Preparar archivos .csv (valor separado por comas) para importar nuevos dispositivos en FND

Contenido

Introducción

Este documento describe los pasos para preparar el archivo .csv para Field Network Director (FND). Para proporcionar una administración de red segura, el FND no proporciona la detección y el registro automáticos o dinámicos de activos. Para poder agregar un nuevo dispositivo a una implementación de FND, se debe crear una entrada de base de datos única para ella mediante la importación de un archivo .csv personalizado a través de la interfaz de usuario web.

Este artículo proporciona plantillas .csv que se pueden utilizar y personalizar para agregar nuevos terminales, routers de área de campo o routers de cabecera a una solución existente. Además de esto, cada campo de base de datos (DB) se definirá y explicará para ayudar con el diseño e implementación de nuevos dispositivos.

> **Nota:** Para poder utilizar esta guía, debe tener una solución de Connected Grid Network Management System (CG-NMS)/FND completamente configurada e instalada.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Servidor de aplicaciones CG-NMS/FND 1.0 o posterior instalado y ejecutándose con acceso de interfaz de usuario web disponible.
- Servidor proxy de aprovisionamiento de túnel (TPS) instalado y en ejecución.

- Servidor de base de datos Oracle instalado y configurado correctamente.
- setupCgms.sh se ejecuta correctamente al menos una vez con db_migration correcta primera vez.
- Todavía puede utilizar esta guía si aún no ha instalado y configurado sus servidores DHCP, pero se recomienda encarecidamente que antes de utilizar este documento, su organización haya planificado completamente los esquemas de direccionamiento IPv4 e IPv6 para la implementación. Esto incluye longitudes y rangos de prefijo para túneles IPSec IPv4, túneles de encapsulación de routing genérico (GRE) IPv6 y direccionamiento de pila dual en loopbacks de Connected Grid Router (CGR).
- También se recomienda encarecidamente que ya haya adquirido o tenga previsto adquirir al menos 1 router de cabecera, al menos 1 router de área de campo y al menos 1 terminal/metro.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FND 3.0.1-36
- SSM basado en software (también 3.0.1-36)
- paquete cgms-tools instalado en el servidor de aplicaciones (3.0.1-36)
- Todos los servidores Linux que ejecutan RHEL 6.5
- Todos los servidores Windows que ejecutan Windows Server 2008 R2 Enterprise
- Cisco Cloud Services Router (CSR) 1000v que se ejecuta en una VM como router de cabecera
- CGR-1120/K9 utilizado como router de área de campo (FAR) con CG-OS 4(3)

Se utilizó un entorno de laboratorio FND controlado durante la creación de este documento. Aunque otras implementaciones serán diferentes, debe cumplir todos los requisitos mínimos de las guías de instalación.

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.

Archivos .csv para agregar dispositivos en FND

LEJOS

Esta plantilla se puede utilizar para FAR que se introducen en la solución por primera vez. Se encontrará en la página **Dispositivos > Dispositivos de campo**. En la página Field Devices (Dispositivos de campo), haga clic en el menú desplegable **Bulk Import (Importación masiva)** y seleccione **Add Devices (Agregar dispositivos)**.

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

Identificador de elementos (eid): identificador único utilizado para identificar el dispositivo en los mensajes de registro, así como en la GUI. Para evitar confusiones, se recomienda que su organización desarrolle un esquema EID. El esquema recomendado es utilizar el número de serie IDevID de CGR como EID. En estos routers, el Número de serie utilizará esta fórmula: PID+SN Por ejemplo: CGR1120/K9+JAFXXXXXXX.

deviceType: se utiliza para identificar la serie o plataforma de hardware. Para los modelos 1120 y 1240, el valor deviceType debe ser cgr1000.

tunnelHerEid - Debido al hecho de que el FND permite el uso de 2 HERs ejecutándose en pares HA o de forma independiente, el campo tunnelHerEid se utiliza para identificar a qué túneles VPN de este CGR terminará. Este valor será simplemente el EID de la HER apropiada.

certEmierCommonName: este campo es un requisito de implementación sin interacción (ZTD) y suele ser el mismo que el nombre DNS de la autoridad de certificados RSA raíz. Si no conoce el nombre común, puede encontrarlo y ejecutar el comando **show crypto ca certificates**. En la cadena del punto de confianza de LDevID, verá el nombre común del emisor raíz en la línea de asunto de 'certificado de CA 0'. También puede acceder a la página Certificados del FND y ver el certificado raíz.

meshPrefixConfig: este valor se asigna a la interfaz del módulo WPAN. Todos los CGE que forman un árbol de lenguaje de políticas de routing (RPL) con este router reciben una dirección IP a través de DHCP (suponiendo que el relé DHCP esté configurado correctamente) con este valor como prefijo de red.

tunnelSrcInterface1: para implementaciones que utilizan túneles IPSec primarios y secundarios, este valor es el nombre de la interfaz del origen del túnel para sus túneles primarios (como cellular4/1). Si hay un túnel de respaldo, asignará la interfaz de origen agregando un valor para tunnelSrcInterface2. Si sólo tiene 1 conexión WAN, sólo utilizará el campo tunnelSrcInterface1.

