Configuration du routeur CGR 1000 avec CGOS pour un déploiement sans intervention

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Configuration et inscription étape par étape

Exemple de configuration

Vérifier

Dépannage

Introduction

Ce document décrit les étapes de configuration requises pour enregistrer avec succès le routeur Cisco Connected Grid Router 1000 (CGR 1000) avec le système d'exploitation Connected Grid (CGOS) sur Field Network Director (FND) en tant que périphérique de terrain. Avant d'être enregistré auprès du FND, un routeur doit remplir plusieurs conditions préalables, notamment l'inscription à l'infrastructure à clé publique (PKI) et la configuration personnalisée. En outre, un exemple de configuration vérifiée sera inclus.

Contribution de Ryan Bowman, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveur d'applications CG-NMS/FND version 1.0 ou ultérieure installé et en cours d'exécution avec accès à l'interface utilisateur Web disponible.
- Serveur proxy TPS (Tunnel Provisioning Server) installé et en cours d'exécution.
- Serveur de base de données Oracle installé et correctement configuré.
- setupCgms.sh a été exécuté au moins une fois avec succès la première fois db_migrate.
- Les serveurs DHCPv4 et DHCPv6 sont déjà configurés et disponibles avec les paramètres proxy enregistrés sur la page Admin > Provisioning Settings de l'interface utilisateur Web FND.
- Le fichier .csv du périphérique doit avoir déjà été importé dans le FND et le périphérique doit être à l'état « non écouté ».

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FND 3.0.1-36
- SSM logiciel (également 3.0.1-36)
- package cgms-tools installé dans le serveur d'applications (3.0.1-36)
- Tous les serveurs Linux exécutant RHEL 6.5
- Tous les serveurs Windows exécutant Windows Server 2008 R2 Entreprise
- CSR 1000v exécuté sur une machine virtuelle en tant que routeur de tête de réseau
- CGR-1120/K9 utilisé en tant que routeur de zone fixe (FAR) avec CG-OS 4(3)

Un environnement de travaux pratiques FND contrôlé a été utilisé lors de la création de ce document. Bien que les autres déploiements soient différents, vous devez respecter toutes les exigences minimales des guides d'installation.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configuration et inscription étape par étape

1. Configurez le nom d’hôte du périphérique.

2. Configurez le nom de domaine.

3. Configurez le ou les serveurs DNS.

4. Configurez et vérifiez l’heure/NTP.

5. Activez les cartes cellulaires et/ou les interfaces Ethernet. Assurez-vous que toutes les interfaces nécessaires ont leurs adresses IP et que le routeur dispose d'une passerelle de dernier recours.
Pour que le FND puisse provisionner correctement l'interface de bouclage 0, elle doit déjà être créée avec des adresses. Créez l'interface de bouclage 0 et vérifiez qu'elle possède des adresses IPv4 et IPv6. Vous pouvez utiliser des adresses IP « jetables », car elles seront remplacées après le provisionnement du tunnel.

6. Activez ces fonctionnalités : ntp, crypto ike, dhcp, tunnel, crypto ipsec virtual-tunnel.

7. Créez votre profil d'inscription trustpoint (il s'agit de l'URL directe de la page Web d'inscription SCEP (Simple Certificate Enrollment Protocol) sur votre autorité de certification RSA. Si vous utilisez une autorité d'enregistrement, l'URL sera différente) :

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

8. Créez votre point de confiance et liez-y le profil d'inscription.

```
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. Authentifiez votre point de confiance avec le serveur 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
```

10. Inscrivez votre point de confiance dans l'infrastructure à clé publique (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. Vérifiez votre chaîne de certificats.

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

12. Configurez les paramètres SNMP requis pour que Callhome fonctionne correctement.

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

13. Configurez les paramètres de base du module 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. Comme le FND s'appuie sur Netconf sur HTTPS pour gérer les FAR, activez et configurez correctement le serveur HTTPS pour écouter sur le port 8443 et authentifier les connexions avec PKI.

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

15. Configurez votre profil 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. Enregistrez la configuration.

17. À ce stade, il vous suffit de recharger le routeur, mais si vous souhaitez démarrer manuellement l'enregistrement sans recharger, vous pouvez configurer cgdm :

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

Exemple de configuration

Voici une configuration vérifiée prise à partir d'un routeur CGR1120 juste avant le succès de ZTD (dans cet environnement de travaux pratiques, l'interface Ethernet2/2 a été utilisée comme source

principale du 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
```

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.