Preparazione di file con estensione csv (valori separati da virgola) per l'importazione di nuovi dispositivi in FND

Sommario

Introduzione

In questo documento viene descritto come preparare il file CSV per Field Network Director (FND). Per garantire una gestione sicura della rete, il FND non fornisce l'individuazione e la registrazione automatiche o dinamiche degli asset. Prima di poter aggiungere un nuovo dispositivo a una distribuzione FND, è necessario creare una voce di database univoca per tale dispositivo importando un file con estensione csv personalizzato tramite l'interfaccia utente Web.

In questo articolo vengono forniti modelli con estensione csv che possono essere utilizzati e personalizzati per aggiungere nuovi endpoint, router per area operativa o router headend a una soluzione esistente. Inoltre, ogni campo del database (DB) verrà definito e spiegato per agevolare la progettazione e l'implementazione di nuovi dispositivi.

> **Nota:** Prima di poter utilizzare questa guida, è necessario disporre di una soluzione Connected Grid Network Management System (CG-NMS)/FND configurata e installata completamente.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- CG-NMS/FND Application Server 1.0 o versione successiva installato e in esecuzione con l'accesso all'interfaccia utente Web disponibile.

- Server proxy Tunnel Provisioning Server (TPS) installato e in esecuzione.
- Oracle Database Server installato e configurato correttamente.
- setupCgms.sh è stato eseguito correttamente almeno una volta con una prima migrazione db_migrate riuscita.
- Èpossibile continuare a utilizzare questa guida se i server DHCP non sono stati ancora installati e configurati, ma si consiglia vivamente di utilizzare questo documento se l'organizzazione ha pianificato completamente gli schemi di indirizzamento IPv4 e IPv6 per la distribuzione. Sono inclusi intervalli e lunghezze dei prefissi per i tunnel IPSec IPv4, i tunnel GRE (Generic Routing Encapsulation) IPv6 e l'indirizzamento a doppio stack sui loopback CGR (Connected Grid Router).
- Si consiglia inoltre di acquistare o prevedere l'acquisto di almeno 1 router headend, almeno 1 router per area operativa e almeno 1 endpoint/metro.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FND 3.0.1-36
- SSM basato su software (anche 3.0.1-36)
- pacchetto cgms-tools installato nel server applicazioni (3.0.1-36)
- Tutti i server Linux con RHEL 6.5
- Tutti i server Windows che eseguono Windows Server 2008 R2 Enterprise
- Cisco Cloud Services Router (CSR) 1000v in esecuzione su una VM come router headend
- CGR-1120/K9 usato come Field Area Router (FAR) con CG-OS 4(3)

Durante la creazione di questo documento è stato utilizzato un ambiente di laboratorio FND controllato. Anche se altre distribuzioni differiscono, è necessario rispettare tutti i requisiti minimi indicati nelle guide all'installazione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

File CSV per aggiungere dispositivi in FND

LONTANO

Questo modello può essere utilizzato per FAR che vengono introdotti per la prima volta nella soluzione. che si trova nella pagina **Dispositivi > Dispositivi da campo**. Nella pagina Dispositivi esterni, fare clic sul menu a discesa **Importazione di massa** e selezionare **Aggiungi dispositivi**.

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

Element Identifier (eid): identificatore univoco utilizzato per identificare il dispositivo nei messaggi

di log e la GUI. Per evitare confusione, si consiglia di sviluppare uno schema EID. Si consiglia di utilizzare il numero di serie IDevID di CGR come EID. Su questi router, il numero di serie utilizzerà la seguente formula: PID+SN. Ad esempio: CGR1120/K9+JAFXXXXXXX

deviceType: utilizzato per identificare la piattaforma o la serie hardware. Per entrambi i modelli 1120 e 1240, il valore deviceType deve essere cgr1000.

