Préparer des fichiers .csv (valeur séparée par des virgules) pour importer de nouveaux périphériques sur FND

Contenu

Introduction

Ce document décrit les étapes de préparation du fichier .csv pour Field Network Director (FND). Afin de fournir une gestion de réseau sécurisée, le FND ne fournit pas la détection et l'enregistrement automatiques ou dynamiques des ressources. Avant qu'un nouveau périphérique puisse être ajouté à un déploiement FND, une entrée de base de données unique doit être créée pour celui-ci en important un fichier .csv personnalisé via l'interface utilisateur Web.

Cet article fournit des modèles .csv qui peuvent être utilisés et personnalisés afin d'ajouter de nouveaux terminaux, routeurs de zone de champ ou routeurs de tête de réseau à une solution existante. En outre, chaque champ de base de données (DB) sera défini et expliqué afin de faciliter la conception et la mise en oeuvre de nouveaux périphériques.

> **Note**: Avant de pouvoir utiliser ce guide, vous devez disposer d'une solution Connected Grid Network Management System (CG-NMS)/FND entièrement configurée et installée.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- CG-NMS/FND Application Server 1.0 ou version ultérieure installé et exécuté avec accès à l'interface utilisateur Web disponible.
- Serveur proxy TPS (Tunnel Provisioning Server) installé et en cours d'exécution.

- Serveur de base de données Oracle installé et correctement configuré.
- setupCgms.sh s'exécute au moins une fois avec une première migration db_migrate réussie.
- Vous pouvez toujours utiliser ce guide si vous n'avez pas encore installé et configuré votre ou vos serveurs DHCP, mais il est fortement conseillé que, avant d'utiliser ce document, votre organisation ait entièrement planifié les schémas d'adressage IPv4 et IPv6 pour le déploiement. Cela inclut les longueurs et les plages de préfixe pour les tunnels IPSec IPv4, les tunnels GRE (Generic Routing Encapsulation) IPv6 et l'adressage double pile sur les boucles du routeur CGR (Connected Grid Router).
- Il est également fortement conseillé d'avoir déjà acheté ou de prévoir d'acheter au moins un routeur de tête de réseau, au moins un routeur de zone de champ et au moins un point d'extrémité/mètre.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FND 3.0.1-36
- SSM logiciel (également 3.0.1-36)
- package cgms-tools installé dans le serveur d'applications (3.0.1-36)
- Tous les serveurs Linux exécutant RHEL 6.5
- Tous les serveurs Windows exécutant Windows Server 2008 R2 Enterprise
- Routeur de services cloud Cisco (CSR) 1000v exécuté sur une machine virtuelle en tant que routeur principal
- CGR-1120/K9 utilisé comme routeur de zone de champ (FAR) avec CG-OS 4(3)

Un environnement de travaux pratiques FND contrôlé a été utilisé lors de la création de ce document. Bien que les autres déploiements diffèrent, vous devez respecter toutes les exigences minimales des guides d'installation.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Fichiers .csv à ajouter aux périphériques dans FND

LOIN

Ce modèle peut être utilisé pour les FAR qui sont présentés à la solution pour la première fois. Elle se trouve sur la page **Périphériques > Périphériques de champ**. Sur la page Périphériques de terrain, cliquez sur le menu déroulant **Importer en masse** et sélectionnez **Ajouter des périphériques**.

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

Element Identifier (eid) - Identificateur unique utilisé pour identifier le périphérique dans les

messages de journal ainsi que dans l'interface utilisateur graphique. Afin d'éviter toute confusion, il est recommandé que votre organisation développe un système d'identification électronique. Le schéma recommandé consiste à utiliser le numéro de série IDevID du CGR comme EID. Sur ces routeurs, le numéro de série utilise la formule suivante : PID+SN. Exemple : CGR1120/K9+JAFXXXXX.

deviceType - Permet d'identifier la plate-forme ou la série matérielle. Pour les modèles 1120 et 1240, la valeur deviceType doit être cgr1000.

