Configurer Field Network Director pour utiliser Plug and Play sur IR800

Contenu

Introduction

Ce document décrit comment démarrer avec Field Network Director (FND) et Plug and Play (PNP) avec l'utilisation d'un ensemble minimal de composants.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Expérience avec Linux et connaissances afin de modifier les fichiers de configuration d'exécution sur une machine Linux
- Au moins un des routeurs pris en charge à gérer par FND. Par exemple IR809 ou IR829. Accès à la consoleIOS® version 15.7(3)M1 minimale
- Fichier OVA déployé sur un hyperviseur (par exemple : VMWare ESXi). Le fichier OVA, s'il y a lieu, peut être téléchargé à l'adresse suivante : https://software.cisco.com/download/home/286287993/type/286320249

Components Used

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

- Fichier OVA pour FND version 4.5.0-122 (CISCO-IOTFND-V-K9-4.5.0-122.zip)
- VMWare ESX
- IR809 avec IOS® version 15.8(3)M2

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

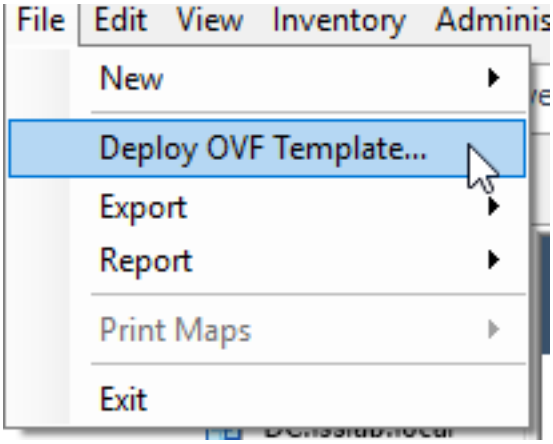
Étant donné que FND propose de nombreuses options de déploiement, l'objectif est de pouvoir configurer une installation minimale mais fonctionnelle pour FND. Cette configuration peut ensuite servir de point de départ pour une personnalisation plus poussée et pour ajouter d'autres fonctionnalités. La configuration expliquée ici est basée sur l'utilisation de l'installation FND d'Open Virtual Appliance (OVA) comme point de départ et utilise le mode facile afin d'éviter la nécessité de l'infrastructure à clé publique (PKI) et du provisionnement de tunnel. Utilisez le protocole PNP, afin de simplifier et d'ajouter des périphériques à l'installation.

Le résultat de ce guide n'est pas destiné à être utilisé en production, car il pourrait y avoir des risques de sécurité en raison de l'absence de mots de passe dans le texte du plan et de tunnels et d'ICP.

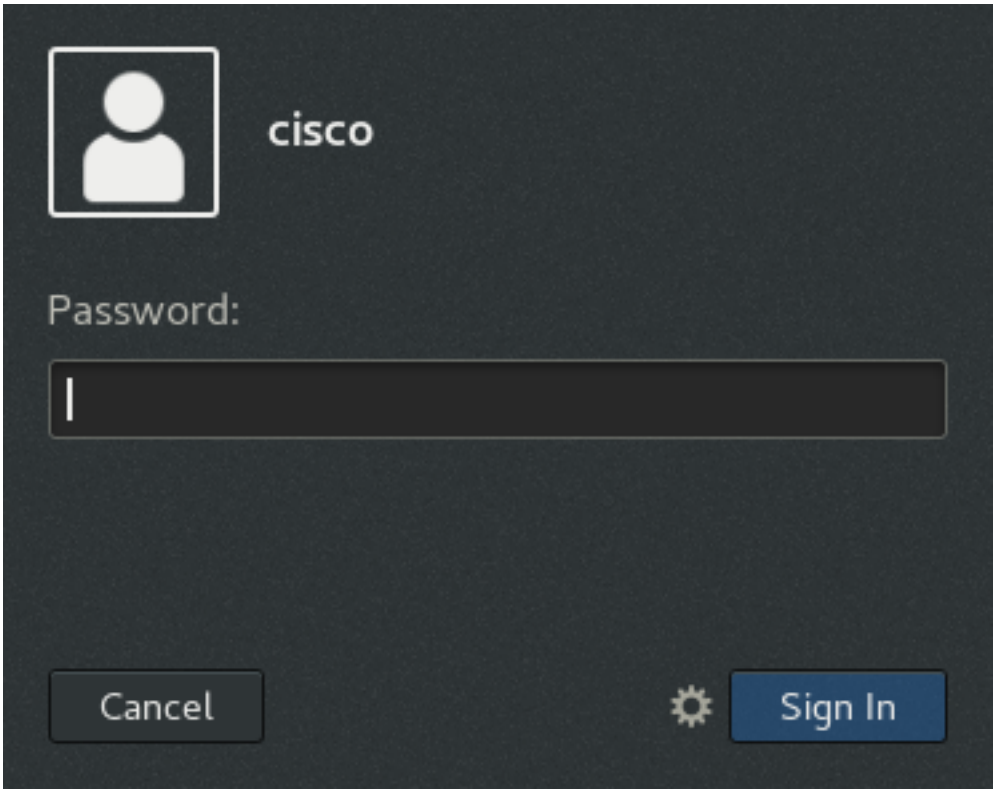
Configuration

Déployer et configurer l'OVA FND

Étape 1. téléchargez et déployez le fichier OVA FND sur votre hyperviseur. Par exemple, pour VMWare, il s'agira de **Fichier > Déployer le modèle OVF** comme indiqué dans l'image.



