FND の新しいデバイスをインポートするために .csv（コンマ区切り値）ファイルを準備して下さい

目次

概要

この資料はフィールド Network Director （FND）の .csv ファイルを準備をするためにステップを記述したものです。 セキュア ネットワーク管理を提供するために、FND は自動かダイナミック アセット ディスカバリおよび登録を提供しません。 新しいデバイスが FND 配置に追加することができる前にユニークなデータベースエントリはそれのために Web ユーザ ユーザー・ インターフェース（UI）によってカスタム .csv ファイルのインポートによって作成する必要があります。

この技術情報は既存 の ソリューシ ョンに新しいエンドポイント、フィールド エリア ルータまたはヘッドエンドルータを追加するために使用され、カスタマイズすることができる .csv テンプレートを提供します。 これに加えて、各データベース（DB）フィールドは新しいデバイスの設計および実装と助けるために定義され、説明されます。

> **注:** このガイドが使用することができる前に申し分なく設定されたおよびインストール済み Connected Grid ネットワーク管理システム（CG-NMS）/FND ソリューションがなければなりません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- 利用可能 な Web UI アクセスとインストールされ、動作する CG-NMS/FND アプリケ– ションサーバ 1.0 またはそれ以降。

- インストールされるトンネル 供給サーバ（TPS）プロキシサーバおよび実行。
- インストールされ、正しく設定される Oracle Database Server。
- setupCgms.sh は一度正常な 1 回目の db_migrate と正常に少なくとも動作します。
- この資料を使用する前に組織は配備のために十分に IPv4 および IPv6 アドレス方式を計画したことがまだ DHCP サーバを強く推奨されればインストールしないし、が、設定したらまだこのガイドを使用できます。 これには接続されたグリッド ルータ（CGR）ループバックの IPv4 IPSecトンネル、IPv6 総称ルーティング カプセル化（GRE）トンネルおよびデュアルスタック アドレッシングのためのプレフィクス長および範囲が含まれています。
- 既に購入するか、または少なくとも 1 つのヘッドエンドルータ、少なくとも 1 フィールド エリア ルータおよび少なくとも 1 エンドポイント/メートルを購入することを計画していることがまた強く推奨されます。

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 （ また 3.0.1-36 ）
- cgms ツールは実装しますアプリケ− ションサーバ（3.0.1-36）にインストールされて
- RHEL 6.5 を動作するすべての Linux サーバ
- Windows サーバ 2008 R2 企業を動作する All ウィンドウ サーバ
- Cisco Cloud はヘッドエンドルータとして VM で動作するルータ（CSR） 1000v を保守します
- CG-OS とフィールド エリア ルータとして（遠い）使用される CGR-1120/K9 4(3)

制御された FND ラボ 環境はこの資料の作成の間に使用されました。 他の配備が異なる間、インストレーションガイドからのすべての最小限の要件に付着する必要があります。

このドキュメントの情報は、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、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

