Preparar arquivos .csv (valor separado por vírgula) para importar novos dispositivos no FND

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Arquivos .csv para adicionar dispositivos no FND](#)
[LONGE](#)
[Roteador central (HER)](#)
[Ponto de Extremidade da Rede Conectada (CGE)](#)
[Examples](#)
[Diagrama de Rede](#)

Introduction

Este documento descreve as etapas para preparar o arquivo .csv para o Field Network Diretor (FND). Para fornecer gerenciamento de rede seguro, o FND não fornece detecção e registro de ativos automáticos ou dinâmicos. Antes que um novo dispositivo possa ser adicionado a uma implantação de FND, uma entrada de banco de dados exclusiva deve ser criada para ele, importando um arquivo .csv personalizado através da interface de usuário da Web (UI).

Este artigo fornece modelos .csv que podem ser usados e personalizados para adicionar novos endpoints, roteadores de área de campo ou roteadores headend a uma solução existente. Além disso, cada campo de banco de dados (DB) será definido e explicado para auxiliar no projeto e na implementação de novos dispositivos.

> **Note**: Antes que este guia possa ser usado, você deve ter uma solução de CG-NMS/FND totalmente configurada e instalada.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- CG-NMS/FND application server 1.0 ou posterior instalado e em execução com acesso à IU da Web disponível.
- Servidor proxy TPS (Tunnel Provisioning Server) instalado e em execução.
- Oracle database server instalado e configurado corretamente.
- setupCgms.sh foi executado com êxito pelo menos uma vez com um db_migrate_first-time

bem-sucedido.
- Você ainda pode usar este guia se ainda não tiver instalado e configurado seus servidores DHCP, mas é altamente recomendável que, antes de usar este documento, sua organização tenha planejado completamente os esquemas de endereçamento IPv4 e IPv6 para a implantação. Isso inclui comprimentos e intervalos de prefixo para túneis IPSec IPv4, túneis GRE (Generic Routing Encapsulation) IPv6 e endereçamento de pilha dupla em loopbacks CGR (Connected Grid Router).
- Também é altamente recomendável que você já tenha comprado ou planeje comprar pelo menos um roteador headend, pelo menos um roteador de área de campo e pelo menos um endpoint/metro.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- FND 3.0.1-36
- SSM baseado em software (também 3.0.1-36)
- pacote cgms-tools instalado no servidor de aplicativos (3.0.1-36)
- Todos os servidores Linux executando RHEL 6.5
- Todos os servidores Windows com Windows Server 2008 R2 Enterprise
- Cisco Cloud Services Router (CSR) 1000v sendo executado em uma VM como roteador headend
- CGR-1120/K9 usado como roteador de área de campo (FAR) com CG-OS 4(3)

Um ambiente de laboratório de FND controlado foi usado durante a criação deste documento. Embora outras implantações sejam diferentes, você deve seguir todos os requisitos mínimos dos guias de instalação.

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.

Arquivos .csv para adicionar dispositivos no FND

LONGE

Este modelo pode ser usado para FAR que são apresentados à solução pela primeira vez. Ele estará localizado na página **Dispositivos > Dispositivos de campo**. Na página Dispositivos de campo, clique no menu suspenso **Importação em massa** e selecione **Adicionar dispositivos**.

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

Element Identifier (eid) - Este é um identificador exclusivo usado para identificar o dispositivo em mensagens de registro, bem como na GUI. Para evitar confusões, recomenda-se que sua organização desenvolva um esquema EID. O esquema recomendado é usar o número de série IDevID do CGR como o EID. Nesses roteadores, o número de série usará esta fórmula: PID+SN.

Por exemplo: CGR1120/K9+JAFXXXXXXX.

deviceType - É usado para identificar a plataforma de hardware ou a série. Para os modelos 1120 e 1240, o valor deviceType deve ser cgr1000.

tunnelHerEid - Devido ao fato de que o FND permite o uso de 2 HERs em execução no par HA ou autônomo, o campo tunnelHerEid é usado para identificar a HER à qual os túneis VPN neste CGR serão terminados. Esse valor será simplesmente o EID do HER apropriado.

certIssuerCommonName - Este campo é um requisito de ZTD (Zero Touch Deployment, implantação de toque zero) e geralmente é igual ao nome DNS de sua autoridade de certificado RSA raiz. Se você não souber o nome comum, poderá encontrá-lo e executar o comando **show crypto ca certificate**. Na cadeia do ponto de confiança LDevID, você vê o nome comum do emissor raiz na linha de assunto de 'Certificado CA 0'. Como alternativa, você pode simplesmente acessar a página Certificados do FND e examinar o certificado raiz.

meshPrefixConfig - Este valor é atribuído à interface do módulo WPAN. Todos os CGEs que formam uma árvore de Idioma da Política de Roteamento (RPL - Routing Policy Language) com este roteador recebem um endereço IP via DHCP (supondo que a retransmissão de DHCP esteja configurada corretamente) com esse valor como prefixo da rede.

