Konfigurieren des CGR 1000 mit CGOS für die Bereitstellung ohne Benutzereingriffe

Inhalt

Einführung

In diesem Dokument werden die erforderlichen Konfigurationsschritte beschrieben, um den Cisco Connected Grid Router 1000 (CGR 1000) mit dem Connected Grid Operating System (CGOS) zu Field Network Director (FND) als Field Device (Feldgerät) erfolgreich zu registrieren. Bevor ein Router beim FND registriert wird, muss er mehrere Voraussetzungen erfüllen, darunter die Anmeldung für Public Key Infrastructure (PKI) und die benutzerdefinierte Konfiguration. Darüber hinaus wird eine animierte Beispielkonfiguration hinzugefügt.

Mitarbeiter: Ryan Bowman, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CG-NMS/FND-Anwendungsserver 1.0 oder höher installiert und ausgeführt mit Web-UI-Zugriff verfügbar.
- Tunnel Provisioning Server (TPS)-Proxyserver installiert und ausgeführt.
- Der Oracle-Datenbankserver wurde installiert und ordnungsgemäß konfiguriert.
- setupCgms.sh wird mindestens einmal erfolgreich mit einem erfolgreichen ersten db_migration ausgeführt.
- DHCPv4- und DHCPv6-Server sind bereits konfiguriert und mit den Proxyeinstellungen verfügbar, die auf der Seite **Admin > Provisioning Settings** (Admin > Bereitstellungseinstellungen) der FND Web User Interface (UI) gespeichert sind.
- Die CSV-Datei des Geräts sollte bereits in den FND importiert worden sein, und das Gerät sollte den Status "ungehört" aufweisen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- FND 3.0.1-36
- Softwarebasiertes SSM (auch 3.0.1-36)
- cgms-tools-Paket installiert im Anwendungsserver (3.0.1-36)
- Alle Linux-Server mit RHEL 6.5
- Alle Windows-Server mit Windows Server 2008 R2 Enterprise
- CSR 1000v wird auf einem VM als Head-End-Router ausgeführt
- CGR-1120/K9 wird als Fire Area Router (FAR) mit CG-OS 4(3) verwendet

Bei der Erstellung dieses Dokuments wurde eine kontrollierte FND-Laborumgebung verwendet. Obwohl sich andere Bereitstellungen unterscheiden, sollten Sie alle Mindestanforderungen aus den Installationsanleitungen einhalten.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Schrittweise Konfiguration und Registrierung

1. Konfigurieren Sie den Geräte-Hostnamen.

2. Konfigurieren Sie den Domänennamen.

3. Konfigurieren Sie die DNS-Server.

4. Zeit/NTP konfigurieren und überprüfen

5. Aufrufen der Mobilfunkkarten und/oder Ethernet-Schnittstellen Stellen Sie sicher, dass alle erforderlichen Schnittstellen ihre IPs haben und dass der Router über ein Gateway der letzten Instanz verfügt.
Damit der FND die Loopback-0-Schnittstelle erfolgreich bereitstellen kann, muss sie bereits mit Adressen erstellt werden. Erstellen Sie die Loopback 0-Schnittstelle, und überprüfen Sie, ob sie über IPv4- und IPv6-Adressen verfügt. Sie können Wegwerf-IPs verwenden, da diese nach der Tunnelbereitstellung ersetzt werden.

6. Aktivieren Sie diese Funktionen: ntp, crypto ike, dhcp, tunnel, crypto ipsec virtual-tunnel.

7. Erstellen Sie Ihr Profil für die Anmeldung von Vertrauenspunkten (Dies ist die direkte URL für die SCEP-Anmeldungs-Webseite (Simple Certificate Enrollment Protocol) auf Ihrer RSA Certificate Authority (CA). Wenn Sie eine Registrierungsstelle verwenden, ist die URL unterschiedlich.)

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

8. Erstellen Sie einen Vertrauenspunkt, und binden Sie das Registrierungsprofil daran.

```
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. Authentifizieren Sie Ihren Vertrauenspunkt mit dem 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. Registrieren Sie Ihren Trustpoint in Public Key Infrastructure (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. Überprüfen Sie Ihre Zellenkette.

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

12. Konfigurieren Sie die erforderlichen SNMP-Parameter, damit Callhome ordnungsgemäß funktioniert.

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

13. Konfigurieren Sie die Moduleinstellungen für diese grundlegenden Wireless Personal Area Network (WPAN)-Module.

```
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. Da das FND für die Verwaltung von FARs auf Netconf über HTTPS angewiesen ist, muss der HTTPS-Server so konfiguriert werden, dass er auf Port 8443 überwacht und Verbindungen mit PKI authentifiziert.

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

15. Konfigurieren Sie Ihr Call Home-Profil.

```
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. Speichern Sie die Konfiguration.

17. An diesem Punkt müssen Sie nur den Router neu laden. Wenn Sie die Registrierung jedoch manuell starten möchten, ohne einen Neustart durchzuführen, können Sie cgdm konfigurieren:

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

Beispielkonfiguration

Es folgt eine animierte Konfiguration, die unmittelbar vor dem erfolgreichen ZTD vom CGR1120 übernommen wurde (in dieser Laborumgebung wurde die Ethernet2/2-Schnittstelle als primäre IPSec-Tunnelquelle verwendet):

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.