تكوين CGR 1000 مع CGOS للنشر من دون لمس

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين والتسجيل خطوة بخطوة
عينة من التكوين
التحقق من الصحة
استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند خطوات التكوين المطلوبة لتسجيل موجه الشبكة المتصلة 1000 (CGR 1000) من Cisco بنجاح مع نظام تشغيل الشبكة المتصلة (CGOS) إلى مدير الشبكة الميدانية (FND) كجهاز حقل. قبل تسجيل الموجه إلى الصندوق الدولي للطبيعة، يجب أن يلبي العديد من المتطلبات الأساسية التي تتضمن التسجيل في البنية الأساسية للمفتاح العام (PKI) والتكوين المخصص. وبالإضافة إلى ذلك، سيتم تضمين نموذج تم تطهيره.

تمت المساهمة من قبل راين بومان، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- يتوفر خادم تطبيق CG-NMS/FND 1.0 أو إصدار أحدث مثبت وقيد التشغيل مع الوصول إلى واجهة مستخدم الويب.
- تم تثبيت خادم وكيل (TPS Tunnel Provisioning Server) وتشغيله.
- تم تثبيت خادم قاعدة بيانات Oracle وتكوينه بشكل صحيح.
- يتم تشغيل setupCgms.sh بنجاح مرة واحدة على الأقل مع db_migrate بنجاح للمرة الأولى.
- تم تكوين خادم (خوادم) DHCPv4 و DHCPv6 ومتوفرا بالفعل مع إعدادات الوكيل المحفوظة على **Admin** > **إعدادات التوفير** في صفحة واجهة مستخدم ويب الخاصة ب UI) FND).
- يجب أن يكون ملف .csv للجهاز قد تم إستيراده بالفعل إلى FND ويجب أن يكون الجهاز في حالة "غير مسموع".

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- د.ت. 36-3,0,1
- SSM المستندة إلى البرامج (أيضا 36-3.0.1)
- حزمة أدوات CGMS المثبتة في خادم التطبيقات (36-3.0.1)
- جميع خوادم Linux التي تعمل بنظام RHEL الإصدار 6.5
- كافة خوادم Windows التي تعمل بنظام التشغيل Windows Server 2008 R2 Enterprise
- CSR 1000v يعمل على جهاز VM كموجه طرفي
- يستخدم CGR-1120/K9 كموجه منطقة مدمجة (FAR) مع 3)4 CG-OS)

تم إستخدام بيئة مختبر FND المتحكم بها أثناء إنشاء هذا المستند. على الرغم من أن عمليات النشر الأخرى ستختلف، إلا أنه يجب عليك الالتزام بجميع المتطلبات الدنيا من أدلة التثبيت.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين والتسجيل خطوة بخطوة

1. قم بتكوين اسم مضيف الجهاز.

2. قم بتكوين domain-name.

3. قم بتكوين خادم (خوادم) DNS.

4. تكوين الوقت/NTP والتحقق منه.

5. قم باستكشاف بطاقات شبكة الجوال و/أو واجهات شبكة إيثرنت. تأكد من أن جميع الواجهات الضرورية تحتوي على عناوين IP الخاصة بها وأن الموجه لديه بوابة المحاولة الأخيرة.
من أجل أن توفر FND بنجاح واجهة الاسترجاع 0، يجب إنشاؤها بالفعل باستخدام العناوين. قم بإنشاء واجهة الاسترجاع 0 وتحقق من أنها تحتوي على عناوين IPv4 و IPv6. يمكنك إستخدام عناوين IP "المرتجلة" لأنه سيتم إستبدالها بعد تزويد النفق.

6. قم بتمكين هذه الميزات: crypto ipSec virtual-tunnel، tunnel، dhcp، crypto ike، ntp.

7. قم بإنشاء ملف تعريف تسجيل تسجيل نقطة الثقة (هذا هو عنوان URL المباشر لصفحة الويب الخاصة بتسجيل بروتوكول تسجيل الشهادة البسيط (SCEP) على مرجع شهادة CA) RSA). إذا كنت تستخدم "مرجع تسجيل"، فسيكون URL مختلفا):

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

8. قم بإنشاء نقطة الثقة الخاصة بك وربط ملف تعريف التسجيل بها.

```
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. مصادقة TrustedPoint الخاصة بك باستخدام خادم SCEP.

```
Router(config)#crypto ca authenticate LDevID
...Trustpoint CA authentication in progress. Please wait for a response
Mar  8 19:02:00 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_CA_AUTHENTICATE_OK: Trustpoint 2017
.LDevID: CA certificates(s) authenticated
```

10. تسجيل نقطة الثقة الخاصة بك في البنية الأساسية للمفتاح العام (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
Mar  8 19:02:24 %$ VDC-1 %$ %CERT_ENROLL-2-CERT_EN_SCEP_ENROLL_OK: Trustpoint LDevID: 2017
.Device identity certificate successfully enrolled to CA
```

11. تحقق من سلسلة السيريتيفيسات.

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

12. قم بتكوين معلمات SNMP المطلوبة ل CallHome للعمل بشكل صحيح.

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

13. قم بتكوين إعدادات الوحدة النمطية للشبكة الشخصية اللاسلكية الأساسية (WPAN) هذه.

```
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 - ونظرا إلى أن الصندوق يعتمد على NetConf عبر HTTPS لإدارة نقاط الوصول البعيدة، فإنه يمكن خادم HTTPS من الاستماع على المنفذ 8443 وتكوينه بشكل مناسب، كما يعتمد على مصادقة الاتصالات مع PKI.

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

15. قم بتكوين ملف تعريف الاستدعاء الرئيسي.

```
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. احفظ التكوين.

17. عند هذه النقطة، كل ما عليك القيام به هو إعادة تحميل الموجه ولكن إذا كنت تريد بدء التسجيل يدويا دون إعادة تحميل، فيمكنك تكوين CGDM:

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

عينة من التكوين

فيما يلي تكوين معطل مأخوذ من CGR1120 قبل ZTD الناجح مباشرة (في بيئة المختبر هذه، تم إستخدام واجهة Ethernet2/2 كمصدر نفق IPSec الأساسي):

```
(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
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).