tunnelSrcInterface1 - Para implantações que utilizam túneis IPSec primários e secundários, este valor é o nome da interface da origem do túnel para os túneis primários (como o celular4/1). Se houver um túnel de backup, você atribuirá a interface de origem adicionando um valor para tunnelSrcInterface2. Se você tiver apenas 1 conexão WAN, usará somente o campo tunnelSrcInterface1.

ipsecTunnelDestAddr1 - Este valor é o endereço de destino do túnel IPv4 para o túnel IPSec principal com a interface de origem atribuída a tunnelSrcInterface1.

adminUsername - Este é o nome de usuário que o FND usará quando você abrir sessões HTTPS e Netconf para o FAR. É necessário que esse usuário tenha permissões completas por AAA ou configurado localmente com a função network-admin.

adminPassword - A senha para a conta adminUsername. Você pode exibir esse nome de usuário na GUI e navegar até a guia Propriedades de configuração da página do dispositivo e olhar para o 'Nome de usuário do administrador' na seção 'Credenciais do roteador'. Para evitar erros, essa senha deve primeiro ser criptografada com a Signature_Tool do pacote cgms-tools RPM. Esta ferramenta criptografa tudo em texto simples usando a cadeia de certificados no cgms_keystore. Para usar a ferramenta de assinatura, altere o diretório para /opt/cgms-tools/bin/ no servidor de aplicativos FND. Em seguida, crie um novo arquivo .txt de texto simples que contenha adminPassword. Depois de ter o arquivo de texto, execute este comando:

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

Copie/cole a saída criptografada no campo adminPassword do arquivo .csv. É recomendável excluir com segurança o arquivo de senha de texto simples quando você terminar de usar a Ferramenta de assinatura.

cgrusername1 - Esta conta de usuário não é necessária, mas se vários usuários com funções diferentes estiverem configurados no CGR, você poderá adicionar outra conta de usuário aqui. É importante saber que somente adminUsername e adminPassword serão usados para o gerenciamento do dispositivo. Nesta configuração de laboratório, use as mesmas credenciais de adminUsername.

cgrpassword1 - A senha para o usuário cgrusername1.

ip - Este é o IP de gerenciamento principal. Quando pings ou rastreamentos forem executados a partir do FND, eles usarão esse IP. As sessões HTTPS do Connected Grid Device Manager (CGDM) também serão enviadas para este IP. Em uma implantação típica, esse será o endereço IP atribuído à interface tunnelSrcInterface1.

meshPanidConfig - A ID PAN atribuída à interface WPAN deste CGR.

wifiSsid - O SSID configurado na interface WPAN.

dhcpV4TunnelLink - O endereço IPv4 que o FND usará em sua solicitação de proxy para o servidor DHCP. Neste ambiente de laboratório, o servidor DHCP é um Cisco Network Registrar (CNR) e o pool de IPsec DHCPv4 está configurado para alugar sub-redes /31. Se você usar o primeiro IP em uma sub-rede /31 disponível para seu valor dhcpv4TunnelLink, o FND provisionará automaticamente ambos os IPs da sub-rede ponto a ponto para o túnel 0 do CGR e o túnel correspondente do HER.

dhcpV6TunnelLink - O endereço IPv6 que o FND usa em sua solicitação de proxy para o servidor DHCP para o túnel GRE (Generic Routing Encapsulation) IPv6. Neste ambiente de laboratório, o CNR é configurado para alugar endereços com o uso de prefixos /127. Assim como o dhcpV4TunnelLink, o FND provisionará automaticamente o 2º IP da sub-rede ponto a ponto para o HER quando você configurar seu túnel GRE.

dhcpV4LoopbackLink - O endereço IPv4 que o FND usará em suas solicitações de proxy para o servidor DHCP ao configurar a interface Loopback 0 do CGR. Neste ambiente de laboratório, o pool de DHCP correspondente no CNR foi configurado para alugar /32 sub-redes.

dhcpV6LoopbackLink - O endereço IPv6 que o FND usará em suas solicitações de proxy para o servidor DHCP quando você configurar a interface Loopback 0 do CGR. Neste ambiente de laboratório, o pool correspondente foi configurado para alugar /128 sub-redes.

Roteador central (HER)

Quando você adiciona um roteador head-end pela primeira vez, este modelo pode ser usado:

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

deviceType - Ao introduzir um ASR ou CSR, o valor 'asr1000' deve ser usado neste campo.

status - Os valores de status aceitos não são ouvidos, inativos e inativos. Use unheard se for a new import (Não ouvido se tratar de uma nova importação).

lastheard - Se este for um novo dispositivo, este campo poderá ser deixado em branco.

runningFirmwareVersion - Este valor também pode ser deixado em branco, mas se você quiser importar a versão, use o número da versão na linha superior da saída **show version**. Por exemplo, nesta saída, a string '03.16.04b.S' deve ser usada:

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

netconfUsername - O nome de usuário configurado para ter acesso Netconf/SSH completo ao HER.

netconfPassword - A senha do usuário especificada no campo netconfUsername.

