Connected Grid Router 솔루션을 통한 제로 터치 구축의 구성 파일 조직

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[개요](#)
[ZTD 서비스](#)
[ZTD 단계](#)
[요약](#)
[구성 파일 조직](#)
[CGR 재프로비저닝](#)
[공장 재프로비저닝](#)
[터널 재프로비저닝](#)
[요약](#)
[FND를 사용하여 컨피그레이션 롤백 단계](#)
[관련 정보](#)

소개

이 문서에서는 ZTD(Zero Touch Deployment) 프로세스의 여러 부분에서 구성 파일을 생성하는 방법과 CGR(Connected Grid Router)의 특정 구성 파일로 롤백하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 CGR이 포함된 ZTD 구축을 기반으로 합니다.

CGR(CGR1120/CGR1240), FND(Field Network Director), TPS(Tunnel Provisioning Server) 및 RA(Registration Authority)를 구성 요소로 포함합니다.

CG-NMS는 이전 버전의 FND이므로 FND와 Cisco CG-NMS(Connected Grid Network Management System)를 상호 변경할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스에서 생성됩니다.이 문서에 사용된 모든 디바이스는 지워진(기본) 컨피그레이션으로 시작되었습니다.네트워크가 가동 중이면 명령의 잠재적인 영향을 파악하십시오.

개요

IoT(Internet of Things) 세계에서 ZTD 기능은 수백만 개의 디바이스의 컨피그레이션 구축을 지원하는 핵심 기능입니다.FND는 CGE(Connected Grid End) 포인트 및 CGR에 모두 ZTD를 지원합니다.

ZTD 서비스

ZTD for CGR은 다음과 같은 다양한 서비스를 제공합니다.

- 최소 및 일관된 컨피그레이션으로 CGR의 초기 구축(제조 컨피그레이션 또는 express-config 파일이라고 함) 최종 위치에 구축되면 이 컨피그레이션을 통해 CGR은 FND로 ZTD 프로세스를 시작하고 최종 컨피그레이션을 검색할 수 있습니다.
- CGR 구성 관리.완전히 구축되면 FND는 CGR 컨피그레이션의 모든 부분을 변경할 수 있는 기능을 통합합니다.
- 어떤 단계에서도 ZTD 프로세스가 실패한 경우 CGR 복구 메커니즘입니다.
- CGR 이미지 업그레이드.

ZTD 단계

1단계. 유틸리티 공개 키 인프라를 사용한 CGR 등록

2단계. CGR 터널 구성 프로비저닝

3단계. CGR 최종 등록(디바이스 컨피그레이션 프로비저닝)

FND에서 수행하는 폴링 또는 검색 메커니즘이 없습니다.각 단계는 CGR에 의해 트리거됩니다.1단계와 2단계 이후에 FND는 롤백 포인트를 생성하여 터널 프로비저닝 또는 디바이스 컨피그레이션 단계를 다시 거치기 전에 CGR을 신뢰할 수 있는 컨피그레이션으로 되돌릴 수 있습니다.

요약

이 표에는 다양한 서비스를 구현하는 데 사용할 ZTD의 단계가 요약되어 있습니다.

기능 또는 이벤트	SCEP(Simple Certificate Enrollment Protocol) 등록	터널 프로비저닝	디바이스 등록	설명
장치 구성 업데이트	아니요	아니요	예	CGR은 2단계 구성으로 롤백됩니다.
CGR 초기 구축	예	예	예	
CGR 예기치 않은 다시 로드	아니요	아니요	예	다시 로드하기 전에 CGR이 등록됨
펌웨어 업그레이드	아니요	예	예	CGR은 1단계 구성으로 롤백됩니다.
제조 구성 또는 공장 재프로비저닝	아니요	예	예	CGR은 1단계 구성으로 롤백됩니다.
터널 구성 재프로비저닝	아니요	예	예	CGR은 1단계 구성으로 롤백됩니다.

