Prepare arquivos .csv (Comma Separated Value) para importar dispositivos novos em FND

Índice

Introdução

Este documento descreve etapas para preparar o arquivo .csv para o diretor da rede do campo (FND). A fim fornecer o Gerenciamento de redes seguro, o FND não fornece a descoberta e o registro automáticos ou dinâmicos do ativo. Antes que um dispositivo novo possa ser adicionado a um desenvolvimento FND uma entrada no base de dados original deve ser criada para ele importando um arquivo do costume .csv através da relação de usuário de web (UI).

Este artigo fornece os moldes .csv que podem ser usados e personalizado a fim adicionar valores-limite novos, roteadores de área do campo ou roteadores de extremidade principais a uma solução existente. Além do que isto, cada campo do base de dados (DB) será definido e explicado a fim ajudar com o projeto e a aplicação de dispositivos novos.

> Nota: Antes que este guia possa ser usado, você deve ter uma solução conectada inteiramente configurada e instalada do sistema de gerenciamento de rede da grade (CG-NMS) /FND.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Server de aplicativo 1.0 ou instalada mais atrasada e ser executado CG-NMS/FND com o acesso da Web UI disponível.
- Servidor proxy do servidor de provisionamento do túnel (TP) instalado e ser executado.
- Server de base de dados Oracle instalado e configurado corretamente.

- setupCgms.sh é executado com sucesso pelo menos uma vez com um db_migrate principiante bem sucedido.
- Você pode ainda usar este guia se você ainda não instalou e configurou seus server DHCP mas se recomenda fortemente que antes que você use este documento sua organização planejou inteiramente para fora métodos de endereçamento do IPv4 e do IPv6 para o desenvolvimento. Isto inclui comprimentos de prefixo e escalas para túneis de IPsec do IPv4, túneis de encapsulamento de roteamento genéricos (GRE) do IPv6 e dual endereçamento da pilha em laços de retorno conectados do roteador da grade (CGR).
- Igualmente recomenda-se fortemente que você já tem comprado ou o está planejando comprar pelo menos 1 roteador de extremidade principal, pelo menos 1 roteador de área do campo e pelo menos 1 valor-limite/medidor.

Componentes Utilizados

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

- FND 3.0.1-36
- SS com base no software (também 3.0.1-36)
- as cgms-ferramentas empacotam instalado no server de aplicativo (3.0.1-36)
- Todos os servidores Linux que executam RHEL 6.5
- Todos os Windows Server que dirigem a empresa R2 de Windows Server 2008
- Cisco nubla-se o roteador dos serviços (CSR) 1000v que é executado em um VM como o roteador de extremidade principal
- CGR-1120/K9 usados como o roteador de área do campo (DISTANTE) com CG-OS 4(3)

Um ambiente de laboratório controlado FND foi usado durante a criação deste documento. Quando outras disposições diferirão, você deve aderir a todos os requisitos mínimos dos Guias de Instalação.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

arquivos .csv para adicionar dispositivos em FND

DISTANTE

Este molde pode ser usado para DISTANTE que são introduzidas à solução pela primeira vez. Isto será ficado situado nos **dispositivos > na** página dos **dispositivos do campo**. No campo os dispositivos paginam, clicam sobre o menu dropdown da **importação de grande escala** e seleto **adicionar dispositivos**.

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

Identificador do elemento (eid) - Este é um identificador exclusivo usado para identificar o dispositivo nos mensagens de registro assim como no GUI. A fim impedir a confusão, recomenda-

se que sua organização desenvolve um esquema EID. O esquema recomendado é usar o número de série do IDevID do CGR como o EID. Neste Roteadores, o número de série usará esta fórmula: PID+SN. Por exemplo: .

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

tunnelHerEid - Devido ao fato de que o FND permite ao uso de 2 o seu que é executado em pares HA ou autônomo, o campo do tunnelHerEid é usado para identificar a que os túneis VPN neste CGR terminará. Este valor será simplesmente o EID do apropriado ELA.

certIssuerCommonName - Este campo é uma exigência do desenvolvimento zero do toque (ZTD) e é geralmente o mesmo que o nome de DNS de seu Certificate Authority da raiz RSA. Se você não conhece o Common Name, você pode encontrá-lo e executar o comando show crypto ca certificates. Na corrente para o ponto confiável de LDevID, você vê o Common Name do expedidor da raiz na linha de assunto 'do certificado de CA 0'. Alternativamente, você pode simplesmente alcançar a página dos Certificados do FND e olhar o certificado de raiz.

meshPrefixConfig - Este valor é atribuído à interface de módulo WPAN. Todo o CGEs que formam uma árvore da língua da política de roteamento (RPL) com este roteador recebe um endereço IP de Um ou Mais Servidores Cisco ICM NT através do DHCP (a transmissão de DHCP presumida é configurada apropriadamente) com este valor como o prefixo de rede.

tunnelSrcInterface1 - Para as disposições que utilizam túneis de IPsec preliminares e secundários, este valor é o nome da relação do origem de túnel para seus túneis preliminares (tais como cellular4/1). Se há um túnel alternativo então você atribuirá a interface de origem adicionando um valor para tunnelSrcInterface2. Se você tem somente 1 conexão de WAN então você usará somente o campo tunnelSrcInterface1.