Ponto de Extremidade da Rede Conectada (CGE)

Adicionar um novo ponto de extremidade de malha ao DB é muito simples. Este modelo pode ser usado:

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

deviceType - Neste ambiente de laboratório, 'cgmesh' foi usado para adicionar um medidor inteligente como um CGE.

lat - A coordenada de latitude GPS onde o CGE será instalado.

lng - A longitude do GPS.

Examples

Inclusão 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
```

Adição:

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

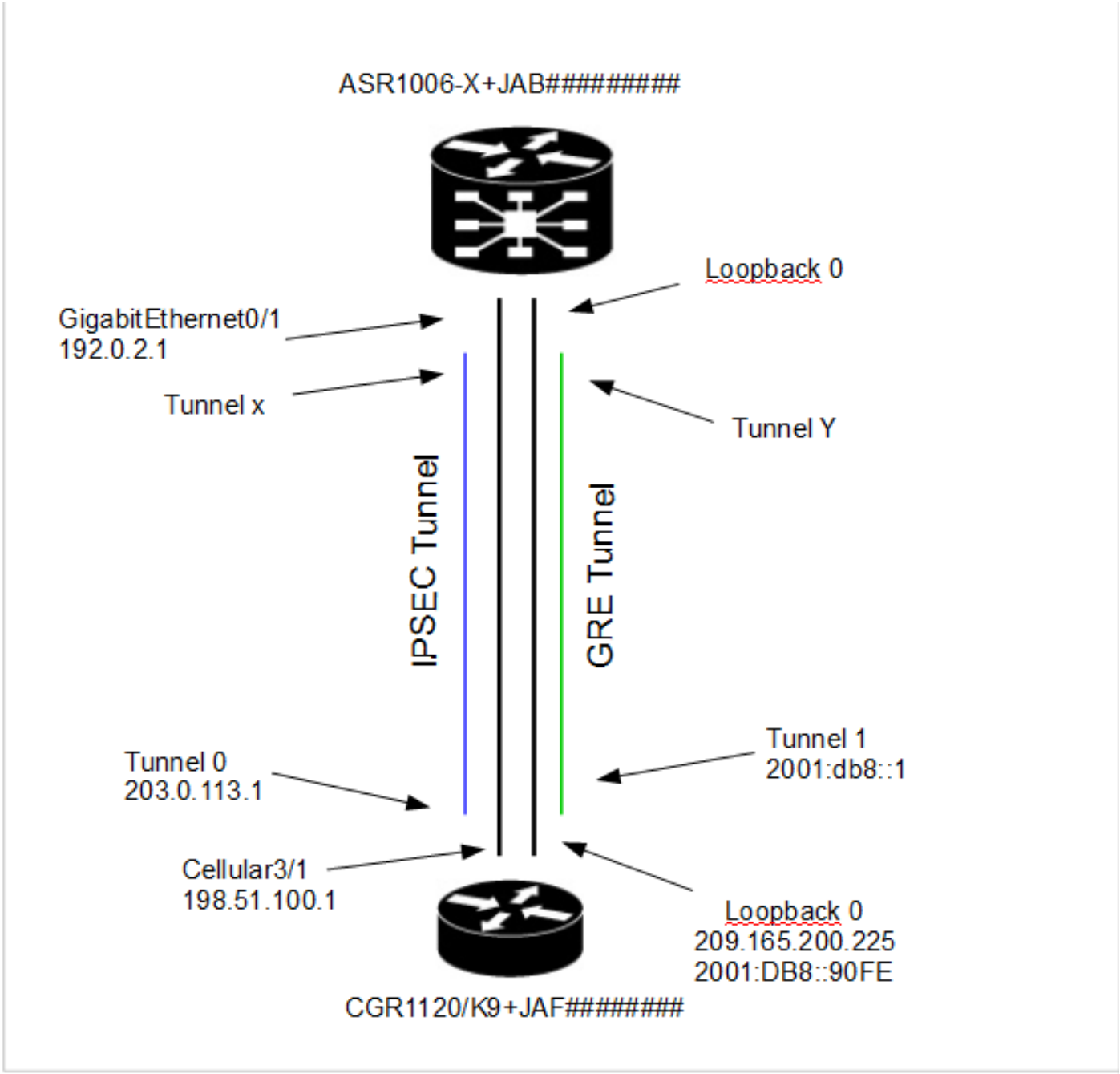
Adição CGE:

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

Diagrama de Rede

> **Note**: O provisionamento de túnel funciona de forma diferente com base no fato de um FAR estar executando CG-OS ou IOS. CG-OS: Uma nova interface de túnel IPSEC será configurada no FAR e no HER. O FND enviará uma solicitação de proxy ao servidor DHCP para 2 IPs por túnel e configurará o 2º IP automaticamente na interface de túnel correspondente. IOS: A HER usará um modelo Flex-VPN que usa um túnel IPSEC ponto a multiponto. Com essa configuração, somente os FARs recebem novas interfaces de túnel.

Neste diagrama de topologia, 'Tunnel x' refere-se à interface de túnel IPSEC relativa no HER, enquanto 'Tunnel Y' corresponde ao túnel GRE incorporado à interface de loopback no HER. Além disso, os IPs e as interfaces no diagrama correspondem diretamente aos exemplos de configuração nos modelos .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########