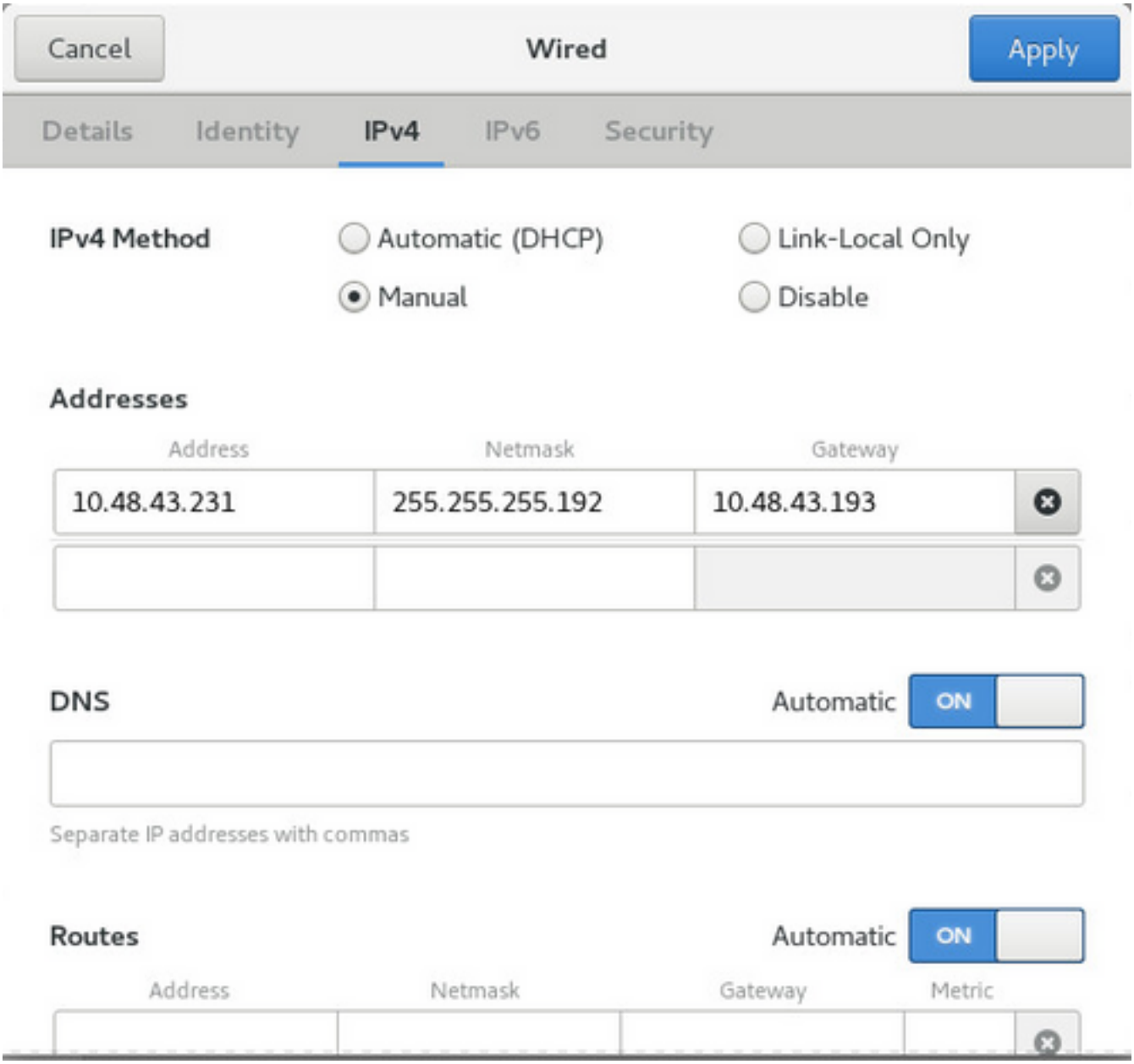
Étape 2. Une fois déployé, vous pouvez démarrer la machine virtuelle et un écran de connexion s'affiche, comme le montre l'image.



Les mots de passe par défaut du fichier OVA sont les suivants :