구성 파일 조직

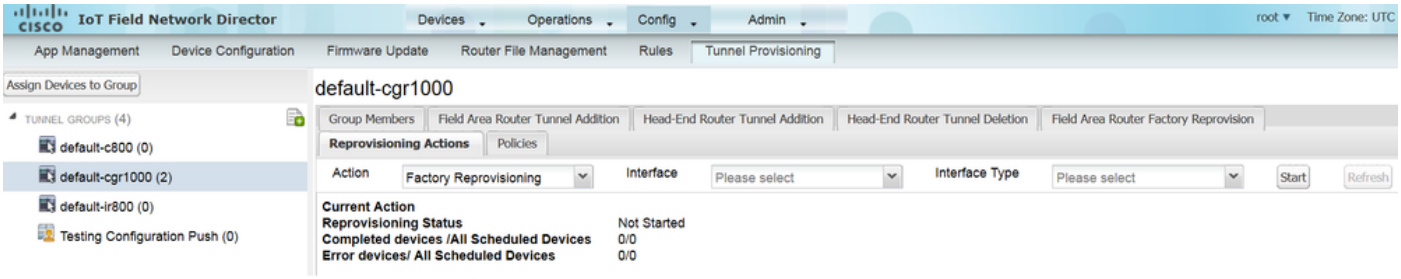
프로세스의 서로 다른 부분에서 구성 파일이 생성됩니다.CGR의 상태를 신뢰하지 않거나 CGR 컨피그레이션의 특정 부분을 업데이트하려는 경우 FND가 CGR 컨피그레이션을 롤백하는 데 사용할 수 있는 신뢰 지점을 생성하는 것이 좋습니다.이러한 컨피그레이션 파일은 CGR 플래시에 저장됩니다.

이름	정의	작성자	생성 시
cisco 기본 컨피그레이션	Cisco 제조 이외의 구성.	Cisco	Cisco 공장
제조 구성 (express-config)	SCEP 및 ZTD를 시작하기 위해 사전 컨피그레이션이 필요합니다. express-setup-config 파일은 제조 컨피그레이션이 적용되면 생성됩니다. = 유틸리티 PKI에 등록 후 manufacturing-config.	타사 또는 유틸리티	최종 구축 전
터널 구성 전 (ps-start-config)	유일한 차이점은 CGR https 서버가 LDevID라는 FAR 유틸리티 인증서를 사용하도록 재구성되었다는 것입니다.이 파일은 터널 컨피그레이션이 적용되기 전에 FND에 의해 생성됩니다.이 파일은 첫 번째로 신뢰할 수 있는 구성 파일이며 CGR이 나중에 터널 프로비저닝을 다시 거쳐야 하는 경우에 사용됩니다.	FND	터널 컨피그레이션이 적용되기 전
등록 전 구성 (골든 컨피그레이션)	= FND에서 푸시된 before-tunnel-config + 터널 구성 이 파일은 디바이스 컨피그레이션이 푸시되기 전에 FND에서 두 번째 신뢰 지점으로 생성합니다.디바이스 컨피그레이션을 변경해야 하는 경우 이 파일이 사용됩니다.	FND	필드의 CGR, 터널 프로비저닝 후
최종 구성	= before-tunnel-config + Tunnel config + Device Config = before-registration-config + 디바이스 컨피그레이션 이 컨피그레이션은 일반적으로 startup-config에 저장됩니다.	FND	필드의 CGR, 터널 프로비저닝 후

CGR 재프로비저닝

CGR에 대한 재프로비저닝은 특정 컨피그레이션 파일에 대한 롤백 컨피그레이션에 수행됩니다.

IoT FND에서 Tunnel Provisioning(터널 프로비저닝) 페이지의 Reprovisioning Actions(재프로비저닝 작업) 창에서 이러한 재프로비저닝 작업을 수행합니다(Config > Tunnel Provisioning).



