Troubleshoot CSMP Registration on Field Area Networks

Contents

Introduction

This document describes the details of the CSMP protocol along with the steps to troubleshoot registration issues.

Components Used

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, ensure that you understand the potential impact of any command.

CoAP Simple Management Protocol (CSMP)

CoAP Simple Management Protocol (CSMP) is a remote network management protocol intended for embedded networking devices running within large-scale bandwidth-constrained networks.

CSMP is built on top of the Constrained Application Protocol (CoAP). CoAP is a UDP-based binary protocol that is designed to provide HTTP-like semantics (GET/POST of resources with URLs) with minimal header overhead in a constrained, multicast-friendly environment.

CSMP defines a small set of CoAP resources identified by specific URL paths that represent endpoints for data exchange.

The NMS and the end devices communicate with each other directly over CoAP, with no intervening proxies or gateways.

A management agent running on the embedded device uses CoAP as a client to communicate directly with a network management application.

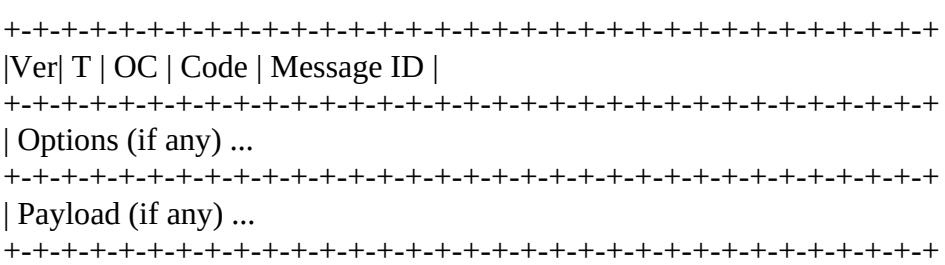
The CSMP client in the embedded device sends requests to particular CoAP resources provided by a CSMP server in the application.

With the FAN solution, the network management application is the Field Network Director (FND).

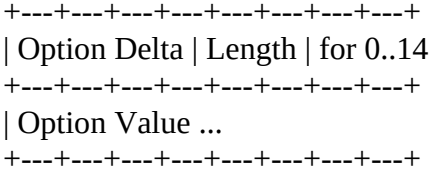
In addition, the management agent running on the embedded device uses CoAP as a server to accept requests from a FND running in a remote location.

The CSMP client in the FND sends requests to particular CoAP resources provided by a CSMP server in the embedded devices.

For reference, a CoAP message has this structure:



The Options are CoAP-specific TLVs that have this structure:



The CoAP HTTP-like method code or response code is contained in the “Code” field. The set of CoAP options includes the resource URL (split into host, port, path, and query portions).

Use of CSMP in Field Area Networks

FND manages the Mesh or Meter Endpoints, be it a gas meter, water meter, or power meter. FND communicates with meter endpoints using CSMP protocol as mentioned above.

CSMP messages are encrypted. HSM or SSM stores the keys used for encrypting the CSMP messages.

SSM (Software Security Module) or HSM (Hardware Security Module) also stores the CSMP certificate needed for communication.

Troubleshoot CSMP

Signature Errors

Server.log points to meters having signature errors.

%IOTFND-6-
UNSPECIFIED: %[ch=HandleMessage][eid=0007810800CA759B][sev=INFO][tid=CoAP Conformant-3]:
Running firmware group on the device is id=243 but must be id=317(Invalid CSMP Signature).
Sending GroupAssign.

Validate meter hardware/firmware info

For example, the resulting output for meter EID "fd00:abd:51:c000:207:8108:e7:6fda"

[root@lcdcfndappp01 bin]# /opt/cgms-tools/bin/csmp-request -r [fd00:abd:51:c000:207:8108:e7:6fda] 75

