CGR 1000 configureren met CGOS voor Nul-Touch implementatie

Inhoud

Inleiding

Dit document beschrijft de configuratiestappen die nodig zijn om Cisco Connected Grid-router 1000 (CGR 1000) met Connected Grid-besturingssysteem (CGOS) naar Veldnetwerkdirecteur (FND) te registreren als een veldapparaat. Voordat een router aan de FND is geregistreerd, moet deze voldoen aan verschillende vooraf ingestelde vereisten, waaronder inschrijving in Public Key Infrastructure (PKI) en aangepaste configuratie. Daarnaast zal een geanimeerde voorbeeldconfiguratie worden opgenomen.

Bijgedragen door Ryan Bowman, Cisco TAC Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CG-NMS/FND toepassingsserver 1.0 of later geïnstalleerd en actief met web UI-toegang beschikbaar.
- TPS-proxy (Tunnel Provisioning Server) geïnstalleerd en actief.
- Oracle database server geïnstalleerd en correct ingesteld.
- SetupCgms.sh starten minstens één keer met een succesvol eerste db_migraat.
- DHCPv4- en DHCPv6-server(s) al geconfigureerd en beschikbaar bij proxy-instellingen die zijn opgeslagen op de pagina **Admin > Provisioning Settings** van de FND web User Interface (UI).
- Het device .csv bestand zou al naar het FND geïmporteerd moeten zijn en het apparaat zou in de 'ongekende' status moeten staan.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FND 3.0.1-36
- Op software gebaseerde SSM (ook 3.0.1-36)
- cgms-tools pakket geïnstalleerd op toepassingsserver (3.0.1-36)
- Alle Linux-servers die RHEL 6.5 draaien
- Alle Windows-servers die Windows Server 2008 R2 Enterprise gebruiken
- CSR 1000v op een VM als head-end router
- CGR-1120/K9 gebruikt als glasvezelrouter (FAR) met CG-OS 4(3)

Tijdens het maken van dit document werd een gecontroleerde FND-labomgeving gebruikt. Hoewel andere implementaties zullen verschillen, dient u alle minimumeisen uit de installatiehandleidingen in acht te nemen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Stap voor stap Configuratie en inschrijving

1. Configureer de hostname van het apparaat.

2. Het configureren van de domeinnaam.

3. Het configureren van de DNS-server(s).

4. Het instellen en controleren van de tijd/NTP.

5. Breng de cellulaire kaarten en/of Ethernet interfaces op. Zorg ervoor dat alle gewenste interfaces hun IP's hebben en dat de router een gateway van laatste toevlucht heeft.
Om de FND in staat te stellen de Loopback 0-interface succesvol op te zetten, moet deze al met adressen aangemaakt worden. Maak de Loopback 0 interface en controleer of het IPv4- en IPv6-adressen heeft. U kunt IP's van de weg gebruiken omdat zij na tunnelvoorziening zullen worden vervangen.

6. Schakel deze functies in: ntp, crypto zoals, dhcp, tunnel, crypto ipsec virtuele tunnel.

7. Maak uw profiel voor het inschrijven van uw trustpunt (dit is de directe URL voor de Simple certificaatinschrijving Protocol (SCEP) op uw RSA-certificeringsinstantie (CA). Als u een Registratie-instantie gebruikt, is de URL anders):

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

8. Maak uw vertrouwen en verbind het inschrijvingsprofiel er aan.

```
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. Verifieer uw vertrouwen met de SCEP server.

```
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. Voer uw trustpunt in in de openbare sleutelinfrastructuur (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 identity certificate successfully enrolled to CA.
```

11. Controleer uw ketting.

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

12. Configureer de SNMP-parameters die vereist zijn voor Terugbellen om correct te kunnen werken.

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

13. Het configureren van deze basisinstellingen voor Wireless Local Area Network (WPAN).

```
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. Aangezien het FND afhankelijk is van NetConf over HTTPS om FAR's te beheren, kunt u de HTTPS-server inschakelen en op de juiste manier configureren om op poort 8443 te luisteren en verbindingen met PKI te authentiseren.

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

15. Configureer het oproepprofiel.

```
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. Sla de configuratie op.

17. Op dit punt hoeft u de router alleen te laden maar als u de registratie handmatig wilt starten zonder opnieuw te laden, kunt u Cgdm configureren:

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

Monsterconfiguratie

Hier is een geanimeerde configuratie die is afgeleid van een CGR1120 net voor een succesvolle ZTD (in deze labomgeving werd de Ethernet2/2 interface gebruikt als de primaire IPSec-tunnelbron):

```
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
```

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.