

Solución de problemas de registro CSMP en redes de área de campo

Contenido

[Introducción](#)

[Componentes Utilizados](#)

[Protocolo de administración simple \(CSMP\) CoAP](#)

[Uso de CSMP en redes de área de campo](#)

[Solucionar problemas de CSMP](#)

[Errores de firma](#)

[Validar información de hardware/firmware del medidor](#)

[Validar certificado de medidor](#)

[Validar el archivo de configuración XML en el medidor](#)

[Sincronización del reloj FND con NTP](#)

[Se informa de que los medidores han caído en FND](#)

[Mensajes de Load-BalancingPolicy y CSMP](#)

[Ejemplo de flujo de llamadas CSMP:](#)

[Medidor a FND](#)

[Actualización manual de la métrica para un medidor desde FND](#)

[Respuesta del medidor durante la solicitud de actualización de métrica manual \(desde FND\)](#)

[Diagrama de flujo para el registro CSMP](#)

Introducción

Este documento describe los detalles del protocolo CSMP junto con los pasos para resolver problemas de registro.

Componentes Utilizados

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Protocolo de administración simple (CSMP) CoAP

CoAP Simple Management Protocol (CSMP) es un protocolo de administración de red remota diseñado para dispositivos de red integrados que se ejecutan dentro de redes con limitaciones de ancho de banda a gran escala.

CSMP se crea sobre el protocolo de aplicación restringida (CoAP). CoAP es un protocolo binario

basado en UDP que está diseñado para proporcionar semántica similar a HTTP (GET/POST de recursos con URL) con una sobrecarga de encabezado mínima en un entorno restringido y compatible con multidifusión.

CSMP define un pequeño conjunto de recursos CoAP identificados por rutas URL específicas que representan extremos para el intercambio de datos.

El NMS y los dispositivos finales se comunican entre sí directamente a través de CoAP, sin proxies ni gateways intervinientes.

Un agente de administración que se ejecuta en el dispositivo incrustado utiliza CoAP como cliente para comunicarse directamente con una aplicación de administración de red.

El cliente CSMP del dispositivo incrustado envía solicitudes a recursos CoAP concretos proporcionados por un servidor CSMP en la aplicación.

Con la solución FAN, la aplicación de gestión de red es Field Network Director (FND).

Además, el agente de administración que se ejecuta en el dispositivo incrustado utiliza CoAP como servidor para aceptar solicitudes de un FND que se ejecuta en una ubicación remota.

El cliente CSMP en FND envía solicitudes a recursos CoAP particulares proporcionados por un servidor CSMP en los dispositivos embebidos.

Como referencia, un mensaje CoAP tiene esta estructura:

```
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|Ver| T | OC | Code | ID del mensaje |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| Opciones (si las hubiera)...
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| Carga útil (si la hay) ...
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
```

Las opciones son TLV específicos de CoAP que tienen esta estructura:

```
+--+--+--+--+--+--+--+--+--+--+--+
| Delta de opción | Longitud | para 0.14
+--+--+--+--+--+--+--+--+--+--+--+
| Valor de opción...
+--+--+--+--+--+--+--+--+--+--+--+
```

El código de método o el código de respuesta del tipo HTTP de CoAP se incluye en el campo "Código". El conjunto de opciones CoAP incluye la URL del recurso (dividida en partes de host, puerto, ruta y consulta).

Uso de CSMP en redes de área de campo

FND gestiona los terminales de malla o medidor, ya sea un medidor de gas, de agua o de energía. FND se comunica con los terminales del medidor mediante el protocolo CSMP, como se mencionó anteriormente.

Los mensajes CSMP están cifrados. HSM o SSM almacena las claves utilizadas para cifrar los mensajes CSMP.

SSM (módulo de seguridad de software) o HSM (módulo de seguridad de hardware) también almacena el certificado CSMP necesario para la comunicación.

