されているクライアントをリストし、クライアントが追加されていることを確認します。

   ```
   [TestLunaSA1] lunash:>client list
   registered client 1: cg-nms
   registered client 2: hsm_client_name
   Command Result : 0 (Success)
   ```

   c. クライアントをパーティションに割り当てます。

   [TestLunaSA1] lunash:>client assignPartition -c *hsm_client_name* **-p** *partition_name*
   ```
   'client assignPartition' successful.
   Command Result : 0 (Success)
   ```

   d. HSM からログアウトします。

10. HSM クライアントを実行しているサーバ上で、HSM クライアントのインストールを確認します。

```
vtl verify
The following Luna SA Slots/Partitions were found:
Slot    Serial #    Label
====    ========    =====
1    151285008     TestPart1
```

11. HSM クライアントのインストールが完了したら、テスト スイートの ckdemo を実行します。

```
ckdemo
Ckdemo is the property of SafeNet Inc and is provided to our customers for
diagnostic and development purposes only.  It is not intended for use in
production installations.  Any re-distribution of this program in whole or
in part is a violation of the license agreement.

CrystokiConnect()            (modified on Oct 18 2012 at 20:57:53)

*** CHRYSTOKI DEMO - SIMULATION LAB ***


Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
```

```
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 1

Slots available:
    slot#1 - LunaNet Slot
    slot#2 - Luna UHD Slot
    slot#3 - Luna UHD Slot
    slot#4 - Luna UHD Slot
Select a slot: 1

SO[0] or normal user[1]?

You must enter a number between 0 and 1: 1

Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
```

```
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 3
Security Officer[0]
Crypto-Officer  [1]
Crypto-User     [2]: 1
Enter PIN          : 9JT5-WMYG-E5FE-TExs

Status: Doing great, no errors (CKR_OK)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo
```

```
Enter your choice : 27

Enter handle of object to display (-1 to list available objects) :

You must enter a number between -1 and 10000000: -1

No objects found

Enter handle of object to display (-1 to list available objects) :

You must enter a number between -1 and 10000000:

You must enter a number between -1 and 10000000:

You must enter a number between -1 and 10000000: 0
ERROR: Can not find object with handle 0

Status: C_GetObjectSize returned error. (CKR_OBJECT_HANDLE_INVALID)

TOKEN FUNCTIONS
    ( 1) Open Session  ( 2) Close Session  ( 3) Login
    ( 4) Logout        ( 5) Change PIN     ( 6) Init Token
    ( 7) Init Pin      ( 8) Mechanism List ( 9) Mechanism Info
    (10) Get Info      (11) Slot Info      (12) Token Info
    (13) Session Info  (14) Get Slot List  (15) Wait for Slot Event
                       (18) Factory Reset  (19) CloneMofN
OBJECT MANAGEMENT FUNCTIONS
    (20) Create object (21) Copy object    (22) Destroy object
    (23) Object size   (24) Get attribute  (25) Set attribute
                       (26) Find object    (27) Display Object
SECURITY FUNCTIONS
    (40)  Encrypt file (41) Decrypt file   (42)  Sign
    (43)  Verify       (44) Hash file      (45)  Simple Generate Key
                                           (46)  Digest Key
HIGH AVAILABILITY RECOVERY FUNCTIONS
    (50) HA Init       (51) HA Login
KEY FUNCTIONS
    (60) Wrap key      (61) Unwrap key     (62) Generate random number
    (63) Derive Key    (64) PBE Key Gen    (65) Create known keys
    (66) Seed RNG      (67) EC User Defined Curves
CA FUNCTIONS
    (70) Set Domain    (71) Clone Key      (72) Set MofN
    (73) Generate MofN (74) Activate MofN  (75) Generate Token Keys
    (76) Get Token Cert(77) Sign Token Cert(78) Generate CertCo Cert
    (79) Modify MofN   (86) Dup. MofN Keys (87) Deactivate MofN
    (88) Get Token Certificates     (112) Set Legacy Cloning Domain
OTHERS
    (90) Self Test
    (94) Open Access    (95) Close Access
    (97) Set App ID     (98) Options      (100) LKM Commands
OFFBOARD KEY STORAGE:
   (101) Extract Masked Object            (102) Insert Masked Object
   (103) Multisign With Value             (104) Clone Object
   (105) SIMExtract                       (106) SIMInsert
   (107) SimMultiSign                     (118) Extract Object
                                          (119) Insert Object
SCRIPT EXECUTION:
   (108) Execute Script                   (109) Execute Asynchronous Script
                                          (110) Execute Single Part Script
CLUSTER EXECUTION:
   (111) Get Cluster State
```

```
SRK FUNCTIONS:
   (200) SRK Get State  (201) SRK Restore  (202) SRK Resplit
   (203) SRK Zeroize    (204) SRK Enable/Disable

   (  0) Quit demo

Enter your choice : 0

Exiting GESC SIMULATION LAB
```

HSM HA クライアントの設定

(注) HSM サーバが 1 つのみであっても、この項の手順を実行する必要があります。さらに、HSM サーバを含むグループを作成する必要もあります。

HSM HA クライアントを設定するには、次の手順を実行します。

1. IoT FND サーバ上への HSM クライアントのインストールの説明に従って、HSM クライアントを設定し、両方の HSM サーバと接続するようにします。
2. /usr/safenet/lunaclient/bin/ ディレクトリに移動します。

   /usr/safenet/lunaclient/bin/

3. このコマンドを実行して、最初の HSM サーバのパーティションのみを含むグループを作成します。それからパーティションにアクセスするために、**./vtl verify** コマンド(10)を実行して取得した HSM サーバのシリアル番号(*serial_num*)、グループ名(*group_name*)、およびパスワード(*prtn_password*)を入力します。

   ./vtl haAdmin newGroup -serialNum *serial_num* **-label** *group_name* **-password** *prtn_password*

   次に例を示します。

```
./vtl haAdmin newGroup -serialNum 151285008 -label testGroup1 -password TestPart1

Warning:  There are 2 objects currently on the new member.
          Do you wish to propagate these objects within the HA
          group, or remove them?

          Type 'copy' to keep and propagate the existing
          objects, 'remove' to remove them before continuing,
          or 'quit' to stop adding this new group member.
          > copy

New group with label "testGroup1" created at group number 1151285008.
Group configuration is:

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008
                    Needs sync:  no
```

4. 2 番目の HSM のパーティションをグループに追加します。

次に例を示します。

```
./vtl haAdmin addMember -group testGroup1 -serialNum 151268008 -password TestPart1
Member 151268008 successfully added to group testGroup1. New group
configuration is:

                HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
```

```
                  Group Members:  151285008, 151268008
                     Needs sync:  yes

Please use the command 'vtl haAdmin -synchronize' when
you are ready to replicate data between all members of the
HA group. (If you have additional members to add, you may
wish to wait until you have added them before synchronizing
to save time by avoiding multiple synchronizations.)
```

5. 両方のパーティションをリストできることを確認します。

```
./vtl haAdmin -listGroups

If you would like to see synchronization data for group testGroup1,
please enter the password for the group members. (Press enter to
skip the synchronization check):
> *********

                 HA Group Label:  testGroup1
               HA Group Number:  1151285008
               Synchronization:  enabled
                 Group Members:  151285008, 151268008
                    Needs sync:  yes

          HA auto recovery:  disabled
                HA logging:  disabled
```

6. HA 自動リカバリを有効にします。

```
[root@localhost bin]# ./vtl haAdmin -autoRecovery

vtl haAdmin -autoRecovery [ -retry <count> | -interval <seconds> ] -retry <retry count>
-interval <seconds>
```

   - **retry** 値を -1 ～ 500 の間で設定します。ここで -1 は回数制限なく無限に再試行することを示し、0 は自動再試行を無効にすることを示します。
   - 自動リカバリのポーリング**間隔**を秒単位で指定します。

7. HA を有効にします。

```
./vtl haAdmin -HAOnly -enable
```

HSM のグループ名とパスワードの設定

HSM のグループ名とパスワードは、製造時にシスコにより提供されます。

ユーザが設定した HSM グループ名とパスワードを許可するには、次の手順を実行します。

1. **cgms.properties** ファイルを編集して、次のプロパティを追加します。

- hsm-keystore-name *<name>*
- hsm-keystore-password *<encrypted password>*

ヒント:HSM サーバ上に複数のパーティションを作成し、HSM クライアントを設定し、cgms.properties ファイル内にパーティション名とパーティション パスワードを指定することで、複数の IoT FND インストール システムに対して同じ HSM サーバを使用できます。

2. cgms.properties ファイルを保存します。
3. これらの変更を適用するには、IoT FND を再起動します。

```
service cgms start
```

トンネルのプロビジョニングの管理

ここでは、IoT FND を設定してトンネルのプロビジョニングを行う方法、および FAR（CGR と C800）および HER を接続するトンネルを管理およびモニタする方法について説明します。具体的な内容は、次のとおりです。

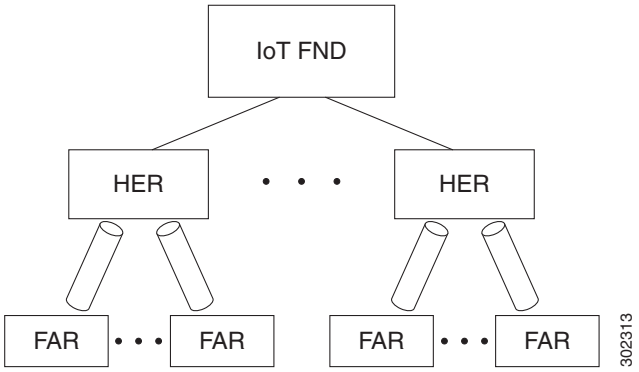
概要

IoT FND は、トンネルのプロビジョニング テンプレートを処理することにより生成されたコマンドを FAR および HER に送信し、その間に安全なトンネルをプロビジョニングします。デフォルトの IoT FND テンプレートには CLI コマンドが含まれ、GRE および IPsec トンネルをセットアップおよび構成します。1 つの HER で、同じ HER EID および名前を持つ複数のトンネルを含む、500 までの FAR を実行できます。

（注）IoT FND リリース 3.1.x を使用して始める場合、ネットワークへの FAR の導入前に、FAR と HER の間に IPSec トンネルのプロビジョニングを設定する必要がなくなります（図 1 に示します）。

代わりに、トンネル プロビジョニング テンプレートに CLI が含まれないようにして設定する、IPSec なしの ZTD を開始できます。工場出荷時の設定なしにネットワークを起動するこの最初のアプローチを実行しても、今後ネットワークで IPSec が使用できなくなるわけではありません。

図 1　トンネルは、FAR とそれに対応する HER を接続します



HER および FAR の間にトンネルをプロビジョニングするため、IoT FND はこれらのデバイスで CLI トンネル設定コマンドを実行します。デフォルトでは、IoT FND は CLI トンネル設定コマンドを含む基本的なトンネル設定テンプレートを提供します。また、お使いのテンプレートを使用することもできます。トンネルのプロビジョニング プロセスは自動ですが、最初にトンネル プロビジョニング設定プロセスに概要が示されている設定手順を実行する必要があります。この後、FAR がオンラインになると必ず、IoT FND により自動的にトンネルでプロビジョニングされます。IoT FND をトンネルのプロビジョニング用に設定する前に、IoT FND TPS プロキシがインストールおよび実行されていることを確認します。

トンネル プロビジョニング設定プロセス

トンネルのプロビジョニングを設定する前に、IoT FND 上にキーストア ファイルおよび TPS プロキシを生成する必要があります。次に、相互に通話するようIoT FNDおよび TPS プロキシを設定します（TPS プロキシの設定およびTPS プロキシを使用するための IoT FND の設定）

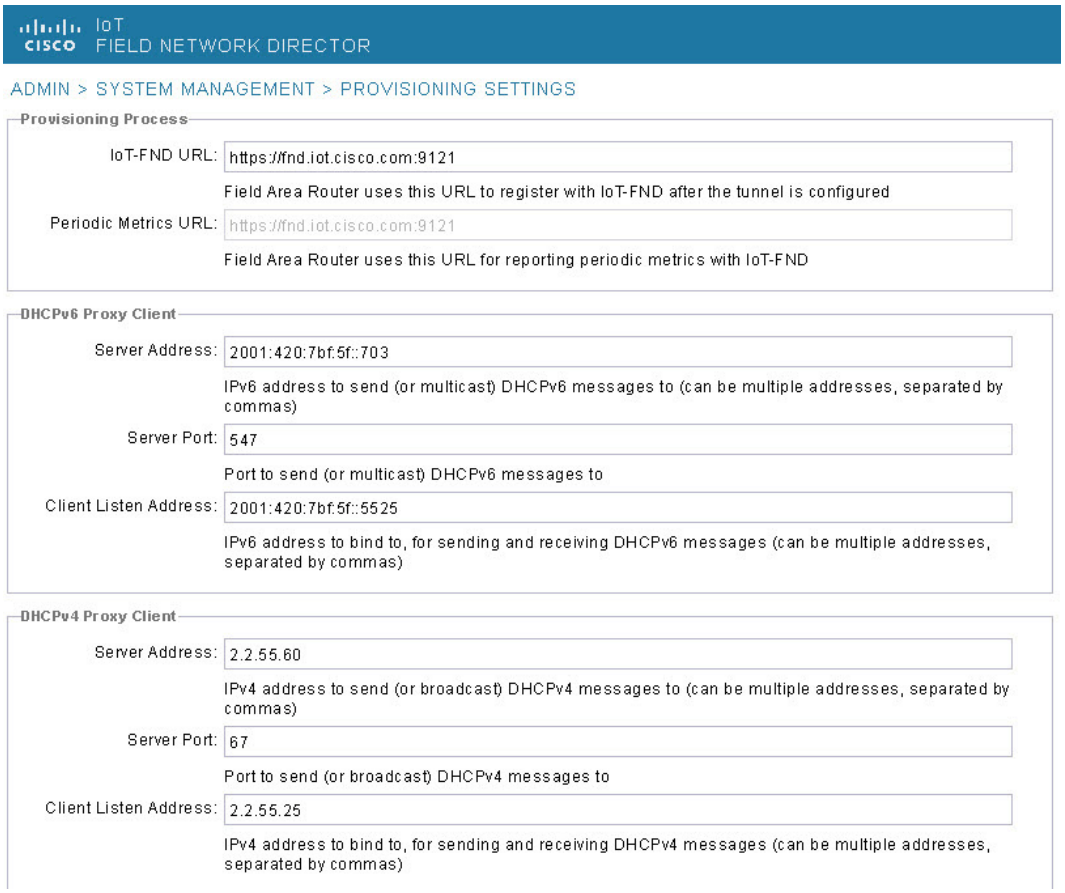
IoT FND を設定してトンネル プロビジョニングを行うには、次の手順を実行します。