[75/FirmwareImageInfo]: {"index": 1,"fileHash":
"\x25\x9c\xcf\x36\xf9\x19\x8d\x4e\x13\xaa\x7f\x83\xa3\x94\x4a\xee\xe8\xc1\xc6\xc1\x0d\x7e\x11\xd2\xc0\x2d\x4
"cg-mesh-node-5.6.2 1","version": "5.6.21","fileSize": 305408,"isDefault": false,"isRunning":
true,"hwInfo": {"hwId": "RFLAN/3.60/3.80"}} [75/FirmwareImageInfo]: {"index": 2,"fileHash":
"\x25\x9c\xcf\x36\xf9\x19\x8d\x4e\x13\xaa\x7f\x83\xa3\x94\x4a\xee\xe8\xc1\xc6\xc1\x0d\x7e\x11\xd2\xc0\x2d\x4
"cg-mesh-node-5.6.2 1","version": "5.6.21","fileSize": 305408,"blockSize": 650,"isDefault":
false,"isRunning": false,"hwInfo": {"hwId": "RFLAN/3.60/3.80"}} [75/FirmwareImageInfo]: {"index":
3,"fileHash":
"\x25\x9c\xcf\x36\xf9\x19\x8d\x4e\x13\xaa\x7f\x83\xa3\x94\x4a\xee\xe8\xc1\xc6\xc1\x0d\x7e\x11\xd2\xc0\x2d\x4
"cg-mesh-node-5.6.2 1","version": "5.6.21","fileSize": 305408,"blockSize": 650,"isDefault":
true,"isRunning": false,"hwInfo": {"hwId": "RFLAN/3.60/3.80"}} [75/FirmwareImageInfo]: {"index":
4,"fileHash":
"\x3d\x03\xe4\x6c\xa7\x10\x3c\x75\x21\xf2\x41\x8f\x88\x4f\x56\x0e\x46\x7a\x06\xfc\x78\x24\x69\xeb\x0e\x8b\xf
"cg-mesh-itron30-sl -REL-5.2.25","version": "5.2.25","fileSize": 40960} [root@lcdcfndappp01 bin]#

Validate meter certificate

Using TLV 43 code for CGMSSTATUS and verifying the field NMSCertValid.

The NMSCertValid field can identify whether the FND cert is valid or not.

If it is a hardware corruption, all parameters read from the flash are NULL, for example, the SSID field. Hence if the SSID name is present, it is not hardware corruption.

If the SSID name is correct and the NMSCertValid field is reported as false, it is possibly an issue with the cert file copied on the meter.

Validate the XML configuration file on the meter

<DevCfgSchema> , if the meter is left in Demo mode , contact meter vendor for support.

<DemoMode_Cfg> <DemoModeEnable>true</DemoModeEnable> </DemoMode_Cfg>

FND Clock synchronization with NTP

This error is seen :

%IOTFND-7-UNSPECIFIED: %[ch=EventProducer][sev=DEBUG][tid=CoAP-7]: Event Object which is send = EventObject [netElementId=1149847, eventTime=1622146931202, eventSeverity=0,

eventSource=cgmesh, eventTypeName=signatureFailure, eventDisplayName=Invalid CSMP Signature, eventTypeId=1085, eventMessage=Verify certificate setup. Also verify that device and IoT-FND are time synchronized., lat=1000.0, lng=1000.0, geoHash=null, eid=F433280000005DE8, issueId=0, eventSev=CRITICAL, moduleId=null, domainName=root]

Symptom: In FND, the associated device goes into a 'registering' state instead of showing UP.

1. Check if the FND and NTP clocks are in sync,
2. Check if the FND and Endpoints clocks are in sync.

Meters are reported down in FND

If the ME/meters are reported as DOWN in FND, check if there is a firewall blocking incoming CSMP messages.

To fix the issue on the FND server, disable the firewalld service:

```
[root@iot-fnd ~]# systemctl list-unit-files | grep firewalld
firewalld.service disabled
```

