

FND에서 새 디바이스를 가져올 .csv(쉼표로 구분된 값) 파일 준비

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[FND에서 디바이스를 추가할 .csv 파일](#)

[멀리](#)

[헤드 엔드 라우터\(HER\)](#)

[CGE\(Connected Grid Endpoint\)](#)

[예](#)

[네트워크 다이어그램](#)

소개

이 문서에서는 FND(Field Network Director)를 위해 .csv 파일을 준비하는 단계를 설명합니다. 보안 네트워크 관리를 제공하기 위해 FND는 자동 또는 동적 자산 검색 및 등록을 제공하지 않습니다. FND 구축에 새 디바이스를 추가하려면 웹 UI(User Interface)를 통해 사용자 정의 .csv 파일을 가져와서 고유한 데이터베이스 항목을 생성해야 합니다.

이 문서에서는 기존 솔루션에 새 엔드포인트, LAN 라우터 또는 FE 라우터를 추가하기 위해 사용 및 사용자 지정할 수 있는 .csv 템플릿을 제공합니다. 이 외에도 새 디바이스의 설계 및 구현을 지원하기 위해 각 데이터베이스(DB) 필드가 정의되고 설명됩니다.

참고: 이 가이드를 사용하려면 CG-NMS(Connected Grid Network Management System)/FND 솔루션이 완전히 구성되어 설치되어 있어야 합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CG-NMS/FND 애플리케이션 서버 1.0 이상이 설치되어 웹 UI 액세스를 사용하여 실행 중입니다.
- TPS(Tunnel Provisioning Server) 프록시 서버가 설치 및 실행되고 있습니다.
- Oracle 데이터베이스 서버가 설치되고 올바르게 구성되었습니다.
- setupCgms.sh가 첫 번째 db_migrate에 성공하여 한 번 이상 성공적으로 실행되었습니다.
- 아직 DHCP 서버를 설치 및 구성하지 않은 경우에도 이 설명서를 사용할 수 있지만, 이 문서를 사용하기 전에 조직에서 구축을 위한 IPv4 및 IPv6 주소 지정 체계를 완전히 계획했다는 것이

좋습니다. 여기에는 IPv4 IPsec 터널, IPv6 GRE(Generic Routing Encapsulation) 터널 및 CGR(Connected Grid Router) 루프백의 듀얼 스택 주소 지정에 대한 접두사 길이와 범위가 포함됩니다.

- 또한 이미 1개 이상의 헤드 엔드 라우터, 최소 1개의 현장 영역 라우터, 최소 1개의 엔드포인트 /미터 이상을 구매했거나 구매할 계획인 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FND 3.0.1-36
- 소프트웨어 기반 SSM(3.0.1-36)
- 응용 프로그램 서버에 설치된 cgms-tools 패키지(3.0.1-36)
- RHEL 6.5를 실행하는 모든 Linux 서버
- Windows Server 2008 R2 Enterprise를 실행하는 모든 Windows 서버
- VM에서 헤드 엔드 라우터로 실행되는 Cisco CSR(Cloud Services Router) 1000v
- CG-OS 4(3)에서 FAR(Field Area Router)로 사용되는 CGR-1120/K9

이 문서를 작성하는 동안 제어된 FND 랩 환경이 사용되었습니다. 다른 구축은 다르지만 설치 가이드의 최소 요구 사항을 모두 준수해야 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

FND에서 디바이스를 추가할 .csv 파일

멀리

이 템플릿은 솔루션에 처음 도입된 FAR에 사용할 수 있습니다. 이는 Devices(디바이스) > Field Devices(필드 디바이스) 페이지에 있습니다. Field Devices 페이지에서 Bulk Import(대량 가져오기) 드롭다운 메뉴를 클릭하고 Add Devices(디바이스 추가)를 선택합니다.

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

Element Identifier(eid) - 로그 메시지 및 GUI에서 디바이스를 식별하는 데 사용되는 고유 식별자입니다. 혼동을 방지하려면 조직에서 EID 체계를 개발하는 것이 좋습니다. 권장되는 방법은 CGR의 IDevID 일련 번호를 EID로 사용하는 것입니다. 이러한 라우터에서 일련 번호는 다음 공식을 사용합니다. PID+SN. 예: CGR1120/K9+JAFXXXXXXX.

deviceType - 하드웨어 플랫폼 또는 시리즈를 식별하는 데 사용됩니다. 1120 및 1240 모델 모두에서 deviceType 값은 cgr1000이어야 합니다.

