Troubleshooting Steps for ZTD in FAN Solution

Contents

Introduction

This document describes how to troubleshoot common problem while Zero Touch Deployment (ZTD) in Field Area Network (FAN) solution that consists of Connected Grid Router (CGR) and Field Network Director (FND).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on ZTD deployment with CGR.
It includes CGR (CGR1120/CGR1240), FND, Tunnel Provisioning Server (TPS), Registration Authority (RA), Certificate Authority (CA), Domain Name Server (DNS) 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 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.

Troubleshooting Steps as per ZTD Process in FAN Solutions

Field Area Router (FAR) Manufacturing Configuration

Everything starts from this manufacturing configuration so this step is key for a successful deployment.

This configuration will trigger first two phases: Simple Certificate Enrollment Protocol (SCEP) and Tunnel provisioning.

A successful test is a FAR deployed with its manufacturing configuration and able to go through the ZTD process to finally register with CG-NMS without any intervention.

Usual suspects:

- Credentials between FAR and CG-NMS don't match.
- Connected Grid NMS Agent (CGNA) URL for tunnel provisioning is incorrect (make sure it's https and not http).
- Domain Name Serer (DNS) misconfigured to resolve TPS fully qualified domain name (FQDN).

If at the time of troubleshoot of those two phases, the manufacturing configuration must be updated, this process should be followed:

- Block FAR connectivity with the HE (physically or logically)
- Rollback the FAR to its express-setup-config
- Apply the changes
- Create a new express-setup-config file
- Save the config in nvram
- Restore connectivity so the FAR can trigger the ZTD process again

SCEP Enrollment

The goals of this phase is to authorize FAR to receive its local device identity (LDevID) certificate from the RSA Public Key Infrastructure (PKI) and to get certificate after authorization. This step is a pre-requisite for the next one where FAR needs its certificate to communicate with the TPS and establish its IPSec tunnel with the HER.

The components involved are: FAR, RA, SCEP server, Radius server and its DB.

A Tool Command Language (TCL) script called tm_ztd_scep.tcl will automatically initiate SCEP process and keeps trying until the enrollment is successful.

Steps	Components involved	Troubleshooting Guidelines	Useful Commands
event manager starts tm_ztd_scep.tcl script	FAR	• Verify event manager configuration • Verify environment	deb event manager tcl commands wi highlight all the CLI commands applied by the script

		variables configuration used by the script	
RA FQDN resolution	FAR, DNS	• Check connectivity between FAR and DNS • Check the DNS record to resolve this name • Check FAR enrollment profile configuration	ping the RA FQDN from the FAR
FAR sends SCEP request to the RA	FAR, RA	• Check connectivity between RA and FAR • Check RA configuration. PKI server must be UP	debug crypto pki transactions debug crypto provisioning
PKI authorization	RA, RADIUS	• Check connectivity between RA and RADIUS server • Check RA PKI authorization configuration • Check Radius server configuration	debug crypto pki scep debug crypto pki transactions debug crypto pki server debug crypto provisioning
FAR certificate issuing	RA, Issuer CA	• Check connectivity between RA and Issuer CA	RA: debug crypto pki If issuer CA is an IOS-CA then same debug command can be used as wel

Tunnel Provisioning

At the time of this phase, the FAR will communicate with the TPS (acts as a proxy on-behalf of CG-NMS) to get its tunnel configuration from CG-NMS. This phase is initiated by the SCEP tcl script once the enrollment is done by activating the CGNA profile.

Components involved are: FAR, DNS, TPS, CG-NMS.