In case it is enabled, you can disable it using the command below:

```
[root@iot-fnd ~]# systemctl disable firewalld
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

Load-Balancing Policy and CSMP messages

In a Load-balancing cluster environment, check the communication between the source and destination addresses, and the ports between meter endpoints (ME) and FND.

Verify CSMP statistics with the getStats.sh output. If one of the application servers has a much higher CSMP processing rate than the others, then load balancing is probably configured incorrectly. Furthermore, when you analyze the output, if you see your queue sizes increase it confirms that there is a bottleneck process somewhere.

CSMP call flow example:

CSMP Request to the meter during periodic metric registration.

Meter to FND

Src ip Meter IPv6 address

Destination IPv6 FND Ip address

Source UDP port 61624

DST UDP port 61624

Manual Metric refresh for a meter from FND

Source ip FND ipv6 address

Destination IP Meter IPv6 address

Source UDP port any example: 9251

DST UDP port 61624

Meter response during manual metric refresh request (from FND)

Source ip Meter IPv6 address

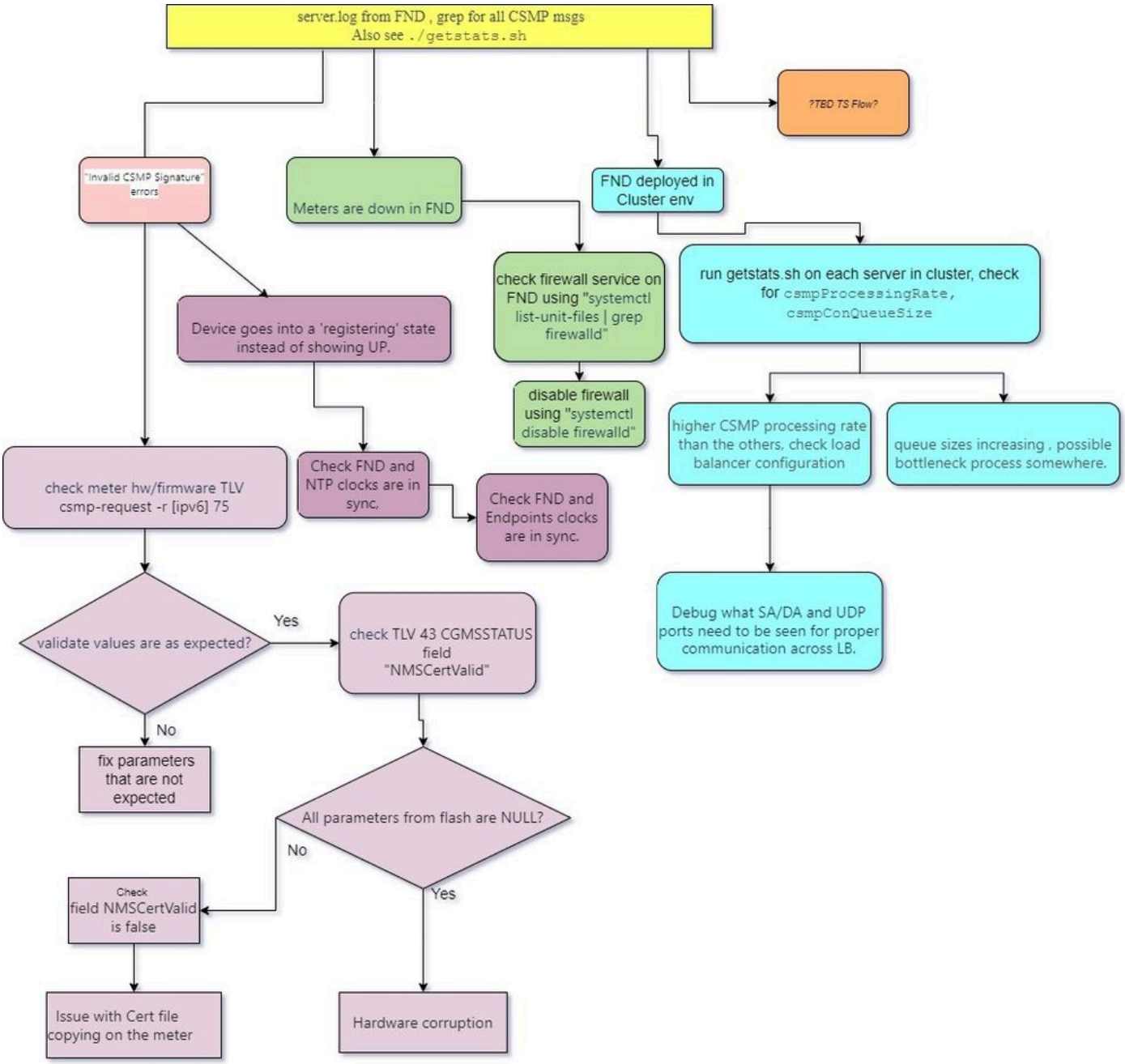
Destination IP FND ipv6 address

Source UDP port 61624

DST UDP port which it sent on example: 9251

If the ME is sending a reply to the Load balancer IP (VIP) rather than the requested IP address on which it received the CSMP "request" on, " it needs to be properly routed using additional configuration.

Flowchart for CSMP Registration


server.log from FND , grep for all CSMP msgs
Also see ./getstats.sh
?TBD TS Flow?
"Invalid CSMP Signature" errors
Meters are down in FND
FND deployed in Cluster env
check firewall service on FND using "systemctl list-unit-files | grep firewalld"
run getstats.sh on each server in cluster, check for csmpProcessingRate, csmpConQueueSize
Device goes into a 'registering' state instead of showing UP.
disable firewall using "systemctl disable firewalld"
higher CSMP processing rate than the others, check load balancer configuration
queue sizes increasing , possible bottleneck process somewhere.
check meter hw/firmware TLV csmp-request -r [ipv6] 75
Check FND and NTP clocks are in sync.
Check FND and Endpoints clocks are in sync.
Debug what SA/DA and UDP ports need to be seen for proper communication across LB.
validate values are as expected?
Yes
check TLV 43 CGMSSTATUS field "NMSCertValid"
No
fix parameters that are not expected
All parameters from flash are NULL?
No
Yes
Check field NMSCertValid is false
Issue with Cert file copying on the meter
Hardware corruption