Configuration Files Organization in Zero Touch Deployment with Connected Grid Router Solution

Contents

Introduction
Prerequisites
Requirements
Components Used
Overview
ZTD Services
ZTD Phases
Summary
Configuration Files Organization
Reprovisioning CGRs
Factory Reprovisioning
Tunnel Reprovisioning
Summary
Steps Behind the Configuration Roll Back using FND
Related Information

Introduction

This document describes how configuration files are created at different parts of the Zero Touch Deployment (ZTD) process and steps to roll back to any specific configuration file on the Connected Grid Router (CGR).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on ZTD deployment with CGRs.

It includes CGR (CGR1120/CGR1240), Field Network Director (FND), Tunnel Provisioning Server (TPS), and Registration Authority (RA) as components.

FND and Cisco Connected Grid Network Management System (CG-NMS) are interchangeable as CG-NMS is an earlier version of FND.

The information in this document is created from the devices in a specific lab environment. All devices used in this document started with a cleared (default) configuration. If your network is live, understand the potential impact of commands.

Overview

In the Internet of Things (IoT) world, ZTD capability is a key to support the configuration deployment of millions of devices. FND supports ZTD for both Connected Grid End (CGE) points and CGRs.

ZTD Services

ZTD for CGR provides a wide range of services, which include:

- Initial deployment of CGR with a minimum and consistent configuration (called manufacturing configuration or express-config file). Once deployed to its final location, this configuration will allow the CGR to initiate the ZTD process with FND and retrieve its final configuration.
- CGR configuration management. Once fully deployed, FND integrates the capability to change any part of the CGR configuration.
- CGR recovery mechanism if ZTD process failed at any stage.
- CGR image upgrade.

ZTD Phases

Step 1. CGR enrollment with the utility public key infrastructure

Step 2. CGR tunnel configuration provisioning

Step 3. CGR final registration (device configuration provisioning)

There is no polling or discovery mechanism done by FND. Each phase is triggered by the CGR. After phase 1 and 2, FND creates a rollback point so it can bring the CGR back to a trusted configuration before going through either the tunnel provisioning or device configuration phase again.

Summary

The table summarizes which phase of ZTD will be used to implement different services:

Functionality or Event	SCEP (Simple Certificate Enrollment Protocol) Enrollment	Tunnel Provisioning	Device Registration	Comments
Device configuration update	No	No	Yes	CGR will roll back to phase 2 configuration
CGR initial deployment	Yes	Yes	Yes	
CGR unexpected reload	No	No	Yes	The CGR was registered before the reload

Firmware upgrade	No	Yes	Yes	CGR will roll back to phase 1 configuration
Manufacturing configuration or factory reprovisioning	No	Yes	Yes	CGR will roll back to phase 1 configuration
Tunnel configuration reprovisioning	No	Yes	Yes	CGR will roll back to phase 1 configuration

Configuration Files Organization

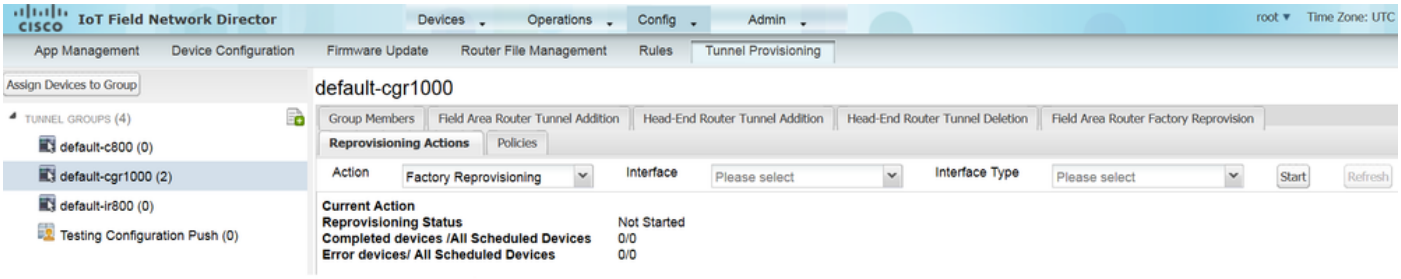
Different configuration files are created at different parts of the process. The idea is to create trust points which FND can use to roll back CGR configuration, in case it does not trust the state of the CGR or wants to update a specific part of the CGR configuration. These configuration files are store in the CGR flash.

