FND 上で新しいデバイスをインポートするための .csv (コンマ区切り値) ファイルの準備

目次

概要

このドキュメントは Field Network Director (FND) 用に .csv ファイルを準備する手順について説明します。 安全なネットワーク運用を実現するため、FND は自動的または動的なアセットの検出と登録は行いません。 FND 導入に新しいデバイスを追加するには、先に Web ユーザ インターフェイス (UI) からカスタム .csv ファイルをインポートしてデバイス用の一意のデータベース エントリを作成する必要があります。

この記事では、既存のソリューションに新しいエンドポイントやフィールド エリア ルータ、ヘッドエンド ルータを追加するために使用でき、カスタマイズできる .csv テンプレートを提供します。 これに加え、新しいデバイスの設計と実装に役立つようにデータベース (DB) の各フィールドについて定義および説明しています。

> **注:** この説明書を使用する前に、すべての設定とインストールが完了した Connected Grid Network Management System (CG-NMS) /FND ソリューションが必要です。

前提条件

要件

次の項目に関する知識が推奨されます。

- Web UI でアクセスできる、インストール済みで実行中の CG-NMS/FND アプリケーション サーバ 1.0 以降。
- インストール済みで実行中の Tunnel Provisioning Server (TPS) プロキシ サーバ。
- インストールされ、正しく設定されている Oracle データベース サーバ。
- 正常な初回の db_migrate により、少なくとも 1 回 setupCgms.sh を正常に実行します。

- DHCP サーバがインストールがまだで、未設定でもこのドキュメントを使用することはできますが、本書の使用の前に所属組織で IPv4 および IPv6 のアドレッシング方式の導入が完全に計画されていることを強く推奨します。 これには IPv4 IPsec トンネルおよび IPv6 Generic Routing Encapsulation（GRE）トンネル用のプレフィックス長と範囲、Connected Grid ルータ（CGR）ループバックのデュアル スタック アドレッシングが含まれます。
- また、ヘッドエンド ルータ、フィールド エリア ルータ、エンドポイントメーターをそれぞれ最低 1 つはすでに購入しているか購入を計画していることも強くお勧めします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- FND 3.0.1-36
- ソフトウェア ベースの SSM（これも 3.0.1-36）
- アプリケーション サーバにインストールされている cgms-tools パッケージ（3.0.1-36）
- RHEL 6.5 を実行するすべての Linux サーバ
- Windows Server 2008 R2 Enterprise を実行するすべての Windows サーバ
- ヘッドエンド ルータとして VM で実行されている Cisco Cloud Services Router（CSR）1000v
- CG-OS 4(3) でのフィールド エリア ルータ（FAR）として使用されている CGR-1120/K9

このドキュメントの作成時には、管理された FND ラボ環境が使用されました。 その他の導入は異なりますが、インストール ガイドのすべての最小要件に従う必要があります。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

FND にデバイスを追加する .csv ファイル

FAR

このテンプレートはソリューションに初めて導入される FAR に使用できます。 これは、[Devices] > [Field Devices] のページにあります。 [Field Devices] のページで、[Bulk Impot] のドロップダウン メニューをクリックし、[Add Devices] を選択します。

