Préparez les fichiers .csv (valeur Virgule-séparée) pour importer de nouveaux périphériques sur FND

Contenu

Introduction

Ce document décrit des étapes pour préparer le fichier .csv pour le directeur de réseau de champ (FND). Afin de fournir la Gestion de réseau sécurisé, le FND ne fournit pas la détection et l'enregistrement automatiques ou dynamiques de ressource. Avant qu'un nouveau périphérique puisse être ajouté à un déploiement FND une seule entrée de base de données doit être créée pour elle en important un fichier de la coutume .csv par l'intermédiaire de l'interface utilisateur d'utilisateur web (UI).

Cet article prévoit les modèles .csv qui peuvent être utilisés et personnalisés afin d'ajouter de nouveaux points finaux, Routeurs de zone de champ ou routeurs de tête de réseau à une solution existante. En plus de ceci, chaque champ de base de données (DB) sera défini et expliqué afin d'assister la conception et réalisation de nouveaux périphériques.

> Remarque: Avant que ce guide puisse être utilisé, vous devez avoir une solution connectée saturée et installée du système d'administration de réseaux de grille (CG-NMS) /FND.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Serveur d'applications 1.0 ou installé postérieur et s'exécuter CG-NMS/FND avec l'accès du Web UI disponible.

- Percez un tunnel le serveur proxy du serveur de mise en service (TPS) installé et s'exécuter.
- Serveur de base de données d'Oracle installé et correctement configuré.
- setupCgms.sh fonctionnent avec succès au moins une fois avec un db_migrate pour la première fois réussi.
- Vous pouvez encore utiliser ce guide si vous n'avez pas encore installé et avez configuré vos serveurs DHCP mais on lui informe fortement qu'avant que vous utilisiez ce document votre organisation a entièrement prévu des systèmes d'adressage d'ipv4 et d'IPv6 pour le déploiement. Ceci inclut des longueurs de préfixe et des plages pour des tunnels d'IPSec d'ipv4, des tunnels d'Encapsulation de routage générique (GRE) d'IPv6 et conjugue pile adressant sur des bouclages connectés du routeur de grille (CGR).
- On lui informe également fortement que vous déjà avez acheté ou prévoyez d'acheter au moins 1 routeur de tête de réseau, au moins 1 routeur de zone de champ et au moins 1 point final/mètre.

Composants utilisés

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

- FND 3.0.1-36
- SSM articulé autour d'un logiciel (aussi 3.0.1-36)
- les cgms-outils empaquettent installé dans le serveur d'applications (3.0.1-36)
- Tous les serveurs Linux exécutant RHEL 6.5
- Tous les Windows Server exécutant l'entreprise R2 des Windows Server 2008
- Exécution 1000v du routeur de services en nuage de Cisco (CSR) sur une VM comme routeur de tête de réseau
- CGR-1120/K9 utilisés en tant que routeur de région de champ (LOINTAIN) avec CG-OS 4(3)

Un environnement de travaux pratiques commandé FND a été utilisé pendant la création de ce document. Tandis que d'autres déploiements différeront, vous devriez adhérer à toutes les conditions requises minimum des guides d'installation.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

fichiers .csv pour ajouter des périphériques dans FND

LOIN

Ce modèle peut être utilisé pour LOIN qui sont introduits à la solution pour la première fois. Ceci se trouvent sur les **périphériques > la** page de **périphériques de champ**. Sur le champ les périphériques paginent, cliquent sur en fonction le menu déroulant **en vrac d'importation** et choisi **ajoutez les périphériques**.