		備考
1.	（CG-OS CGR）DHCP サーバを設定します。 DHCP サーバを設定して IoT FND に一意の IP アドレスを提供します。デフォルトの IoT FND トンネル プロビジョニング テンプレートにより、トンネルを作成するために必要なループバック インターフェイスと IP アドレスが設定されます。 Cisco IOS CGR は FlexVPN を使用します。テンプレートに含まれるのがループバック インターフェイスのアドレスのみであることを確認します。	DHCP サーバーにトンネル プロビジョニングを設定。
2.	トンネル設定を行います。 IoT FND のプロビジョニング設定ページで NMS URL と DHCP プロキシ クライアントの設定を行います（[Admin] > [System Management] >[Provisioning Settings]）。	詳細については、「Cisco IoT Field Network Director, Release 4.0.x」の『Managing System Settings』の章を参照してください。
3.	（CG-OS CGR）FAR 登録要求を最初のコンタクト（*call home*）で受け入れるように IoT FND を設定してトンネルのプロビジョニングを要求します。 Cisco IOS CGR は CGNA サービスを利用します。	
4.	HER 管理を設定します。 SSH で NETCONF を使用した IoT FND による管理を行うため HER を設定します。	IoT FND へ追加する前の HER の設定。 詳細については、「Cisco IoT Field Network Director, Release 4.0.x」の『Managing Devices』の章を参照してください。
5.	HER を IoT FND に追加します。	IoT FND に HER を追加します。 詳細については、「Cisco IoT Field Network Director, Release 4.0.x」の『Managing Devices』の章を参照してください。
6.	IoT FND トンネル プロビジョニング テンプレートを確認して、正しいタイプのトンネルを作成していることを確認します。	
7.	（任意）トンネルのプロビジョニングに独自のテンプレートを使用する場合、1 つ以上のトンネルプロビジョニング グループを作成して、デフォルトのトンネル プロビジョニング テンプレートを変更します。	トンネル プロビジョニング テンプレートの設定
8.	（CG-OS CGR）Call Home を発信するため FAR を設定します。 FAR が IoT FND TPS プロキシを通じて HTTPS で IoT FND に連絡するように設定します。	この手順は通常、FAR が TPS プロキシに連絡するよう設定されている工場で実行されます。
9.	FAR を IoT FND に追加します。 出荷通知 XML ファイルを使用して FAR を IoT FND にインポートします。	
10.	FAR を対応する HER にマッピングします。	トンネル プロビジョニング設定プロセス

以上の手順を完了した後、FAR を展開し、電源を入れます。トンネルのプロビジョニングが自動的に行われます。

以下は、FAR をオンにした後のイベントのシーケンスです。

1. FAR がオンになり、アップリンク ネットワークに接続すると、証明書の登録のリクエストを送信します。
2. その後、IoT FND TPS プロキシによって IoT FND にトンネルのプロビジョニングを要求します。
3. IoT FND は IoT FND データベースの FAR レコードを調べ、使用するトンネル プロビジョニング テンプレートを決定します。IoT FND は、トンネルを確立するため HER の経路を調べます。
4. Cisco IOS CGR では、デフォルトのテンプレートは FlexVPN を使用するよう CGR を設定します。FlexVPN クライアントが CGR に設定され、CGR は HER に連絡して FlexVPN トンネルが動的に構築されるよう要求します。以上が、HER が CGR の新しいトンネル エンドポイント インターフェイスを動的に追加する方法です。
5. FAR のテンプレートを処理する前に、IoT FND は HER トンネル削除テンプレートを処理し、その結果であるコマンドを HER に送信します。これは、各 HER に対して行われ、FAR に関連付けられている可能性がある既存のトンネル設定を削除します。
6. IoT FND は FreeMarker テンプレート エンジンを使用して、FAR トンネル追加テンプレートを処理します。エンジンはテンプレートを IoT FND により CLI 設定コマンドと仮定されるテキストに変換します（CGR ごとに CG-OS または Cisco IOS）。IoT FND はこれらのコマンドを使用して、FAR にトンネルの一端を設定し、立ち上げます。
7. IoT FND は FreeMarker テンプレート エンジンを使用して、HER トンネル追加テンプレートを処理します。エンジンはテンプレートを、IoT FND により HER のトンネル設定のためのコマンドと仮定されるテキストに変換します。
8. この手順は OS に固有のものです。
   - Cisco IOS CGR では、テンプレートにより生成されたコマンドを FAR と HER に適用してエラーが起きなければ、IoT FND は新しくアクティブな CGNA プロファイル「cg-nms-register」を設定し、「cg-nms-tunnel」プロファイルを無効にします。Cg-nms-register プロファイルは、IoT FND URL を使用します。
   - CG-OS CGR では、IoT FND は Call Home URL をプロビジョニング設定ページ（[ADMIN] > [System Management] > [Provisioning Settings]）で指定される IoT FND URL に再設定します。



指定された URL は、トンネル プロビジョニング ポートの代わりに IoT FND の登録ポート（デフォルトで 9121）を使用します。この URL の 完全修飾ドメイン名（FQDN）は異なっており、トンネル経由でのみ到達可能な IP アドレスに解決します。

トンネル プロビジョニングの設定

ここでは、トンネル プロビジョニング用に IoT FND を設定する方法について説明します。

- DHCP サーバーにトンネル プロビジョニングを設定
- CNR を使用したトンネルのプロビジョニング用 DHCP 設定

DHCP サーバーにトンネル プロビジョニングを設定

トンネルのプロビジョニングを成功させるには、IoT FND によって使用される DHCP サーバーを設定し、アドレスを指定して FAR と HER の間にトンネルを作ります。たとえば、パーマネント リースの原則に基づき、DHCP サーバを設定して、トンネルのプロビジョニングに IP アドレスを提供します。

IoT FND はトンネル プロビジョニング テンプレートで定義された設定に基づいて DHCP 要求を行います。トンネルのプロビジョニングの間、IoT FND テンプレートは 2 種類の DHCP 要求を行うことができます。

- IP アドレスを要求した後、テンプレートで使用可能にします。
- 2 つの IP アドレスのサブネットを要求し、両方のアドレスをテンプレートで使用可能にします。

IoT FND は これらの要求を IPv4 アドレス、IPv6 アドレス用に行うことができます。

テンプレートから DHCP アドレスを要求する機能は、トンネルの設定を定義する際の柔軟性を最大に高めます。各 FAR および対応する HER のインターフェイスに必要な正確なアドレスを割り当てるためです。提供されるデフォルトのトンネル プロビジョニング テンプレートは、最も一般的な使用法の例、FAR とそれに対応する HER の間の 1 つの IPsec トンネルを定義します。この IPsec トンネルの両端が、動的に割り当てられた IPv4 アドレスを取得します。

- ご使用の DHCP サーバがサブネットの割り当てをサポートしている場合、同じサブネットに属する 2 つのアドレスを取得するためにこれを使用します。
- ご使用の DHCP サーバが、アドレスの割り当てのみをサポートしている場合、2 つの DHCP アドレスが IPsec トンネルの両端として使用できるリターン アドレスを要求するように設定します。
- ルーティング プランが、各 FAR に一意の IPv4 アドレスを割り当て、それを、IPsec トンネル上のループバック インターフェイスに割り当てる必要がある場合、IoT FND テンプレートを使用してこのアドレスを割り当てます。

IPv6 GRE トンネルを作成することを選択する場合、DHCP プレフィックス委任または個々のアドレス要求を使用して、トンネルの両端に IPv6 アドレスを割り当てます。

ここでは、トンネルのプロビジョニングの DHCP 設定例について説明します。これらの設定の設定方法は、ご使用の装置によって異なります。この項では、Cisco Network Registrar（CNR）を使用してトンネルのプロビジョニング向けに DHCP サーバを設定するための一般的な注意事項を説明します。

CNR を使用したトンネルのプロビジョニング用 DHCP 設定

次にあげる CNR の CLI スクリプト例は、IoT FND のデフォルトのトンネル プロビジョニング テンプレートから発信したリクエストを処理するよう、CNR DHCP サーバを設定します。このスクリプトを使用する際は、サブネットがご使用の DHCP サーバ環境に適していることを確認してください。

CNR DHCP サーバ のトンネル プロビジョニング スクリプト例

```
# These commented out commands support re-applying the configuration by first
# removing any previously applied configuration, in reverse order. This should
# not be done in a production environment, but may be useful when initially
# developing and testing a configuration.

# scope v4address-perm delete
# dhcp-address-block v4subnet-perm delete
# prefix v6subnet-perm delete
# prefix v6address-perm delete
# policy permanent delete

# Configure the server to automatically map any IPv4 or IPv6 user class
# option values to selection tags. By default CG-NMS includes a value of
# "CG-NMS" for the user class in its requests. The tag is used to insure
# prefixes and scopes configured to satisfy requests from CG-NMS are only
# used for that purpose.

dhcp set map-user-class-id=append-to-tags

# Since CG-NMS uses the leased addresses and subnets in router
# configuration the addresses and subnets must be permanently allocated
# for that purpose. Create a policy that instructs the DHCP server to
# offer a permanent lease.

policy permanent create
policy permanent set permanent-leases=enabled

# Configure DHCPv6.

# The default CG-NMS tunnel template will request IPv6 addresses for
# use with CGR loopback interfaces.
```

```
prefix v6address-perm create 2001:DB8:0:0:1::/80 dhcp-type=dhcp
prefix v6address-perm set description="Pool for leasing addresses for loopback interfaces."
prefix v6address-perm set policy=permanent
prefix v6address-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv6 prefixes for
# use with GRE tunnels. Force use of a /127 prefix.

prefix v6subnet-perm create 2001:DB8:0:0:2::/80 dhcp-type=prefix-delegation
prefix v6subnet-perm set description="Pool for leasing prefixes for GRE tunnels."
prefix v6subnet-perm set policy=permanent
prefix v6subnet-perm set selection-tags=CG-NMS
prefix-policy v6subnet-perm set default-prefix-length=127
prefix-policy v6subnet-perm set shortest-prefix-length=127

# Configure DHCPv4.

# The default CG-NMS tunnel template will request IPv4 subnets for
# use with IPsec tunnels. Note that currently address pools for
# IPv4 subnet allocation can only be configured using the CLI as the
# CNR Web UI does not currently support them.

# If CNR allowed you to set a description on DHCP address blocks it would be:
# "Pool for leasing subnets for IPsec tunnels."

dhcp-address-block v4subnet-perm create 192.0.2.0/24
dhcp-address-block v4subnet-perm set default-subnet-size=31
dhcp-address-block v4subnet-perm set policy=permanent
dhcp-address-block v4subnet-perm set selection-tags=CG-NMS

# The default CG-NMS tunnel template will request IPv4 addresses for
# use with loopback interfaces.

scope v4address-perm create 198.51.100.0 255.255.255.0
scope v4address-perm set description="Pool for leasing addresses for loopback interfaces."
scope v4address-perm set policy=permanent
scope v4address-perm addRange 198.51.100.2 198.51.100.254
scope v4address-perm set selection-tag-list=CG-NMS

# Configure detailed logging of incoming and outgoing packets. This is useful when
# debugging issues involving DHCP, however this level of logging will lower the
# performance of the DHCP server. If this is a production server under heavy load
# it may be necessary to forgo detailed packet logging.

dhcp set
log-settings=missing-options,incoming-packet-detail,outgoing-packet-detail,unknown-criteria,client-deta
il,client-criteria-processing,dropped-waiting-packets,v6-lease-detail

# Save the changes and reload the server to have them take effect.
save
dhcp reload

# List the current configuration.

policy list
prefix list
dhcp-address-block list
scope list
dhcp show
```

トンネル グループ 設定の構成

FAR のトンネル プロビジョニングを一括で設定するには、IoT FND でグループを使用します。デフォルトでは、すべての FAR が IoT FND に追加されます。(「*Cisco IoT Field Network Director User Guide, 4.0x*」の『Device Management』の章で、「Adding Devices in Bulk in the Performing Bulk Import Actions」セクションを参照してください。

Release 3.2.x) 適切なデフォルト グループは、**default-cgr1000** または **default-c800** です。デフォルト グループには、IoT FND がトンネルのプロビジョニングに使用する 3 つのテンプレートが含まれています。

ここでは、次の内容を説明します。

トンネル グループの作成

すべての FAR に 1 組のテンプレートの使用を予定している場合、使用するのがデフォルトのテンプレート、修正されたデフォルトのテンプレート、またはカスタム テンプレートのいずれであっても、追加のグループは作成しないでください。複数組のテンプレートを定義するには、グループを作成し、それらのグループのテンプレートをカスタマイズします。

(注) ご使用のカスタム テンプレートが両方のルータのタイプに適用可能な場合、CGR と C800 を同じトンネル プロビジョニング グループに入れることができます。

トンネル グループを作成する方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. 左ペインの [+] アイコンをクリックして、グループを追加します。
3. 新しいグループの名前を入力し、[OK] をクリックします。

   グループが [Tunnel Groups] ペインに表示されます。

トンネル グループを作成した後、FAR の別のグループへの移動に示すように、他のグループから FAR を移動します。

トンネル グループの削除

空白のグループのみが削除できます。トンネル グループを削除するには、そこに含まれているデバイスを他のグループに移動する必要があります。

空白のトンネル グループを削除する方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] 左ペインで、削除するトンネル グループを選択します。
3. (−)をクリックしてグループを削除します。
4. [Yes] をクリックして削除の確認を行います。

トンネル グループの表示

トンネルのプロビジョニング ページでは、既存のトンネル グループに関する情報を一覧表示します。

IoT FND に定義されたトンネル グループを表示するには、次の手順を実行します。

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [Group Members] タブをクリックします。
3. [TUNNEL GROUPS] ペイン（左）で、グループを選択します。

IoT FND は、グループ内の各ルータに関して、次のトンネル グループ情報を表示します。必ずしもすべてのルータで全フィールドがサポートされているわけではありません。（表 1 を参照）。

表 1　トンネル グループ フィールド

フィールド	説明
Name	ルータ EID（デバイス ID）。
Status	ルータのステータス： ■ Unheard：ルータはまだ IoT FND にコンタクトしていません。 ■ Unsupported：FAR は IoT FND ではサポートされていません。 ■ Up：ルータが稼働しています。 ■ Down：ルータはオフになっています。
Last Heard	ルータが IoT FND に最後にコンタクトした、またはメトリックを送信した時間。ルータが IoT FND にコンタクトしていなければ、このフィールドに **never** が表示されます。そうでない場合、IoT FND は最後のコンタクトの日時、たとえば **4/10 19:06** を表示します。
Tunnel Source Interface 1 Tunnel Source Interface 2	トンネルで使用されているルータ インターフェイス。
OSPF Area 1 OSPF Area 2	Open Shortest Path First（OSPF）のエリア 1 および 2。
OSPFv3 Area 1 OSPFv3 Area 1	OSPFv3 のエリア 1。 OSPFv3 のエリア 2。
IPsec Dest Addr 1 IPsec Dest Addr 2	トンネルの IPv4 宛先アドレス。
GRE Tunnel Dest Addr 1 GRE Tunnel Dest Addr 2	IPv6 宛先アドレス。
Certificate Issuer Common Name	証明書を発行した CA の名前。