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

adminUsername - Este é o username que o FND usará quando você abre o HTTPS e as sessões de Netconf ao DISTANTE. Exige-se que este usuário está dado permissões completas pelo AAA ou configurado localmente com o papel rede-admin.

adminPassword - A senha para a conta do adminUsername. Você pode ver este username no GUI e navegar à aba das propriedades da configuração da página do dispositivo e olhar o “nome de usuário de administrador” na seção do “das credenciais roteador. A fim evitar erros, esta senha deve primeiramente ser cifrada com o Signature_Tool do pacote das cgms-ferramentas RPM. Esta ferramenta cifra qualquer coisa no texto simples usando o certificate chain no cgms_keystore. Para usar a ferramenta da assinatura, mude o diretório a /opt/cgms-tools/bin/ no server de aplicativo FND. Em seguida, crie um arquivo novo de .txt do texto simples que contenha o adminPassword. Uma vez que você tem o arquivo de texto, execute este comando:

```
./signature-tool encrypt /opt/cgms/server/cgms/conf/cgms_keystore password-file.txt
```
Cópia/pasta a saída cifrada no campo do adminPassword de seu arquivo .csv. É uma boa ideia suprimir firmemente do arquivo de senha do texto simples quando você termina para usar a ferramenta da assinatura.

cgrusername1 - Esta conta de usuário não é exigida, mas se os usuários múltiplos com papéis diferentes são configurados no CGR, você pode adicionar uma outra conta de usuário aqui. É importante saber que somente o adminUsername e o adminPassword estarão usados para o Gerenciamento do dispositivo. Nesta instalação de laboratório, use as mesmas credenciais que o adminUsername.

cgrpassword1 - A senha para o usuário cgrusername1.

IP - Este é o IP de gerenciamento preliminar. Quando os sibilos ou os traços são executados do FND usarão este IP. As sessões HTTPS para o gerenciador de dispositivo conectado da grade (CGDM) serão enviadas a este IP também. Em uma implementação típica, este será o endereço IP de Um ou Mais Servidores Cisco ICM NT atribuído a sua relação tunnelSrcInterface1.

meshPanidConfig - A BANDEJA ID atribuída à relação WPAN deste CGR.

wifiSsid - O SSID configurado na relação WPAN.

dhcpV4TunnelLink - O endereço do IPv4 que o FND usará em sua solicitação de proxy ao servidor DHCP. Neste ambiente de laboratório, o servidor DHCP é um Cisco Network Registrar (CNR) e o pool do IPsec DHCPv4 é configurado para alugar sub-redes de /31. Se você usa o primeiro IP em uma sub-rede disponível de /31 para seu valor dhcpv4TunnelLink então o FND provision automaticamente o IPs da sub-rede ponto a ponto ao tunnel0 do CGR e o túnel correspondente do HER.

dhcpV6TunnelLink - O endereço do IPv6 que o FND usa em sua solicitação de proxy ao servidor DHCP para o túnel de encapsulamento de roteamento genérico (GRE) do IPv6. Neste ambiente de laboratório, o CNR é configurado para alugar endereços com o uso de prefixos de /127. Apenas como o dhcpV4TunnelLink, o FND provision automaticamente o ò IP da sub-rede ponto a ponto ao ELA quando você configura seu túnel GRE.

dhcpV4LoopbackLink - O endereço do IPv4 que o FND usará em suas solicitações de proxy ao servidor DHCP ao configurar a relação de Loopback0 do CGR. Neste ambiente de laboratório, o conjunto de DHCP correspondente no CNR foi configurado para alugar sub-redes de /32.

dhcpV6LoopbackLink - O endereço do IPv6 que o FND usará em suas solicitações de proxy ao servidor DHCP quando você configurar a relação de Loopback0 do CGR. Neste ambiente de laboratório, o pool correspondente foi configurado para alugar sub-redes de /128.

Roteador de extremidade principal ()

Quando você adiciona um roteador de extremidade principal pela primeira vez, este molde pode ser usado:

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

deviceType - Quando você introduz um ASR ou um CSR, o valor 'asr1000 deve ser usado neste campo.

estado - Os valores de status aceitados são inauditos, para baixo e levantam. Use inaudito se é uma importação nova.

lastheard - Se este é um dispositivo novo, este campo pode ser saido vazio.

runningFirmwareVersion - Este valor pode ser deixado vazio também mas se você quer importar a versão, usa o número de versão da linha superior mesma das **saídas de versão da mostra**. Por exemplo, nesta saída, a corda '03.16.04b.S deve ser usada:

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

netconfUsername - O username do configurado pelo usuário para ter o acesso completo Netconf/SSH ao ELA.

netconfPassword - A senha para o usuário especificada no campo do netconfUsername.

Valor-limite conectado da grade (CGE)

Para adicionar um valor-limite novo da malha ao DB é muito simples. Este molde pode ser usado:

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

deviceType - Neste ambiente de laboratório, o “cgmesh” foi usado para adicionar um medidor esperto como um CGE.