tunnelHerEid - FND가 HA 쌍 또는 독립형 모드로 실행되는 HER 2개를 사용할 수 있도록 하기 때문에 tunnelHerEid 필드를 사용하여 이 CGR의 VPN 터널이 종료될 HER를 식별합니다. 이 값은 해당

HER의 EID가 됩니다.

certIssuerCommonName - 이 필드는 ZTD(Zero Touch Deployment)의 요구 사항이며 일반적으로 루트 RSA 인증 기관의 DNS 이름과 동일합니다. 공용 이름을 모르는 경우 이를 찾아 `show crypto ca certificates` 명령을 실행할 수 있습니다. LDevID 신뢰 지점의 체인에서 'CA certificate 0'의 제목 줄에 루트 발급자 공통 이름이 표시됩니다. 또는 FND의 Certificates(인증서) 페이지에 액세스하여 루트 인증서를 확인하기만 하면 됩니다.

meshPrefixConfig - 이 값은 WPAN 모듈 인터페이스에 할당됩니다. 이 라우터가 있는 RPL(Routing Policy Language) 트리를 구성하는 모든 CGE는 DHCP를 통해 IP 주소를 수신합니다(DHCP 릴레이가 적절하게 구성된 것으로 가정). 이 값을 네트워크 접두사로 사용합니다.

tunnelSrcInterface1 - 기본 및 보조 IPsec 터널을 사용하는 구축의 경우 이 값은 기본 터널(예: cellular4/1)에 대한 터널 소스의 인터페이스 이름입니다. 백업 터널이 있는 경우 tunnelSrcInterface2에 대한 값을 추가하여 소스 인터페이스를 할당합니다. WAN 연결이 1개만 있는 경우 tunnelSrcInterface1 필드만 사용합니다.

ipsecTunnelDestAddr1 - 이 값은 tunnelSrcInterface1에 할당된 소스 인터페이스가 있는 기본 IPsec 터널의 IPv4 터널 대상 주소입니다.

adminUsername - FND가 FAR에 대한 HTTPS 및 Netconf 세션을 열 때 사용할 사용자 이름입니다. 이 사용자에게 AAA에 의해 모든 권한이 부여되거나 네트워크 관리자 역할로 로컬로 구성되어야 합니다.

adminPassword - adminUsername 계정의 비밀번호입니다. GUI에서 이 사용자 이름을 보고 디바이스 페이지의 Config Properties(구성 속성) 탭으로 이동하여 'Router Credentials(라우터 자격 증명)' 섹션에서 'Administrator Username(관리자 사용자 이름)'을 확인할 수 있습니다. 오류를 방지하려면 먼저 cgms-tools RPM 패키지의 Signature_Tool을 사용하여 이 비밀번호를 암호화해야 합니다. 이 도구는 cgms_keystore의 인증서 체인을 사용하여 일반 텍스트로 모든 것을 암호화합니다. 서명 도구를 사용하려면 FND 응용 프로그램 서버의 디렉토리를 /opt/cgms-tools/bin/로 변경합니다. 그런 다음 adminPassword가 포함된 새 일반 텍스트 .txt 파일을 만듭니다. 텍스트 파일이 있으면 다음 명령을 실행합니다.

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

암호화된 출력을 .csv 파일의 adminPassword 필드에 복사/붙여넣습니다. 서명 도구 사용이 완료되면 일반 텍스트 암호 파일을 안전하게 삭제하는 것이 좋습니다.

cgrusername1 - 이 사용자 계정은 필수는 아니지만 CGR에 역할이 다른 여러 사용자가 구성된 경우 여기에 다른 사용자 계정을 추가할 수 있습니다. adminUsername 및 adminPassword만 디바이스 관리에 사용된다는 점을 알아야 합니다. 이 Lab 설정에서 adminUsername과 동일한 자격 증명을 사용합니다.

cgrpassword1 - cgrusername1 사용자의 비밀번호입니다.

ip - 기본 관리 IP입니다.FND에서 ping 또는 추적을 실행하면 이 IP를 사용합니다
.CGDM(Connected Grid Device Manager)용 HTTPS 세션은 이 IP에도 전송됩니다.일반적인 구축
에서는 tunnelSrcInterface1 인터페이스에 할당된 IP 주소가 됩니다.

meshPanidConfig - 이 CGR의 WPAN 인터페이스에 할당된 PAN ID입니다.

wifiSsid - WPAN 인터페이스에 구성된 SSID입니다.