Solucionar problemas de CSMP

Errores de firma

Server.log apunta a medidores que tienen errores de firma.

```
%IOTFND-6-UNSPECIFIED:
```

```
 %[ch=HandleMessage][eid=0007810800CA759B][sev=INFO][tid=CoAP Conformant-3]: La ejecución del grupo de firmware en el dispositivo es id=243, pero debe ser id=317 (firma CSMP no válida). Enviando asignación de grupo.
```

Validar información de hardware/firmware del medidor

Por ejemplo, la salida resultante para el medidor EID "fd00:abd:51:c000:207:8108:e7:6fda"

```
[root@lcdcfdndapp01 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" "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" "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" "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" "cg-mesh-itron30-sl -REL-5.2.25","version": "5.2.25","fileSize": 40960} [root@lcdcfdndapp01 bin]#
```

Validar certificado de medidor

Uso del código TLV 43 para CGMSSTATUS y verificación del campo NMSCertValid.

El campo NMSCertValid puede identificar si el certificado FND es válido o no.

Si es un daño de hardware, todos los parámetros leídos desde la memoria flash son NULL, por ejemplo, el campo SSID. Por lo tanto, si el nombre de SSID está presente, no está dañado por el hardware.

Si el nombre de SSID es correcto y el campo NMSCertValid aparece como false, es posible que se trate de un problema con el archivo de certificado copiado en el medidor.

Validar el archivo de configuración XML en el medidor

<DevCfgSchema> , si el medidor se deja en modo de demostración , comuníquese con el proveedor del medidor para obtener soporte.

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

Sincronización del reloj FND con NTP

Este error se ve :

[%IOTFND-7-UNSPECIFIED](#): %[ch=EventProducer][sev=DEBUG][tid=CoAP-7]: Objeto de evento que se envía = EventObject [netElementId=1149847, eventTime=1622146931202, eventSeverity=0, eventSource=cgmesh, eventTypeName=signatureFailure, eventDisplayName=Invalid CSMP Signature, eventTypeId=1085, eventMessage=certificate setup. Compruebe también que el dispositivo y IoT-FND están sincronizados por hora., lat=1000.0, lng=1000.0, geoHash=null, eid=F433280000005DE8, issued=0, eventSev=CRITICAL, moduleId=null, domainName=root]

Síntoma: en FND, el dispositivo asociado pasa a un estado de "registro" en lugar de aparecer UP.

1. Compruebe si los relojes FND y NTP están sincronizados,
2. Compruebe si los relojes FND y Endpoints están sincronizados.

Se informa de que los medidores han caído en FND

Si se informa que los medidores de ME están INACTIVOS en FND, verifique si hay un firewall que bloquee los mensajes CSMP entrantes.

Para solucionar el problema en el servidor FND, desactive el servicio de firewall:

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

En caso de que esté habilitada, puede inhabilitarla mediante el siguiente comando:

```
[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.
```

Directiva de equilibrio de carga y mensajes CSMP

En un entorno de clúster de equilibrio de carga, compruebe la comunicación entre las direcciones de origen y destino, y los puertos entre los extremos de medidor (ME) y FND.

Verifique las estadísticas de CSMP con el resultado `getStats.sh`. Si uno de los servidores de aplicaciones tiene una velocidad de procesamiento de CSMP mucho más alta que los demás, es probable que el equilibrio de carga esté configurado incorrectamente. Además, cuando analiza el resultado, si observa que el tamaño de la cola aumenta, confirma que hay un proceso de cuello de botella en algún lugar.

Ejemplo de flujo de llamadas CSMP:

Solicitud CSMP al medidor durante el registro periódico de métricas.

Medidor a FND

Dirección IPv6 del medidor de IP de origen

Dirección IP FND IP Address de destino IPv6

Puerto UDP de origen 61624

Puerto UDP DST 61624

Actualización manual de la métrica para un medidor desde FND

Dirección IP FND ipv6 de origen

Dirección IPv6 del medidor IP de destino

Puerto UDP de origen en cualquier ejemplo: 9251

Puerto UDP DST 61624

Respuesta del medidor durante la solicitud de actualización de métrica manual (desde FND)