トンネル グループの名前の変更

トンネル グループの名前はいつでも変更できます。シスコでは、短くわかりやすい名前を使用することをお勧めしています。名前は 250 文字以内である必要があります。

トンネル グループの名前を変更する方法：

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、名前を変更するトンネル グループをロールオーバーして、[Edit] の鉛筆のアイコン（ ）をクリックします。

3. 新しいグループ名を入力して [OK] をクリックします。

   (注) 無効な文字(@、#、!、+ など)が入力された入力フィールドは赤色で強調表示され、[OK] ボタンが使用できなくなります。

FAR の別のグループへの移動

FAR を別のグループに移動するには、次の 2 つの方法があります。

- FAR を手動で別のグループに移動
- FAR を一括で別のグループに移動

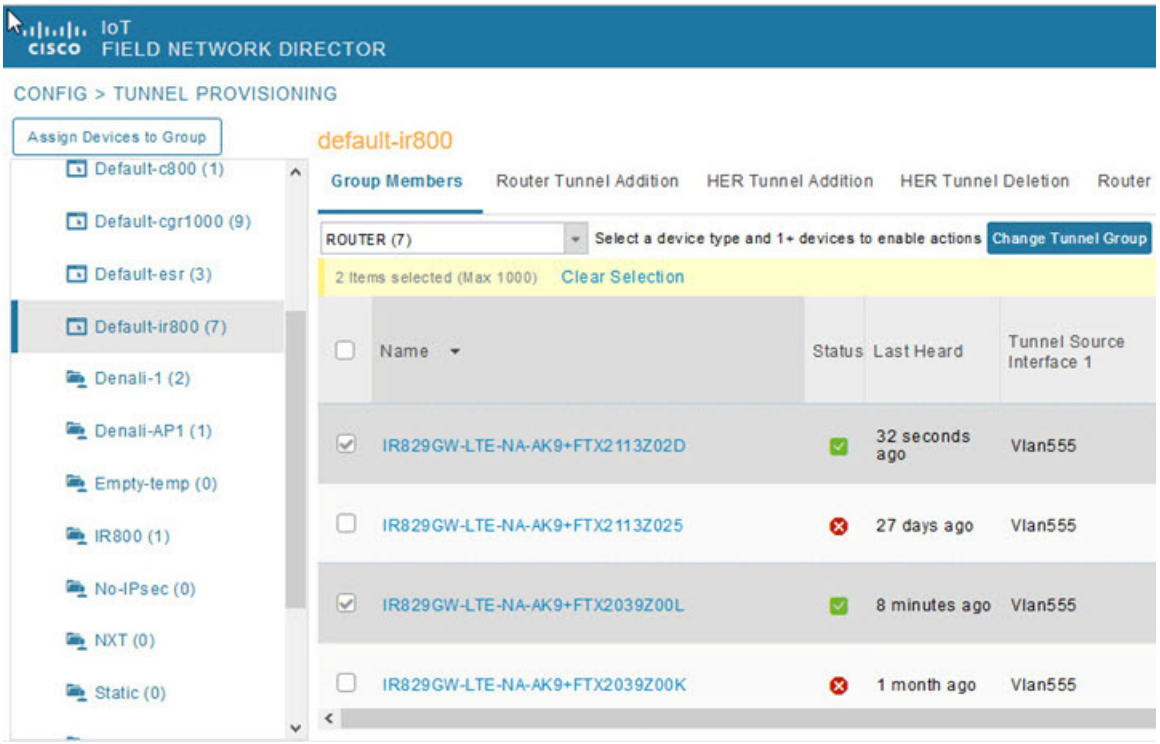
FAR を手動で別のグループに移動

FAR を手動で別のグループに移動する方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [Group Members] タブをクリックします。
3. [TUNNEL GROUPS] ペインで、移動するトンネル グループとルータを選択します。
4. [Select a device type] ドロップダウン メニューから、デバイスのタイプを選択します。
5. 移動する FAR のチェック ボックスにチェックを入れます。

   グループ内のすべての FAR を選択するには、カラムの一番上にあるチェック ボックスをクリックします。デバイスを選択すると、選択されたデバイスの数を表示し、[Clear Selection] と [Select All] のコマンドがある黄色いバーが表示されます。選択できるデバイスの最大数は 1000 です。

6. [Change Tunnel Group] ボタンをクリックします。



7. ドロップダウン メニューから、FAR の移動先のトンネル グループを選択します。
8. [Change Tunnel Group] をクリックします。
9. [OK] をクリックして、ダイアログボックスを閉じます。

FAR を一括で別のグループに移動

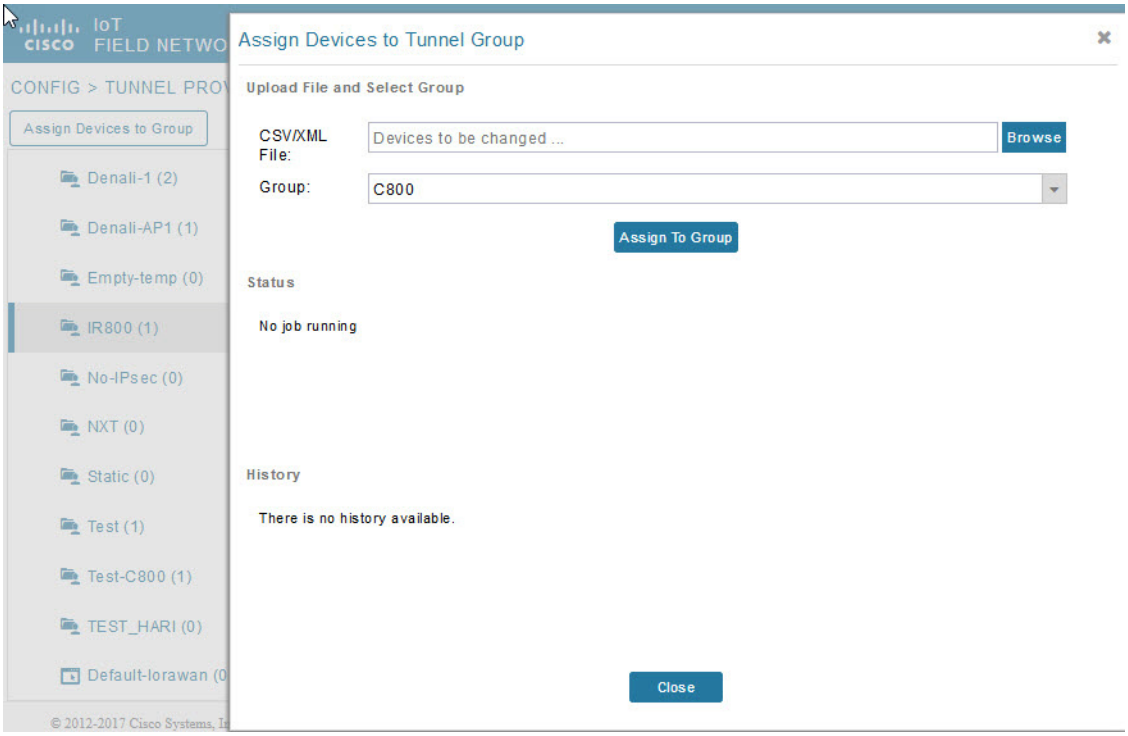
移動する FAR の名前を含む CSV または XML ファイルをインポートすることで、FAR を一括で別のグループに移動できます。エントリが、次にあげるフォーマットでファイルに含まれていることを確認してください。

```
eid
CGR1120/k9+JSM1
CGR1120/k9+JSM2
CGR1120/k9+JSM3
CGR1120/k9+JSM4
C819HGW-S-A-K9+FTX174685V0
```

最初の行はヘッダーで、残りの行に FAR EID が入ることを IoT FND に 伝えます(1 行あたり FAR EID 1 つ)。

FAR を一括で別のグループに移動する方法:

1. 異なるグループに移動するデバイスの EID を 含む CSV または XML ファイルを作成します。
2. [CONFIG] > [Tunnel Provisioning] の順に選択します。
3. [Assign Devices to Tunnel Group] をクリックして、入力パネルを開きます。



4. [Browse] をクリックし、移動する FAR が含まれるファイルを検索します。
5. [Group] ドロップダウン メニューから、移動先のトンネル グループを選択します。
6. [Assign To Group] をクリックします。
7. [Close] をクリックします。

トンネル プロビジョニング テンプレートの設定

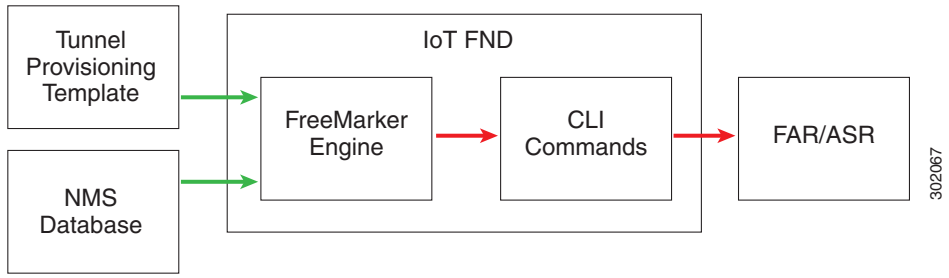
IoT FND には、デフォルトのトンネル プロビジョニング テンプレートが 3 つ含まれています。

- フィールド エリア ルータ トンネル追加：IoT FND はこのテンプレートを使用して FAR 上の IPsec トンネルの一端を作成するための CLI 設定コマンドを生成します。
- ヘッドエンド ルータ トンネル追加：IoT FND はこのテンプレートを使用して HER 上の IPsec トンネルの反対の端を作成するための CLI 設定コマンドを生成します。
- ヘッドエンド ルータ トンネル削除：IoT FND はこのテンプレートを使用して、トンネルの反対側にある FAR への既存のトンネルを削除するための CLI 設定コマンドを生成します。

トンネル プロビジョニング テンプレートのシンタックス

IoT FND のトンネル プロビジョニング テンプレートは FreeMarker のシンタックスで表されます。FreeMarker は、テンプレートを処理するための Java ベース オープン ソース エンジンで、IoT FND に組み込まれています。図 2 に示すとおり、FreeMarker は、入力として トンネル プロビジョニング テンプレートおよび IoT FND より提供されるデータを取得し、IoT FND が「configure terminal」コンテキストにおいて FAR と HER 上で実行する CLI コマンドを生成します。

図 2　IoT FND のテンプレートからの CLI コマンド生成



IoT FND では、トンネル プロビジョニング テンプレートはルータ CLI コマンド、FreeMarker の変数およびディレクティブで構成されています。FreeMarker のシンタックスを使用することにより、IoT FND は 1 つのテンプレートを定義して複数のルータをプロビジョニングすることができます。

ここでは、トンネル プロビジョニング テンプレートにおける FreeMarker の基本的なシンタックスについて説明します。FreeMarker について詳しくは、http://freemarker.sourceforge.net/ にアクセスしてください。

- テンプレートのシンタックス
- データ モデル

テンプレートのシンタックス

表 2 で、デフォルトのトンネル プロビジョニング テンプレートにおけるシンタックスについて説明します。

表 2　トンネル プロビジョニング テンプレートのシンタックス

コンポーネント	説明
テキスト	標識のないテキストは FAR の CG-OS CLI 設定コマンド、HER の Cisco IOS CLI コマンドとして転送されます。
挿入	${variable} FreeMarker は、IoT FND によって提供される文字列変数の値とこの構成を置き換えます。この例では、IoT FNDは FAR の EID を提供します。 `description IPsec tunnel to ${far.eid}`
デフォルト値	${variable!" Default" } FreeMarker はこの構成を文字列変数の値で置き換えます。変数を設定しないと、FreeMarker は、この構成を **Default** で置き換えます。

表 2　トンネル プロビジョニング テンプレートのシンタックス（続き）

コンポーネント	説明

条件	<#if condition> output1 <#else> output2 </#if>
	
	FreeMarker は出力で使用するテキストを決定するためにこの構成を使用します。次に例を示します。
	
	`<#if far.ipsecTunnelDestAddr1??>`
	`  <#assign destinationAddress=far.ipsecTunnelDestAddr1>`
	`<#else>`
	`  <#assign destinationAddress=`
	`her.interfaces("GigabitEthernet0/0/0")[0].v4.addresses[0].address>`
	`</#if>`

リスト上の反復	<#list list as variable> ${variable} </#list> FreeMarker はリスト上の反復にこの構造を使用します。
注	<#-- this is a comment --> FreeMarker ではコメントができますが、出力には保持されません。

ステートメントの指定	<#assign name=value>
	
	この構造は、テンプレート内のローカル変数を宣言し、それに値を割り当てます。その後、変数を参照するのにこの構成を使用します。
	
	${name}
	
	次に例を示します。
	
	`<#assign interfaceNumber=0>`
	`...`
	`interface Tunnel${interfaceNumber}`

マクロ	これらの構成は関数呼出しに似ています。
	
	<#macro name(param1,param2, ... ,paramN)>
	
	... ${param1} ...
	