tunnelHerEid - Étant donné que le FND autorise l'utilisation de 2 HER s'exécutant en paire HA ou autonome, le champ tunnelHerEid est utilisé pour identifier à quel HER les tunnels VPN de ce CGR se termineront. Cette valeur sera simplement l'EID de l'HER approprié.

certIssueCommonName - Ce champ est obligatoire pour le déploiement automatique (ZTD) et est généralement identique au nom DNS de votre autorité de certification RSA racine. Si vous ne connaissez pas le nom commun, vous pouvez le trouver et exécuter la commande **show crypto ca certificate**. Dans la chaîne du point de confiance LDevID, vous voyez le nom commun de l'émetteur racine dans la ligne d'objet du 'certificat CA 0'. Vous pouvez également accéder à la page Certificats du FND et consulter le certificat racine.

meshPrefixConfig - Cette valeur est attribuée à l'interface du module WPAN. Tous les CGE qui forment une arborescence RPL (Routing Policy Language) avec ce routeur reçoivent une adresse IP via DHCP (en supposant que le relais DHCP soit configuré de manière appropriée) avec cette valeur comme préfixe réseau.

tunnelSrcInterface1 - Pour les déploiements utilisant des tunnels IPSec principal et secondaire, cette valeur est le nom d'interface de la source du tunnel pour vos tunnels principaux (tels que les tunnels cellulaires4/1). S'il existe un tunnel de sauvegarde, vous attribuerez l'interface source en ajoutant une valeur pour tunnelSrcInterface2. Si vous n'avez qu'une connexion WAN, vous n'utiliserez que le champ tunnelSrcInterface1.

ipsecTunnelDestAddr1 - Cette valeur est l'adresse de destination du tunnel IPv4 pour le tunnel IPSec principal avec l'interface source affectée à tunnelSrcInterface1.

adminUsername : nom d'utilisateur que le FND utilisera lorsque vous ouvrirez des sessions HTTPS et Netconf au FAR. Il est nécessaire que cet utilisateur bénéficie d'autorisations complètes par AAA ou qu'il soit configuré localement avec le rôle admin réseau.

adminPassword - Mot de passe du compte adminUsername. Vous pouvez afficher ce nom d'utilisateur dans l'interface utilisateur graphique et accéder à l'onglet Config Properties de la page du périphérique et consulter le nom d'utilisateur administrateur dans la section Router Credential. Afin d'éviter les erreurs, ce mot de passe doit d'abord être chiffré avec Signature_Tool du package RPM cgms-tools. Cet outil chiffre tout ce qui est en texte brut à l'aide de la chaîne de certificats dans le magasin cgms_keystore. Pour utiliser l'outil de signature, modifiez le répertoire en /opt/cgms-tools/bin/ sur le serveur d'applications FND. Ensuite, créez un nouveau fichier .txt en

texte brut qui contient le adminPassword. Une fois que vous avez le fichier texte, exécutez la commande suivante :

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

Copiez/collez la sortie chiffrée dans le champ adminPassword de votre fichier .csv. Il est recommandé de supprimer en toute sécurité le fichier de mot de passe en texte brut lorsque vous avez fini d'utiliser l'outil de signature.

cgrusername1 - Ce compte d'utilisateur n'est pas requis, mais si plusieurs utilisateurs avec des rôles différents sont configurés sur le CGR, vous pouvez ajouter un autre compte d'utilisateur ici. Il est important de savoir que seuls les adminUsername et adminPassword seront utilisés pour la gestion du périphérique. Dans cette configuration de travaux pratiques, utilisez les mêmes informations d'identification que adminUsername.

cgrpassword1 : mot de passe de l'utilisateur cgrusername1.

ip : adresse IP de gestion principale. Lorsque des requêtes ping ou des traces sont exécutées à partir du FND, elles utilisent cette adresse IP. Des sessions HTTPS pour Connected Grid Device Manager (CGDM) seront également envoyées à cette adresse IP. Dans un déploiement type, il s'agit de l'adresse IP attribuée à votre interface tunnelSrcInterface1.

meshPanidConfig - ID PAN attribué à l'interface WPAN de ce CGR.

wifiSsid : SSID configuré sur l'interface WPAN.