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

Identifiant d'élément (eid) - C'est un identifiant unique utilisé pour identifier le périphérique dans les messages de log aussi bien que le GUI. Afin d'empêcher la confusion, l'il est recommandé que votre organisation élabore un schéma EID. Le schéma recommandé est d'utiliser le numéro de série d'IDevID du CGR comme EID. Sur ces Routeurs, le numéro de série utilisera cette formule : PID+SN. Exemple : .

deviceType - Ceci est utilisé pour identifier la plate-forme matérielle ou les séries. Pour 1120 et 1240 modèles, la valeur de deviceType devrait être cgr1000.

tunnelHerEid - Étant donné que le FND permet à l'utilisation de 2 le sien qui s'exécute dans des paires ha ou autonome, le champ de tunnelHerEid est utilisé pour l'identifier au lequel ELLE les tunnels VPN sur ce CGR se terminera. Cette valeur sera simplement l'EID de l'approprié ELLE.

certIssuerCommonName - Ce champ est une condition requise du déploiement nul de toucher (ZTD) et est habituellement identique que le nom DNS de votre autorité de certification de la racine RSA. Si vous ne connaissez pas le nom commun, vous pouvez le trouver et exécuter le **show crypto ca certificat de** commande. Dans la chaîne pour le point de confiance de LDevID, vous voyez le nom commun d'émetteur de racine dans le champ objet du 'certificat de CA 0'. Alternativement, vous pouvez simplement accéder à la page de Certificats du FND et regarder le certificat racine.

meshPrefixConfig - Cette valeur est assignée à l'interface de module WPAN. Tout le CGEs qui forment une arborescence du langage de stratégie de routage (RPL) avec ce routeur reçoit une adresse IP par l'intermédiaire du DHCP (le relais supposant DHCP est configuré convenablement) avec cette valeur comme préfixe réseau.

tunnelSrcInterface1 - Pour des déploiements utilisant les tunnels primaires et secondaires d'IPSec, cette valeur est le nom d'interface de la source du tunnel pour vos tunnels principaux (tels que cellular4/1). S'il y a un tunnel de sauvegarde puis vous assignerez l'interface de source en ajoutant une valeur pour tunnelSrcInterface2. Si vous avez seulement 1 connexion WAN puis vous utiliserez seulement le champ tunnelSrcInterface1.

ipsecTunnelDestAddr1 - Cette valeur est l'adresse de destination de tunnel d'ipv4 pour le tunnel primaire d'IPSec avec l'interface de source assignée à tunnelSrcInterface1.

adminUsername - C'est le nom d'utilisateur que le FND utilisera quand vous ouvrez HTTPS et sessions de Netconf au LOIN. On l'exige que cet utilisateur est donné de pleines autorisations par AAA ou localement configuré avec le rôle de réseau-admin.

adminPassword - Le mot de passe pour le compte d'adminUsername. Vous pouvez visualiser ce nom d'utilisateur dans le GUI et naviguer vers l'onglet de Properties de config de la page du périphérique et regarder « nom d'utilisateur d'administrateur » dans la section « de qualifications de routeur ». Afin d'éviter des erreurs, ce mot de passe doit d'abord être chiffré avec le Signature_Tool du paquet rpm de cgms-outils. Cet outil chiffrent n'importe quoi en texte brut

utilisant la chaîne de certificat dans le cgms_keystore. Pour utiliser l'outil de signature, répertoire de modification à /opt/cgms-tools/bin/ sur le serveur d'applications FND. Ensuite, créez un nouveau fichier de .txt de texte brut qui contient l'adminPassword. Une fois que vous avez le fichier texte, exécutez cette commande :

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

Copiez/pâte la sortie chiffrée dans le champ d'adminPassword de votre fichier .csv. C'est une bonne idée de supprimer sécurisé le fichier de mot de passe de texte brut quand vous terminez pour utiliser l'outil de signature.

cgrusername1 - Ce compte utilisateur n'est pas exigé, mais si des plusieurs utilisateurs avec différents rôles sont configurés sur le CGR, vous pouvez ajouter un autre compte utilisateur ici. Il est important de savoir que seulement l'adminUsername et l'adminPassword seront utilisés pour la Gestion du périphérique. Dans cette installation de laboratoire, utilisez les mêmes qualifications que l'adminUsername.

cgrpassword1 - Le mot de passe pour l'utilisateur cgrusername1.