tunnelHerEid - Poiché il FND consente l'uso di 2 HER in esecuzione in coppia HA o in modalità standalone, il campo tunnelHerEid viene utilizzato per identificare a quale HER i tunnel VPN su questo CGR termineranno. Questo valore sarà semplicemente l'EID della HER appropriata.

certIssuerCommonName - Questo campo è un requisito di Zero Touch Deployment (ZTD) ed è in genere lo stesso nome DNS della RSA Certificate Authority principale. Se non si conosce il nome comune, è possibile trovarlo ed eseguire il comando **show crypto ca certificates**. Nella catena per il trust point LDevID viene visualizzato il nome comune dell'autorità emittente radice nella riga dell'oggetto di 'Certificato CA 0'. In alternativa, è sufficiente accedere alla pagina Certificati del FND e controllare il certificato radice.

meshPrefixConfig: questo valore viene assegnato all'interfaccia del modulo WPAN. Tutti i CGE che formano un albero RPL (Routing Policy Language) con questo router ricevono un indirizzo IP tramite DHCP (supponendo che il relay DHCP sia configurato correttamente) con questo valore come prefisso di rete.

tunnelSrcInterface1: per le distribuzioni che utilizzano tunnel IPSec primari e secondari, questo valore è il nome dell'interfaccia dell'origine del tunnel per i tunnel primari (ad esempio, la rete cellulare4/1). Se è presente un tunnel di backup, l'interfaccia di origine viene assegnata aggiungendo un valore per tunnelSrcInterface2. Se è presente solo una connessione WAN, verrà utilizzato solo il campo tunnelSrcInterface1.

ipsecTunnelDestAddr1: questo valore rappresenta l'indirizzo di destinazione del tunnel IPv4 per il tunnel IPSec primario con l'interfaccia di origine assegnata a tunnelSrcInterface1.

adminUsername: nome utente che il FND utilizzerà quando si aprono le sessioni HTTPS e Netconf in FAR. È necessario che l'utente disponga di autorizzazioni complete da parte di AAA o sia configurato localmente con il ruolo di amministratore di rete.

adminPassword - Password per l'account adminUsername. È possibile visualizzare questo nome utente nella GUI e andare alla scheda Config Properties nella pagina del dispositivo e controllare 'Administrator Username' nella sezione 'Router Credentials'. Per evitare errori, la password deve essere prima crittografata con Signature_Tool dal pacchetto RPM cgms-tools. Questo strumento consente di crittografare qualsiasi elemento in testo normale utilizzando la catena di certificati in cgms_keystore. Per utilizzare lo strumento firma, passare alla directory /opt/cgms-tools/bin/ sul server applicazioni FND. Creare quindi un nuovo file txt di testo normale contenente adminPassword. Una volta ottenuto il file di testo, eseguire questo comando:

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

Copiare/incollare l'output crittografato nel campo adminPassword del file CSV. È consigliabile eliminare in modo sicuro il file di password di solo testo quando si finisce di utilizzare lo strumento Firma.

cgrusername1 - Questo account utente non è necessario, ma se in CGR sono configurati più utenti con ruoli diversi, è possibile aggiungere un altro account utente. È importante sapere che per la gestione del dispositivo verranno utilizzati solo adminUsername e adminPassword. In questa installazione lab utilizzare le stesse credenziali di adminUsername.

cgrpassword1 - Password dell'utente cgrusername1.

ip - Si tratta dell'IP di gestione principale. Quando i ping o le tracce vengono eseguiti dal FND, utilizzeranno questo IP. Anche le sessioni HTTPS per Connected Grid Device Manager (CGDM) verranno inviate a questo IP. In una distribuzione tipica, questo sarà l'indirizzo IP assegnato all'interfaccia tunnelSrcInterface1.

meshPanidConfig - ID PAN assegnato all'interfaccia WPAN di questo CGR.

wifiSsid - SSID configurato sull'interfaccia WPAN.

