CSV-Dateien (durch Komma getrennte Werte) vorbereiten, um neue Geräte auf FND zu importieren

Inhalt

Einführung

In diesem Dokument werden die Schritte zum Vorbereiten der CSV-Datei für Field Network Director (FND) beschrieben. Um ein sicheres Netzwerkmanagement zu gewährleisten, bietet der FND keine automatische oder dynamische Erkennung und Registrierung von Ressourcen. Bevor ein neues Gerät einer FND-Bereitstellung hinzugefügt werden kann, muss ein eindeutiger Datenbankeintrag erstellt werden, indem eine benutzerdefinierte CSV-Datei über die Webbenutzeroberfläche (UI) importiert wird.

Dieser Artikel enthält CSV-Vorlagen, die verwendet und angepasst werden können, um einer vorhandenen Projektmappe neue Endpunkte, Field Area Router oder Head-End-Router hinzuzufügen. Darüber hinaus wird jedes Datenbankfeld (DB) definiert und erläutert, um das Design und die Implementierung neuer Geräte zu unterstützen.

> **Hinweis**: Bevor dieses Handbuch verwendet werden kann, muss eine vollständig konfigurierte und installierte Connected Grid Network Management System (CG-NMS)/FND-Lösung vorhanden sein.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- CG-NMS/FND-Anwendungsserver 1.0 oder höher installiert und ausgeführt mit Web-UI-Zugriff

verfügbar.
- Tunnel Provisioning Server (TPS)-Proxyserver installiert und ausgeführt.
- Der Oracle-Datenbankserver wurde installiert und ordnungsgemäß konfiguriert.
- setupCgms.sh wird mindestens einmal erfolgreich mit einem erfolgreichen ersten db_migration ausgeführt.
- Sie können dieses Handbuch weiterhin verwenden, wenn Sie Ihre DHCP-Server noch nicht installiert und konfiguriert haben. Es wird jedoch dringend empfohlen, dass Ihr Unternehmen vor der Verwendung dieses Dokuments die IPv4- und IPv6-Adressierungsschemata für die Bereitstellung vollständig geplant hat. Dazu gehören Präfixlängen und -bereiche für IPv4 IPSec-Tunnel, IPv6 Generic Routing Encapsulation (GRE)-Tunnel und Dual Stack-Adressierung auf Connected Grid Router (CGR)-Loopbacks.
- Es wird außerdem dringend empfohlen, mindestens einen Head-End-Router, mindestens einen Field Area Router und mindestens einen Endpunkt/Meter zu erwerben bzw. zu kaufen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- FND 3.0.1-36
- Softwarebasiertes SSM (auch 3.0.1-36)
- cgms-tools-Paket installiert im Anwendungsserver (3.0.1-36)
- Alle Linux-Server mit RHEL 6.5
- Alle Windows-Server mit Windows Server 2008 R2 Enterprise
- Cisco Cloud Services Router (CSR) 1000v auf einem VM als Head-End-Router
- CGR-1120/K9 wird als Field Area Router (FAR) mit CG-OS 4(3) verwendet

Bei der Erstellung dieses Dokuments wurde eine kontrollierte FND-Laborumgebung verwendet. Obwohl sich andere Bereitstellungen unterscheiden, sollten Sie alle Mindestanforderungen aus den Installationsanleitungen einhalten.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

CSV-Dateien zum Hinzufügen von Geräten in FND

WEIT

Diese Vorlage kann für FAR verwendet werden, die erstmals in die Lösung aufgenommen werden. Diese finden Sie auf der Seite **Geräte > Feldgeräte**. Klicken Sie auf der Seite Feldgeräte auf das Dropdown-Menü **Massenimport**, und wählen Sie **Geräte hinzufügen aus**.