공장 재프로비저닝

이를 제조 컨피그레이션 재프로비저닝이라고도 합니다.

IoT FND의 공장 재프로비저닝 기능을 사용하여 CGR(express-setup-config)의 공장 구성을 변경합니다.

터널 재프로비저닝

이 기능을 사용하면 Utility NOC에서 터널 프로비저닝 단계 중에 푸시되는 터널 컨피그레이션의 모든 부분을 변경할 수 있습니다.

IoT FND는 CGR의 컨피그레이션을 ps-start-config 템플릿 파일에 정의된 컨피그레이션으로 롤백합니다.

요약

요약하자면, CGR의 최종 구성은 각각 구체적인 목표를 가진 세 가지 블록을 기반으로 구축됩니다.

구성 블록	목표	주요 기능	구성 블록을 성하는 데 되는 CG-N 템플릿
제조 구성 파일	ZTD의 시작점	- 백홀 네트워크에 연결 - SCEP 등록 트리거 - RA에 연결할 수 있어야 함	제조 또는 리티 사양
before-tunnel-config 파일	새 터널 컨피그레이션을 프로비저닝하기 위한 롤백 지점 제공	- 백홀 네트워크에 연결 - TPS 서버에 연결할 수 있어야 함	RA에서 SC 추가
등록 전 구성 파일	새 디바이스 컨피그레이션을 프로비저닝하기 위한 롤백 지점 제공	- FND로 보안 경로 구축 - 백홀 네트워크로의 트래픽 유출 방지 - 터널 내부에 예상 라우팅 경로 제공	FAR 터널
device-config 템플릿 (이 컨피그레이션이 적용되면 생성된 특정 파일이 없음)	FAR 구성 완료	- 메시 인터페이스 구성 - 구성 강화 - 터널 프로비저닝 단계에서 필요하지 않은 나머지 기능일부는 FND로 하드코딩되어 템플릿 위에 추가됩니다.	FAR 장치 템플릿

FND를 사용하여 컨피그레이션 롤백 단계

FND 또는 CG-NMS에는 라우터의 특정 컨피그레이션 파일로 롤백할 수 있는 기능이 있습니다.이 기능은 **config replace** 명령을 실행합니다.

FND는 CGR을 before-tunnel-config 또는 before-registration-config 컨피그레이션 파일로 롤백할 때마다 이 기능을 활용하지만, 경우에 따라 실패할 수 있으므로 이러한 시나리오에서 복구하기 위해 일부 논리가 필요합니다.이러한 로직은 실제로 no-config-replace.tcl이라는 전용 TCL 스크립트를 통해 구현됩니다(Cisco IOS® 이미지에 포함됨).FND는 CGR을 특정 구성 파일로 롤백해야 할 때마다 해당 스크립트를 사용합니다.스크립트에는 이러한 입력이 필요합니다.

입력	정의	가치
구성 파일	롤백할 구성 파일	flash:/before tunnel-config 또는 flash:/before-registration-config
프로필 이름	컨피그레이션 교체 후 활성화할 CGNA 프로파일	cg-nms-tunnel 또는 cg-nms-register
바꾸기 플래그	True는 구성을 교체하려고 시도함을 의미합니다.	1(TRUE)
이름 바꾸기 플래그	True는 컨피그레이션을 바꾸지 않고 파일의 이름만 바꾸는 것을 의미합니다.	0(거짓)

FND는 이러한 명령을 전송하여 CGR에서 이 스크립트를 한 번만 실행합니다.이 예에서 FND는 디바이스 등록 전에 CGR을 컨피그레이션으로 롤백하려고 합니다.

- cgna exec 프로필
- add-command 이벤트 관리자가 no_config_replace.tcl flash:/before-registration-config cg-nms-register 1 0 실행
- 간격 1
- 활성

관련 정보

- **제로 터치 구축에 대한 개괄적인 설명**
- **기술 지원 및 문서 – Cisco Systems**