	</#macro>
	
	以下は、マクロ定義の例です。
	
	`<#macro configureTunnel(interfaceNamePrefix,ospfCost)>`
	`  <#assign wanInterface=far.interfaces(interfaceNamePrefix)>`
	`  <#if (wanInterface[0].v4.addresses[0].address)??>`
	`  <#assign interfaceName=wanInterface[0].name>`
	`  interface Tunnel${her.unusedInterfaceNumber()}`
	`  description IPsec tunnel to ${far.eid}`
	`  ...`
	`  ip ospf cost ${ospfCost}`
	`  ...`
	`</#macro>`

マクロ呼出し	トンネル プロビジョニング テンプレートでマクロを呼び出す方法: <@name param1, param2 ... paramN> FreeMarker は、すべての変数を解決した後、マクロ呼出しをマクロの出力と置き換えます。 次に例を示します。 `<@configureTunnel far.tunnelSrcInterface1!"Wimax", 100/>`

データ モデル

ここでは、トンネル プロビジョニング テンプレートにおけるデータ モデルについて説明します。**far** および **her** のプレフィックスはそれぞれ、FAR および HER のプロパティへのアクセスを提供します。これらのプロパティは IoT FND のデータベースに保存されています。表 3 では、トンネル プロビジョニング テンプレートのデータ モデルによって提供される情報の参照を示します。

表 3　データ モデル

プロパティ	説明
far.eid	FAR の EID を返します。次に例を示します。 `${far.eid}`
far.hostname	FAR のホスト名を返します。
far.tunnelSrcInterface1	トンネルを確立する FAR のインターフェイスの名前を返します。
far.ipsecTunnelDestAddr1	HER 上のトンネル宛先 IP アドレスの名前を返します。

far.ipv4Address(*clientId*, *linkAddress*, *userClass*)	IPv4 アドレスを返します。IPv4 アドレス メソッドはこれらのパラメータを入力として受け取ります。
	
	■ clientId：DHCP 要求の DCHP クライアント ID
	
	■ linkAddress：DHCP 要求のリンク アドレス
	
	■ userClass：DHCP ユーザー クラス オプション（デフォルトの「CG-NMS」）の値
	
	ループバック インターフェイスを確立し、それにアドレスを割り当てるには：
	
	`interface Loopback0`
	`ip address ${far.ipv4Address(dhcpClientId(far.enDuid, 0), far.dhcpV4LoopbackLink).address}/32`
	`ipv6 address ${far.ipv6Address(far.enDuid, 0, far.dhcpV6LoopbackLink).address}/128`
	`exit`

far.ipv4Subnet()	DHCP IPv4 サブネット リースを返します。このコールは引数として clientId と linkAddress を取得します。 テンプレート API で提供される dhcpClientId() メソッドを使用して、FAR EID およびインターフェイス ID 番号から clientId を組み立てます。この方法では、入力として DHCPv6 アイデンティティ アソシエーション ID（IAID）および DHCP 固有 ID（DUID）を取得し、RFC 4361 に指定されるとおり DHCPv4 クライアント ID を生成します。この方法は、ネットワーク要素が DHCP サーバにより識別される方法に一貫性を与えます。 次に例を示します。 `<#assign lease=far.ipv4Subnet(dhcpClientId(far.enDuid,iaId), far.dhcpV4TunnelLink)>`
far.[any device property]	指定されたプロパティの値を返します。 たとえば、far.tunnelSrcInterface1 は FAR の tunnelSrcInterface1 プロパティの値を返します。

表 3　データ モデル(続き)

プロパティ	説明

far.interfaces(interfaceNamePrefix)	そのプレフィックスをもつデバイスから検出されたインターフェイスのリストを返します(大文字と小文字の区別なし)。
	
	インデックス リストのメンバーには角カッコ、たとえば [0] [1] [2] を使用します。リストのメンバーを繰り返すには、**<#list>**構成を使用します。
	
	次に例を示します。
	
	`<#assign wanInterface = far.interfaces(interfaceNamePrefix)>`
	`  <#if (wanInterface[0].v4.addresses[0].address)??>`
	`...`

アドレス

表 4 で、トンネル プロビジョニング テンプレートで参照するアドレスを示します。

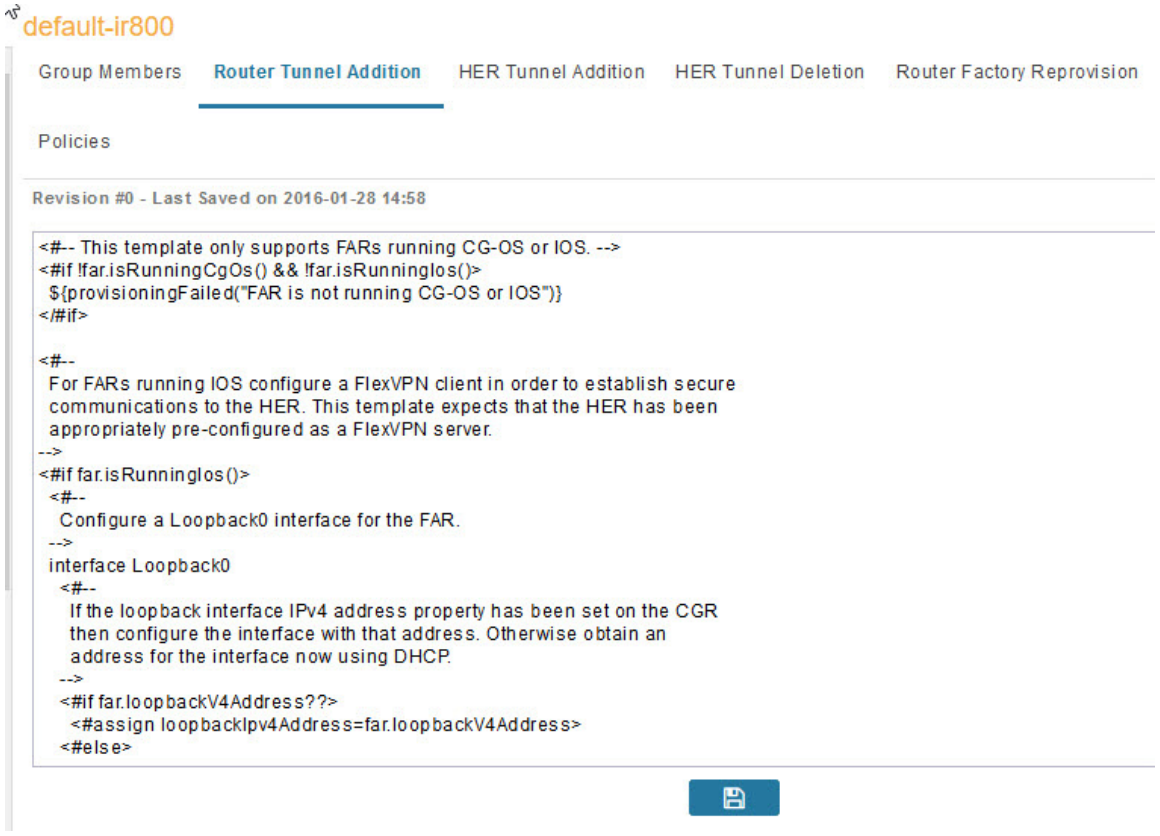
表 4　参照アドレス

プロパティ	説明
address.address	インターフェイスのアドレスを返します。
address.prefixLength	アドレスのプレフィックス長が返されます。
address.prefix	アドレス プレフィックスを返します。
address.subnetMask	アドレスのサブネット マスクを返します。
address.wildcardMask	サブネットのワイルドカード マスクを返します。

フィールド エリア ルータ トンネル追加テンプレートの設定

FAR トンネル追加テンプレートを編集して、グループ内の FAR に IPsec トンネルの一方の端を作る方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、編集するテンプレートのあるトンネル グループを選択します。
3. [Router Tunnel Addition] タブをクリックします。



4. デフォルトのテンプレートを変更します。

   ヒント:テンプレートを変更するには、テキスト エディタを使用し、テキストを IoT FND のテンプレート フィールドにコピーします。

5. ディスク アイコンをクリックして変更内容を保存します。

6. [OK] をクリックして、変更内容を確定します。

トンネル プロビジョニング テンプレートのシンタックスも参照してください。

ヘッドエンド ルータ トンネル追加テンプレートの設定

(注)両エンドポイントが一致するサブネットにあることを確認するには、このテンプレートで FAR テンプレートと同じ IAID を使用する必要があります。

HER トンネル追加テンプレートを編集して、グループ内の HER に IPsec の反対側の端を作成する方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。

2. [TUNNEL GROUPS] ペインで、トンネル グループを選択します。

3. [HER Tunnel Addition] タブをクリックします。

4. デフォルトの HER 追加テンプレートを変更します。

5. ディスク アイコンをクリックして変更内容を保存します。

6. [OK] をクリックして、変更内容を確定します。

HER トンネル削除テンプレートの設定

HER トンネル削除テンプレートを編集して、トンネルの反対側にある FAR への既存のトンネルを削除する方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、テンプレートを編集するトンネル グループを選択します。
3. [HER Tunnel Deletion] タブをクリックします。
4. デフォルトの HER 削除テンプレートを変更します。
5. ディスク アイコンをクリックして変更内容を保存します。
6. [OK] をクリックして、変更内容を確定します。

トンネル ステータスのモニタリング

トンネルのステータスを表示するには、[OPERATIONS] > [Tunnel Status] の順に選択します。トンネル ステータスのページには、デバイスおよびプロビジョニングされたトンネルの一覧を表示し、トンネルおよびステータスに関する関連情報が表示されます。トンネルは HER と FAR の間にプロビジョニングされます。

ページ上部の [Show Filter] を選択する(選択することで [Hide Filter] に置き換えられます)と、いくつかの検索フィールドが表示されます。表 5 に記載されているすべてのフィールド名でフィルタリングできます。1 つの検索フィールドに値を入力すると、使用できる他のフィールドが選択されます。検索フィールドを削除するには、[Hide Filter] を選択します。

表 5 で、トンネル ステータス フィールドを示します。リスト内のトンネルのソート順序を名前で変更するには、[HER Name] カラムのヘッダーをクリックします。ヘッダーの横の小さな矢印がソート順を示します。

(注)新しく作成されたトンネルのステータスが IoT FND に反映されるには時間がかかります。

表 5　トンネル ステータス フィールド

フィールド	説明
HER Name	トンネルの一方の端の HER の EID。HER の詳細を表示するには、その EID をクリックします。 (注)HER は 1 つが最大 500 の FAR を実行できるため、同じ HER EID をもつ複数のトンネルがリストにある可能性があります。 [Device Info] ページの [Network Interfaces] 領域には、HER に設定されたトンネルのリストが表示されます。[Config Properties] と [Running Config] タブには、この HER に設定されているトンネルに関する情報も含まれています。
HER Interface	HER トンネル インターフェイスの名前。これらの名前は、トンネル作成時に(Tunnel1、Tunnel2、Tunnel3、あるいは Virtual-Interface1、Virtual-Interface 2 のように)自動的に作成されます。
Admin Status	トンネルの管理ステータス([up] または [down])。これにより、管理者がトンネルを有効化または無効化したかが示されます。
Oper.Status	トンネルの動作ステータス([up] または [down])。トンネルがダウンであれば、トラフィックは、トラブルシュートに問題を表示しているトンネルを通過しません。HER および FAR に ping を行ってオンラインであるか判断するか、SSH を介してルータにログインし、問題の原因を判断します。
Protocol	トンネルに使用されるプロトコル(IPSEC、PIM、GRE)。
HER Tunnel IP Address	HER 側のトンネルの IP アドレス。使用されるプロトコルにより、IP アドレスがドット付き 10 進法(IPv4)または 16 進法(IPv6)スラッシュ表記で表示されます。
HER IP Address	HER 側のトンネルの宛先 IP アドレス。
FAR IP Address	FAR 側のトンネルの宛先 IP アドレス。

表 5　トンネル ステータス フィールド（続き）

フィールド	説明
FAR Interface	トンネルによって使用される FAR インターフェイスの名前。
FAR Tunnel IP Address	FAR 側のトンネルの IP アドレス。 (注) トンネルの両端の IP アドレスは同じサブネット上にあります。
FAR Name	FAR の EID。FAR の詳細を表示するには、その EID をクリックします。 [Device Info] ページの [Network Interfaces] 領域には、FAR に設定されたトンネルのリストが表示されます。[Config Properties] と [Running Config] タブには、この FAR に設定されているトンネルに関する情報も含まれています。

CGR のプロビジョニング

IoT FND では、CGR 再プロビジョニングは CGR の設定ファイルを変更するプロセスです。

- CGR 再プロビジョニングの基本
- トンネル再プロビジョニング
- 出荷時再プロビジョニング

(注) C800 は再プロビジョニングをサポートしていません。

CGR 再プロビジョニングの基本

- CGR 再プロビジョニングのアクション
- CGR 再プロビジョニングのシーケンス

CGR 再プロビジョニングのアクション

IoT FND では、[Tunnel Provisioning] ページの [Reprovisioning Actions] ペインで以下の 2 つの CGR 再プロビジョニング アクションを実行できます（[CONFIG] > [Tunnel Provisioning] > [Reprovisioning Actions]）。メッシュ ファームウェアを有効化することもできます

再プロビジョニング アクション	説明
出荷時再プロビジョニング	ドロップダウン メニューでは、工場出荷時設定で CGR に読み込まれた express-setup-config ファイルを変更することができます。 このファイルには、最小限の情報セットが含まれており、出荷時に CGR にロードされます。このファイルは、CGR が展開されて電源がオンになった後、TPS プロキシ経由で IoT FND にコンタクト（Call Home）するための情報を提供します。
トンネル再プロビジョニング	ドロップダウン メニューでは、CGR の golden-config ファイルを変更することができます。このファイルには CGR に定義されたトンネル構成があります。
メッシュ ファームウェアの有効化	ドロップダウン メニューでは、インターフェイス（携帯電話、イーサネットなど）とインターフェイス タイプ（IPv6 または IPv4）を選択できます。

表 6 で、[Reprovisioning Actions] ペインのフィールドについて説明します。

表 6　[Reprovisioning Actions] ペインのフィールド

フィールド	説明
Current Action	現在実行されている再プロビジョニング アクションと、関連するインターフェイス。
Reprovisioning Status	再プロビジョニング アクションのステータス。
Completed devices /All Scheduled Devices	プロセスがスケジュール設定されたすべての CGR の数に対し、処理された CGR の数。
Error devices/ All Scheduled Devices	プロセスがスケジュール設定されたすべての CGR の数に対し、エラーを報告した CGR の数。
Name	CGR の EID。
Reprovisioning Status	この CGR の再プロビジョニング アクションのステータス。
Last Updated	この CGR の再プロビジョニング アクションのステータスが最後に更新された時間。
Template Version	適用されるフィールド エリア ルータの出荷時再プロビジョニング テンプレートのバージョン。
エラー メッセージ	CGR によって報告されたエラー メッセージ（ある場合）。
Error Details	エラーの詳細。

CGR 再プロビジョニングのシーケンス

トンネル プロビジョニング グループに対してトンネル再プロビジョニングまたは出荷時再プロビジョニングを開始すると、再プロビジョニング アルゴリズムが一度に 12 の CGR を連続して処理し、再プロビジョニングします。

IoT FND が正常にルータを再プロビジョニングした後、またはエラーが報告されると、IoT FND はグループ内の次のルータの再プロビジョニング プロセスを開始します。すべての CGR が再プロビジョニングされるまで、IoT FND はこのプロセスを繰り返します。

グループ内の各 CGR を再プロビジョニングする場合、4 時間でタイムアウトします。CGR が正常な再プロビジョニングを報告しなかったり、タイムアウト時間内にエラーがあった場合、IoT FND は CGR の再プロビジョニングのステータスを [Error] に変更し、タイムアウト エラーを表示します。その他の詳細情報はすべて、[Error Details] フィールドに表示されます。