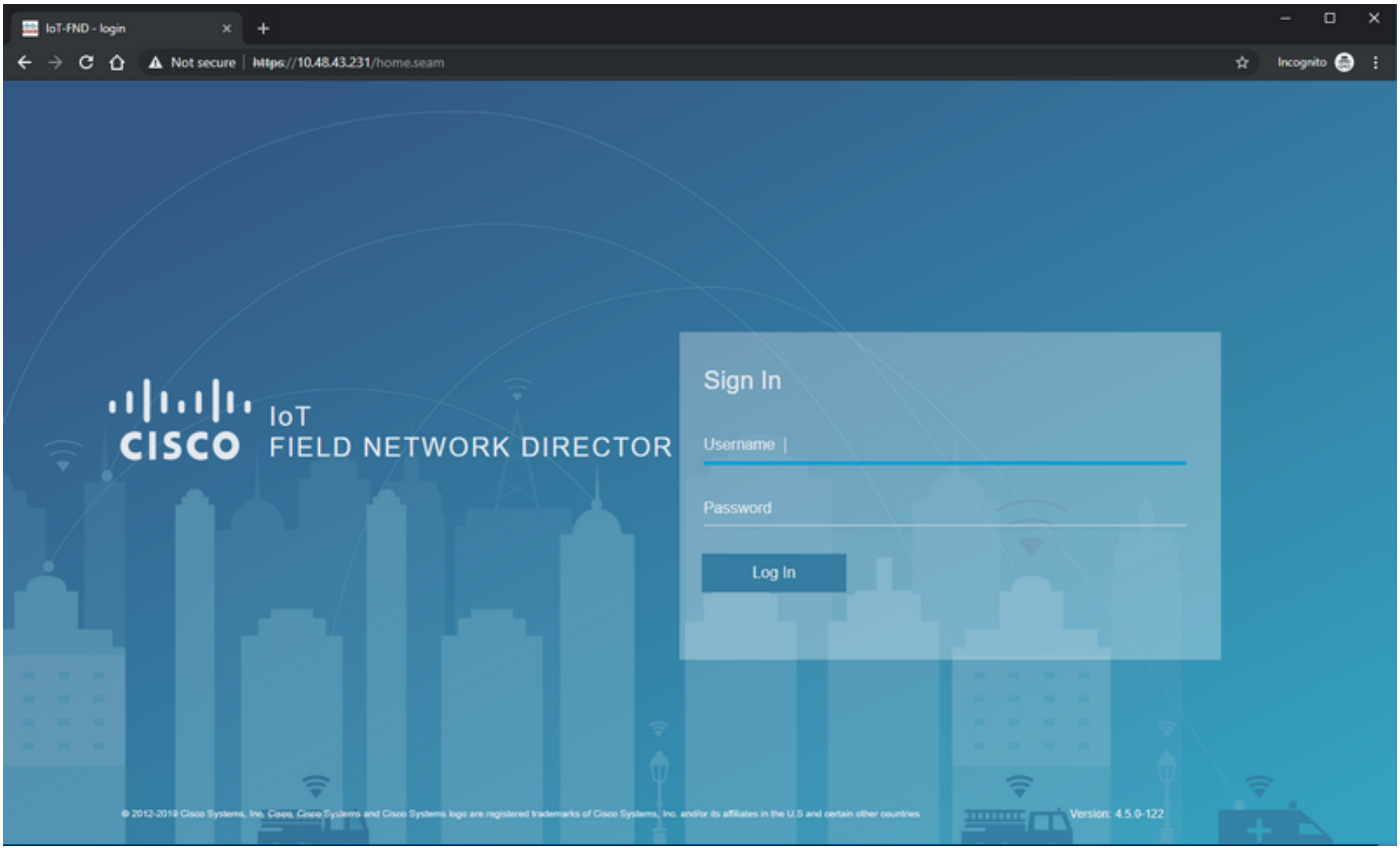
- username (nom d'utilisateur) : mot de passe racine : **cisco123**
- username (nom d'utilisateur) : mot de passe cisco : **C_sco123**

Étape 3. Connectez-vous avec l'utilisateur et le mot de passe cisco et accédez à **Applications > System Tools > Settings > Network.** Ajoutez un profil câblé et, dans l'onglet IPv4, définissez l'adresse IP ou DHCP souhaitée comme indiqué dans l'image.



Étape 4. Cliquez sur **Apply** et activez la connexion pour vous assurer que les nouveaux paramètres sont appliqués.

Àce stade, vous devez être en mesure de naviguer jusqu'à l'**interface utilisateur graphique FND** avec votre navigateur et l'adresse IP configurée comme indiqué dans l'image.



Étape 5. Connectez-vous à l'interface utilisateur graphique à l'aide du nom d'utilisateur et du mot de passe par défaut : **racine/racine123**

Vous êtes invité à modifier votre mot de passe immédiatement, puis à le rediriger à nouveau vers la connexion.

Si tout se passe bien, vous devriez pouvoir vous connecter avec votre nouveau mot de passe et naviguer dans l'interface utilisateur FND.

En outre, les modes PNP et de démonstration sont décrits, suivis de la configuration de FND.

Àpropos de PNP

Le protocole PNP est la méthode Cisco la plus récente pour le déploiement automatique (ZTD). Avec l'utilisation du protocole PNP, un périphérique peut être entièrement configuré et la nécessité de modifier manuellement la configuration ne se fera pas sentir.

Pour FND, avec l'utilisation du protocole PNP, la nécessité d'amorcer le routeur est évitée. En fait, tout ce que fait PNP, le redirige vers le FND, de manière sécurisée, et récupère la configuration du bootstrap.

Une fois que la configuration du bootstrap est présente dans le périphérique, le reste du processus se poursuit comme avec un périphérique de démarrage classique.