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunne
lDestAddr1,adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhc
pV4TunnelLink,dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink
```

Element Identifier (eid) - Dies ist eine eindeutige Kennung zur Identifizierung des Geräts in Protokollnachrichten sowie der GUI. Um Verwechslungen zu vermeiden, wird empfohlen, ein EID-Schema zu entwickeln. Es wird empfohlen, die IDevID-Seriennummer des CGR als EID zu verwenden. Auf diesen Routern verwendet die Seriennummer folgende Formel: PID+SN. Beispiel: CGR1120/K9+JAFXXXXXXX.

deviceType - Hiermit wird die Hardwareplattform oder -reihe identifiziert. Für das Modell 1120 und 1240 muss der deviceType-Wert cgr1000 sein.

tunnelYourEid - Da der FND die Verwendung von 2 HERs zulässt, die im HA-Paar oder eigenständig ausgeführt werden, wird das tunnelYourEid-Feld verwendet, um zu bestimmen, auf welche HER die VPN-Tunnel auf diesem CGR enden. Dieser Wert ist lediglich die EID der entsprechenden HER.

certIssuerCommonName - Dieses Feld ist eine Anforderung für die Zero Touch Deployment (ZTD) und entspricht in der Regel dem DNS-Namen Ihrer Root-RSA-Zertifizierungsstelle. Wenn Sie den allgemeinen Namen nicht kennen, können Sie ihn finden und den Befehl **show crypto ca certificate** ausführen. In der Kette für den LDevID-Trustpoint wird der gemeinsame Stammname des Emittenten in der Betreffzeile von "CA certificate 0" angezeigt. Alternativ können Sie einfach auf die Zertifikatsseite des FND zugreifen und das Stammzertifikat anzeigen.

MeshPrefixConfig: Dieser Wert wird der WPAN-Modulschnittstelle zugewiesen. Alle CGEs, die mit diesem Router einen RPL-Tree (Routing Policy Language) bilden, erhalten eine IP-Adresse über DHCP (vorausgesetzt, DHCP-Relay ist entsprechend konfiguriert), wobei dieser Wert als Netzwerkpräfix gilt.

tunnelSrcInterface1 - Bei Bereitstellungen, die primäre und sekundäre IPSec-Tunnel verwenden, ist dieser Wert der Schnittstellenname der Tunnelquelle für Ihre primären Tunnel (z. B. zellulär4/1). Wenn ein Backup-Tunnel vorhanden ist, weisen Sie die Quellschnittstelle zu, indem Sie einen Wert für tunnelSrcInterface2 hinzufügen. Wenn Sie nur eine WAN-Verbindung haben, verwenden Sie nur das Feld tunnelSrcInterface1.

ipsecTunnelDestAddr1 - Dieser Wert ist die IPv4-Tunnel-Zieladresse für den primären IPSec-Tunnel, wobei die Quellschnittstelle TunnelSrcInterface1 zugewiesen ist.

adminUsername - Dies ist der Benutzername, den der FND verwendet, wenn Sie HTTPS- und Netconf-Sitzungen für die FAR öffnen. Dieser Benutzer muss die volle Berechtigung durch AAA erhalten oder lokal mit der Rolle "network-admin" konfiguriert werden.

adminPassword - Das Kennwort für das adminUsername-Konto. Sie können diesen Benutzernamen in der GUI anzeigen und zur Registerkarte Config Properties (Konfigurationseigenschaften) auf der Seite des Geräts navigieren und im Abschnitt "Router Credentials" den Administratorbenutzernamen anzeigen. Um Fehler zu vermeiden, muss dieses Kennwort zuerst mit dem Signature_Tool aus dem RPM-Paket cgms-tools verschlüsselt werden. Dieses Tool verschlüsselt alles im Klartext mit der Zertifikatskette cgms_keystore. Um das

Signaturtool zu verwenden, ändern Sie das Verzeichnis auf dem FND-Anwendungsserver in /opt/cgms-tools/bin/. Erstellen Sie anschließend eine neue TXT-Datei mit Nur-Text, die das adminPassword enthält. Führen Sie nach dem Speichern der Textdatei den folgenden Befehl aus:

```
./signature-tool encrypt /opt/cgms/server/cgms/conf/cgms_keystore password-file.txt
```

Kopieren Sie die verschlüsselte Ausgabe in das adminPassword-Feld Ihrer CSV-Datei, und fügen Sie sie ein. Es empfiehlt sich, die unverschlüsselte Kennwortdatei sicher zu löschen, wenn Sie das Signature-Tool vollständig verwenden.

cgrusername1 - Dieses Benutzerkonto ist nicht erforderlich. Wenn jedoch mehrere Benutzer mit unterschiedlichen Rollen auf dem CGR konfiguriert sind, können Sie hier ein anderes Benutzerkonto hinzufügen. Es ist wichtig zu wissen, dass nur der adminUsername und das adminPassword für die Verwaltung des Geräts verwendet werden. Verwenden Sie in dieser Übung dieselben Anmeldeinformationen wie adminUsername.

cgrpassword1 - Das Kennwort für den Benutzer cgrusername1.

ip - Dies ist die primäre Management-IP. Wenn Pings oder Traces vom FND ausgeführt werden, wird diese IP verwendet. HTTPS-Sitzungen für den Connected Grid Device Manager (CGDM) werden ebenfalls an diese IP gesendet. In einer typischen Bereitstellung ist dies die IP-Adresse, die der tunnelSrcInterface1-Schnittstelle zugewiesen ist.

MeshPanidConfig - Die der WPAN-Schnittstelle dieses CGR zugewiesene PAN-ID.

wifiSsid - Die auf der WPAN-Schnittstelle konfigurierte SSID.

dhcpV4TunnelLink - Die IPv4-Adresse, die der FND in seiner Proxy-Anfrage an den DHCP-Server verwendet. In dieser Laborumgebung ist der DHCP-Server ein Cisco Network Registrar (CNR), und der DHCPv4 IPsec-Pool ist so konfiguriert, dass /31-Subnetze geleast werden. Wenn Sie die erste IP in einem verfügbaren /31-Subnetz für Ihren dhcpv4TunnelLink-Wert verwenden, stellt der FND automatisch beide IPs aus dem Point-to-Point-Subnetz für den CGR-Tunnel 0 und den zugehörigen Tunnel der HER bereit.

dhcpV6TunnelLink - Die IPv6-Adresse, die der FND in seiner Proxy-Anforderung an den DHCP-Server für den IPv6 Generic Routing Encapsulation (GRE)-Tunnel verwendet. In dieser Laborumgebung wird die CNR so konfiguriert, dass Adressen mithilfe von /127-Präfixen geleast werden. Genau wie der dhcpV4TunnelLink stellt der FND beim Konfigurieren des GRE-Tunnels automatisch die zweite IP des Point-to-Point-Subnetzes für die HER bereit.

dhcpV4LoopbackLink - Die IPv4-Adresse, die der FND bei seinen Proxyanforderungen an den DHCP-Server verwendet, wenn er die Loopback 0-Schnittstelle des CGR konfiguriert. In dieser Laborumgebung wurde der entsprechende DHCP-Pool auf dem CNR so konfiguriert, dass /32-Subnetze geleast werden.

dhcpV6LoopbackLink - Die IPv6-Adresse, die der FND beim Konfigurieren der Loopback 0-Schnittstelle des CGR für seine Proxyanforderungen an den DHCP-Server verwendet. In dieser Laborumgebung wurde der entsprechende Pool so konfiguriert, dass /128 Subnetze geleast werden.

Head-End-Router (HER)

Wenn Sie einen Headend-Router zum ersten Mal hinzufügen, kann diese Vorlage verwendet werden:

```
eid,deviceType,name,status,lastHeard,runningFirmwareVersion,ip,netconfUsername,netconfPassword
```

deviceType: Wenn Sie einen ASR oder CSR einführen, sollte in diesem Feld der Wert 'asr1000' verwendet werden.

Status - Akzeptierte Statuswerte sind nicht zu hören, nicht verfügbar, nicht verfügbar und nicht verfügbar. Verwenden Sie ungehört, wenn es sich um einen neuen Import handelt.

lastheard: Wenn es sich um ein neues Gerät handelt, kann dieses Feld leer gelassen werden.

runningFirmwareVersion - Dieser Wert kann ebenfalls leer gelassen werden. Wenn Sie die Version jedoch importieren möchten, verwenden Sie die Versionsnummer in der oberen Zeile der Ausgabe **show version**. In dieser Ausgabe sollte beispielsweise die Zeichenfolge '03.16.04b.S' verwendet werden:

```
Router#show version
Cisco IOS XE Software, Version 03.16.04b.S - Extended Support Release
```

netconfUsername - Der Benutzername des Benutzers, der so konfiguriert ist, dass er vollen Netconf/SSH-Zugriff auf die HER hat.

netconfPassword - Das Kennwort für den im Feld netconfUsername angegebenen Benutzer.

Connected Grid-Endgerät (CGE)

Ein neuer Mesh-Endpunkt zur DB hinzuzufügen ist sehr einfach. Diese Vorlage kann verwendet werden:

```
EID,deviceType,lat,lng
```

deviceType - In dieser Laborumgebung wurde mithilfe von "cgMesh" ein intelligenter Zähler als CGE hinzugefügt.

lat - Die GPS-Breitenkoordinate für die Installation des CGE.

lng - Der GPS-Längengrad.

Beispiele

FAR-Hinzufügung:

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunne
lDestAddr1,
adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhcpV4TunnelLi
nk,
dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink CGR1120/K9+JAF########,cgr1000,ASR1006-
X+JAB#########,root-ca-common-name,2001:db8::/32,cellular3/1,
192.0.2.1,Administrator,ajfiea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,Administrator,
ajfiea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,198.51.100.1,5,meshssid,203.0.113.1,2001:d
b8::1,
209.165.200.225,2001:db8::90FE
```

Hinzufügen:

```
eid,deviceType,name,status,lastHeard,runningFirmwareVersion,ip,netconfUsername,netconfPassword
ASR1006-X+JAB#########,CSR1000V+JAB########,asr1000,CSR1000V+JAB########,unheard,,,192.0.2.1,
Administrator,ofhel35s804502gagh=
```