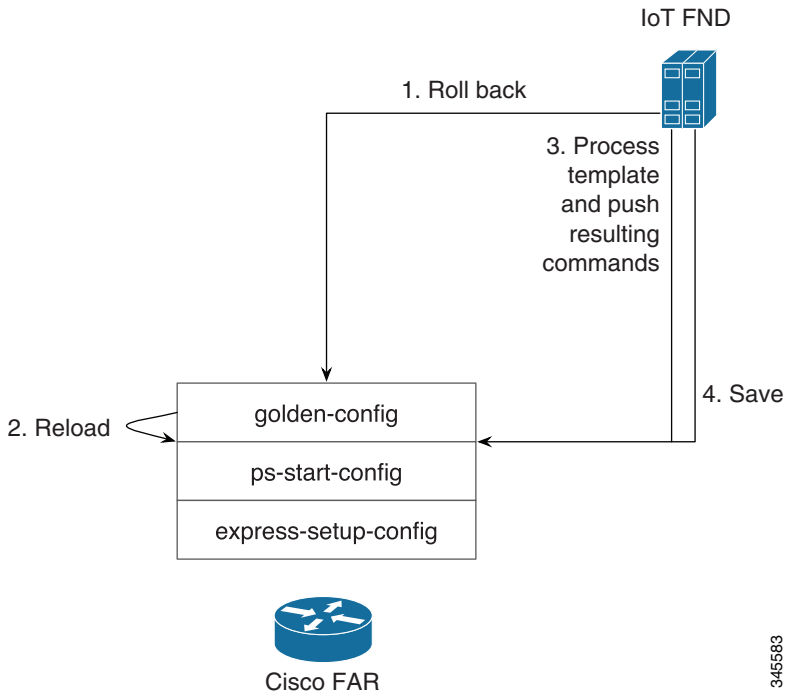
トンネル再プロビジョニング

フィールド エリア ルータ トンネル追加テンプレートを変更し、すでに IoT FND に接続したすべての CGR を変更されたテンプレートに基づく新しいトンネルで再プロビジョニングする場合、IoT FND のトンネル再プロビジョニング機能を使用します。

トンネル再プロビジョニングは、CGR をトンネルが設定されていない状態にし、その後、新しいトンネル プロビジョニング要求を開始します。トンネルを再プロビジョニングするため、IoT FND はトンネル プロビジョニング グループ内の FAR を連続して処理します（一度に 12）。各 CGR に対し、IoT FND は CGR の構成を ps-start-config テンプレート ファイルに定義された状態にロールバックします。

ps-start-config へのロールバックの後、CGR は IoT FND にコンタクトしてトンネル プロビジョニングを要求します。IoT FND はフィールド エリア ルータ トンネル追加テンプレートを処理し、その結果として得られた新しいトンネル作成の設定コマンドを CGR に送信します。図 3 に示すとおり、トンネル プロビジョニング プロセスには、新しい設定情報が含まれるよう golden-config ファイルを更新することが含まれます。

図 3　トンネル再プロビジョニング プロセス



(注) CG-OS CGR では、ロールバックにより CGR がリロードされます。また、IoT FND が CGR をロールバックすると、IoT FND は対応するトンネル情報を CGR が接続された HER から削除します。

Cisco IOS ベースの CGR に構成の置換を実行します。

(注) フィールド エリア ルータ出荷時再プロビジョニング テンプレートは、トンネル再プロビジョニングの実行時には使用されません。

トンネル再プロビジョニングを設定してトリガーする方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、テンプレートを再プロビジョニングするトンネル グループを選択します。
3. [Reprovisioning Actions] タブをクリックします。

4. [Action] ドロップダウン メニューから、[Tunnel Reprovisioning] を選択します。
5. [Start] をクリックします。

   IoT FND は [Reprovisioning Status] フィールドを [Initialized] に変更し、次に [Running] に変更します。

   (注) トンネル再プロビジョニングの実行中に [Stop] をクリックすると、IoT FND は選択されなかったキューの FAR についてのみ、再プロビジョニング プロセスを停止します。ただし、再プロビジョニングを選択したキューの CGR に関しては、プロセスは完了され(正常またはエラー)、停止することはできません。

   再プロビジョニング プロセスは、IoT FND がトンネル プロビジョニング グループ内の各 CGR を再プロビジョニングする試みを終了した後、完了します。CGR が 1 つでも再プロビジョニングできなければ、IoT FND は CGR が報告したエラー メッセージを表示します。

出荷時再プロビジョニング

IoT FND の出荷時再プロビジョニング機能を使って、CGR の工場出荷時の設定(express-setup-config)を変更します。

出荷時再プロビジョニングでは次の手順を行います。

1. CGR にロールバック コマンドを送信します。
2. CGR をリロードします。
3. フィールド エリア ルータ出荷時再プロビジョニング テンプレートを処理し、結果として得られたコマンドを CGR にプッシュします。
4. express-setup-config ファイルの構成を保存します。

これらの手順が正常に完了した後、IoT FND はフィールド エリア ルータ トンネル追加、ヘッドエンド ルータ トンネル追加、およびヘッドエンド ルータ トンネル削除の各テンプレートを処理し、結果として得られたコマンドを CGR にプッシュします(トンネル プロビジョニング設定プロセス参照)。

出荷時再プロビジョニングを設定してトリガーする方法:

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、テンプレートを編集するトンネル グループを選択します。
3. [Router Factory Reprovision] タブをクリックし、適用する設定コマンドを含むテンプレートを入力します。

   (注) このルータ出荷時再プロビジョニング テンプレートは、出荷時再プロビジョニングの間に 2 回(設定をプッシュするときに 1 回、設定を express-setup-config に保存する前にもう 1 回)処理されます。この理由により、個人的にテンプレートを作るときは、デフォルトのテンプレートで定義された特定の if/else 条件モデルを使用してください。

4. ディスク アイコンをクリックして保存します。
5. 必要に応じて、フィールド エリア ルータ トンネル追加、ヘッドエンド ルータ トンネル追加、およびヘッドエンド ルータ トンネル削除の各テンプレートに必要な変更を加えます。
6. [Reprovisioning Actions] タブをクリックします。
7. [Factory Reprovisioning] タブを選択します。

8. [Interface] ドロップダウン メニューから、再プロビジョニングのため FAR との接続に使用するIoT FND の CGR インターフェイスを選択します。
9. [Interface Type] ドロップダウン メニューから [IPv4] または [IPv6] を選択します。
10. [Start] ボタンをクリックします。

    IoT FND は [Reprovisioning Status] フィールドを [Initialized] に変更し、次に [Running] に変更します。

    (注)出荷時再プロビジョニング実行中に [Stop] をクリックすると、IoT FND は選択されなかったキューの FAR についてのみ、再プロビジョニング プロセスを停止します。ただし、再プロビジョニングを選択したキューの CGR に関しては、プロセスは完了され、停止することはできません。

再プロビジョニング プロセスは、IoT FND がトンネル プロビジョニング グループ内の各 CGR を再プロビジョニングする試みを終了した後、完了します。CGR が 1 つでも再プロビジョニングできなければ、IoT FND は CGR が報告したエラー メッセージを表示します。

フィールド エリア ルータ出荷時再プロビジョニング テンプレートの例

このテンプレートの例は、工場出荷時構成の WiFi SSID およびパスフレーズを変更します。

```
<#--IMPORTANT: This template is processed twice during factory reprovisioning. The if/else condition
described below is needed to determine which part of the template is applied.
part of the if/else section is applied.During the second pass, this template runs the commands in the
else section and the no scheduler command is applied.If modifying this template, do not remove the
if/else condition or else the template fails.-->

<#if !far.runningConfig.text?contains("scheduler schedule name wimaxMigrationRebootTimer")>

<#--Comment: This is a sample of generating wifi ssid and passphrase randomly-->

wifi ssid ${far.randomSSID("PREFIX_")}
authentication key-management wpa2
wpa2-psk ascii ${far.randomPassword(10)}
exit

feature scheduler
scheduler job name wimaxMigration
reload
exit

scheduler schedule name wimaxMigrationRebootTimer
time start +02:00
job name wimaxMigration
exit

<#else>

no scheduler job name wimaxMigration
no scheduler schedule name wimaxMigrationRebootTimer

</#if>
```

ハイ アベイラビリティのインストールの管理

ここでは、ハイ アベイラビリティ用に IoT FND を設定する方法について説明します。具体的な内容は次のとおりです。

IoT FND ハイ アベイラビリティの概要

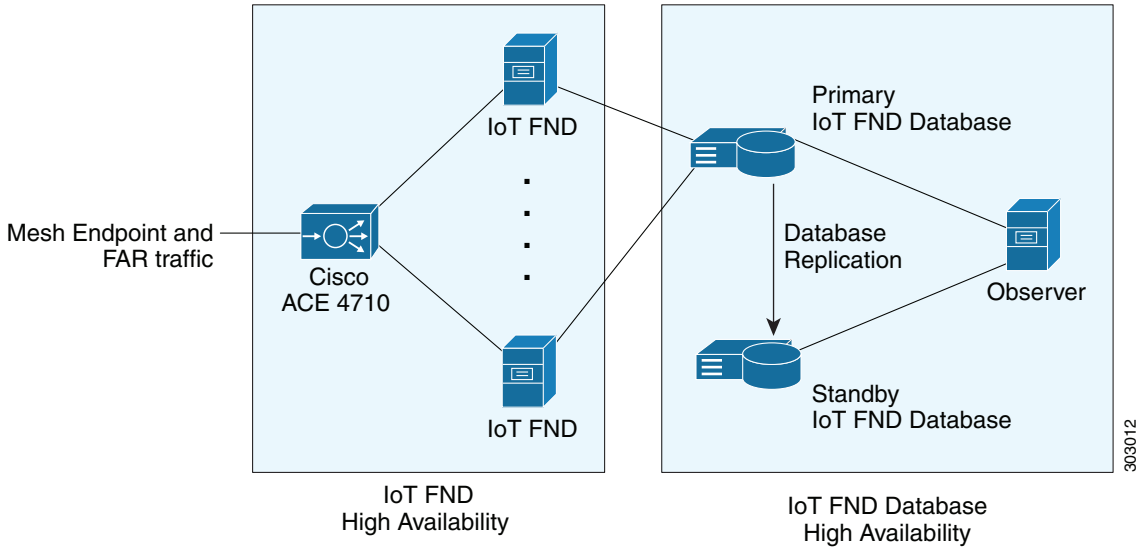
ここでは、IoT FND ハイ アベイラビリティのインストールの概要を提供します。具体的な内容は次のとおりです。

IoT FND は、Connected Grid のモニタおよび管理にとって重要なアプリケーションです。IoT FND ハイ アベイラビリティ（IoT FND HA）ソリューションは、ソフトウェア、ネットワーク、またはハードウェアの障害発生時に、IoT FND の全体的な可用性に対応します。

図 1 に示すように、IoT FND は 2 つの主要なレベルの HA を提供します。

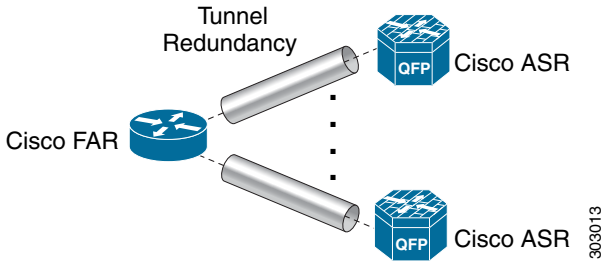
- IoT FND サーバ HA：これは複数の IoT FND サーバを Cisco ACE 4710 ロード バランサに接続することで実現されます。ME、FAR、ASR で発生するトラフィックは、ロード バランサに送られます。ロード バランサは、ラウンドロビン プロトコルを使用して IoT FND クラスタ サーバ間で負荷を分散します。
- IoT FND データベース HA：これは 2 つの IoT FND データベース サーバ（プライマリ サーバとスタンバイ（セカンダリ）サーバ）を設定することで実現されます。プライマリ データベースは新しいデータを受信すると、コピーをスタンバイ データベースに送信します。別のシステムがオブザーバを実行します。オブザーバは IoT FND データベース サーバをモニタするプログラムで、スタンバイ サーバでも実行できます。プライマリ データベースに障害が発生すると、オブザーバはスタンバイ サーバを新しいプライマリ データベースとして設定します。IoT FND データベース HA は、シングルおよびクラスタ IoT FND サーバ展開でも機能します。

図 1　IoT FND サーバおよびデータベース HA



IoT FND サーバとデータベース HA に加え、トンネルの冗長性を加えることで IoT FND の信頼性が向上します。これは 1 つの FAR と複数の ASR 間で複数のトンネルを定義することで実現されます。1 つのトンネルで障害が発生すると、FAR は別のトンネル経由でトラフィックをルーティングします。

図 2　IoT FND トンネルの冗長性



IoT FND HA は、以下の障害シナリオに対応します。

障害のタイプ	説明
IoT FND サーバの障害	IoT FND サーバ クラスタ内の 1 台のサーバに障害が発生すると、ロード バランサがクラスタ内の他のサーバにトラフィックをルーティングします。
IoT FND データベースの障害	プライマリ データベースに障害が発生すると、関連付けられたスタンバイ データベースがプライマリ データベースになります。これは IoT FND サーバに対してトランスペアレントです。クラスタ内のすべての IoT FND サーバが新しいプライマリ データベースに接続します。
トンネルの障害	トンネルに障害が発生すると、トラフィック フローは別のトンネルを経由します。

ロード バランサ

ロード バランサ(LB)は以下のタスクを実行するため、IoT FND HA において重要な役割を担います。

- IoT FND へのトラフィックを負荷分散します。
- クラスタ内のサーバとのハートビートを維持し、障害を検出します。IoT FND サーバに障害が発生すると、LB は他のクラスタ メンバーにトラフィックを向けます。

この展開では、ロード バランサとして Cisco ACE 4710(Cisco ACE)を使用することを推奨します。Cisco ACE 4710 の詳細については、http://www.cisco.com/en/US/partner/products/ps7027/tsd_products_support_series_home.html を参照してください。

サーバのハートビート

LB は、クラスタ内の各 IoT FND サーバとのハートビートを維持します。IoT FND ソリューション(代替ソリューションあり)で採用されているヘルス モニタリング メカニズムでは、ハートビートはポート 80 での IoT FND への 通常の GET メッセージです。IoT FND はアクティブな IoT FND サーバからの「HTTP 200 OK」の応答を求めます。

