為CGR 1000配置CGOS，實現零接觸部署

目錄

簡介

本檔案將說明成功將連線電網作業系統(CGOS)的思科連線電網路由器1000(CGR 1000)註冊到現場網路導向器(FND)作為現場裝置所需的設定步驟。路由器在註冊到FND之前，必須滿足幾個前提條件，包括註冊到公鑰基礎設施(PKI)和自定義配置。除此之外，還將包括經過消毒的示例配置。

作者：Ryan Bowman，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- 安裝並運行CG-NMS/FND應用伺服器1.0或更高版本，並且可以使用Web UI訪問。
- 已安裝並運行隧道調配伺服器(TPS)代理伺服器。
- Oracle資料庫伺服器已安裝並正確配置。
- setupCgms.sh成功運行至少一次，並首次成功運行db_migrate。
- DHCPv4和DHCPv6伺服器已經配置並且可用代理設定，這些設定儲存在FND Web使用者介面(UI)的Admin > Provisioning Settings頁面上。
- 裝置.csv檔案應已匯入到FND，且裝置應處於「未聽」狀態。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FND 3.0.1-36
- 基於軟體的SSM（也是3.0.1-36）
- 應用伺服器中安裝的cgms-tools包(3.0.1-36)

- 所有運行RHEL 6.5的Linux伺服器
- 所有運行Windows Server 2008 R2 Enterprise的Windows伺服器
- CSR 1000v，在VM上作為頭端路由器運行
- CGR-1120/K9用作CG-OS 4(3)的廣域路由器(FAR)

在本文檔建立過程中使用了受控的FND實驗室環境。雖然其他部署會有所不同，但您應該遵守安裝指南中的所有最低要求。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

逐步配置和註冊

1.配置裝置主機名。

2.配置域名。

3.配置DNS伺服器。

4.配置並驗證時間/NTP。

5.開啟蜂窩卡和/或乙太網介面。確保所有必要的介面都有各自的IP，並確保路由器具有最後選用網關。
為了使FND能夠成功設定Loopback 0介面，必須已經使用地址建立該介面。建立Loopback 0介面並檢驗它是否具有IPv4和IPv6地址。您可以使用即插即用IP，因為它們將在隧道調配後被替換。

6.啟用以下功能：ntp、crypto ike、dhcp、tunnel、crypto ipsec virtual-tunnel。

7.建立您的信任點註冊配置檔案(這是RSA證書頒發機構(CA)上簡單證書註冊協定(SCEP)註冊網頁的直接URL。 如果您使用註冊機構，URL將不同):

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

8.建立信任點並將註冊配置檔案繫結到該信任點。

```
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.使用SCEP伺服器驗證您的信任點。

```
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
```

10.將您的信任點註冊到公共金鑰基礎設施(PKI)。

```
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 identi
```

11.驗證您的證書鏈。

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

12.配置Callhome正常工作所需的SNMP引數。

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

13.配置這些基本無線個人區域網路(WPAN)模組設定。

```
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.由於FND依賴通過HTTPS的Netconf來管理FAR，因此啟用並適當配置HTTPS伺服器以偵聽埠8443並驗證與PKI的連線。

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

15.配置您的Callhome配置檔案。

```
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.儲存配置。

17.此時，您只需重新載入路由器，但如果您要手動啟動註冊而不進行重新載入，則可以配置cgdm:

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

示例配置

以下是在成功ZTD之前，從CGR1120獲取的經過消毒的配置（在此實驗環境中，Ethernet2/2介面被用作主IPSec隧道源）：

```
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
```

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。