dhcpV4TunnelLink : adresse IPv4 que le FND utilisera dans sa requête proxy au serveur DHCP. Dans cet environnement de travaux pratiques, le serveur DHCP est un serveur Cisco Network Registrar (CNR) et le pool DHCPv4 IPsec est configuré pour louer des sous-réseaux /31. Si vous utilisez la première adresse IP d'un sous-réseau /31 disponible pour votre valeur dhcpv4TunnelLink, le FND approvisionne automatiquement les deux adresses IP du sous-réseau point à point vers le tunnel 0 du routeur CGR et le tunnel correspondant du routeur HER.

dhcpV6TunnelLink : adresse IPv6 utilisée par le FND dans sa requête proxy au serveur DHCP pour le tunnel GRE (Generic Routing Encapsulation) IPv6. Dans cet environnement de travaux pratiques, le CNR est configuré pour louer des adresses à l'aide des préfixes /127. Tout comme dhcpV4TunnelLink, le FND approvisionne automatiquement le 2ème IP du sous-réseau point à point en HER lorsque vous configurez son tunnel GRE.

dhcpV4LoopbackLink : adresse IPv4 que le FND utilisera dans ses requêtes proxy vers le serveur DHCP lors de la configuration de l'interface de bouclage 0 du routeur CGR. Dans cet environnement de travaux pratiques, le pool DHCP correspondant sur le CNR a été configuré pour louer des sous-réseaux /32.

dhcpV6LoopbackLink : adresse IPv6 que le FND utilisera dans ses requêtes proxy vers le serveur DHCP lorsque vous configurerez l'interface de bouclage 0 du routeur CGR. Dans cet environnement de travaux pratiques, le pool correspondant a été configuré pour louer des sous-réseaux /128.

Routeur principal (HER)

Lorsque vous ajoutez un routeur de tête de réseau pour la première fois, ce modèle peut être utilisé :

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

deviceType - Lorsque vous introduisez un ASR ou un CSR, la valeur asr1000 doit être utilisée dans ce champ.

status - Les valeurs d'état acceptées ne sont pas entendues, descendantes et ascendantes. Utilisez unheard s'il s'agit d'une nouvelle importation.

lastheard - S'il s'agit d'un nouveau périphérique, ce champ peut être laissé vide.

runningFirmwareVersion - Cette valeur peut également être laissée vide, mais si vous voulez importer la version, utilisez le numéro de version à partir de la ligne supérieure de la sortie **show version**. Par exemple, dans cette sortie, la chaîne '03.16.04b.S' doit être utilisée :

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

netconfUsername : nom d'utilisateur de l'utilisateur configuré pour avoir un accès complet à la fonction HER via Netconf/SSH.

netconfPassword : mot de passe de l'utilisateur spécifié dans le champ netconfUsername.

Point d'extrémité de la grille connectée (CGE)

Ajouter un nouveau point de terminaison de maillage à la base de données est très simple. Ce modèle peut être utilisé :

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

deviceType - Dans cet environnement de travaux pratiques, 'cgmesh' a été utilisé pour ajouter un compteur intelligent en tant que CGE.

lat - Coordonnée de latitude GPS où le CGE sera installé.

lng - La longitude GPS.

Exemples

Ajout FAR :

```
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
```

Ajout :