Il existe différentes manières d'utiliser le protocole PNP :

- Grâce au service Cisco PNP (devicehelper.cisco.com), avec l'utilisation d'un compte Smart. Activé par défaut hors usine sur certains périphériques
- Avec l'option DHCP 43 afin de fournir l'IP ou le nom d'hôte auquel se connecter pour

l'amorçage
- En configurant manuellement le serveur PNP dans la configuration

Pour cette configuration, l'adresse IP du serveur PNP est définie manuellement, c'est-à-dire l'adresse IP du serveur FND, et le port du périphérique. Si vous souhaitez effectuer cette opération avec DHCP, vous devez fournir les informations suivantes :

Pour Cisco IOS®, le serveur DHCP doit être configuré comme suit :

```
ip dhcp pool pnp_pool
network 192.168.10.0 255.255.255.248
default-router 192.168.10.1
dns-server 8.8.8.8
option 43 ascii "5A;K4;B2;I10.48.43.231;J9125"
!
```

Pour DHCPd sur Linux :

```
[jedepuyd@KJK-SRVIOT-10 ~]$ cat /etc/dhcp/dhcpd.conf
subnet 192.168.100.0 netmask 255.255.255.0 {

option routers 192.168.100.1;
range 192.168.100.100 192.168.100.199;
option domain-name-servers 192.168.100.1;
option domain-name "test.dom";
option vendor-encapsulated-options "5A;K4;B2;I10.48.43.231;J9125";
}
```

Dans cette configuration pour l'option 43 ou les options encapsulées par le fournisseur, vous devez spécifier les chaînes ASCII suivantes :

```
"5A;K4;B2;I10.50.215.252;J9125"
```

Il peut être adapté comme suit :

- 5 - Code de type DHCP 5
- A - Code de fonctionnement de la fonctionnalité active
- K4 - Protocole de transport HTTP
- B2 - Le type d'adresse IP du serveur PnP/TPS/FND est IPv4
- I10.48.43.231 : adresse IP du serveur FND
- J9125 - Numéro de port 9125 (port pour PNP sur serveur FND)

Vous trouverez plus d'informations sur le protocole PNP avec DHCP ici : https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_3/iot_fnd_ug4_3/sys_mgmt.html#31568 dans la section : **Configuration de DHCP Option 43 sur le serveur DHCP Cisco IOS®**

Àpropos de EasyMode

Easy mode a été introduit depuis FND 4.1, bien qu'il ait été appelé mode de démonstration à l'époque, et vous permet d'exécuter FND de manière moins sécurisée. Bien que cela ne soit pas recommandé pour la production, c'est un bon moyen de commencer.

Avec l'utilisation du mode facile, vous pouvez vous concentrer sur le processus PNP, le bootstrap et la configuration du routeur. Si quelque chose ne fonctionne pas, vous n'avez pas besoin de suspecter la construction du tunnel ou des certificats.

Modifications qui se produisent lorsque vous configurez FND pour qu'il s'exécute en mode facile :

- Il n'est pas nécessaire de disposer d'un routeur de tête de réseau (HER) ou d'un tunnel vers le serveur FND.
- Pas besoin d'installer une infrastructure à clé publique (PKI) et le protocole SCEP (Simple Certificate Enrollment Protocol).
- Pas besoin de certificats de routeur, de point de confiance et de SSL.
- Toutes les communications ont lieu sur HTTP au lieu de HTTPS.

Vous trouverez plus d'informations sur le mode facile ici :

https://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/iot_fnd/guide/4_1_B/iot_fnd_ug4_1_b/device_mgmt.html#85516

Configurer FND pour PNP et Easy Mode

Maintenant, vous savez quel est le mode de démonstration/PNP et pourquoi il est utilisé dans ce contexte. Modifions la configuration FND afin de l'activer :

Sur la machine virtuelle FND, qui provient du fichier OVA, connectez-vous à SSH et modifiez les **propriétés cgms.properties** comme suit :

```
[root@iot-fnd ~]# cat /opt/fnd/data/cgms.properties
cgms-keystore-password-hidden=dD5KmzJHa64Oyvpqdu8SCg==
use-router-ip-from-db=true
rabbit-broker-ip=
rabbit-broker-port=
rabbit-broker-username=
rabbit-broker-password=
fogd-ip=192.68.5.3
enable-reverse-dns-lookup=false
enableApiAuth=false
fnd-router-mgmt-mode=1
enable-bootstrap-service=true
proxy-bootstrap-ip=10.48.43.231
```

Les trois dernières lignes ont été modifiées dans le fichier de configuration.

- Ligne 10 : active le mode facile
- Ligne 11 : active le protocole PNP
- Ligne 12 : définit l'adresse IP du serveur FND à contacter

Après avoir modifié le fichier, redémarrez le conteneur FND afin d'adapter les modifications apportées :

```
[root@iot-fnd ~]# /opt/fnd/scripts/fnd-container.sh restart
Stopping FND container...
fnd-container
[root@iot-fnd ~]# Starting FND container...
fnd-container
```

Une fois redémarré, le reste de la configuration peut être effectué à l'aide de l'interface utilisateur graphique.

Préparation du CSV et ajout du routeur au FND

Il peut sembler un peu illogique d'ajouter le périphérique à ce stade du processus de configuration, mais malheureusement, certaines parties de la configuration ne sont pas disponibles tant que certains types de périphériques n'ont pas été ajoutés.

