Настройте CGR 1000 с CGOS для нулевых сенсорных развертываний

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Пошаговая конфигурация и регистрация](#)
[Пример конфигурации](#)
[Проверка](#)
[Устранение неполадок](#)

Введение

Этот документ описывает действия настройки , требуемые успешно зарегистрировать Cisco Связанный маршрутизатор 1000 Сетки (CGR 1000) со Связанной операционной системой сетки (CGOS) Полевому управляющему узлу сети (FND) как Устройство на объекте. Прежде чем маршрутизатор зарегистрирован к FND, он должен встретить несколько предварительных условий, которые включают регистрацию в Инфраструктуру открытых ключей (PKI) и настраиваемую конфигурацию. В дополнение к этому будет включен санированный пример конфигурации.

Внесенный Райаном Боуменом, специалистом службы технической поддержки Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Сервер приложений CG-NMS/FND 1.0 или позже установленный и работающий с веб-доступным доступом UI.
- Установленный прокси-сервер Туннельного сервера инициализации (TPS) и выполнение.
- Установленный сервер базы данных Oracle и правильно настроенный.
- setupCgms.sh успешно работают, по крайней мере, однажды с успешным новым db_migrate.
- DHCPv4 и сервер (серверы) DHCPv6, уже настроенный и доступный с параметрами прокси, экономили **на Admin> Инициализация Страницы настроек** Интерфейса веба - пользователя FND (UI).
- Файл .csv устройства должен был быть уже импортирован в FND, и устройство должно

быть в 'неуслышанном' статусе.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- FND 3.0.1-36
- Программный SSM (также 3.0.1-36)
- пакет cgms-программных-средств, установленный в сервере приложений (3.0.1-36)
- Все серверы Linux рабочий RHEL 6.5
- Все Windows Server, выполняющие Предприятие R2 Windows Server 2008 года
- CSR 1000v работа VM как маршрутизатор головного узла
- CGR-1120/K9 используемый в качестве Областного маршрутизатора Fied (FAR) с ОС CG 4 (3)

Управляемая лабораторная среда FND использовалась во время создания этого документа. В то время как другие развертывания будут отличаться, необходимо придерживаться всех минимальных требований из руководств по установке.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Пошаговая конфигурация и регистрация

1. Настройте имя хоста устройства.

2. Настройте domain-name.

3. Настройте сервер (серверы) DNS.

4. Настройте и проверьте время/NTP.

5. Переведите в рабочее состояние сотовые карты и/или Интерфейсы Ethernet. Гарантируйте, что все необходимые интерфейсы имеют свой IPs и что маршрутизатор имеет шлюз последней очереди.
Для FND для успешной инициализации Loopback 0 интерфейсов это должно уже быть создано с адресами. Создайте Loopback 0 интерфейсов и проверьте, что это имеет IPv4 и адреса IPv6. Можно использовать холостой" IPs, потому что они будут заменены после туннельной инициализации.

6. Активируйте эти опции: ntp, крипто-ike, dhcp, туннель, крипто-действительный туннель ipsec.

7. Создайте свой профиль регистрации точки доверия (Это - прямой URL для веб-страницы регистрации Протокола SCEP (SCEP) на вашем Центре сертификации (CA) RSA. При использовании Центра регистрации URL будет другим):

```
Router(config)#crypto ca profile enrollment LDevID_Profile
Router(config-enroll-profile)#enrollment url
```

```
http://networkdeviceenrollmentserver.your.domain.com/CertSrv/mscep/mscep.dll
```

8. Создайте свою точку доверия и свяжите профиль регистрации с ним.

```
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. Аутентифицируйте свою точку доверия с сервером 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. Зарегистрируйте свою точку доверия в Инфраструктуре открытых ключей (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. Проверьте свою ceritifcate цепочку.

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

12. Настройте параметры SNMP, требуемые для Callhome работать правильно.

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

13. Настройте эти Персональная сеть базового беспроводного подключения (WPAN) параметры настройки модуля.

```
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. Поскольку FND полагается на Netconf по HTTPS, чтобы управлять ФАРСОМ, включить и соответственно настроить сервер HTTPS, чтобы слушать на порту 8443 и аутентифицировать соединения с PKI.

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

15. Настройте свой профиль 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. Сохраните конфигурацию.

17. На этом этапе все, что необходимо сделать, повторно загрузить маршрутизатор, но если вы хотите вручную запустить регистрацию без повторной загрузки, можно настроить cgdm:

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

Пример конфигурации

Вот санированная конфигурация, взятая от CGR1120 незадолго до успешного ZTD (в этой лабораторной среде, интерфейс Ethernet2/2 использовался в качестве основного источника Туннеля 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
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.