为零接触部署配置CGR 1000和CGOS

目录

简介

本文档介绍成功将Cisco Connected Grid Router 1000(CGR 1000)与Connected Grid Operating System(CGOS)注册到Field Network Director(FND)作为现场设备所需的配置步骤。路由器在注册到FND之前，必须满足几个先决条件，包括在公钥基础设施(PKI)中注册和自定义配置。除此之外，还将包括经过清理的示例配置。

作者：Cisco TAC工程师Ryan Bowman。

先决条件

要求

Cisco 建议您了解以下主题：

- 安装并运行CG-NMS/FND应用服务器1.0或更高版本，并可访问Web UI。
- 已安装并运行隧道调配服务器(TPS)代理服务器。
- Oracle数据库服务器已安装并正确配置。
- setupCgms.sh成功运行至少一次，并且第一次成功运行db_migrate。
- DHCPv4和DHCPv6服务器已经配置并且可用于FND Web用户界面(UI)的Admin > Provisioning Settings页面上保存的代理设置。
- 设备.csv文件应已导入FND，且设备应处于“未听”状态。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- FND 3.0.1-36
- 基于软件的SSM（也是3.0.1-36）

- 应用服务器中安装的cgms-tools软件包(3.0.1-36)
- 运行RHEL 6.5的所有Linux服务器
- 运行Windows Server 2008 R2 Enterprise的所有Windows服务器
- CSR 1000v作为头端路由器在虚拟机上运行
- CGR-1120/K9用作带CG-OS 4(3)的广域路由器(FAR)

在本文档的创建过程中使用了受控的FND实验环境。虽然其他部署会有所不同，但您应遵守安装指南中的所有最低要求。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

分步配置和注册

1.配置设备主机名。

2.配置域名。

3.配置DNS服务器。

4.配置并验证时间/NTP。

5.启用蜂窝卡和/或以太网接口。确保所有必要的接口都有自己的IP，并确保路由器具有最后选用网关。
为了使FND能够成功调配Loopback 0接口，必须已创建该接口及其地址。创建Loopback 0接口并检验它是否具有IPv4和IPv6地址。您可以使用即插即用IP，因为它们将在隧道调配后被替换。

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

7.创建信任点注册配置文件(这是RSA证书颁发机构(CA)上简单证书注册协议(SCEP)注册网页的直接URL。 如果您使用注册机构，URL将不同):

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

8.创建信任点并将注册配置文件绑定到信任点。

```
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服务器对信任点进行身份验证。

```
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.在公钥基础设施(PKI)中注册信任点。

```
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.验证证书链。

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

12.配置Callhome正常工作所需的SNMP参数。

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

13.配置这些基本无线个人局域网(WPAN)模块设置。

```
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.由于FND依赖HTTPS上的Netconf来管理FAR，因此启用并适当配置HTTPS服务器以侦听端口

8443并使用PKI验证连接。

```
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配置文件。

```
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.保存配置。

17.此时，您只需重新加载路由器，但如果您要手动启动注册而不重新加载，您可以配置cgdm:

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

配置示例

以下是在ZTD成功之前从CGR1120获取的清理配置（在本实验环境中，Ethernet2/2接口用作主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
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。