Name	Definition	Creator	When created
cisco default configuration	Configuration out of Cisco manufacturing.	Cisco	Cisco Factory
manufacturing-config (express-config)	Pre-configuration required to initiate SCEP and ZTD. express-setup-config file is created once the manufacturing config as been applied. = manufacturing-config after enrollment with Utility PKI.	Third-party or Utility	Before final deployment
before-tunnel-config (ps-start-config)	The only difference is now the CGR https server has been reconfigured to use the FAR Utility certificate called LDevID. This file is created by FND before the tunnel configuration is applied. This is the first trusted configuration file and is used in case CGR must go through the tunnel provisioning again in the future. = before-tunnel-config + Tunnel configuration pushed by FND.	FND	Before tunnel configuration is applied
before-registration-config (golden config)	This file is created by FND as the second trust point before the device configuration is pushed. This file will be used if the device configuration must be changed. = before-tunnel-config + Tunnel config + Device Config.	FND	CGR in the field, post tunnel provisioning
Final Config	= before-registration-config + Device Config. This configuration is saved the usual way, that is, to startup-config	FND	CGR in the field, post tunnel provisioning

Reprovisioning CGRs

Reprovisioning on CGR is done to the rollback configuration to certain configuration files.

In IoT FND, perform these reprovisioning actions in the Reprovisioning Actions pane of the Tunnel Provisioning page (Config > Tunnel Provisioning).



Factory Reprovisioning

This is also called Manufacturing configuration reprovisioning.

Use the Factory Reprovisioning feature in IoT FND to change the factory configuration of CGRs (express-setup-config).

Tunnel Reprovisioning

This function allows the Utility NOC to change any part of the tunnel configuration that is being pushed during the tunnel provisioning phase.

IoT FND rolls back the configuration of the CGR to that defined in the ps-start-config template file.

Summary

To summarize, the CGR final configuration is built based on three different blocks, each one with specific goals.

Config block	Objective	Main features	CG-NMS template used to generate the config block
manufacturing-config file	Starting point for ZTD	- Connection to backhaul network - Trigger SCEP enrollment - Must be able to reach RA	Manufacture or utility specifications
before-tunnel-config file	Provide a rollback point to provision new tunnel configuration	- Connection to backhaul network - Must be able to reach TPS servers	SCEP addition from RA
before-registration-config file	Provide a rollback point to provision new device configuration	- Establish a secure path with FND - Avoid traffic leaks to the backhaul network - Provide expected routing path inside the tunnel - Mesh interface configuration - Config hardening	FAR Tunnel addition
device-config template (no specific file created once this configuration has been applied)	Finalize FAR configuration	- Any remaining features not required during the tunnel provisioning phase. Some of them are hardcoded into FND and added on top of the template.	FAR Device configuration template

Steps Behind the Configuration Roll Back using FND

FND or CG-NMS has the capability to roll back to a specific configuration file on the router. This capability is based on the **config replace** command.

FND leverages this capability each time it rolls back CGR to either its before-tunnel-config or before-registration-config configuration files, but because it might fail sometimes, some logic is required to recover from such a scenario. Such logic is actually implemented via a dedicated TCL script called no-config-replace.tcl (also embedded in the Cisco IOS® image). FND will use that script each time it needs to roll back CGR to a specific configuration file. The script needs these inputs.

Inputs	Definition	Value
configFile	Configuration file to rollback to	flash:/before-tunnel-config or flash:/before registration-config
profileName	CGNA profile to activate after the config replace	cg-nms-tunnel or cg-nms-register
replaceFlag	True means try to replace the configuration	1 (TRUE)
renameFlag	True means just rename the file without replacing the configuration	0 (FALSE)

FND sends these commands to execute this script on the CGR only once. In this example, FND wants to roll back CGR to its configuration before device registration:

- cgna exec-profile
- add-command event manager run no_config_replace.tcl flash:/before-registration-config cg-nms-register 1 0
- interval 1
- active

Related Information

- **High-Level Description of Zero Touch Deployment**
- **Technical Support & Documentation - Cisco Systems**