dhcpV4TunnelLink - FND가 DHCP 서버에 대한 프록시 요청에서 사용할 IPv4 주소입니다.이 랩 환
경에서 DHCP 서버는 Cisco CNR(Network Registrar)이고 DHCPv4 IPsec 풀은 /31 서브넷을 임대
하도록 구성됩니다.dhcpv4TunnelLink 값에 사용 가능한 /31 서브넷에서 첫 번째 IP를 사용하는 경
우 FND는 포인트-투-포인트 서브넷에서 CGR의 터널 0과 HER의 해당 터널로 두 IP를 자동으로 프
로비저닝합니다.

dhcpV6TunnelLink - FND가 IPv6 GRE(Generic Routing Encapsulation) 터널을 위해 DHCP 서버에
대한 프록시 요청에서 사용하는 IPv6 주소입니다.이 랩 환경에서 CNR은 /127 접두사를 사용하여
주소를 임대하도록 구성됩니다.dhcpV4TunnelLink와 마찬가지로 FND는 GRE 터널을 구성할 때 포
인트 투 포인트 서브넷의 두 번째 IP를 HER에 자동으로 프로비저닝합니다.

dhcpV4LoopbackLink - CGR의 루프백 0 인터페이스를 구성할 때 FND가 프록시 요청에 사용할
IPv4 주소입니다.이 랩 환경에서 CNR의 해당 DHCP 풀이 /32 서브넷을 임대하도록 구성되었습니
다.

dhcpV6LoopbackLink - CGR의 루프백 0 인터페이스를 구성할 때 FND가 프록시 요청에서 DHCP
서버에 사용할 IPv6 주소입니다.이 랩 환경에서 해당 풀이 /128 서브넷을 임대하도록 구성되었습니
다.

헤드 엔드 라우터(HER)

헤드엔드 라우터를 처음 추가할 때 이 템플릿을 사용할 수 있습니다.

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

deviceType - ASR 또는 CSR을 도입할 때 이 필드에 'asr1000' 값을 사용해야 합니다.

status - 수락된 상태 값은 수신 거부, 다운 및 업입니다.새 가져오기인 경우 [Monthly] 명령을 사용합
니다.

lastheard - 새 디바이스인 경우 이 필드를 비워 둘 수 있습니다.

runningFirmwareVersion - 이 값은 비워 둘 수도 있지만 버전을 가져오려면 **show version** 출력의 맨

위 행에서 버전 번호를 사용합니다. 예를 들어 이 출력에서 '03.16.04b.S' 문자열을 사용해야 합니다.

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

netconfUsername - HER에 대한 전체 Netconf/SSH 액세스를 가지도록 구성된 사용자의 사용자 이름입니다.

netconfPassword - netconfUsername 필드에 지정된 사용자의 비밀번호입니다.

CGE(Connected Grid Endpoint)

DB에 새 메시 엔드포인트를 추가하는 것은 매우 간단합니다. 이 템플릿을 사용할 수 있습니다.

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

deviceType - 이 랩 환경에서 'cgmesh'는 스마트 측정기를 CGE로 추가하는 데 사용되었습니다.

lat - CGE를 설치할 GPS 위도 좌표입니다.

lng - GPS 경도입니다.

예

FAR 추가:

```
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, ajf1ea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl,
Administrator, ajf1ea30agbzhjelleabbjk3900=aazbzhje8903saadaio0eahgl, 198.51.100.1, 5, meshssid, 203.0.113.1, 2001:db8::1,
209.165.200.225, 2001:db8::90FE
```

그녀의 추가:

```
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 추가:

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

네트워크 다이어그램

참고:터널 프로비저닝은 FAR에서 CG-OS 또는 IOS를 실행하는지 여부에 따라 다르게 작동합니다. CG-OS:FAR과 HER에 새 IPSEC 터널 인터페이스가 구성됩니다. FND는 터널당 2개의 IP에 대한 프록시 요청을 DHCP 서버에 전송하고 해당 터널 인터페이스에서 2번째 IP를 자동으로 구성합니다. IOS:HER는 point-to-multipoint IPSEC 터널을 사용하는 Flex-VPN 템플릿을 사용합니다. 이 컨피그레이션에서는 FAR만 새 터널 인터페이스를 수신합니다.

이 토폴로지 다이어그램에서 'Tunnel x'는 HER의 상대 IPSEC 터널 인터페이스를, 'Tunnel Y'는 HER의 루프백 인터페이스에서 작성된 GRE 터널에 해당합니다. 또한 다이어그램의 IP 및 인터페이스는 .csv 템플릿의 컨피그레이션 예에 직접 해당합니다.