Cela permet d'éviter que l'interface utilisateur graphique ne soit trop saturée, car différents périphériques introduisent différentes options.

Ici, essayons d'ajouter un IR809 à FND.

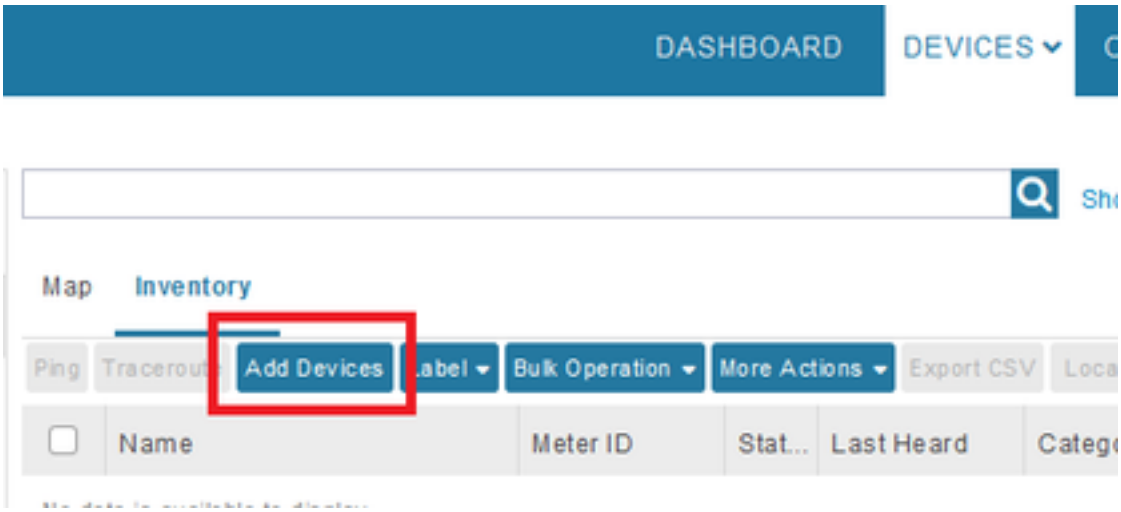
Le CSV se présente comme suit :

```
deviceType,eid,adminUsername,adminPassword,ip
ir800,IR809G-LTE-GA-K9+JMX2022X04S,fndadmin,C1sc0123!,10.48.43.250
```

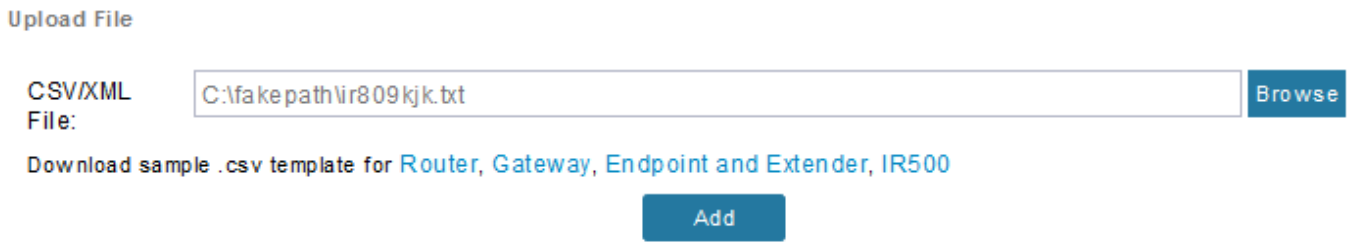
Les champs du CSV sont les suivants :

- **deviceType** : ir800
- **eid** : PID et série avec +
- **adminUsername** : ce nom d'utilisateur sera ajouté à la configuration du routeur et sera utilisé ultérieurement pour terminer le processus d'enregistrement
- **adminPassword** : mot de passe pour adminUsername
- **ip:** L'adresse IP à remplacer dans la configuration du périphérique après le déploiement

Pour ajouter ce périphérique, connectez-vous à l'interface utilisateur graphique et accédez à **Périphériques > Périphériques de champ > Inventaire > Ajouter des périphériques** comme indiqué dans l'image.

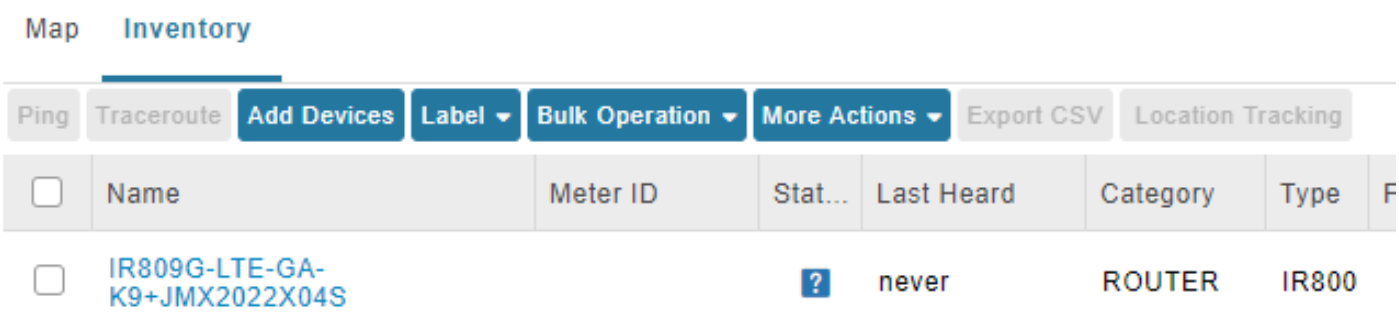


Dans la boîte de dialogue, spécifiez l'emplacement de votre fichier CSV et cliquez sur **Ajouter** pour l'ajouter au fichier FND comme indiqué dans l'image.