ipsecTunnelDestAddr1 - Este valor es la dirección de destino del túnel IPv4 para el túnel IPSec primario con la interfaz de origen asignada a tunnelSrcInterface1.

adminUsername - Éste es el nombre de usuario que el FND utilizará cuando abra sesiones HTTPS y Netconf en el FAR. Se requiere que AAA otorgue a este usuario permisos completos o configurados localmente con la función de administrador de red.

adminPassword: la contraseña de la cuenta adminUsername. Puede ver este nombre de usuario en la interfaz gráfica de usuario y navegar hasta la ficha Propiedades de configuración de la página del dispositivo y ver el nombre de usuario del administrador en la sección "Credenciales del router". Para evitar errores, esta contraseña primero debe cifrarse con la Signature_Tool del paquete cgms-tools RPM. Esta herramienta cifra cualquier cosa en texto sin formato usando la cadena de certificados en el cgms_keystore. Para utilizar la herramienta de firma, cambie el directorio a /opt/cgms-tools/bin/ en el servidor de aplicaciones FND. A continuación, cree un nuevo archivo .txt de texto sin formato que contenga adminPassword. Una vez que tenga el

archivo de texto, ejecute este comando:

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

Copie/pegue el resultado cifrado en el campo adminPassword del archivo .csv. Es una buena idea eliminar de forma segura el archivo de contraseña de texto sin formato cuando termine de utilizar la herramienta Signature.

cgrusername1: Esta cuenta de usuario no es necesaria, pero si se configuran varios usuarios con diferentes funciones en CGR, puede agregar otra cuenta de usuario aquí. Es importante saber que sólo se utilizarán adminUsername y adminPassword para la administración del dispositivo. En esta configuración de laboratorio, utilice las mismas credenciales que adminUsername.

cgrpassword1 - La contraseña para el usuario cgrusername1.

ip - Ésta es la IP de administración principal. Cuando se ejecutan pings o seguimientos desde el FND, utilizarán esta IP. También se enviarán sesiones HTTPS para Connected Grid Device Manager (CGDM) a esta IP. En una implementación típica, ésta será la dirección IP asignada a la interfaz tunnelSrcInterface1.

meshPanidConfig: ID de PAN asignado a la interfaz WPAN de esta CGR.

wifiSsid: SSID configurado en la interfaz WPAN.

dhcpV4TunnelLink: Dirección IPv4 que el FND utilizará en su solicitud de proxy al servidor DHCP. En este entorno de laboratorio, el servidor DHCP es un Cisco Network Registrar (CNR) y el conjunto DHCPv4 IPsec se configura para arrendar subredes /31. Si utiliza la primera IP en una subred /31 disponible para su valor dhcpv4TunnelLink, el FND aprovisionará automáticamente ambas IP de la subred punto a punto al túnel 0 de CGR y al túnel HER correspondiente.

dhcpV6TunnelLink: dirección IPv6 que el FND utiliza en su solicitud de proxy al servidor DHCP para el túnel IPv6 Generic Routing Encapsulation (GRE). En este entorno de laboratorio, el CNR se configura para arrendar direcciones con el uso de prefijos /127. Al igual que el dhcpV4TunnelLink, el FND aprovisionará automáticamente la segunda IP de la subred punto a punto a HER cuando configure su túnel GRE.

dhcpV4LoopbackLink: Dirección IPv4 que el FND utilizará en sus solicitudes de proxy al servidor DHCP al configurar la interfaz Loopback 0 del CGR. En este entorno de laboratorio, el conjunto DHCP correspondiente en el CNR se configuró para arrendar subredes /32.

dhcpV6LoopbackLink: Dirección IPv6 que el FND utilizará en sus solicitudes de proxy al servidor DHCP cuando configure la interfaz Loopback 0 del CGR. En este entorno de laboratorio, el conjunto correspondiente se configuró para arrendar subredes /128.

Router de cabecera (HER)

Cuando agrega un router headend por primera vez, se puede utilizar esta plantilla:

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

deviceType: cuando introduzca un ASR o CSR, el valor 'asr1000' se debe utilizar en este campo.

status: los valores de estado aceptados son unheard, down y up. Utilice unheard si se trata de una nueva importación.

lastheard: si se trata de un dispositivo nuevo, este campo se puede dejar en blanco.

runningFirmwareVersion - Este valor también se puede dejar en blanco pero si desea importar la versión, utilice el número de versión de la línea superior del resultado **show version**. Por ejemplo, en este resultado, se debe utilizar la cadena '03.16.04b.S':

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

netconfUsername - El nombre de usuario del usuario configurado para tener acceso Netconf/SSH completo a HER.

netconfPassword - La contraseña para el usuario especificada en el campo netconfUsername.

Punto final de Connected Grid (CGE)

Agregar un nuevo punto final de malla a la base de datos es muy simple. Esta plantilla se puede utilizar:

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

deviceType: en este entorno de laboratorio, se utilizó 'cgmesh' para agregar un medidor inteligente como CGE.

lat - La coordenadas de latitud GPS donde se instalará el CGE.

lng - La longitud del GPS.