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

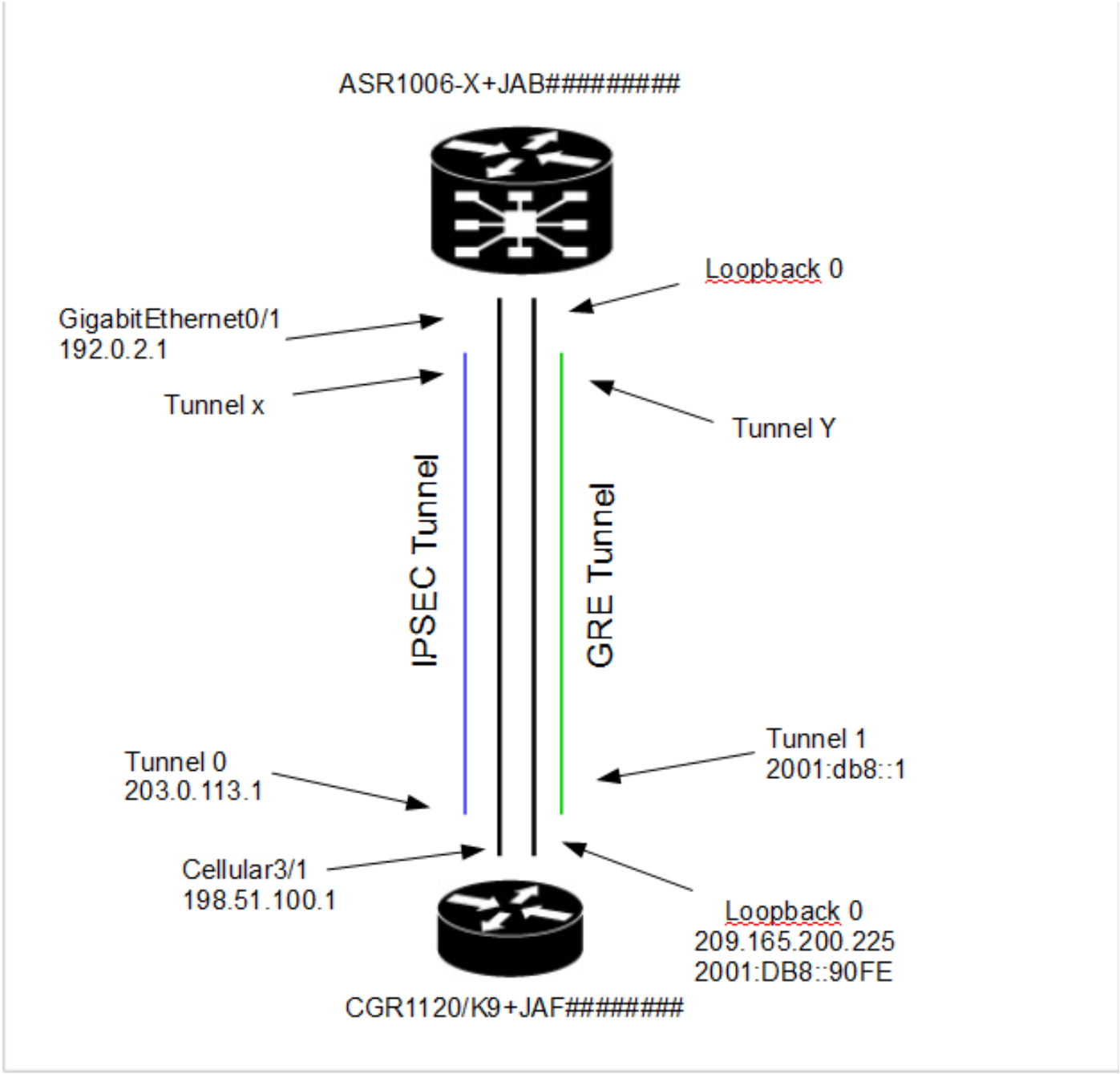
Ajout CGE :

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

Diagramme du réseau

> **Note**: Le provisionnement du tunnel fonctionne différemment selon qu'un FAR exécute CG-OS ou IOS. CG-OS : Une nouvelle interface de tunnel IPSEC sera configurée à la fois sur le FAR et sur le HER. Le FND enverra une requête proxy au serveur DHCP pour 2 IP par tunnel et configurera automatiquement la 2e IP sur l'interface de tunnel correspondante. IOS: Le HER utilise un modèle Flex-VPN qui utilise un tunnel IPSEC point à multipoint. Avec cette configuration, seuls les FAR reçoivent de nouvelles interfaces de tunnel.

Dans ce diagramme de topologie, 'Tunnel x' fait référence à l'interface de tunnel IPSEC relative sur HER tandis que 'Tunnel Y' correspond au tunnel GRE construit à partir de l'interface de bouclage sur HER. En outre, les adresses IP et les interfaces du schéma correspondent directement aux exemples de configuration des modèles .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########