Si tout va bien, vous devriez voir l'élément d'historique pour la liste « TERMINÉ ». Après avoir fermé la boîte de dialogue, le périphérique doit apparaître dans l'inventaire comme indiqué dans

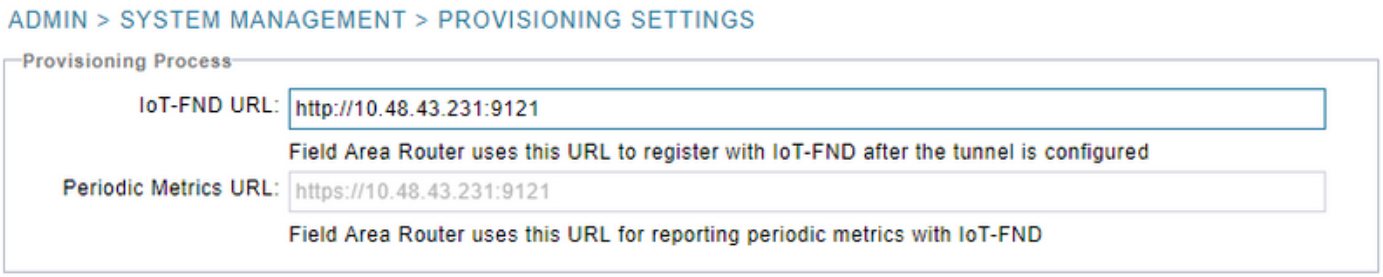
l'image.



Depuis l'ajout du périphérique deviceType ir800, les modèles et groupes applicables seront disponibles dans l'interface utilisateur graphique à ce stade.

Préparer les paramètres d'approvisionnement, le modèle de démarrage et le modèle de configuration

Étant donné que FND est configuré pour le mode de démonstration, il est nécessaire de modifier l'URL de provisionnement pour utiliser HTTP à la place. Accédez à **Admin > Provisioning Settings** afin de le faire :



Remplacez l'URL IoT-FND par **http://<FND IP> :9121**

Ensuite, configurez deux modèles minimaux pour le bootstrap et la configuration.

Le premier, appelé modèle de **configuration de démarrage du routeur**, est la configuration qui est envoyée au routeur une fois qu'il est capable de contacter FND avec succès avec l'utilisation de PNP.

Si PNP n'est pas utilisé, il s'agit de la configuration qui est placée manuellement sur le routeur ou en usine au moment du processus de démarrage. Cette configuration contient juste assez d'informations pour que le routeur puisse démarrer le processus d'enregistrement dans FND.

La seconde, appelée modèle de configuration, sera la configuration qui est ajoutée à la configuration en cours du périphérique. En fait, il peut être vu comme un incrément de la configuration existante.

Dans la plupart des cas, cela entraîne une situation étrange. Il est donc recommandé d'effacer d'abord toutes les configurations du routeur avant de l'ajouter à FND.

Afin de définir le modèle de reconfiguration d'usine du routeur, accédez à **Configure > Tunnel Provisioning > Router Bootstrap Configuration** et remplacez-le par le modèle suivant :

```
<#if isBootstrapping = true>
<#assign mgmtintf = "GigabitEthernet0">
<#assign fndserver = "10.48.43.231">
<#assign sublist=far.eid?split("+")[0..1]>
<#assign pid=sublist[0]>
<#assign sn=sublist[1]>

<#-- General parameters  -->
hostname ${sn}BS
ip domain-name ${sn}
ip host fndserver.fnd.iot ${fndserver}
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
!
<#-- Users  -->
username backup privilege 15 password C1sc0123!
username ${far.adminUsername} privilege 15 password ${far.adminPassword}
!
<#-- Interfaces  -->
interface ${mgmtintf}
  ip address ${far.ip} 255.255.255.192
exit
!
<#-- Clock  -->
clock timezone UTC +2
!
<#-- Archive  -->
file prompt quiet
do mkdir flash:archive
archive
  path flash:/archive
  maximum 8
exit
!
<#-- HTTP -->
ip http server
ip http client connection retry 5
ip http client connection timeout 5
ip http client source-interface ${mgmtintf}
ip http authentication local
ip http timeout-policy idle 600 life 86400 requests 3
ip http max-connections 2
!
<#-- WSMA -->
wsma profile listener exec
  transport http path /wsma/exec
exit
!
wsma profile listener config
  transport http path /wsma/config
exit
!
wsma agent exec
  profile exec
exit
!
wsma agent config
  profile config
exit
!
<#-- CGNA -->
cgna gzip
```

```
!
cgna profile cg-nms-register
  add-command show hosts | format flash:/managed/odm/cg-nms.odm
  add-command show interfaces | format flash:/managed/odm/cg-nms.odm
  add-command show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
  add-command show ipv6 interface | format flash:/managed/odm/cg-nms.odm
  add-command show platform hypervisor | format flash:/managed/odm/cg-nms.odm
  add-command show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
  add-command show iox host list detail | format flash:/managed/odm/cg-nms.odm
  add-command show version | format flash:/managed/odm/cg-nms.odm
  interval 10
  url http://fndserver.fnd.iot:9121/cgna/ios/registration
  gzip
  active
exit
!
<#-- Script to generate RSA for SSH -->
event manager applet genkeys
  event timer watchdog name genkeys time 30 maxrun 60
    action 10 cli command "enable"
    action 20 cli command "configure terminal"
    action 30 cli command "crypto key generate rsa modulus 2048"
    action 80 cli command "no event manager applet genkeys"
    action 90 cli command "exit"
    action 99 cli command "end"
exit

end
</#if>
```