IP - C'est l'IP primaire de Gestion. Quand des pings ou les suivis sont exécutés du FND ils utiliseront cet IP. Des sessions HTTPS pour le gestionnaire de périphériques connecté de grille (CGDM) seront aussi bien envoyées à cet IP. Dans un déploiement typique, ce sera l'adresse IP assignée à votre interface tunnelSrcInterface1.

meshPanidConfig - L'ID de CASSEROLE assigné à l'interface WPAN de ce CGR.

wifiSsid - Le SSID configuré sur l'interface WPAN.

dhcpV4TunnelLink - L'ipv4 addres que le FND utilisera dans sa demande de proxy au serveur DHCP. Dans cet environnement de travaux pratiques, le serveur DHCP est un Cisco Network Registrar (le CNR) et le groupe DHCPv4 IPsec est configuré pour louer des sous-réseaux de /31. Si vous utilisez le premier IP dans un sous-réseau disponible de /31 pour votre valeur dhcpv4TunnelLink puis le FND provision automatiquement l'IPS du sous-réseau point par point au tunnel 0 du CGR et le tunnel correspondant du HER.

dhcpV6TunnelLink - L'ipv6 addres que le FND utilise dans sa demande de proxy au serveur DHCP pour le tunnel d'Encapsulation de routage générique (GRE) d'IPv6. Dans cet environnement de travaux pratiques, le CNR est configuré pour louer des adresses avec l'utilisation des préfixes de /127. Juste comme le dhcpV4TunnelLink, le FND provision automatiquement le 2ème IP du sous-réseau point par point au ELLE quand vous configurez son tunnel GRE.

dhcpV4LoopbackLink - L'ipv4 addres que le FND utilisera dans son proxy demande au serveur DHCP en configurant le bouclage 0 interfaces du CGR. Dans cet environnement de travaux pratiques, le pool DHCP correspondant sur le CNR a été configuré pour louer des sous-réseaux de /32.

dhcpV6LoopbackLink - L'ipv6 addres que le FND utilisera dans son proxy demande au serveur DHCP quand vous configurez le bouclage 0 interfaces du CGR. Dans cet environnement de travaux pratiques, le groupe correspondant a été configuré pour louer des sous-réseaux de /128.

Routeur de tête de réseau (ELLE)

Quand 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 - Quand vous introduisez un ASR ou un CSR, la valeur 'asr1000 devrait être utilisée dans ce domaine.

état - Les valeurs reçues d'état sont inentendues, vers le bas et se lèvent. Utilisez inentendu si c'est une nouvelle importation.

lastheard - Si c'est un nouveau périphérique, ce champ peut être blanc de gauche.

runningFirmwareVersion - Cette valeur peut être blanc de gauche aussi bien mais si vous voulez importer la version, utilise le numéro de version de la ligne supérieure même de la sortie de **show version**. Par exemple, dans cette sortie, la chaîne '03.16.04b.S devrait être utilisée :

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

netconfUsername - Le nom d'utilisateur de l'utilisateur configuré pour avoir plein accès Netconf/SSH au ELLE.

netconfPassword - Le mot de passe pour l'utilisateur spécifié dans le domaine de netconfUsername.

Point final connecté de grille (CGE)

Pour ajouter un nouveau point final de maille au DB est très simple. Ce modèle peut être utilisé :

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

deviceType - Dans cet environnement de travaux pratiques, le « cgmesh » a été utilisé pour ajouter un mètre intelligent comme CGE.

lat - La coordonnée de latitude de GPS où le CGE sera installé.

GNL - La longitude de GPS.