FND のデバイスを追加する .csv ファイル

ずっと

このテンプレートはずっとに使用することができますソリューションにはじめて導入される。 これは **Devices ページ デバイス > フィールド**にあります。 Devices ページ フィールドで**バルク インポート** ドロップダウンメニューをクリックし、**デバイスを**『Add』 を選択 して下さい。

```
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、また GUI のデバイスを識別するのに使用される固有の識別番号です。 組織が EID 方式を開発することが混合を防ぐために、推奨されます。 お勧めの方式は EID として CGR の IDevID シリアル番号を使用することです。 これらのルータで、シリアル番号はこの数式を使用します: PID+SN. 次に、例を示します。 .

deviceType -これがハードウェアプラットフォームかシリーズを識別するのに使用されています。 1120 および 1240 のモデルに関しては、deviceType 値は cgr1000 であるはずです。

tunnelHerEid - FND が 2 の使用に HA ペアで動作するか、またはスタンドアロン彼女の物を与えるというファクトが原因で彼女がこの CGR の VPN トンネル終わる tunnelHerEid フィールドが識別するのに使用されています。 この値は適切のの EID 彼女単にです。

certIssuerCommonName -このフィールドはゼロ タッチ配備（ZTD）の要件で、通常ルート RSA の DNS名と認証局（CA）同じです。 Common Name を知らない場合、それを見つけ、コマンド **show crypto ca certificates を**実行できます。 LDevID トラストポイントのためのチェーンでは、「CA 認証 0' の件名のルート発行元 Common Name を見ます。 また、FND の認証 ページに単にアクセスでき、原証明を検知 します。

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。 すべての CGEs はこの値の DHCP によってネットワークプレフィクスとしてこのルータが付いているルーティングポリシー言語（RPL）ツリーを形成する IP アドレスを（DHCPリレーを仮定することは適切に設定されます）受け取ります。

tunnelSrcInterface1 -プライマリおよびセカンダリ IPSecトンネルを利用する配備に関してはこの値はプライマリ トンネルにおけるトンネル ソースのインターフェイス名です（cellular4/1 のような）。 バックアップ トンネルがあれば tunnelSrcInterface2 に値の追加によってソースインターフェイスを割り当てます。 1 つの WAN 接続をそして tunnelSrcInterface1 フィールド 使用だけもらえばただ。

ipsecTunnelDestAddr1 -この値は tunnelSrcInterface1 に割り当てられるソースインターフェイスが付いているプライマリ IPSecトンネルのための IPv4 トンネル宛先 アドレスです。

adminUsername -これはに HTTPS および Netconf セッションをずっと開くとき FND が使用するユーザ名です。 このユーザが AAA によって完全な権限を与えられるか、またはネットワーク Admin ロールでローカルで設定されることが必要となります。

adminPassword - adminUsername アカウントのためのパスワード。 GUI のこのユーザ名を表示し、デバイスのページの Config Properties タブにナビゲートでき、「ルータ 資格情報のセクションの「管理者のユーザ名」を検知 します。 エラーを防ぐために、このパスワードは cgms ツール RPM パッケージからの Signature_Tool と最初に暗号化する必要があります。 cgms_keystore の証明書 チェーンを使用して平文のこのツール 暗号化何でも。 シグニチャ ツールを使用するために、FND アプリケ− ションサーバの /opt/cgms-tools/bin/ にディレクトリを変更して下さい。 次に、平文 .txt 新しいファイルを作成して下さい adminPassword が含まれている。 テキストファイルがあったら、このコマンドを実行して下さい:

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

暗号化された出力 .csv ファイルの adminPassword フィールドへのコピーして下さい/貼り付け。 シグニチャ ツールを使用するために終わるとき安全に 平文 パスワードファイルを削除することが得策です。

cgrusername1 -このユーザアカウントが必要となりません、異なるロールの複数のユーザが CGR で設定されれば、別のユーザアカウントをここに追加できます。 adminUsername および adminPassword だけデバイスの管理のために使用されることを確認することは重要です。 このラボ の セットアップでは、adminUsername と同じ資格情報を使用して下さい。

cgrpassword1 - cgrusername1 ユーザ向けのパスワード。

IP -これはプライマリ 管理 IP です。 ping かトレースが FND から実行される場合この IP を使用します。 接続されたグリッド デバイスマネージャ（CGDM）のための HTTPS セッションはこの IP に同様に送信 されます。 典型的な配備では、これは tunnelSrcInterface1 インターフェイスに割り当てられた IP アドレスです。

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

wifiSsid - WPAN インターフェイスで設定される SSID。

dhcpV4TunnelLink - FND が DHCPサーバにプロキシ要求で使用する IPv4 アドレス。 このラボ環境では、DHCPサーバは Cisco Network Registrar （CNR）であり、/31 サブネットをリースするために DHCPv4 IPsec プールは設定されます。 dhcpv4TunnelLink 値のために /31 利用可能 なサブネットで最初の IP を使用すれば FND は自動的にポイントツーポイント サブネットから CGR のトンネル 0 および HER の対応した トンネルに両方の IP を提供します。

dhcpV6TunnelLink - FND が IPv6 一般的ルーティングカプセル化のために DHCPサーバに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 プレフィックスの使用のアドレスをリースするために、CNR は設定されます。 dhcpV4TunnelLink と同様に、FND はに自動的にGREトンネルを設定する場合ポイントツーポイント サブネットの第 2 IP を彼女提供します。

dhcpV4LoopbackLink - FND が場合の CGR のループバック 0 インターフェイスを設定するDHCPサーバに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 サブネットをリースするために、CNR の対応した DHCPプールは設定されました。

dhcpV6LoopbackLink - CGR のループバック 0 インターフェイスを設定する場合の FND がDHCPサーバに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 サブネットをリースするために、対応したプールは設定されました。

ヘッドエンドルータ（彼女）

ヘッドエンドルータをはじめて追加するとき、このテンプレートは使用することができます:

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

deviceType - ASR か CSR を導入するとき、'asr1000 値はこのフィールドで使用する必要があります。

ステータス-受け入れられたステータス値は聞こえなく、活動化します。 それが新しいインポートである場合聞こえない使用して下さい。

lastheard -これが新しいデバイスである場合、このフィールドは空白のままにすることができます。

runningFirmwareVersion -この値はことができましたり同様に空白のままにするバージョンをインポートしたいと思えば **show version 出力**まさに上行からのバージョン番号を使用します。 たとえば、この出力で、'03.16.04b.S ストリングは使用する必要があります:

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

netconfUsername -に完全な Netconf/SSH アクセスを持つユーザ設定のユーザ名彼女。

netconfPassword - netconfUsername フィールドで規定 される ユーザ向けのパスワード。

接続されたグリッド エンドポイント (CGE)

DB へ新しいメッシュ エンドポイントを追加することは非常に簡単です。 このテンプレートは使用することができます:

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

deviceType -このラボ 環境では、CGE としてスマートなメートルを追加するのに「cgmesh」が使用されました。

lat - CGE がインストールされる GP 緯度座標。

液化天然ガス- GP 経度。

例

遠い付加:

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunnelDestAddr1,
adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhcpV4TunnelLink,
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:db8::1,
209.165.200.225,2001:db8::90FE
```