Afin de définir le modèle de configuration. Accédez à **Config > Device Configuration > Edit Configuration Template** et ajoutez ce modèle :

```
<#-- Enable periodic inventory notification every 1 hour to report metrics. -->
    cgna profile cg-nms-periodic
      interval 60
    exit
<#-- Enable periodic configuration (heartbeat) notification every 15 min. -->
   cgna heart-beat interval 15

<#-- Enable SSH access -->
line vty 0 4
  transport input ssh
  login local
exit
```

Ce modèle sera la configuration en cours du routeur résultant. Toute configuration spécifique pour ce groupe de configuration doit donc être ajoutée ici.

Le plus simple est de commencer avec ce modèle minimal. Une fois le modèle réussi, mettez à jour et adaptez-le en fonction de vos besoins.

Àce stade, la configuration/préparation de FND est effectuée et vous pouvez commencer par préparer le routeur.

Préparation du IR800 pour Provisioning/PNP

Si le périphérique que vous souhaitez provisionner contient déjà une configuration ou a déjà été utilisé auparavant, il est préférable d'effacer complètement la configuration du routeur avant de l'ajouter à FND avec PNP.

Évidemment, s'il s'agit d'un nouveau périphérique, cette étape peut être ignorée.

La façon la plus simple d'y parvenir est d'utiliser la commande **write erase** et reload the router avec l'utilisation de la console.

```
ir809kjk#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
*Oct 18 11:42:54.367 UTC: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
ir809kjk#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]

Starting File System integrity check
NOTE: File System will be deinited and later rebuilt
```

Après un certain temps, le IR800 doit revenir avec l'invite pour exécuter la boîte de dialogue de configuration initiale :

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!
```

Assurez-vous qu'il ne reste plus aucune tentative PNP/ZTD précédente, il est préférable de recréer l'archive et le répertoire et de supprimer la **configuration avant enregistrement** sur le routeur également :

```
IR800#delete /f before-*
IR800#delete /f /r archive*
IR800#mkdir archive
Create directory filename [archive]?
Created dir flash:/archive
IR800#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#archive
IR800(config-archive)#path flash:/archive
IR800(config-archive)#maximum 8
IR800(config-archive)#end
```

Actuellement, vous avez un nouveau périphérique ou un périphérique avec une configuration vide, donc, si nécessaire, c'est le moment où une configuration minimale afin que le routeur puisse atteindre FND peut être appliquée.

Dans le cas où vous avez un serveur DHCP, la plupart de ceci devrait aller automatiquement.

La configuration manuelle suivante est sélectionnée sur le périphérique :

```
IR800>enable
IR800#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
IR800(config)#int gi0
IR800(config-if)#ip addr dhcp
```

```
IR800(config-if)#no shut
IR800(config-if)#end
*Aug 1 12:02:02.887: %SYS-5-CONFIG_I: Configured from console by console

IR800#ping 10.48.43.231
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.48.43.231, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
IR800#
```

Comme vous le voyez, une requête ping rapide a été exécutée afin de tester si le routeur a pu atteindre FND avec la configuration IP appliquée.

Configuration du routeur IR800

Àce stade, toutes les conditions préalables sont remplies et vous pouvez lancer le processus PNP. Cela se fait manuellement dans cette instance.

Dans un environnement de production, très probablement, PNP sera utilisé avec l'option DHCP 43. Cela signifie qu'une fois le routeur démarré, il reçoit une adresse IP et la configuration PNP et vous pouvez ignorer cette étape et la suivante.

Afin de configurer manuellement PNP sur le IR800 sans DHCP, vous devez spécifier la destination des requêtes, qui sera le serveur FND.

Cela peut se faire comme suit :

