Configurazione di CGR 1000 con CGOS per un'installazione zero-touch

Sommario

Introduzione

In questo documento viene descritta la procedura di configurazione necessaria per registrare correttamente Cisco Connected Grid Router 1000 (CGR 1000) con Connected Grid Operating System (CGOS) in Field Network Director (FND) come dispositivo sul campo. Prima di essere registrato nel FND, un router deve soddisfare diversi prerequisiti che includono la registrazione nell'infrastruttura a chiave pubblica (PKI) e la configurazione personalizzata. Inoltre, verrà inclusa una configurazione del campione igienizzato.

Contributo di Ryan Bowman, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CG-NMS/FND Application Server 1.0 o versione successiva installato e in esecuzione con l'accesso all'interfaccia utente Web disponibile.
- Server proxy Tunnel Provisioning Server (TPS) installato e in esecuzione.
- Oracle Database Server installato e configurato correttamente.
- setupCgms.sh è stato eseguito correttamente almeno una volta con una prima migrazione db_migrate riuscita.
- Server DHCPv4 e DHCPv6 già configurati e disponibili con le impostazioni proxy salvate nella pagina **Amministrazione > Impostazioni di provisioning** dell'interfaccia utente Web di FND.
- Il file .csv del dispositivo deve essere già stato importato nel FND e lo stato del dispositivo deve essere 'unheard'.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FND 3.0.1-36
- SSM basato su software (anche 3.0.1-36)
- pacchetto cgms-tools installato nel server applicazioni (3.0.1-36)
- Tutti i server Linux con RHEL 6.5
- Tutti i server Windows che eseguono Windows Server 2008 R2 Enterprise
- CSR 1000v in esecuzione su una VM come router headend
- CGR-1120/K9 usato come router a area delimitata (FAR) con CG-OS 4(3)

Durante la creazione di questo documento è stato utilizzato un ambiente di laboratorio FND controllato. Anche se altre distribuzioni differiscono, è necessario rispettare tutti i requisiti minimi indicati nelle guide all'installazione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione e registrazione dettagliate

1. Configurare il nome host del dispositivo.

2. Configurare il nome di dominio.

3. Configurare i server DNS.

4. Configurare e verificare l'ora/NTP.

5. Visualizzare le schede cellulari e/o le interfacce Ethernet. Verificare che tutte le interfacce necessarie dispongano dei relativi IP e che il router disponga di un gateway di ultima istanza. Affinché il provisioning dell'interfaccia di loopback 0 venga eseguito correttamente, è necessario che sia già stata creata con indirizzi. Creare l'interfaccia Loopback 0 e verificare che contenga indirizzi IPv4 e IPv6. Gli IP "usa-e-mail" possono essere usati perché verranno sostituiti dopo il provisioning del tunnel.

6. Abilitare le seguenti funzioni: ntp, crypto ike, dhcp, tunnel, crypto ipsec virtual-tunnel.

7. Creare il profilo di registrazione del trust point (URL diretto della pagina Web di registrazione SCEP (Simple Certificate Enrollment Protocol) nella CA RSA. Se si utilizza un'autorità di registrazione, l'URL sarà diverso):

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

8. Creare il trust point e associarvi il profilo di iscrizione.

```
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. Autenticare il trust point con il server SCEP.

```
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. Registrare il trust point nell'infrastruttura a chiave pubblica (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. Verificare la catena di certificati.

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

12. Configurare i parametri SNMP necessari per il corretto funzionamento di Callhome.

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

13. Configurare le impostazioni di base del modulo WPAN (Wireless Personal Area Network).

```
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. Poiché il FND si basa su Netconf su HTTPS per gestire FAR, abilitare e configurare in modo appropriato il server HTTPS per l'ascolto sulla porta 8443 e per autenticare le connessioni con PKI.

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

15. Configurare il profilo di callhome.

```
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. Salvare la configurazione.

17. A questo punto, è sufficiente ricaricare il router, ma se si desidera avviare manualmente la registrazione senza ricaricare è possibile configurare cgdm:

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

Esempio di configurazione

Di seguito è riportata una configurazione purificata presa da un CGR1120 poco prima del completamento di ZTD (in questo ambiente di laboratorio l'interfaccia Ethernet2/2 è stata utilizzata come origine principale del tunnel IPSec):

```
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
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.