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunnelDestAddr1,adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhcpV4TunnelLink,dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink
```

要素識別子（eid）：これは、ログ メッセージや GUI でデバイスを特定するために使用する固有識別子です。 混乱を防ぐため、組織で EID のスキームを開発することをお勧めします。 推奨されるスキームは EID として CGR の IDevID シリアル番号を使用する方法です。 これらのルータでは、シリアル番号に次の式を使用します。 PID+SN。 次に、例を示します。 CGR1120/K9+JAFXXXXXXX。

deviceType：ハードウェア プラットフォームまたはシリーズを特定するのにこれが使用されます

。 1120 および 1240 モデルの両方では、deviceType 値は cgr1000 となります。

tunnelHerEid：FND が HA ペアもしくはスタンドアロンで実行される 2 つの HER の使用を許可しているため、tunnelHerEid フィールドはこの CGR の VPN トンネル終端がどちらの HER につながるか識別するために使用されます。 この値は、単に適切な HER の EID になります。

certIssuerCommonName：このフィールドはゼロタッチ導入（ZTD）の要件で、通常、ルート RSA 認証局の DNS 名と同じです。 共通名がわからない場合は、コマンド **show crypto ca certificates** を実行して調べることができます。 LDevID トラストポイントのチェーンで、「CA certificate 0'」の件名内にルート発行者の共通名が表示されます。 または、単に FND の [Certificates] ページにアクセスすれば、ルート証明書を表示できます。

meshPrefixConfig：この値は WPAN モジュール インターフェイスに割り当てられます。 このルータでルーティング ポリシー言語（RPL）ツリーを形成するすべての CGE は DHCP（DHCP リレーが適切に設定されているという前提）からネットワーク プレフィックスとしてこの値が付与されている IP アドレスを受信します。

tunnelSrcInterface1：プライマリとセカンダリ IPsec トンネルを使用した導入では、この値はプライマリ トンネルのトンネル ソース インターフェイス名です（cellular4/1 など）。 バックアップ トンネルがある場合は、tunnelSrcInterface2 の値を足して、送信元インターフェイスを割り当てます。 WAN 接続が 1 つのみの場合、tunnelSrcInterface1 フィールドのみを使用します。

ipsecTunnelDestAddr1：この値は送信元インターフェイスが tunnelSrcInterface1 に割り当てられたプライマリ IPsec トンネル用の IPv4 トンネル宛先アドレスです。

adminUsername：これは FAR で HTTPS、Netconf セッションを開くのに FND が使用するユーザ名です。 このユーザは AAA からすべての権限を付与されているか、またはネットワーク管理者の役割に口ーカルで設定されている必要があります。

adminPassword：adminUsername アカウントのパスワード。 このユーザ名は、GUI のデバイス ページの [Config Properties] タブに移動し、[Router Credential] のセクションの [Administrator Username] で確認できます。 エラーを避けるため、このパスワードは cgms ツール RPM パッケージから Signature_Tool で最初に暗号化する必要があります。 このツールは任意のプレーン テキストを cgms_keystore の証明書チェーンを使用して暗号化します。 署名ツールを使用するには、FND アプリケーション サーバのディレクトリを /opt/cgms-tools/bin/ に変更します。 次に、adminPassword を含む、新規のプレーン テキストの .txt ファイルを作成します。 テキスト ファイルができたら、次のコマンドを実行します。

```
./signature-tool encrypt /opt/cgms/server/cgms/conf/cgms_keystore password-file.txt
```

暗号化された出力内容を .csv ファイルの adminPassword フィールドにコピー/貼り付けします。 署名ツールの使用が終わったら、プレーン テキストのパスワード ファイルを安全に削除することをお勧めします。

cgrusername1：このユーザ アカウントは必須ではありませんが、異なる役割の複数のユーザが

CGR で設定されている場合、ここで別のユーザ アカウントを追加できます。 デバイスの管理には adminUsername と adminPassword しか使用されない点にご注意ください。 このラボのセットアップでは、adminUsername と同じクレデンシャルを使用します。

cgrpassword1：cgrusername1 ユーザのパスワードです。

ip：これは、プライマリ管理用 IP です。 ping やトレースが FND で実行されると、この IP が使用されます。 Connected Grid Device Manager（CGDM）の HTTPS セッションはこの IP にも送信されます。 一般的な導入では、これは tunnelSrcInterface1 インターフェイスに割り当てられている IP アドレスです。

meshPanidConfig：この CGR の WPAN のインターフェイスに割り当てられた PAN ID。

wifiSsid：WPAN のインターフェイスに設定されている SSID。

dhcpV4TunnelLink：FND が DHCP サーバにプロキシ要求をするときに使用する IPv4 アドレス。 このラボ環境では、DHCP サーバは Cisco Network Registrar（CNR）で、DHCPv4 IPsec プールは /31 のサブネットをリースするように設定されています。 dhcpv4TunnelLink 値に利用可能な /31 のサブネット内の最初の IP を使用する場合、FND はポイントツーポイント サブネットから CGR トンネル 0 および HER で対応するトンネルに両方の IP をプロビジョニングします。

dhcpV6TunnelLink：FND が IPv6 Generic Routing Encapsulation（GRE）トンネル用に DHCP サーバへのプロキシ要求で使用する IPv6 アドレス。 このラボ環境では /127 のプレフィックスを使用するアドレスをリースするために、CNR が設定されます。 dhcpV4TunnelLink のように、GRE トンネルを設定すると、FND は HER へのポイントツーポイント サブネットの 2 番目の IP を自動的にプロビジョニングします。

dhcpV4LoopbackLink：CGR のループバック 0 インターフェイスを設定する際に FND が DHCP サーバへのプロキシ要求で使用する IPv4 アドレス。 このラボ環境では /32 のサブネットをリースするために、対応する CNR の DHCP プールが設定されています。

dhcpV6LoopbackLink：CGR のループバック 0 インターフェイスを設定する際に FND が DHCP サーバへのプロキシ要求で使用する IPv6 アドレス。 このラボ環境では /128 のサブネットをリースするために、対応するプールが設定されています。

ヘッドエンド ルータ（HER）

ヘッドエンド ルータを初めて追加するときに、このテンプレートを使用できます。