```
IR800(config)#pnp profile pnp-zero-touch
IR800(config-pnp-init)#transport http ipv4 10.48.43.231 port 9125
IR800(config-pnp-init)#end
```

Dès que vous entrez la ligne commençant par « transport », le routeur démarre le processus PNP et tente de contacter FND sur l'adresse IP et le port donnés.

Si tout se passe bien, le périphérique passe par ces étapes :

- [UPDATING_ODM] : mettre à jour les fichiers ODM (Operational Data Model) sur le périphérique pour qu'ils correspondent à ceux valides pour la version FND actuelle
- [MISE À JOUR_ODM_VERIFY_HASH] : vérifier si les fichiers mis à jour sont corrects
- [UPDATED_ODM]
- [COLLECTING_INVENTORY] : collecter les informations de configuration et de périphérique actuelles
- [INVENTAIRE_COLLECTÉ]
- [CONFIGURATION_VALIDATION] : essayez d'appliquer la configuration à partir de la configuration de bootstrap (modèle de reconfiguration d'usine de routeur substitué)
- [CONFIGURATION_VALIDÉE]
- [FICHIER_CONFIGURATION_BOOTSTRAP] : appliquer la configuration validée
- [PUSHING_BOOTSTRAP_CONFIG_VERIFY_HASH] : vérifier si la configuration appliquée est correcte
- [FICHIER_CONFIGURATION_DÉMARRAGE_POUSSÉ]
- [CONFIGURING_STARTUP_CONFIG]:écrivez la configuration en tant que configuration de démarrage
- [CONFIGURED_STARTUP_CONFIG]

- [APPLYING_CONFIG] : appliquer la configuration de démarrage
- [CONFIGURATION_APPLIQUÉE]
- [TERMINATING_BS_PROFILE] : arrêtez le bootstrap.

Vous pouvez suivre le processus dans le fichier serveur FND.log.

Dans l'interface utilisateur graphique, le périphérique se déplace lorsque vous accédez à **Unheard > Boostrapping > Bootstrapped**

Une fois le bootstrap terminé, le routeur dispose du modèle de reconfiguration usine du routeur substitué et se comporte comme un périphérique de démarrage normal sans PNP.

En d'autres termes, un profil CGNA sur le IR800 tente de s'enregistrer auprès du serveur FND.

Vérifiez l'état du profil CGNA :

```
JMX2022X04SBS#sh cgna profile-state all
Profile 1:
Profile Name: cg-nms-register
Activated at: Thu Aug  1 15:31:14 2019
URL: http://fndserver.fnd.iot:9121/cgna/ios/registration
Payload content type: xml
Interval: 10 minutes
gzip: activated
Profile command:
    show hosts | format flash:/managed/odm/cg-nms.odm
    show interfaces | format flash:/managed/odm/cg-nms.odm
    show ipv6 dhcp | format flash:/managed/odm/cg-nms.odm
    show ipv6 interface | format flash:/managed/odm/cg-nms.odm
    show platform hypervisor | format flash:/managed/odm/cg-nms.odm
    show snmp mib ifmib ifindex | format flash:/managed/odm/cg-nms.odm
    show iox host list detail | format flash:/managed/odm/cg-nms.odm
    show version | format flash:/managed/odm/cg-nms.odm
State: Wait for timer for next action
Timer started at Thu Aug  1 15:31:14 2019
Next update will be sent in 9 minutes 30 seconds
Last successful response not found
Last failed response not found
```

Avec la configuration fournie, le périphérique tentera de s'enregistrer auprès de FND au bout de dix minutes. Vous pouvez voir que dans ce résultat, il reste neuf minutes et trente secondes avant que le routeur ne démarre le processus d'enregistrement.

Vous pouvez attendre la fin du compteur ou exécuter manuellement le profil **cg-nms-register** immédiatement :

```
IR800-Bootstrap#cgna exec profile cg-nms-register
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Le périphérique doit passer à l'état UP dans FND, comme l'illustre l'image.

Device Info | Events | Config Properties | Running Config | Router Files | Raw Sockets | Work Order | A

Time	Event Name	Severity	Message
2018-10-18 14:01:03:535	Up	INFO	Device is up.
2018-10-18 14:00:58:380	Registration Success	INFO	Registration successful.
2018-10-18 14:00:58:377	Registration Request	INFO	Registration request from device.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Afin de dépanner le processus de démarrage, vérifiez les points suivants :

- Connexion du serveur FND : **/opt/fnd/logs/server.log**
- Augmentez la verbalité de la connexion : **Admin > Logging > Log Level Settings > Router Bootstrapping > Debug**
- Àpartir de la console IR800 : **show pnp ? ou debug pnp ?**
- Dans l'interface utilisateur FND : **Périphériques > Inventaire > Sélectionner un périphérique > Événements**
- La plupart des problèmes de cette étape sont liés à des erreurs (de syntaxe) dans le modèle de reconfiguration d'usine du routeur

Afin de dépanner le processus d'enregistrement, vérifiez les points suivants :

- Connexion du serveur FND : **/opt/fnd/logs/server.log**
- Àpartir de la console IR800 :

  show cgna profile-state alldebug cgna logging ?debug wsma agent
- Dans l'interface utilisateur FND : **Périphériques > Inventaire > Sélectionner un périphérique > Événements**
- Vérifiez la connectivité WSMA via HTTP au IR800 à partir de la machine virtuelle FND
  URI utilisé par FND : http://10.48.43.231:80/wsma/execMéthode : POSTSécurité: **authentification de base**