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

GNL - A longitude de GPS.

Exemplos

Adição DISTANTE:

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

SUA 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=
```

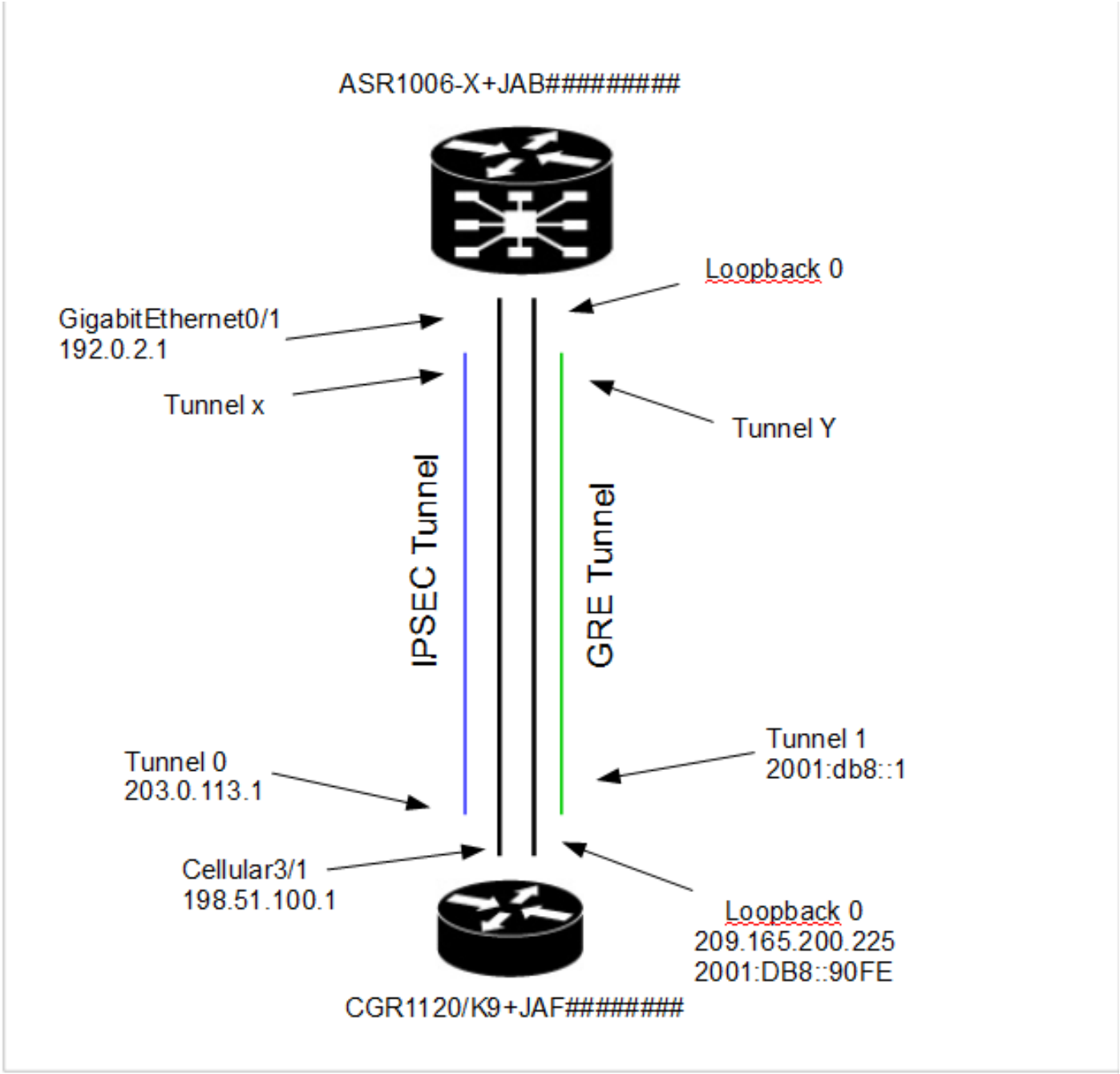
Adição CGE:

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

Diagrama de Rede

> Nota: Trabalhos do abastecimento do túnel baseados diferentemente sobre se a DISTANTE está executando CG-OS ou IO. CG-OS: Uma relação nova do túnel de IPsec será configurada no DISTANTE e ELA. O FND enviará uma solicitação de proxy ao servidor DHCP para 2 IPs pelo túnel e configurará o ò IP automaticamente na interface de túnel correspondente. IO: Usará um molde Cabo-VPN que use um túnel de IPsec point-to-multipoint. Com esta configuração, somente o FARs recebe interfaces de túnel novas.

Neste diagrama de topologia “túnel x” refere-lhe a relação relativa do túnel de IPsec no quando o “túnel Y” corresponder com o túnel GRE construído fora da interface de loopback no ELA. Além disso, os IPs e as relações no diagrama correspondem diretamente aos exemplos de configuração nos moldes .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########