```
eid,deviceType,name,status,lastHeard,runningFirmwareVersion,ip,netconfUsername,netconfPassword
```

deviceType：ASR または CSR を導入する際は、「asr1000」の値をこのフィールドに使用します。

ステータス：承認ステータス値は unheard および down、up です。 新しいインポートには unheard を使用します。

lastheard：新しいデバイスの場合は、このフィールドは空白のままにしておくことができます。

runningFirmwareVersion：この値は空白にしておくこともできますが、バージョンをインポートする場合は、**show version output** の一番上の行からのバージョン番号を使用します。 たとえば、次の出力では、「03.16.04b.S」の文字列を使用してください。

```
Router#show version
Cisco IOS XE Software, Version 03.16.04b.S - Extended Support Release
```

netconfUsername：HER への完全な Netconf/SSH アクセス権を有するユーザ設定のユーザ名。

netconfPassword：[netconfUsername] フィールドに指定したユーザのパスワード。

Connected Grid エンドポイント（CGE）

非常に簡単に DB へ新しいメッシュ エンドポイントを追加できます。 このテンプレートを使用できます。

```
EID,deviceType,lat,lng
```

deviceType：このラボ環境では、CGE としてスマート メーターを追加するのに cgmesh が使用されました。

lat：CGE がインストールされる場所の GPS 緯度。

lng：GPS 経度。

例

FAR の追加：

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunne
lDestAddr1,
adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhcpV4TunnelLi
nk,
dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink CGR1120/K9+JAF########,cgr1000,ASR1006-
X+JAB#########,root-ca-common-name,2001:db8::/32,cellular3/1,
192.0.2.1,Administrator,ajfiea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,Administrator,
ajfiea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,198.51.100.1,5,meshssid,203.0.113.1,2001:d
b8::1,
209.165.200.225,2001:db8::90FE
```

HER の追加：

```
eid,deviceType,name,status,lastHeard,runningFirmwareVersion,ip,netconfUsername,netconfPassword
ASR1006-X+JAB#########,CSR1000V+JAB########,asr1000,CSR1000V+JAB########,unheard,,,192.0.2.1,
Administrator,ofhel35s804502gagh=
```