Examples

Adición de 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
```

Su adición:

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

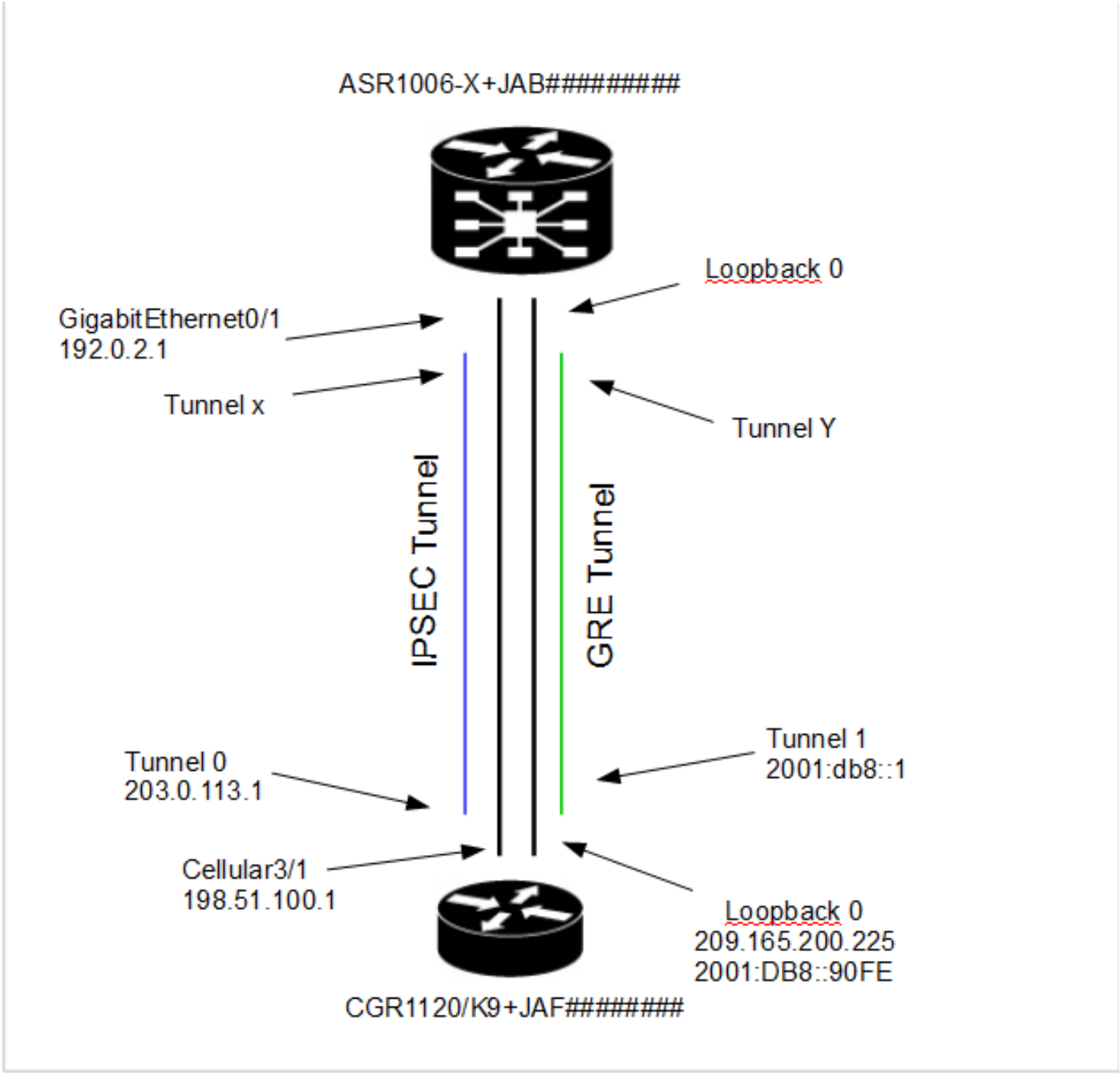
Adición de CGE:

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

Diagrama de la red

> **Nota:** El aprovisionamiento del túnel funciona de manera diferente en función de si un FAR está ejecutando CG-OS o IOS. CG-OS: Se configurará una nueva interfaz de túnel IPSEC tanto en el FAR como en el HER. El FND enviará una solicitud de proxy al servidor DHCP para 2 IP por túnel y configurará la segunda IP automáticamente en la interfaz de túnel correspondiente. IOS: HER utilizará una plantilla Flex-VPN que utilice un túnel IPSEC punto a multipunto. Con esta configuración, sólo los FAR reciben nuevas interfaces de túnel.

En este diagrama de topología 'Túnel x' se refiere a la interfaz de túnel IPSEC relativa en HER mientras que 'Túnel Y' corresponde con el túnel GRE construido fuera de la interfaz de loopback en HER. Además, las IPs e interfaces del diagrama se corresponden directamente con los ejemplos de configuración de las plantillas .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########