Exemples

Ajout LOINTAIN :

```
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
```

SON 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=
```

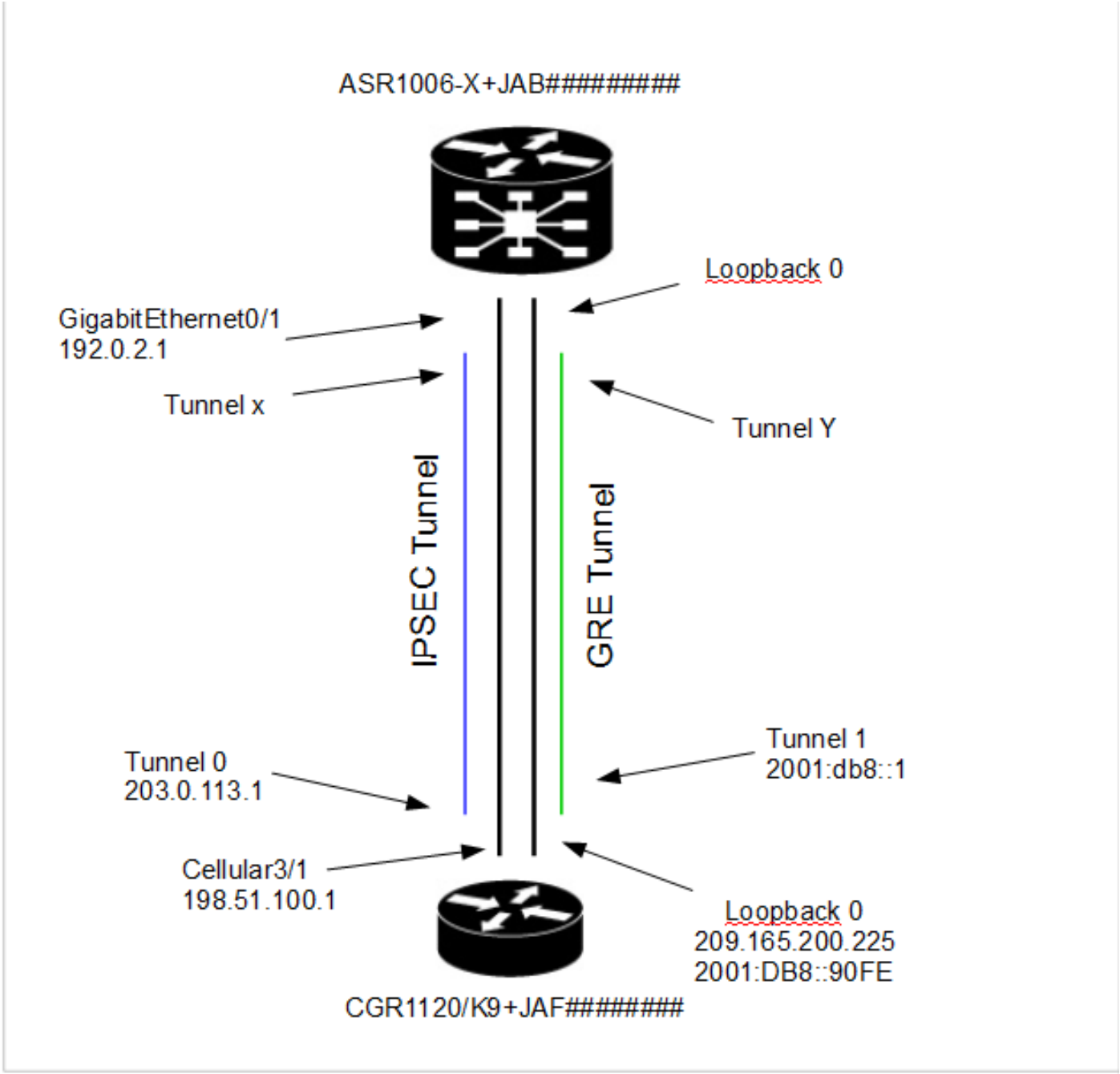
Ajout CGE :

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

Diagramme du réseau

> Remarque: Le ravitaillement de tunnel fonctionne différemment basé en fonction si a LOIN exécute CG-OS ou IOS. CG-OS : Une nouvelle interface de tunnel IPSEC sera configurée sur LOIN et ELLE. Le FND enverra une demande de proxy au serveur DHCP 2 IPS par tunnel et configurera le 2ème IP automatiquement sur l'interface de tunnel correspondante. IOS : ELLE utilisera un modèle Flexible-VPN qui utilise un tunnel point-à-multipoint IPSEC. Avec cette configuration, seulement le FARs reçoivent de nouvelles interfaces de tunnel.

Dans ce diagramme de topologie le « tunnel X » se rapporte à l'interface de tunnel relative IPSEC sur ELLE tandis que le « tunnel Y » correspond au tunnel GRE construit hors fonction de l'interface de bouclage sur ELLE. En outre, les IPS et les interfaces dans le diagramme correspondent directement aux exemples de configuration dans les 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########