dhcpV4TunnelLink - Indirizzo IPv4 che il FND utilizzerà nella richiesta proxy al server DHCP. In questo ambiente lab, il server DHCP è un CNR (Cisco Network Registrar) e il pool IPsec DHCPv4 è configurato per il lease di subnet /31. Se si utilizza il primo IP in una subnet /31 disponibile per il valore dhcpv4TunnelLink, il FND eseguirà automaticamente il provisioning di entrambi gli IP dalla subnet point-to-point al tunnel 0 del CGR e al tunnel corrispondente del HER.

dhcpV6TunnelLink - Indirizzo IPv6 utilizzato dal servizio FND nella richiesta proxy al server DHCP per il tunnel GRE (Generic Routing Encapsulation) IPv6. In questo ambiente lab, il CNR è configurato per assegnare in lease gli indirizzi utilizzando i prefissi /127. Analogamente al dhcpV4TunnelLink, il FND effettua automaticamente il provisioning del secondo IP della subnet point-to-point nell'HER quando si configura il tunnel GRE.

dhcpV4LoopbackLink - L'indirizzo IPv4 che il FND utilizzerà nelle richieste proxy al server DHCP quando si configura l'interfaccia di loopback 0 di CGR. In questo ambiente lab, il pool DHCP corrispondente nel CNR è stato configurato per il lease di subnet /32.

dhcpV6LoopbackLink - Indirizzo IPv6 che il FND utilizzerà nelle richieste proxy al server DHCP quando si configura l'interfaccia di loopback 0 del CGR. In questo ambiente lab, il pool corrispondente è stato configurato per il lease di subnet /128.

Head-End Router (HER)

Quando si aggiunge un router headend per la prima volta, è possibile utilizzare questo modello:

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

deviceType: quando si introduce un ASR o un CSR, in questo campo deve essere utilizzato il valore 'asr1000'.

status - I valori di status accettati sono unheard, down e up. Utilizzare unheard se si tratta di una nuova importazione.

lastheard - Se si tratta di un nuovo dispositivo, questo campo può essere lasciato vuoto.

runningFirmwareVersion: è possibile lasciare vuoto anche questo valore, ma se si desidera importare la versione, utilizzare il numero di versione indicato nella riga superiore dell'output **show version**. Ad esempio, in questo output, si dovrebbe usare la stringa '03.16.04b.S':

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

netconfUsername: il nome utente dell'utente configurato per avere accesso completo Netconf/SSH a HER.

netconfPassword - Password dell'utente specificato nel campo netconfUsername.

Connected Grid Endpoint (CGE)

Aggiungere un nuovo punto finale mesh al database è molto semplice. Questo modello può essere utilizzato:

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

deviceType - In questo ambiente lab, 'cgmesh' è stato utilizzato per aggiungere uno smart meter come CGE.

lat - Coordinata di latitudine GPS in cui verrà installato il CGE.

lng - La longitudine del GPS.

Esempi

Aggiunta remota:

```
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
```

Aggiunge:

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

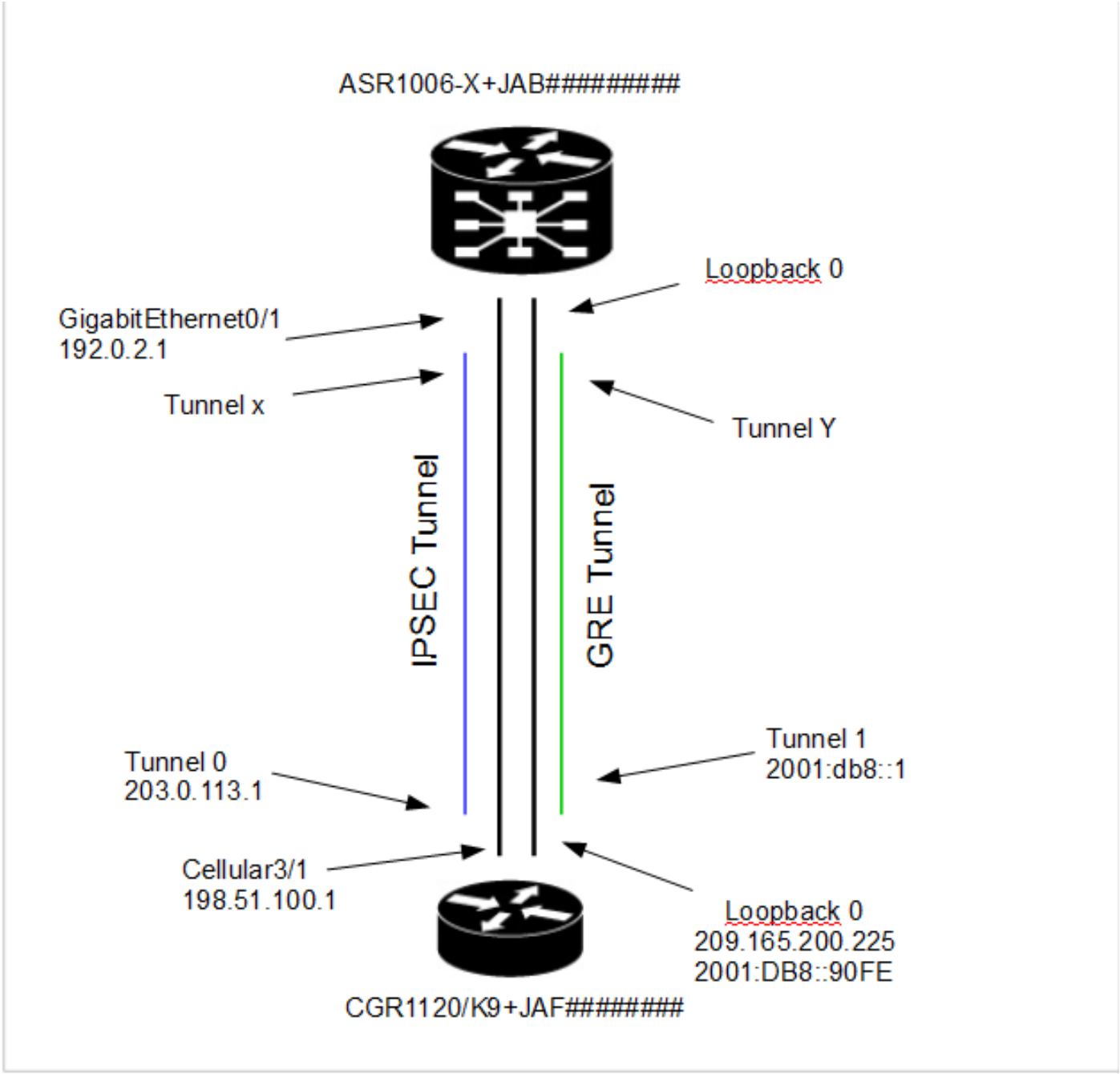
Aggiunta CGE:

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

Esempio di rete

> **Nota:** Il provisioning del tunnel funziona in modo diverso a seconda che su un FAR sia in esecuzione CG-OS o IOS. CG-OS: Una nuova interfaccia del tunnel IPSEC verrà configurata sia su FAR che su HER. Il FND invierà una richiesta proxy al server DHCP per 2 IP per tunnel e configurerà automaticamente il secondo IP sull'interfaccia del tunnel corrispondente. IOS: Il modello HER utilizzerà un modello Flex-VPN che utilizza un tunnel IPSEC point-to-multipoint. Con questa configurazione, solo le FAR ricevono le nuove interfacce del tunnel.

In questo diagramma della topologia, il termine 'tunnel x' si riferisce all'interfaccia del tunnel IPSEC relativa sull'interfaccia HER, mentre il termine 'tunnel Y' corrisponde al tunnel GRE creato dall'interfaccia di loopback sull'interfaccia HER. Inoltre, gli indirizzi IP e le interfacce nel diagramma corrispondono direttamente agli esempi di configurazione nei modelli .csv.


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########