LB で次のハートビート パラメータを設定できます。

- Periodicity of probes:これはハートビート間の秒数です。Cisco ACE でのデフォルト値は 15 秒です。
- Number of retries:これは LB が応答しない IoT FND サーバにダウンを宣言する前に、ハートビートの送信を試行する回数です。デフォルトの再試行回数は 3、
- Regular checks after failure detection:LB はこの時間間隔でサーバがオンラインに戻ったかどうかを確認します。障害検出チェックのデフォルト値は 60 秒です。

データベース ハイ アベイラビリティ

IoT FND データベース HA は、IoT FND シングル サーバーとクラスタ展開で機能します。IoT FND HA は Oracle Active Dataguard を使用して、Oracle HA を展開します。IoT FND データベース用に HA を設定するには、Oracle Recovery Manager(RMAN)と Dataguard Management CLI(DGMGRL)を使用します。

IoT FND データベース HA 設定プロセスには以下が含まれます。

- 別の物理サーバでプライマリ データベースとセカンダリ データベースを同じように設定します。

  (注)セカンダリ データベース サーバは、スタンバイ データベースとも呼ばれます。

  (注)データベースのフェールオーバー時に、データが失われる可能性があります。

- Oracle *ウォレット*を使用して、データ レプリケーションが SSL を介して実行されるように設定します。このウォレットには、迅速な展開を促進する自己署名証明書が含まれています。

  (注)IoT FND RPM にバンドルされている Oracle ウォレットは、自己署名証明書を使用します。カスタム証明書とウォレットを設定して、レプリケーションを円滑に行うことができます。

  (注)SSL を介してデータ レプリケーションを実行しても、パフォーマンスへの影響はありません。

- レプリケーションには、cgms_dev *ではなく*、sys ユーザを使用します。
- パフォーマンスのボトルネックを防止するため、レプリケーションを非同期に設定します。

デフォルトでは、IoT FND は TCP を使用し、ポート 1522 を介してデータベースに接続します。レプリケーションはポート 1622 で TCPS(TCP over SSL)を使用します。

IoT FND データベース HA を設定するためのスクリプトは、IoT FND Oracle Database RPM パッケージ(cgms-oracle-*version_number*.x86_64.rpm)に含まれています。IoT FND データベースをインストールすると、HA スクリプトは $ORACLE_HOME/cgms/scripts/ha に配置されます。

トンネルの冗長性

IoT FND の展開にさらなる冗長性を追加するには、FAR トンネル プロビジョニング グループ内のすべての FAR を複数の ASR に接続する複数のトンネルを設定します。たとえば、すべての FAR に 2 つのトンネルをプロビジョニングするように IoT FND を設定することができます。1 つのトンネルがセルラー インターフェイスを介してアクティブになっている間、冗長トンネルは WiMAX インターフェイスを介して 2 番目の ASR と通信するように設定します。

トンネルの冗長性を設定するには、以下を実行する必要があります。

1. トンネル プロビジョニング グループに ASR を追加します。
2. トンネル プロビジョニング テンプレートを変更して、追加のトンネルを作成するコマンドを含めます。
3. FAR と ASR のインターフェイスで、インターフェイス間のマッピングを決定するポリシーを定義します。
   - トンネル プロビジョニング ポリシーの設定
   - トンネル冗長性のためのトンネル プロビジョニング テンプレートの変更

HA の注意事項および制限事項

IoT FND HA の設定に関して、次の点に注意してください。

- IoT FND HA には、FAR、ASR、ロード バランサなどの他のネットワーク コンポーネントの HA サポートは含まれていません。
- IoT FND HA ではゼロ サービス ダウンタイムを目指していますが、これを保証してはいません。
- IoT FND ノードはすべて同じサブネット上にある必要があります。
- IoT FND ノードはすべて、同じようなハードウェアで実行する必要があります。
- すべての IoT FND ノードが同じソフトウェア バージョンを実行する必要があります。
- すべてのノードで IoT FND セットアップ スクリプト（/opt/cgms/bin/setupCgms.sh）を実行します。
- DB の移行のスクリプト（/opt/cgms/bin/db-migrate）は、1 つのノードでのみ実行します。
- /opt/cgms/bin/print_cluster_view.sh スクリプトは、IoT FND クラスタ メンバーに関する情報を表示します。

HA 用の IoT FND インストールの設定

ここでは、IoT FND HA インストールのさまざまな設定について説明します。具体的な内容は次のとおりです。

- HA 用の IoT FND データベースの設定
- IoT FND データベース HA の無効化
- ロード バランシング ポリシー
- LB の実行コンフィギュレーションの例
- トンネル プロビジョニング ポリシーの設定
- トンネル冗長性のためのトンネル プロビジョニング テンプレートの変更

HA 用の IoT FND データベースの設定

IoT FND HA データベースを設定するには、次の手順を実行します。

1. スタンバイ データベースを設定します(「スタンバイ データベースの設定」を参照)。

   (注) 必ず最初にスタンバイ データベースを設定します。

   - スタンバイ サーバのデフォルト SID は **cgms_s** で、cgms *ではありません*。
   - HA 用のスタンバイ サーバを設定する前に、スタンバイ サーバの環境変数 $ORACLE_SID が **cgms_s** に設定されていることを確認します。
   - ポートは常に 1522 です。

2. プライマリ データベースを設定します(「プライマリ データベースの設定」を参照)。

   - プライマリ サーバのデフォルト SID は **cgms** です。
   - HA 用のプライマリ サーバを設定する前に、プライマリ サーバの環境変数 $ORACLE_SID が **cgms** に設定されていることを確認します。

3. データベース HA 用に IoT FND を設定します(「データベース HA 用の IoT FND の設定」を参照)。
4. データベース オブザーバを設定します(「オブザーバの設定」を参照)。

スタンバイ データベースの設定

HA 用のスタンバイ データベース サーバを設定するには、setupStandbyDb.sh スクリプトを実行します。このスクリプトでは、プライマリ データベースの IP アドレスなど、スタンバイ データベースに必要な設定情報を入力するように求められます。

```
$ ./setupStandbyDb.sh
$ Are you sure you want to setup a standby database ? (y/n)? y

09-20-2012 13:59:18 PDT: INFO: User response: y
09-20-2012 13:59:18 PDT: INFO: CGMS_S database does not exist.
Enter the SYS DBA password. NOTE: This password should be same as the one set on the primary server:
Re-enter password for SYS DBA:
09-20-2012 13:59:58 PDT: INFO: User entered SYS DBA password.

Enter new password for CG-NMS database:
Re-enter new password CG-NMS database:
09-20-2012 14:00:09 PDT: INFO: User entered CG-NMS DB password.
Enter primary database server IP address: 192.168.1.12
09-20-2012 14:00:27 PDT: INFO: Cleaning up instance - cgms_s
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production
…
Total System Global Area  329895936 bytes
Fixed Size    2228024 bytes
Variable Size  255852744 bytes
Database Buffers   67108864 bytes
Redo Buffers    4706304 bytes
...
09-20-2012 14:00:29 PDT: INFO: ========== CGMS_S Database Setup Completed Successfully ==========
```

プライマリ データベースの設定

HA 用のプライマリ データベース サーバを設定するには、setupHaForPrimary.sh スクリプトを実行します。このスクリプトでは、スタンバイ データベースの IP アドレスなど、プライマリ データベースに必要な設定情報を入力するように求められます。

```
$ ./setupHaForPrimary.sh
[oracle@pdb ha]$ ./setupHaForPrimary.sh
09-20-2012 13:58:39 PDT: INFO: ORACLE_BASE: /home/oracle/app/oracle
09-20-2012 13:58:39 PDT: INFO: ORACLE_HOME: /home/oracle/app/oracle/product/11.2.0/dbhome_1
09-20-2012 13:58:39 PDT: INFO: ORACLE_SID : cgms
09-20-2012 13:58:39 PDT: INFO: Make sure the above environment variables are what you expect

Are you sure you wish to configure high availability for this database server ? (y/n)? y

09-20-2012 13:58:45 PDT: INFO: User response: y
Enter standby database server IP address: 192.168.1.10
09-20-2012 13:58:56 PDT: INFO: Secondary listener reachable. Moving on with configuration
mkdir: cannot create directory `/home/oracle/app/oracle/oradata/cgms': File exists
09-20-2012 13:58:58 PDT: INFO: Reloading the listener to pick the new settings

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 13:58:58

…
DGMGRL> 09-20-2012 14:14:54 PDT: INFO: Please start the 'Observer' on appropriate server for ha モニタリング
Total time taken to perform the operation: 975 seconds
09-20-2012 14:14:54 PDT: INFO: ==========  Completed Successfully ==========
```

オブザーバの設定

オブザーバは個別のサーバで実行する必要がありますが、スタンバイ データベースをホストしているサーバで設定できます。

(注) オブザーバの実行に必要なパスワードは、SYS DBA パスワードと同じです。IoT FND Oracle データベースの作成を参照してください。

オブザーバを設定するには、次の手順を実行します。

1. 個別のサーバでオブザーバ スクリプトを実行します。

   ```
   $ ./manageObserver.sh start cgms_s password
   $ DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production
   ...
   Welcome to DGMGRL, type "help" for information.
   DGMGRL> Connected.
   DGMGRL> Observer started
   ```

2. getHaStatus.sh スクリプトを実行して、データベースが HA 用に設定されていることを確認します。

   ```
   $ ./getHaStatus.sh
   ...
   Configuration - cgms_dgconfig

     Protection Mode: MaxPerformance
     Databases:
       cgms   - Primary database
       cgms_s - (*) Physical standby database

   Fast-Start Failover: ENABLED

   Configuration Status:
   SUCCESS
   ```

```
DGMGRL>
Database - cgms

  Role:          PRIMARY
  Intended State:  TRANSPORT-ON
  Instance(s):
    cgms

Database Status:
SUCCESS

DGMGRL>
Database - cgms_s

  Role:          PHYSICAL STANDBY
  Intended State:  APPLY-ON
  Transport Lag:   0 seconds
  Apply Lag:      0 seconds
  Real Time Query: OFF
  Instance(s):
    cgms_s

Database Status:
SUCCESS
```

データベース HA 用の IoT FND の設定

データベース HA 用に IoT FND を設定するには、次の手順を実行します。

1. IoT FND を停止します。
2. setupCgms.sh スクリプトを実行します。

   このスクリプトでは、データベース設定の変更を求められます。**y** を入力します。次に、スクリプトによって、プライマリ データベース サーバの情報（IP アドレス、ポート、データベース SID）を入力するように求められます。この後、スクリプトによって他のデータベース サーバを追加するように求められます。**y** を入力します。次に、スクリプトによって、次のようにスタンバイ データベース サーバの情報（IP アドレス、ポート、データベース SID）を入力するように求められます。

   (注) IoT FND は常にポート 1522 を使用してデータベースと通信します。ポート 1622 は、データベースがレプリケーションのためだけに使用します。

```
# cd /opt/cgms/bin
# ./setupCgms.sh
09-13-2012 17:10:00 PDT: INFO: ========== CG-NMS Setup Started - 2012-09-13-17-10-00 ==========
09-13-2012 17:10:00 PDT: INFO: Log file: /opt/cgms/bin/../server/cgms/log/cgms_setup.log

Are you sure you want to setup CG-NMS (y/n)? y

09-13-2012 17:10:02 PDT: INFO: User response: y

Do you want to change the database settings (y/n)? y

09-13-2012 17:10:05 PDT: INFO: User response: y

Enter database server IP address [128.107.154.246]: 128.107.154.246
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.246

Enter database server port [1522]:
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
```

```
Enter database SID [cgms]:
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms

Do you wish to configure another database server for this CG-NMS ? (y/n)? y

09-13-2012 17:11:18 PDT: INFO: User response: y
Enter database server IP address []: 128.107.154.20
09-13-2012 17:11:02 PDT: INFO: Database server IP: 128.107.154.20
Enter database server port []: 1522
09-13-2012 17:11:07 PDT: INFO: Database server port: 1522
Enter database SID []: cgms_s
09-13-2012 17:11:12 PDT: INFO: Database SID: cgms_s
09-13-2012 17:11:18 PDT: INFO: Configuring database settings. This may take a while. Please wait
...
09-13-2012 17:11:19 PDT: INFO: Database settings configured.

Do you want to change the database password (y/n)? y

09-13-2012 17:15:07 PDT: INFO: User response: y

Enter database password:
Re-enter database password:

09-13-2012 17:15:31 PDT: INFO: Configuring database password. This may take a while. Please wait
...
09-13-2012 17:15:34 PDT: INFO: Database password configured.

Do you want to change the keystore password (y/n)? n

09-13-2012 17:16:18 PDT: INFO: User response: n

Do you want to change the web application 'root' user password (y/n)? n

09-13-2012 17:16:34 PDT: INFO: User response: n

Do you want to change the FTP settings (y/n)? n

09-13-2012 17:16:45 PDT: INFO: User response: n
09-13-2012 17:16:45 PDT: INFO: ========== CG-NMS Setup Completed Successfully ==========
```

IoT FND データベース HA の無効化

IoT FND データベース HA を無効化するには、次の手順を実行します。

1. オブザーバ プログラムを実行しているサーバで、オブザーバを停止します。

```
$ ./manageObserver.sh stop cgms_s password
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Done.
$ Observer stopped
```

2. スタンバイ IoT FND データベース サーバで、スタンバイ データベースを削除します。

```
$ ./deleteStandbyDb.sh

Are you sure you want to delete the standby database ? All replicated data will be lost (y/n)? y

09-20-2012 14:27:02 PDT: INFO: User response: y
09-20-2012 14:27:02 PDT: INFO: Cleaning up instance - cgms_s
```

```
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Done.
DGMGRL> DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Disabled.
DGMGRL> 09-20-2012 14:27:06 PDT: INFO: Removing dataguard configuration
DGMGRL for Linux: Version 11.2.0.3.0 - 64bit Production

Copyright (c) 2000, 2009, Oracle. All rights reserved.

Welcome to DGMGRL, type "help" for information.
DGMGRL> Connected.
DGMGRL> Removed configuration
DGMGRL> 09-20-2012 14:27:07 PDT: INFO: Stopping the database

SQL*Plus: Release 11.2.0.3.0 Production on Thu Sep 20 14:27:07 2012

Copyright (c) 1982, 2011, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL> ORA-01109: database not open


Database dismounted.
ORACLE instance shut down.
SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:27:19

Copyright (c) 1991, 2011, Oracle.  All rights reserved.

Connecting to
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm)(PORT=1522))(CONNECT_DATA=(SERVER=DEDIC
ATED)(SERVICE_NAME=cgms_s)))
The command completed successfully
Cleaning up instance - cgms_s
09-20-2012 14:27:29 PDT: INFO: ==========  Completed Successfully ==========
```

