ゼロ タッチ導入のための CGOS を使用した CGR 1000 の設定

目次

概要

このドキュメントでは、Connected Grid オペレーティング システム（CGOS）を備えた Connected Grid ルータ 1000（CGR 1000）を、フィールド デバイスとして Field Network Director（FND）に正常に登録するために必要な設定手順について説明します。 ルータを FND に登録する前に、Public Key Infrastructure（PKI）の登録、カスタム設定など、いくつかの前提条件を満たす必要があります。 これに加えて、不要な部分がない設定例が含まれます。

著者：Cisco TAC エンジニア、Ryan Bowman

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。
- FND Web ユーザ インターフェイス（UI）の [Admin] > [Provisioning Settings] ページで保存されたプロキシ設定のある、構成済みで使用可能な DHCPv4 および DHCPv6 サーバ。
- device .csv ファイルが FND にすでにインポートされている必要があり、デバイスが「unheard」ステータスである必要があります。

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 で実行される CSR 1000v
- CG-OS 4(3) を備えた Fied Area Router（FAR）として使用される 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。

段階的な設定と登録

1. デバイスのホスト名を設定します。

2. ドメイン名を設定します。

3. DNS サーバを設定します。

4. 時刻/NTP を設定および確認します。

5. セルラー カード、イーサネット インターフェイス、またはこれらの両方を起動します。 必要なすべてのインターフェイスに IP があること、およびルータにラスト リゾート ゲートウェイがあることを確認します。
FND でループバック 0 インターフェイスを正常にプロビジョニングするために、アドレスを使用してこれをすでに作成している必要があります。 ループバック 0 インターフェイスを作成し、それに IPv4 および IPv6 アドレスがあることを確認します。 トンネル プロビジョニングの後、IP は置き換えられるため、一時 IP を使用できます。

6. 以下の機能を有効にします： ntp、crypto ike、dhcp、tunnel、crypto ipsec 仮想トンネル。

7. トラストポイント登録プロファイルを作成します（これは、RSA 認証局（CA）の Simple Certificate Enrollment Protocol（SCEP）登録 Web ページの直接 URL です。 登録局を使用する場合、この URL は異なります）。

```
Router(config)#crypto ca profile enrollment LDevID_Profile
Router(config-enroll-profile)#enrollment url
http://networkdeviceenrollmentserver.your.domain.com/CertSrv/mscep/mscep.dll
```

8. トラストポイントを作成し、それに登録プロファイルをバインドします。

```
Router(config)#crypto ca trustpoint LDevID
Router(config-trustpoint)#enrollment profile LDevID_Profile
Router(config-trustpoint)#rsakeypair LDevID_Keypair 2048
Router(config-trustpoint)#revocation-check none
Router(config-trustpoint)#serial-number
Router(config-trustpoint)#fingerprint
xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
```

9. SCEP サーバを使用してトラストポイントを認証します。

```
Router(config)#crypto ca authenticate LDevID
  Trustpoint CA authentication in progress. Please wait for a response...
  2017 Mar  8 19:02:00 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_CA_AUTHENTICATE_OK: Trustpoint
LDevID: CA certificates(s) authenticated.
```

10. 公開キー インフラストラクチャ（PKI）にトラストポイントを登録します。

```
Router(config)#crypto ca enroll LDevID
Create the certificate request ..
Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.
Challenge password:
Re-enter challenge password:
The serial number in the certificate will be: PID:CGR1120/K9 SN:JAF############
Certificate enrollment in progress. Please wait for a response...
2017 Mar  8 19:02:24 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_ENROLL_OK: Trustpoint LDevID:
Device identity certificate successfully enrolled to CA.
```

11. 証明書チェーンを確認します。

```
Router#show crypto ca certificates
```

12. Callhome を正しく動作させるために必要な SNMP パラメータを設定します。

```
Router(config)#snmp-server contact NAME
Router(config)#snmp-server user admin network-admin
Router(config)#snmp-server community PUBLIC group network-operator
```

13. 以下の基本 Wireless Personal Area Network（WPAN）モジュール設定を行います。

```
Router(config)#interface wpan 4/1
Router(config-if)#no shutdown
Router(config-if)#panid 5
Router(config-if)#ssid meshssid
Router(config-if)#ipv6 add 2001:db8::1/32
```