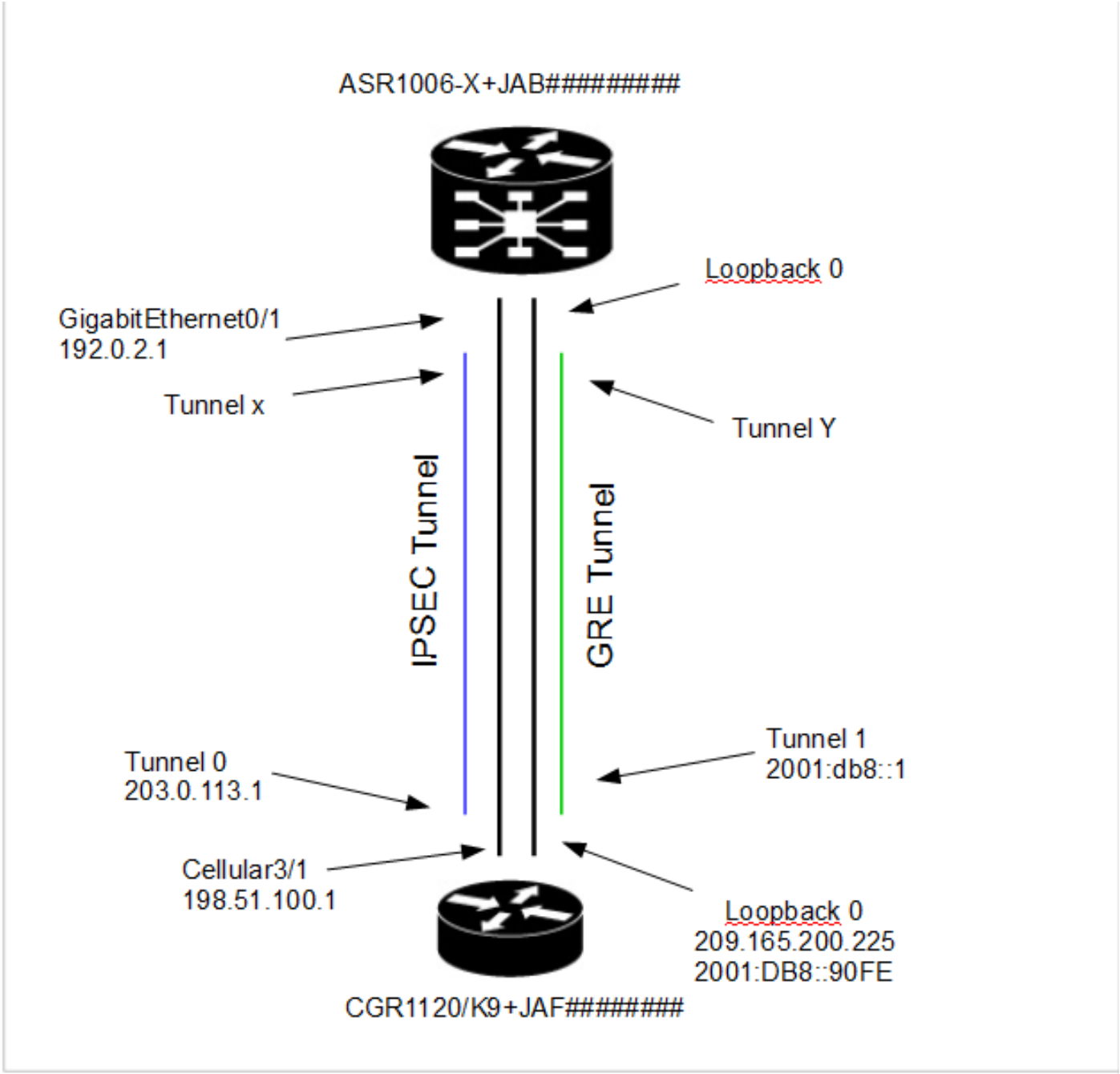
CGE-Hinzufügung:

```
EID,deviceType,lat,lng
###############,cgmesh,64.434562,-102.750984
```

Netzwerkdiagramm

> **Hinweis**: Die Tunnelbereitstellung funktioniert je nachdem, ob ein FAR CG-OS oder IOS verwendet. CG-OS: Sowohl auf der FAR als auch auf der HER wird eine neue IPSEC-Tunnel-Schnittstelle konfiguriert. Der FND sendet eine Proxyanforderung an den DHCP-Server für zwei IPs pro Tunnel und konfiguriert die zweite IP automatisch auf der entsprechenden Tunnelschnittstelle. IOS: Der HER verwendet eine Flex-VPN-Vorlage, die einen Point-to-Multipoint IPSEC-Tunnel verwendet. Bei dieser Konfiguration erhalten nur die FARs neue Tunnelschnittstellen.

In diesem Topologiediagramm bezieht sich "Tunnel x" auf die relative IPSEC-Tunnelschnittstelle auf der HER, während "Tunnel Y" mit dem GRE-Tunnel übereinstimmt, der von der Loopback-Schnittstelle auf der HER erstellt wurde. Außerdem entsprechen die IPs und Schnittstellen im Diagramm direkt den Konfigurationsbeispielen in den CSV-Vorlagen.


ASR1006-X+JAB########
Loopback 0
GigabitEthernet0/1
192.0.2.1
Tunnel x
Tunnel Y
IPSEC Tunnel
GRE Tunnel
Tunnel 0
203.0.113.1
Tunnel 1
2001:db8::1
Cellular3/1
198.51.100.1
Loopback 0
209.165.200.225
2001:DB8::90FE
CGR1120/K9+JAF########