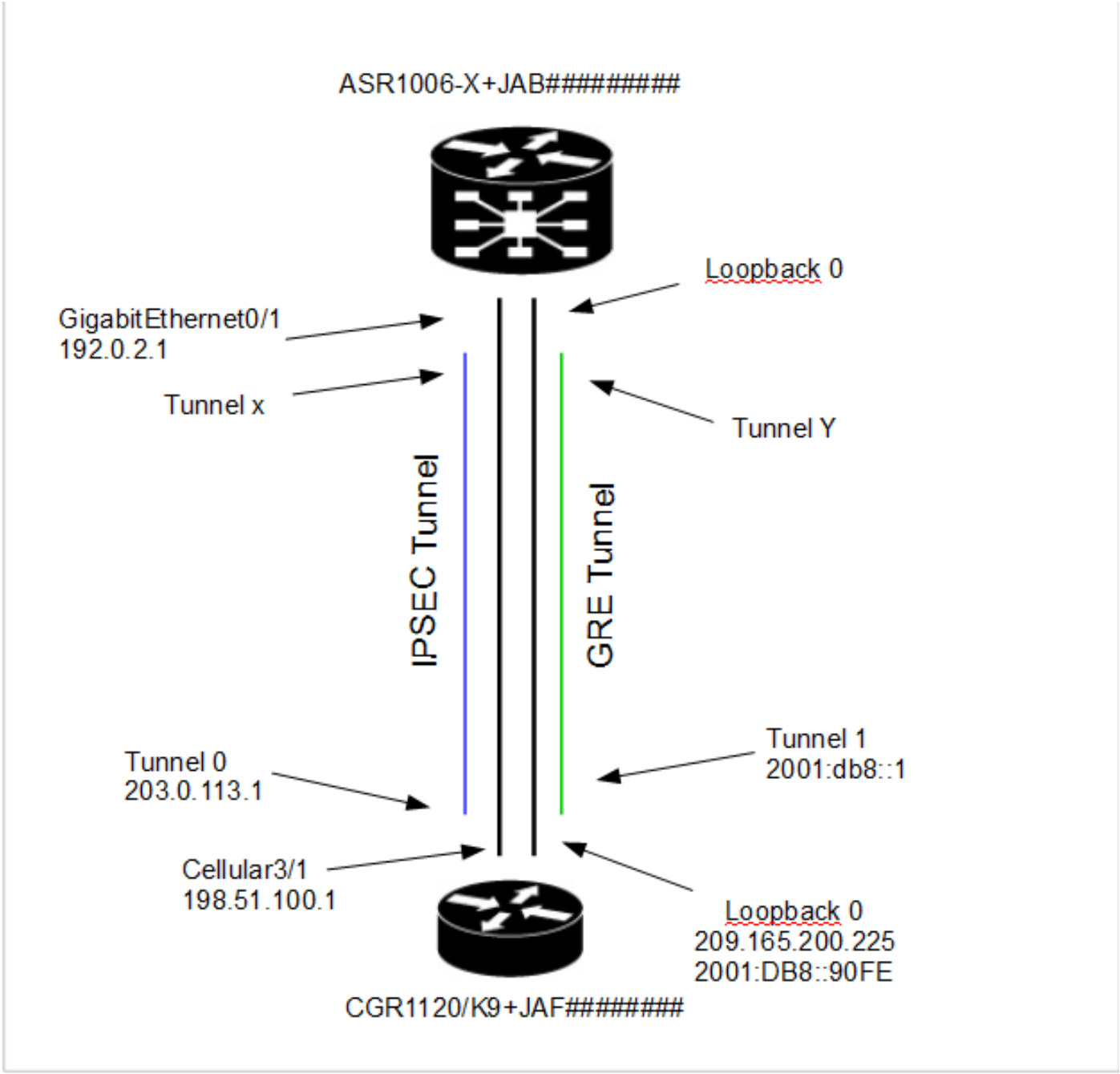
CGE の追加：

```
EID,deviceType,lat,lng
##############,cgmesh,64.434562,-102.750984
```

ネットワーク図

> **注:** FAR が CG-OS を実行するか、IOS を実行するかでトンネルのプロビジョニング作業が異なります。 CG-OS： 新しい IPsec トンネル インターフェイスが FAR と HER の両方に設定されます。 FND はトンネルあたり 2 つの IP のプロキシ要求を DHCP サーバに送信し、対応するトンネル インターフェイスで 2 番目の IP を自動的に設定します。 IOS： HER はポイントツーマルチポイントの IPsec トンネルを使用する Flex VPN テンプレートを使用します。 この設定では、FAR のみに新しいトンネル インターフェイスが届きます。

このトポロジ図では、「トンネル x」は HER に相対する IPsec トンネル インターフェイスを意味し、「トンネル Y」は HER のループバック インターフェイスから構築された GRE トンネルに対応します。 さらに、図の IP とインターフェイスは .csv テンプレートの設定例に直接対応します。


ASR1006-X+JAB########
Loopback 0
GigabitEthernet0/1
192.0.2.1
Tunnel x
Tunnel Y
IPSEC Tunnel
GRE Tunnel
Tunnel 0
203.0.113.1
Tunnel 1
2001:db8::1
Cellular3/1
198.51.100.1
Loopback 0
209.165.200.225
2001:DB8::90FE
CGR1120/K9+JAF########