3. プライマリ IoT FND データベース サーバで、HA 設定を削除します。

```
$ ./deletePrimaryDbHa.sh
Are you sure you want to delete the high availability configuration ? All replicated data will be
lost (y/n)? y

09-20-2012 14:25:25 PDT: INFO: User response: y
09-20-2012 14:25:25 PDT: INFO: Removing secondary configuration from primary

SQL*Plus: Release 11.2.0.3.0 Production on Thu Sep 20 14:25:25 2012
```

```
Copyright (c) 1982, 2011, Oracle.  All rights reserved.


Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
System altered.
...
SQL> Disconnected from Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options
09-20-2012 14:25:28 PDT: INFO: Removing data guard config files
09-20-2012 14:25:28 PDT: INFO: Removing standby redo logs
09-20-2012 14:25:29 PDT: INFO: Creating listener file
09-20-2012 14:25:29 PDT: INFO: Listener successfully configured.
09-20-2012 14:25:29 PDT: INFO: Recreating tnsnames ora file
09-20-2012 14:25:29 PDT: INFO: reloading the listener

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:25:29

Copyright (c) 1991, 2011, Oracle.  All rights reserved.

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm-db2)(PORT=1522)))
The command completed successfully

LSNRCTL for Linux: Version 11.2.0.3.0 - Production on 20-SEP-2012 14:25:30

Copyright (c) 1991, 2011, Oracle.  All rights reserved.

Starting /home/oracle/app/oracle/product/11.2.0/dbhome_1/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 11.2.0.3.0 - Production
System parameter file is /home/oracle/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
Log messages written to
/home/oracle/app/oracle/diag/tnslsnr/test-scale-15krpm-db2/cgmstns/alert/log.xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=test-scale-15krpm-db2)(PORT=1522)))

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=test-scale-15krpm-db2)(PORT=1522)))
STATUS of the LISTENER
------------------------
Alias                     cgmstns
Version                   TNSLSNR for Linux: Version 11.2.0.3.0 - Production
Start Date                20-SEP-2012 14:25:30
Uptime                    0 days 0 hr. 0 min. 0 sec
Trace Level               off
Security                  ON: Local OS Authentication
SNMP                      OFF
Listener Parameter File
/home/oracle/app/oracle/product/11.2.0/dbhome_1/network/admin/listener.ora
Listener Log File
/home/oracle/app/oracle/diag/tnslsnr/test-scale-15krpm-db2/cgmstns/alert/log.xml
Listening Endpoints Summary...
  (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=test-scale-15krpm-db2)(PORT=1522)))
Services Summary...
Service "cgms" has 1 instance(s).
  Instance "cgms", status UNKNOWN, has 1 handler(s) for this service...
The command completed successfully
09-20-2012 14:25:30 PDT: INFO: ==========  Completed Successfully ==========
```

ロード バランシング ポリシー

次の表に、LB がサポートするトラフィック タイプごとのロード バランシング ポリシーを示します。

トラフィック	ロード バランシング ポリシー
ブラウザおよび IoT FND API クライアント（IPv4：ポート 80 および 443）間の HTTPS トラフィック	LB は Web ブラウザおよび IoT FND API クライアントからのすべてのトラフィックにレイヤ 7 の ロード バランシングを使用します。 LB は一般的な HTTPS トラフィックにでスティッキ性を使用します。
ポート 9121 および 9120 に向かう FAR IPv4 トラフィックの場合： ■ HTTPS を介したポート 9120 でのトンネル プロビジョニング ■ HTTPS を介したポート 9121 での通常の定期的な登録	LB はすべての FAR トラフィックにレイヤ 3 のロード バランシングを使用します。これが FAR から IoT FND へのトラフィックです。
メッシュ エンドポイント（ME）との IPv6 CSMP トラフィックの場合： ■ ポート 61624 を介した UDP トラフィック – 登録 – メトリックの定期的な送信 – ファームウェア プッシュ – 設定転送 ■ ポート 61625 を介した UDP トラフィック ME によって送信される停止通知用。	LB はポート 61624 へのすべての ME トラフィックとポート 61625 への停止メッセージに、レイヤ 3 のロード バランシングを使用します。

LB の実行コンフィギュレーションの例

以下に、適切に設定された IoT FND LB の実行コンフィギュレーションの例を示します。

```
# show running-config
Generating configuration....

ssh maxsessions 10

boot system image:c4710ace-t1k9-mz.A5_1_1.bin

hostname cgnmslb2
interface gigabitEthernet 1/1
  switchport access vlan 10
  no shutdown
interface gigabitEthernet 1/2
  description server-side
  switchport access vlan 11
  no shutdown
interface gigabitEthernet 1/3
  description client-side
  switchport access vlan 8
  no shutdown
```

```
interface gigabitEthernet 1/4
  switchport access vlan 55
  no shutdown



access-list ALL line 8 extended permit ip any any
access-list everyone line 8 extended permit ip any any
access-list everyone line 16 extended permit icmp any any
access-list ipv6_acl line 8 extended permit ip anyv6 anyv6
access-list ipv6_acl2 line 8 extended permit icmpv6 anyv6 anyv6



ip domain-lookup
ip domain-name cisco.com
ip name-server 171.68.226.120
ip name-server 171.70.168.183

probe http probe_cgnms-http
  port 80
  interval 15
  passdetect interval 60
  expect status 200 200
  open 1

rserver host 12-12-1-31
  ip address 12.12.1.31
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 12-12-1-32
  ip address 12.12.1.32
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 2002-cafe-server-202
  description realserver 2002:cafe:server::202
  ip address 2002::202
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice
rserver host 2002-cafe-server-211
  ip address 2002:cafe:server::211
  conn-limit max 4000000 min 4000000
  probe probe_cgnms-http
  inservice

serverfarm host cgnms_2
  description cgnms-serverfarm
  probe probe_cgnms-http
  rserver 2002-cafe-server-202 61624
    conn-limit max 4000000 min 4000000
    inservice
  rserver 2002-cafe-server-211 61624
    conn-limit max 4000000 min 4000000
    inservice
serverfarm host cgnms_2_ipv4
  probe probe_cgnms-http
  rserver 12-12-1-31
    conn-limit max 4000000 min 4000000
    inservice
  rserver 12-12-1-32
    conn-limit max 4000000 min 4000000
    inservice
```

```
sticky ip-netmask 255.255.255.255 address source CGNMS_SRC_STICKY
  serverfarm cgnms_2_ipv4


class-map type management match-any remote_access
  2 match protocol xml-https any
  3 match protocol icmp any
  4 match protocol telnet any
  5 match protocol ssh any
  6 match protocol http any
  7 match protocol https any
  8 match protocol snmp any
class-map type management match-all ssh_allow_access
  2 match protocol ssh any
class-map match-any virtual-server-cgnms
  2 match virtual-address 2002:server:cafe::210 udp eq 61624
class-map match-any vs_cgnms_ipv4
  3 match virtual-address 12.12.1.101 tcp eq https
  4 match virtual-address 12.12.1.101 tcp eq 9120
  5 match virtual-address 12.12.1.101 tcp eq 9121
  6 match virtual-address 12.12.1.101 tcp eq 8443
  7 match virtual-address 12.12.1.101 tcp any

policy-map type management first-match remote_mgmt_allow_policy
  class remote_access
    permit

policy-map type loadbalance first-match virtual_cgnms_l7
  class class-default
    serverfarm cgnms_2
policy-map type loadbalance first-match vs_cgnms_l7_v4
  class class-default
    sticky-serverfarm CGNMS_SRC_STICKY

policy-map multi-match cgnms_policy_ipv6
  class virtual-server-cgnms
    loadbalance vip inservice
    loadbalance policy virtual_cgnms_l7
    loadbalance vip icmp-reply active
policy-map multi-match int1000
  class vs_cgnms_ipv4
    loadbalance vip inservice
    loadbalance policy vs_cgnms_l7_v4
    loadbalance vip icmp-reply active

interface vlan 8
  bridge-group 1
  access-group input everyone
  access-group input ipv6_acl
  no shutdown
interface vlan 10
  bridge-group 2
  access-group input everyone
  access-group input ipv6_acl
  service-policy input int1000
  no shutdown
interface vlan 11
  bridge-group 2
  access-group input everyone
  access-group input ipv6_acl
  no shutdown
```

```
interface vlan 55
  bridge-group 1
  access-group input everyone
  access-group input ipv6_acl
  service-policy input cgnms_policy_ipv6
  no shutdown

interface bvi 1
  ipv6 enable
  ip address 2002:server:cafe::206/64
  no shutdown
interface bvi 2
  ip address 12.12.1.100 255.255.255.0
  no shutdown

domain cisco.com

ip route 2011::/16 2002:server:cafe::101
ip route 2001:server:cafe::/64 2002:cafe::101
ip route 11.1.0.0 255.255.0.0 12.12.1.33
ip route 15.1.0.0 255.255.0.0 12.12.1.33
ip route 13.211.0.0 255.255.0.0 12.12.1.33

context VC_Setup1
  allocate-interface vlan 40
  allocate-interface vlan 50
  allocate-interface vlan 1000

username admin password 5 $1$CB34uAB9$BW8a3ijjxvBGttuGtTcST/  role Admin domain
default-domain
username www password 5 $1$q/YDKDp4$9PkZl1SBMQW7yZ7E.sOZA/  role Admin domain de
fault-domain

ssh key rsa 1024 force
```

トンネル プロビジョニング ポリシーの設定

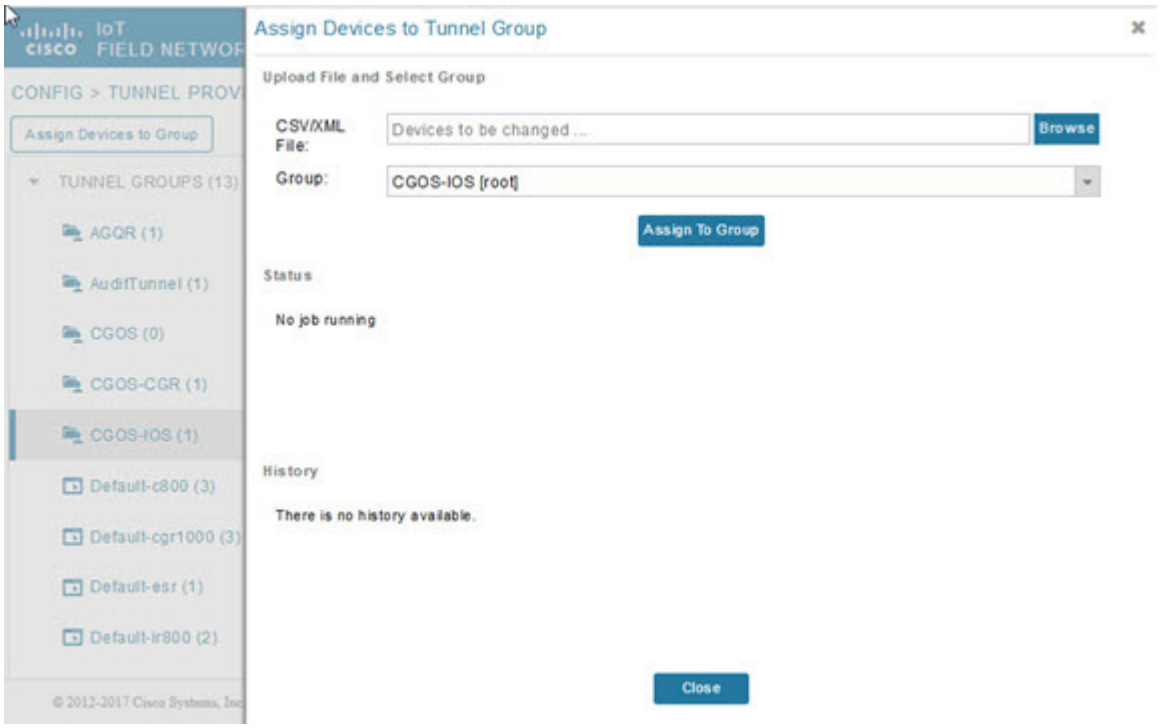
トンネル ポリシーを使用して、FAR に複数のトンネルを設定します。各トンネルは FAR および HER のインターフェイスに関連付けられています。トンネル プロビジョニング グループに 1 つ以上の HER がある場合、IoT FND は [Tunnel Provisioning Policies] タブ（[Config] > [Tunnel Provisioning]）にポリシーを表示します。このポリシーを使用して、FAR と HER 間にインターフェイス マッピングを設定します。

IoT FND で FAR と HER インターフェイスをマッピングするには、次の手順を実行します。

1. [CONFIG] > [Tunnel Provisioning] の順に選択します。
2. [TUNNEL GROUPS] ペインで、トンネルの冗長性を設定するグループを選択します。
3. HER をリストした CSV ファイルまたは XML ファイルを作成して、次のように *EID, device type* の形式でグループに追加します。

   ```
   eid,deviceType
   asr-0, asr1000
   asr-1, asr1000
   asr-2, asr1000
   ```

4. [Assign Devices to Group] をクリックして、ファイルをインポートして HER をグループに追加します。



(注) HER は複数のトンネル プロビジョニング グループのメンバーになることができます。

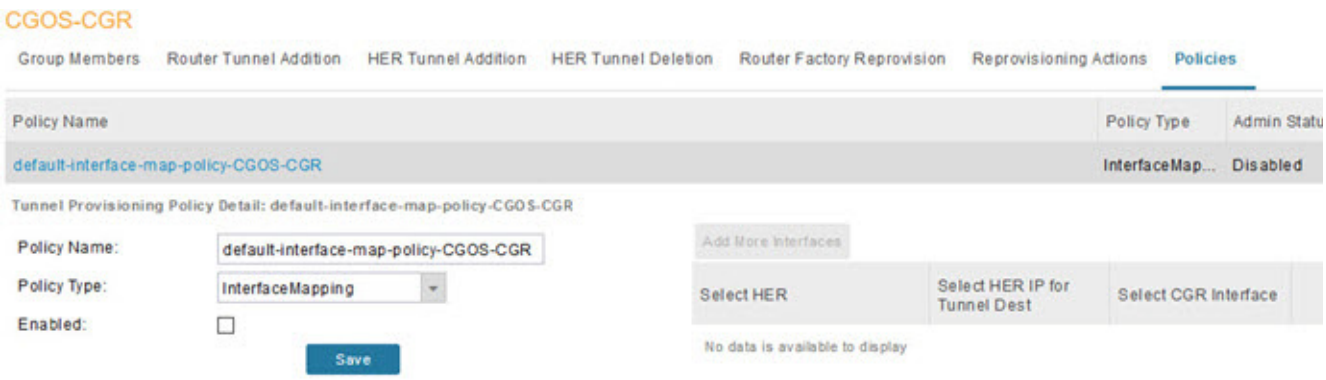
5. トンネル プロビジョニング グループを選択し、[Policies] タブをクリックします。