Steps	Componenets Involved	Troubleshooting Guidlines	Useful Commands
TCL script to activate the CGNA profile	FAR	Verify the right profile is configured for ZTD_SCEP_CGNA_Profile environment variable	"show cgna profile-all" to verify the profile is active
CGNA profile resolve TPS FQDN	FAR, DNS	• Verify connectivity between DNS and FAR • Check the DNS record to resolve this name • Check TPS FQDN configuration in the CGNA URL	FAR: ping TPS FQ*D*N
CGNA profile establish HTTPS	FAR, TPS	• Check TPS service is running • Check TPS keystore file	TPS log file is located at : /opt/cgms-tpsproxy/log/tpsproxy.log

session with TPS		• Check TPS receives TPS packets from the CGR • Check CGNA profile configuration	
TPS forward tunnel request to CG-NMS	TPS, CG-NMS	• Verify TPS and CG-NMS properties • Verify connectivity between TPS and CG-NMS • Check TPS and CG-NMS logs	FND log file is located at :cd /opt/cgms/server/cgms/log

The FAR Contacts TPS with a Tunnel-Provisioning Request with HTTPS on Port 9120

```
4351: iok-tps: Jul 13 2016 14:46:12.328 +0000: %CGMS-6-UNSPECIFIED: %[ch=1c3d5104]
[eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Inbound proxy request from [192.168.1.1] with client certificate subject
[SERIALNUMBER=PID:IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]

4352: iok-tps: Jul 13 2016 14:46:12.382 +0000: %CGMS-6-UNSPECIFIED: %[ch=1c3d5104]
[eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Completed inbound proxy request from [192.168.1.1] with client certificate subject
[SERIALNUMBER=PID:IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]
```

Logs after Tunnel is this Established Between HER and FAR and Hereafter, FAR can Communicate Directly with the HER

```
4351: iok-tps: Jul 13 2016 14:46:12.328 +0000: %CGMS-6-UNSPECIFIED: %[ch=1c3d5104]
[eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Inbound proxy request from [192.168.1.1] with client certificate subject [SERIALNUMBER=PID:

IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]

4352: iok-tps: Jul 13 2016 14:46:12.382 +0000: %CGMS-6-UNSPECIFIED:
%[ch=1c3d5104][eid=IR809G-LTE-NA-K9+JMX2007X00Z][ip=192.168.1.1][sev=INFO][tid=qtp756319399-23]:
Completed inbound proxy request from [192.168.1.1] with client certificate subject [SERIALN

UMBER=PID:IR809G-LTE-NA-K9 SN:JMX2007X00Z, CN=IR800_JMX2007X00Z.cisco.com]

4353: iok-tps: Jul 13 2016 14:46:12.425 +0000: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyOutboundHandler][ip=192.168.1.1][sev=INFO][tid=qtp687776794-16]:
Outbound proxy request from [192.168.1.2] to [192.168.1.1]

4354: iok-tps: Jul 13 2016 14:46:14.176 +0000: %CGMS-6-UNSPECIFIED:
%[ch=TpsProxyOutboundHandler][ip=10.10.10.61][sev=INFO][tid=qtp687776794-16]:
Outbound proxy request from [192.168.1.2] to [192.168.1.1
```

Device Registration

Step 1. Get ready for Device Registration

CG-NMS will push the configuration of the CGNA profile cg-nms-register. Extra commands are

added so the profile is executed right away instead of waiting for the interval timer to expire.

CG-NMS will deactivate CGNA profile cg-nms-tunnel Tunnel provisioning is considered complete at this point.

Step 2. CG-NMS Receives a Device Registration Request

- Verify FAR is provisioned in its DB
- Verify if the cg-nms.odm and cg-nms-scripts.tcl files are either missing from the FAR flash or must be updated to a new version. CG-NMS will automatically upload them if required.
- Capture FAR current configuration
- Process all the show commands outputs included in the request. Ask for the missing ones if required. The list may vary based on the FAR hardware configuration.

For details to implement Zero Touch Deployment within your network, contact your Cisco partner or Cisco system engineer.

For express-setup-config on router, contact your partner or Cisco system engineer.

Related Information

- http://www.cisco.com/c/en/us/td/docs/routers/connectedgrid/cgr1000/1_0/software/configuration/guide/security/security_Book/sec_ztdv4_cgr1000.html
- **Technical Support & Documentation - Cisco Systems**