Dirección IPv6 del medidor IP de origen

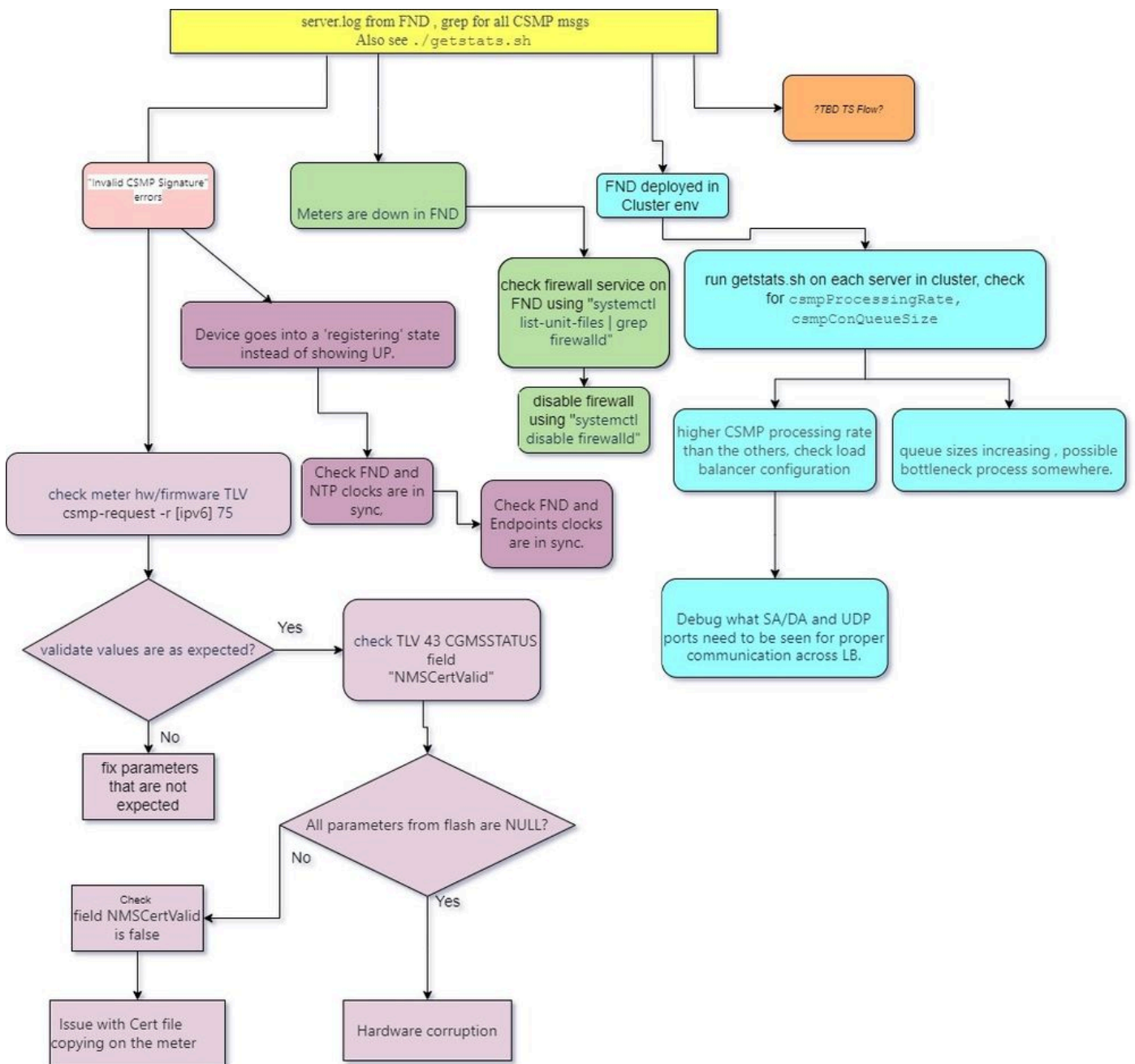
Dirección IP FND ipv6 de destino

Puerto UDP de origen 61624

Puerto UDP DST que envió por ejemplo: 9251

Si el ME está enviando una respuesta a la dirección IP (VIP) del equilibrador de carga en lugar de a la dirección IP solicitada en la que recibió la "solicitud" de CSMP el, " debe enrutarse correctamente mediante la configuración adicional.

Diagrama de flujo para el registro CSMP



Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).