彼女の付加:

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

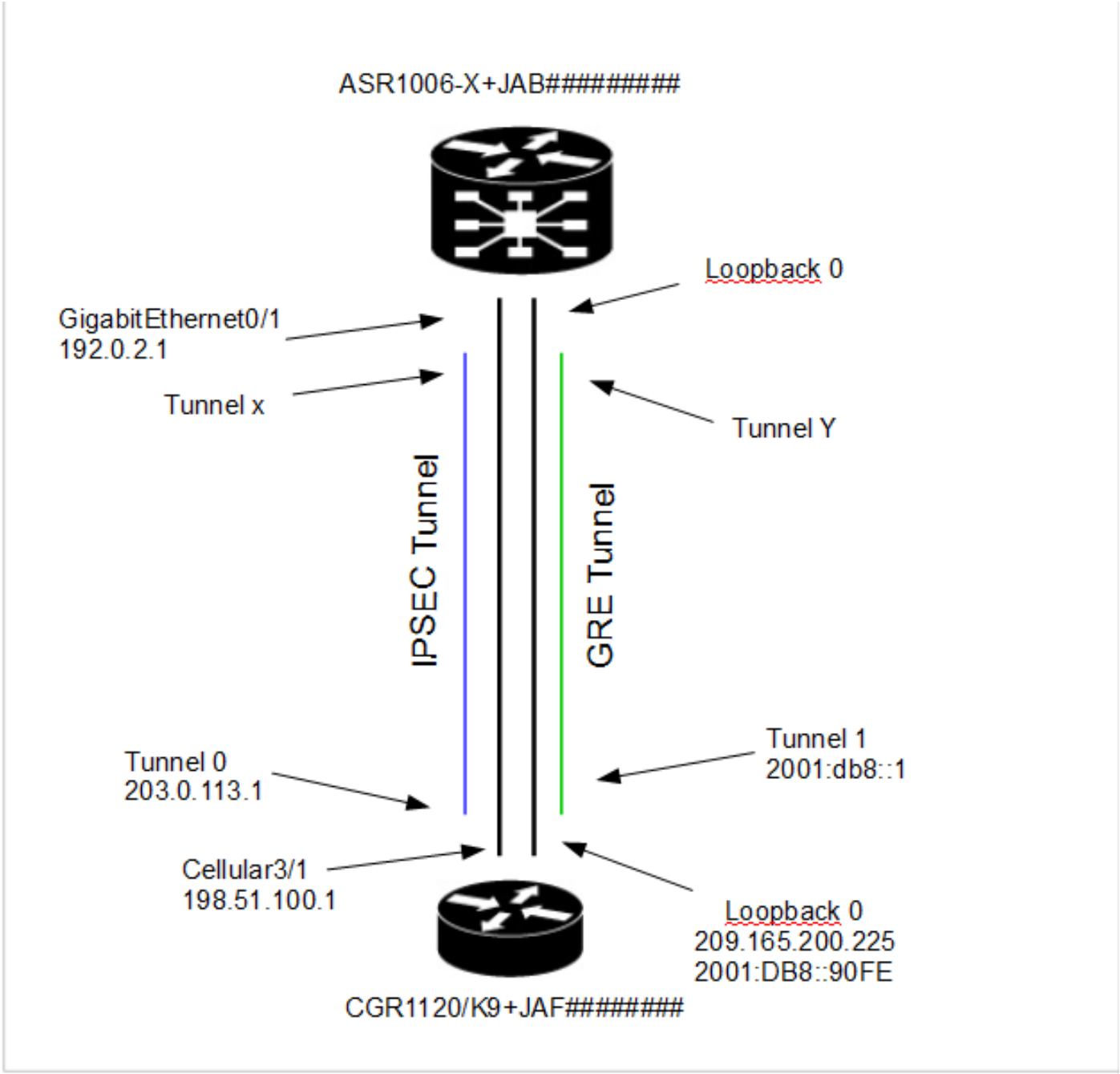
CGE 付加:

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

ネットワーク図

> **注:** ずっと a が CG-OS か IOS を実行しているかどうか基づく作業を別様に提供するトンネル。 CG-OS: 新しい IPSecトンネル インターフェイスはで彼女ずっと設定され。 FND はトンネル毎に 2 IP のための DHCPサーバにプロキシ要求を送信 し、ために対応した トンネル インターフェイスで第 2 IP を自動的に設定して下さい。 IOS： 彼女はポイント マルチポイント間 IPSecトンネルを使用する屈曲 VPN テンプレートを使用します。 この設定を使って、FARs レシーブ新しいトンネルインターフェイスだけ。

このトポロジーダイアグラム「トンネル「トンネル Y」がのループバックインターフェイスの構築される GREトンネルによって彼女対応する間、X で」の相対的 な IPSecトンネル インターフェイスを彼女参照します。 なお、ダイアグラムの IP および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########