デフォルトでは、IoT FND は [Policy Name] パネルに、選択したトンネル グループの **default-interface-mapping-policy-*tunnel-group*** 名を表示します。

(注) interface-mapping は、現在 IoT FND でサポートされている唯一のポリシー タイプです。

IoT FND はグループ内のすべての HER に対して 1 つのインターフェイス マッピング エントリを表示します。インターフェイス マッピング エントリは、必要に応じて追加または削除することができます。

6. [Policy Name] パネル内の [Policy Name] リンクをクリックすると、入力パネルが開きます。[Policy Name] フィールドに、ポリシーの名前を入力します。



ポリシーに interface-mapping エントリを追加するには、[Add More Interfaces]（ページ右側の [Select HER] リストの上にあるボタン）をクリックします。エントリを**削除**するには、そのエントリの [Delete]（[X]）をクリックします。

7. インターフェイス マッピング エントリを設定するには、ポリシー名のリンクをクリックし、必要に応じて以下を実行します。

   a. 別の HER を選択するには、現在選択されている HER をクリックして、[Select a HER] ドロップダウン メニューから別の HER を選択します。

   b. HER でトンネル先の HER IP を選択するには、選択されているインターフェイスをクリックして、[Select HER IP] ドロップダウン メニューから別の HER IP を選択します。

   c. 選択した HER インターフェイスにマップする FAR インターフェイスを選択するには、[Select CGR Interface] ドロップダウン メニューからインターフェイスを選択します。

   d. [Update] をクリックします。

8. ポリシーを有効にするには、[Enabled] チェック ボックスをオンにします。

9. [Save] をクリックします。

トンネル冗長性のためのトンネル プロビジョニング テンプレートの変更

トンネル プロビジョニング グループにトンネル プロビジョニング ポリシーを設定したら、フィールド エリア ルータ トンネル追加テンプレートとヘッドエンド ルータ トンネル追加テンプレートを変更して、ポリシーで定義された複数のトンネルを確立するためのコマンドを含めます。

フィールド エリア ルータ トンネル追加テンプレートの例

この例では、太字は、複数のトンネルを作成するために行ったデフォルトのフィールド エリア ルータ トンネル追加テンプレートへの変更を示しています。

```
<#--
  Configure a Loopback0 interface for the FAR. This is done first as features
  look for this interface and use it as a source.

  This is independent of policies
-->
interface Loopback0
  <#--
    Now obtain an IPv4 address that can be used to for this FAR's Loopback
    interface. The template API provides methods for requesting a lease from
    a DHCP server. The IPv4 address method requires a DHCP client ID and a link
    address to send in the DHCP request. The 3rd parameter is optional and
    defaults to "CG-NMS". This value is sent in the DHCP user class option.
    The API also provides the method "dhcpClientId". This method takes a DHCPv6
    Identity association identifier (IAID) and a DHCP Unique  IDentifier (DUID)
    and generates a DHCPv4 client identifier as specified in RFC 4361. This
    provides some consistency in how network elements are identified by the
    DHCP server.
  -->
  ip address ${far.ipv4Address(dhcpClientId(far.enDuid, 0), far.dhcpV4LoopbackLink).address}/32
  <#--
    Now obtain an IPv6 address that can be used to for this FAR's loopback
    interface. The method is similar to the one used for IPv4, except clients
    in DHCPv6 are directly identified by their DUID and IAID. IAIDs used for
    IPv4 are separate from IAIDs used for IPv6, so we can use zero for both
    requests.
  -->
  ipv6 address ${far.ipv6Address(far.enDuid, 0, far.dhcpV6LoopbackLink).address}/128
exit

<#-- Make certain the required features are enabled on the FAR. -->
feature crypto ike
feature ospf
```

```
feature ospfv3
feature tunnel
<#-- Features ike and tunnel must be enabled before ipsec. -->
feature crypto ipsec virtual-tunnel

<#--
  Toggle on/off the c1222r feature to be certain it uses the Loopback0
  interface as its source IP.
-->
no feature c1222r
feature c1222r

<#-- Configure Open Shortest Path First routing processes for IPv4 and IPv6. -->
router ospf 1
exit
router ospfv3 2
exit

<#--
  Now that OSPF has been configured complete the configuration of Loopback0.
-->
interface Loopback0
  ip router ospf 1 area ${far.ospfArea1!"1"}
  ipv6 router ospfv3 2 area ${far.ospfV3Area1!"0"}
exit

<#-- Configure Internet Key Exchange for use by the IPsec tunnel(s). -->
crypto ike domain ipsec
  identity hostname
  policy 1
    <#-- Use RSA signatures for the authentication method. -->
    authentication rsa-sig
    <#-- Use the 1536-bit modular exponential group. -->
    group 5
  exit
exit
crypto ipsec transform-set IPSecTransformSet esp-aes 128 esp-sha1-hmac
crypto ipsec profile IPSecProfile
  set transform-set IPSecTransformSet
exit

<#--
  Define template variables to keep track of the next available IAID (IPv4)
  and the next available tunnel interface number. We used zero when leasing
  addresses for Loopback0, so start the IAID at one.
-->
<#assign iaId = 1>
<#assign interfaceNumber = 0>

<#--
  The same logic is needed for each of the IPsec tunnels, so a macro is used
  to avoid duplicating configuration. The first parameter is the prefix to
  use when looking for the WAN interface on the FAR to use for the source of
  the tunnel. The second parameter is the OSPF cost to assign to the tunnel.
-->
<#macro configureTunnel interfaceNamePrefix destinationInterface her tunnelIndex ospfCost>
  <#--
    If an interface exists on the FAR whose name starts with the given prefix
    and an IPv4 address as been assigned to that interface then the IPsec
    tunnel can be configured, otherwise no tunnel will be configured. The
    template API interfaces method will return all interfaces whose name
    starts with the given prefix.
  -->
```

```
  <#assign wanInterface = far.interfaces(interfaceNamePrefix)>
  <#-- Check if an interface was found and it has an IPv4 address. -->
  <#if (wanInterface[0].v4.addresses[0].address)??>
    <#--
      Determine the HER destination address to use when configuring the tunnel.
      If the optional property "ipsecTunnelDestAddr1" has been set on this FAR
      then use the value of that property. Otherwise look for that same property
      on the HER. If the property is not set on the FAR or the HER, then fallback
      to using an address on the HER GigabitEthernet0/0/0 interface.
    -->
    <#assign destinationAddress = her.interfaces(destinationInterface)[0].v4.addresses[0].address>

    <#if !(destinationAddress??)>
      ${provisioningFailed("Unable to determine the destination address for IPsec tunnels")}
    </#if>
    interface Tunnel${interfaceNumber}
      <#assign interfaceNumber = interfaceNumber + 1>
      description IPsec tunnel to ${her.eid}
      <#--
        For a tunnel interface two addresses in their own tiny subnet are
        needed. The template API provides an ipv4Subnet method for leasing an
        IPv4 from a DHCP server. The parameters match those of ipv4Address,
        with a fourth optional parameter that can be used to specify the
        prefix length of the subnet to request. If not specified the prefix
        length requested will default to 31, which provides the two addresses
        needed for a point to point link.

        NOTE: If the DHCP server being used does not support leasing an IPv4
        subnet, then this call will have to be changed to use the ipv4Address
        method and the DHCP server will have to be configured to respond
        appropriately to the request made here and the second request that
        will have to be made when configuring the HER side of the tunnel.
        That may require configuring the DHCP server with reserved addresses
        for the client identifiers used in the calls.
      -->
      <#assign lease = far.ipv4Subnet(dhcpClientId(far.enDuid, tunnelIndex), far.dhcpV4TunnelLink)>
      <#assign iaId = iaId + 1>
      <#-- Use the second address in the subnet for this side of the tunnel. -->
      ip address ${lease.secondAddress}/${lease.prefixLength}
      ip ospf cost ${ospfCost}
      ip ospf mtu-ignore
      ip router ospf 1 area ${far.ospfArea1!"1"}
      tunnel destination ${destinationAddress}
      tunnel mode ipsec ipv4
      tunnel protection ipsec profile IPSecProfile
      tunnel source ${wanInterface[0].name}
      no shutdown
    exit
  </#if>
</#macro>

<#--
  Since we are doing policies for each tunnel here, the list of policies passed to this template can be
  iterated over to get the tunnel configuration viz interface mapping

  tunnelObject.ipSecTunnelDestInterface is the "interface on CGR"
  tunnelObject.ipSecTunnelSrcInterface is the "interface on HER"
  tunnelObject.her is the HER of interest
 -->

<#list far.tunnels("ipSec") as tunnelObject>
    <@configureTunnel tunnelObject.ipSecTunnelDestInterface tunnelObject.ipSecTunnelSrcInterface
tunnelObject.her tunnelObject.tunnelIndex 100/>  <----- Loop through policies (aka Tunnels)
</#list>
```

```
<#--
  Make certain provisioning fails if we were unable to configure any IPsec
  tunnels. For example this could happen if the interface properties are
  set incorrectly.
-->
<#if iaId = 1>
  ${provisioningFailed("Did not find any WAN interfaces to use as the source for IPsec tunnels")}
</#if>

<#--
  Configure an IPv6-in-IPv4 GRE tunnel to allow IPv6 traffic to reach the data
  center.
-->
<#macro configureGreTunnel destinationInterface her tunnelIndex>

<#assign destinationAddress = her.interfaces(destinationInterface)[0].v4.addresses[0].address>

<#if !(destinationAddress??)>
     ${provisioningFailed("Unable to determine the destination address for GRE tunnels")}
</#if>

interface Tunnel${interfaceNumber}
  <#assign interfaceNumber = interfaceNumber + 1>
  description GRE IPv6 tunnel to ${her.eid}
  <#--
    The ipv6Subnet method is similar to the ipv4Subnet method except instead
    of obtaining an IPv4 subnet it uses DHCPv6 prefix delegation to obtain an
    IPv6 prefix. The prefix length will default to 127, providing the two
    addresses needed for the point to point link. For the IAID, zero was used
    when requesting an IPv6 address for loopback0, so use one in this request.
  -->
  <#assign lease = far.ipv6Subnet(far.enDuid, tunnelIndex, far.dhcpV6TunnelLink)>
  ipv6 address ${lease.secondAddress}/${lease.prefixLength}
  ipv6 router ospfv3 2 area ${far.ospfV3Area1!"0"}
  ospfv3 mtu-ignore
  tunnel destination ${destinationAddress}
  tunnel mode gre ip
  tunnel source Loopback0
  no shutdown
exit

</#macro>

<#-- Loop through the policies for GRE tunnels -->
<#list far.tunnels("gre") as greTunnelObj>
    <@configureGreTunnel greTunnelObj.greDestInterface greTunnelObj.her greTunnelObj.tunnelIndex/>
</#list>
```

ヘッドエンド ルータ トンネル追加テンプレート

この例では、太字は、複数のトンネルを作成するために行ったデフォルトのヘッドエンド ルータ トンネル追加テンプレートへの変更を示しています。

```
<#--
  Define template variables to keep track of the IAID (IPv4) that was used by
  the FAR template when configuring the other end of the tunnel. This template
  must use the same IAID in order to locate the same subnet that was leased by
  the FAR template so both endpoints are in the matching subnet.
-->
<#assign iaId = 1>
```

```
<#--
  The same logic is needed for each of the IPsec tunnels, so a macro is used.
-->
<#macro configureTunnel ipSecTunnelSrcInterface ipSecTunnelDestInterface her tunnelIndex ospfCost>
  <#--
    Only configure the HER tunnel end point if the FAR tunnel end point was
    configured. This must match the corresponding logic in the FAR tunnel
    template. The tunnel will not have been configured if the WAN interface
    does not exist on the FAR or does not have an address assigned to it.
  -->
  <#assign wanInterface = far.interfaces(ipSecTunnelDestInterface)>
  <#if (wanInterface[0].v4.addresses[0].address)??>
    <#-- Obtain the full interface name based on the prefix. -->
    <#assign interfaceName = wanInterface[0].name>
    <#--
      Locate a tunnel interface on the HER that is not in use. The template
      API provides an unusedInterfaceNumber method for this purpose. All of
      the parameters are optional. The first parameter is a name prefix
      identifying the type of interfaces, it defaults to "tunnel". The second
      parameter is a lower bound on the range the unused interface number must
      be in, it defaults to zero. The third parameter is the upper bound on
      the range, it defaults to max integer (signed). The method remembers
      the unused interface numbers it has returned while the template is
      being processed and excludes previously returned numbers. If no unused
      interface number meets the constraints an exception will be thrown.
    -->
    interface Tunnel${her.unusedInterfaceNumber()}
      description IPsec tunnel to ${far.eid}
      <#assign lease = far.ipv4Subnet(dhcpClientId(far.enDuid, tunnelIndex), far.dhcpV4TunnelLink)>
      <#assign iaId = iaId + 1>
      ip address ${lease.firstAddress} ${lease.subnetMask}
      ip ospf cost ${ospfCost}
      ip ospf mtu-ignore
      tunnel destination ${wanInterface[0].v4.addresses[0].address}
      tunnel mode ipsec ipv4
      tunnel protection ipsec profile IPSecProfile
      tunnel source ${ipSecTunnelSrcInterface}
      no shutdown
    exit
    router ospf 1
      network ${lease.prefix} ${lease.wildcardMask} area ${far.ospfArea1!"1"}
    exit
  </#if>
</#macro>

<#list far.tunnels("ipSec") as tunnelObject>
        <@configureTunnel tunnelObject.ipSecTunnelSrcInterface tunnelObject.ipSecTunnelDestInterface
tunnelObject.her tunnelObject.tunnelIndex 100/>
</#list>

<#--
  Configure an IPv6-in-IPv4 GRE tunnel to allow IPv6 traffic to reach the data
  center.
-->
<#macro configureGreTunnel greSrcInterface her tunnelIndex>
interface Tunnel${her.unusedInterfaceNumber()}
  description GRE IPv6 tunnel to ${far.eid}
  <#assign lease = far.ipv6Subnet(far.enDuid, tunnelIndex, far.dhcpV6TunnelLink)>
  ipv6 address ${lease.firstAddress}/${lease.prefixLength}
  ipv6 enable
  ipv6 ospf 2 area ${far.ospfV3Area1!"0"}
  ipv6 ospf mtu-ignore
  tunnel destination ${far.interfaces("Loopback0")[0].v4.addresses[0].address}
  tunnel mode gre ip
  tunnel source ${greSrcInterface}
```

```
exit
</#macro>

<#-- Loop through the policies for GRE tunnels -->
<#list far.tunnels("gre") as greTunnelObj>
        <@configureGreTunnel greTunnelObj.greSrcInterface greTunnelObj.her greTunnelObj.tunnelIndex/>
</#list>
```