Prepare .csv (Comma-Separated Value) Files to Import New Devices on FND

Contents

Introduction

This document describes steps to prepare .csv file for Field Network Director (FND). In order to provide secure network management, the FND does not provide automatic or dynamic asset discovery and registration. Before a new device can be added to a FND deployment a unique database entry must be created for it by importing a custom .csv file via the web User Interface (UI).

This article provides .csv templates which can be used and customized in order to add new endpoints, field area routers or head-end routers to an existing solution. In addition to this, each database (DB) field will be defined and explained in order to assist with the design and implementation of new devices.

> **Note**: Before this guide can be used, you must have a fully configured and installed Connected Grid Network Management System (CG-NMS)/FND solution.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- CG-NMS/FND application server 1.0 or later installed and running with web UI access available.
- Tunnel Provisioning Server (TPS) proxy server installed and running.
- Oracle database server installed and correctly configured.
- setupCgms.sh successfully run at least once with a successful first-time db_migrate.

- You can still use this guide if you have not yet installed and configured your DHCP server(s) but it is strongly advised that before you use this document your organization has fully planned out IPv4 and IPv6 addressing schemes for the deployment. This includes prefix lengths and ranges for IPv4 IPSec tunnels, IPv6 Generic Routing Encapsulation (GRE) tunnels and dual stack addressing on Connected Grid Router (CGR) loopbacks.
- It is also strongly advised that you already have purchased or are planning to purchase at least 1 head-end router, at least 1 field area router and at least 1 endpoint/meter.

Components Used

The information in this document is based on these software and hardware versions:

- FND 3.0.1-36
- Software-based SSM (also 3.0.1-36)
- cgms-tools package installed in application server (3.0.1-36)
- All Linux servers running RHEL 6.5
- All Windows servers running Windows Server 2008 R2 Enterprise
- Cisco Cloud Services Router (CSR) 1000v running on a VM as head-end router
- CGR-1120/K9 used as Field Area Router (FAR) with CG-OS 4(3)

A controlled FND lab environment was used during the creation of this document. While other deployments will differ, you should adhere to all minimum requirements from the installation guides.

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.

.csv Files to Add Devices in FND

FAR

This template can be used for FAR which are introduced to the solution for the first time. This will be located on the **Devices > Field Devices** page. On the Field Devices page, click on the **Bulk Import** dropdown menu and select **Add Devices**.

```
eid,deviceType,tunnelHerEid,certIssuerCommonName,meshPrefixConfig,tunnelSrcInterface1,ipsecTunnelDestAddr1,adminUsername,adminPassword,cgrusername1,cgrpassword1,ip,meshPanidConfig,wifiSsid,dhcpV4TunnelLink,dhcpV6TunnelLink,dhcpV4LoopbackLink,dhcpV6LoopbackLink
```

Element Identifier (eid) - This is a unique identifier used to identify the device in log messages as well as the GUI. In order to prevent confusion, it is recommended that your organization develops an EID scheme. The recommended scheme is to use the CGR's IDevID Serial Number as the EID. On these routers, the Serial Number will use this formula: PID+SN. For example: CGR1120/K9+JAFXXXXXXX.

deviceType - This is used to identify the hardware platform or series. For both 1120 and 1240 models, the deviceType value should be cgr1000.

tunnelHerEid - Due to the fact that the FND allows the use of 2 HERs running in HA pair or standalone, the tunnelHerEid field is used to identify which HER the VPN tunnels on this CGR will terminate to. This value will simply be the EID of the appropriate HER.

certIssuerCommonName - This field is a requirement of Zero Touch Deployment (ZTD) and is usually the same as the DNS name of your root RSA Certificate Authority. If you don't know the common name, you can find it and run the command **show crypto ca certificates**. In the chain for the LDevID trustpoint, you see the root issuer common name in the subject line of 'CA certificate 0'. Alternatively, you can simply access the Certificates page of the FND and look at the root certificate.

meshPrefixConfig - This value is assigned to the WPAN module interface. All CGEs which form a Routing Policy Language (RPL) tree with this router receives an IP address via DHCP (assuming DHCP relay is configured appropriately) with this value as the network prefix.

tunnelSrcInterface1 - For deployments utilizing primary and secondary IPSec tunnels, this value is the interface name of the tunnel source for your primary tunnels (such as cellular4/1). If there is a backup tunnel then you will assign the source interface by adding a value for tunnelSrcInterface2. If you only have 1 WAN connection then you will only use the tunnelSrcInterface1 field.

ipsecTunnelDestAddr1 - This value is the IPv4 tunnel destination address for the primary IPSec tunnel with the source interface assigned to tunnelSrcInterface1.