14. FND は HTTPS を介した Netconf に基づいて FAR を管理するため、HTTPS サーバを有効にし、ポート 8443 をリッスンし、PKI で接続を認証するようにこの HTTPS サーバを適切に設定します。

```
Router(config)#ip http secure-server
Router(config)#ip http secure-server trustpoint LDevID
Router(config)#ip http secure-port 8443
```

15. callhome プロファイルを設定します。

```
Router(config)#callhome
Router(config-callhome)#email-contact email@domain.com
Router(config-callhome)#phone-contact +1-555-555-5555
Router(config-callhome)#streedaddress TEXT
Router(config-callhome)#destination-profile nms
Router(config-callhome)#destination-profile nms format netconf
Router(config-callhome)#destination-profile nms transport-method http
```

```
Router(config-callhome)#destination-profile nms http https://tpsproxy.your.domain.com:9120
Router(config-callhome)#enable
```

16. 設定を保存します。

17. この時点で実行する必要があるのはルータをリロードすることですが、リロードせずに手動で登録を開始する場合、cgdm を設定できます。

```
Router(config)#cgdm
Router(config-cgdm)#registration start trustpoint LDevID
```

設定例

以下は、正常な ZTD の直前に CGR1120 から取得した不要な部分のない設定です（このラボ環境では、プライマリ IPSec トンネル送信元として Ethernet2/2 インターフェイスを使用しました）。

```
version 5.2(1)CG4(3)
logging level feature-mgr 0
hostname YOUR-HOSTNAME
vdc YOUR-HOSTNAME id 1
   limit-resource vlan minimum 16 maximum 4094
   limit-resource vrf minimum 2 maximum 4096
   limit-resource u4route-mem minimum 9 maximum 9
   limit-resource u6route-mem minimum 24 maximum 24
   limit-resource m4route-mem minimum 58 maximum 58
   limit-resource m6route-mem minimum 8 maximum 8
feature ntp
feature crypto ike
feature dhcp
feature tunnel
feature crypto ipsec virtual-tunnel
username admin password YOURPASSWORD role network-admin
username Administrator password YOURPASSWORD role network-admin
ip domain-lookup
ip domain-name your.domain.com
ip name-server x.x.x.x
crypto key param rsa label LDevID_keypair modulus 2048
crypto key param rsa label YOUR-HOSTNAME.your.domain.com modulus 2048
crypto ca trustpoint LDevID
   enrollment profile LDevID_Profile
   rsakeypair LDevID_keypair 2048
   revocation-check none
   serial-number
   fingerprint xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
crypto ca profile enrollment LDevID_Profile
   enrollment url http://x.x.x.x/CertSrv/mscep/mscep.dll
snmp-server contact NAME
snmp-server user Administrator network-admin
snmp-server community public group network-operator
callhome
   email-contact ciscotac@cisco.tac.com
   phone-contact +1-555-555-5555
   streetaddress Here
   destination-profile nms
   destination-profile nms format netconf
   destination-profile nms transport-method http
   destination-profile nms http https://tpsproxy.your.domain.com:9120 trustpoint LDevID
   destination-profile nms alert-group all
   enable
```

```
ntp server x.x.x.x
ntp server x.x.x.x
crypto ike domain ipsec
vrf context management
vlan 1
service dhcp
ip dhcp relay
line tty 1
line tty 2

interface Dialer1
interface Ethernet2/1
interface Ethernet2/2
   ip address x.x.x.x/30
   no shutdown
interface Ethernet2/3
interface Ethernet2/4
interface Ethernet2/5
interface Ethernet2/6
interface Ethernet2/7
interface Ethernet2/8
interface loopback0
   ip address 1.1.1.1/32
   ipv6 address 2001:x:x::80/128
interface Serial1/1
interface Serial1/2
interface Wpan4/1
   no shutdown
   panid 20
   ssid austiniot
   ipv6 address 2001:db8::1/32
interface Wifi2/1
clock timezone CST -6 0
clock summer-time CST 2 Sun Mar 02:00 1 Sun Nov 02:00 60
line console
line vty
boot kickstart bootflash:/cgr1000-uk9-kickstart.5.2.1.CG4.3.SPA.bin
boot system bootflash:/cgr1000-uk9.5.2.1.CG4.3.SPA.bin
ip route 0.0.0.0/0 x.x.x.x
feature scada-gw
scada-gw protocol t101
scada-gw protocol t104
ip http secure-port 8443
ip http secure-server trustpoint LDevID
ip http secure-server
cgdm
   registration start trustpoint LDevID
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。