adminUsername - This is the username that the FND will use when you open HTTPS and Netconf sessions to the FAR. It is required that this user is given full permissions by AAA or configured locally with the network-admin role.

adminPassword - The password for the adminUsername account. You can view this username in the GUI and navigate to the Config Properties tab of the device's page and look at the 'Administrator Username' in the 'Router Credentials' section. In order to avoid errors, this password must first be encrypted with the Signature_Tool from the cgms-tools RPM package. This tool encrypt anything in plain text using the certificate chain in the cgms_keystore. To use the signature tool, change directory to /opt/cgms-tools/bin/ on the FND application server. Next, create a new plain text .txt file which contains the adminPassword. Once you have the text file, run this command:

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

Copy/paste the encrypted output into the adminPassword field of your .csv file. It is a good idea to securely delete the plain text password file when you finish to use the Signature Tool.

cgrusername1 - This user account is not required, but if multiple users with different roles are configured on the CGR, you can add another user account here. It is important to know that only the adminUsername and adminPassword will be used for management of the device. In this lab setup, use the same credentials as adminUsername.

cgrpassword1 - The password for the cgrusername1 user.

ip - This is the primary management IP. When pings or traces are executed from the FND they will use this IP. HTTPS sessions for Connected Grid Device Manager (CGDM) will be sent to this IP as well. In a typical deployment, this will be the IP address assigned to your tunnelSrcInterface1 interface.

meshPanidConfig - The PAN ID assigned to the WPAN interface of this CGR.

wifiSsid - The SSID configured on the WPAN interface.

dhcpV4TunnelLink - The IPv4 address that the FND will use in its proxy request to the DHCP server. In this lab environment, the DHCP server is a Cisco Network Registrar (CNR) and the DHCPv4 IPsec pool is configured to lease /31 subnets. If you use the first IP in an available /31 subnet for your dhcpv4TunnelLink value then the FND will automatically provision both IPs from the point-to-point subnet to the CGR's Tunnel 0 and the HER's corresponding tunnel.

dhcpV6TunnelLink - The IPv6 address that the FND uses in its proxy request to the DHCP server for the IPv6 Generic Routing Encapsulation (GRE) tunnel. In this lab environment, the CNR is configured to lease addresses with the use of /127 prefixes. Just like the dhcpV4TunnelLink, the FND will automatically provision the 2nd IP of the point-to-point subnet to the HER when you configure its GRE tunnel.

dhcpV4LoopbackLink - The IPv4 address that the FND will use in its proxy requests to the DHCP server when configuring the Loopback 0 interface of the CGR. In this lab environment, the corresponding DHCP pool on the CNR was configured to lease /32 subnets.

dhcpV6LoopbackLink - The IPv6 address that the FND will use in its proxy requests to the DHCP server when you configure the Loopback 0 interface of the CGR. In this lab environment, the corresponding pool was configured to lease /128 subnets.

Head-End Router (HER)

When you add a head-end router for the first time, this template can be used:

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

deviceType - When you introduce an ASR or CSR, the 'asr1000' value should be used in this field.

status - Accepted status values are unheard, down and up. Use unheard if it is a new import.

lastheard - If this is a new device, this field can be left blank.

runningFirmwareVersion - This value can be left blank as well but if you want to import the version, use the version number from the very top line of the **show version** output. For example, in this output, the '03.16.04b.S' string should be used:

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

netconfUsername - The username of the user configured to have full Netconf/SSH access to the HER.

netconfPassword - The password for the user specified in the netconfUsername field.

Connected Grid Endpoint (CGE)

To add a new mesh endpoint to the DB is very simple. This template can be used:

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

deviceType - In this lab environment, 'cgmesh' was used to add a smart meter as a CGE.

lat - The GPS latitude coordinate where the CGE will be installed.

lng - The GPS longitude.

Examples

FAR Addition:

```
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
```

HER Addition:

```
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 Addition:

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

Network Diagram

> **Note**: Tunnel provisioning works differently based on whether a FAR is running CG-OS or IOS. CG-OS: A new IPSEC Tunnel interface will be configured on both the FAR and the HER. The FND will send a proxy request to the DHCP server for 2 IPs per tunnel and will configure the 2nd IP automatically on the corresponding tunnel interface. IOS: The HER will use a Flex-VPN template which uses a point-to-multipoint IPSEC tunnel. With this configuration, only the FARs receive new tunnel interfaces.

In this topology diagram 'Tunnel x' refers to the relative IPSEC tunnel interface on the HER while 'Tunnel Y' corresponds with the GRE tunnel built off of the loopback interface on the HER. Furthermore, the IPs and interfaces in the diagram directly correspond to the configuration examples in the .csv templates.