Referencia de Configuración de OmniSCEF

Este documento describe cada parámetro de configuración para OmniSCEF. La configuración se divide en tres ámbitos de aplicación:

Ámbito	Propósito
`:diameter_ex`	El servicio Diameter **T6a**: identidad, oyentes, aplicación y pares.
`:api_ex`	El punto final de la API REST **T8**: TLS, dirección de enlace y la tabla de rutas.
`:omni_scef`	Comportamiento de OmniSCEF: resolución de identidad, membresía de grupo y monitoreo.

OmniSCEF evalúa los parámetros del servicio Diameter al inicio, por lo que el entorno puede influir en ellos (vea Variables de Entorno). El punto final T8 y la tabla de rutas se fijan en el momento de la construcción.

Tabla de Contenidos

- Servicio Diameter (T6a)
- Punto Final de la API T8
- Configuraciones de Identidad y Grupo
- Configuraciones de Monitoreo
- Variables de Entorno

Servicio Diameter (T6a)

OmniSCEF termina T6a como un servidor Diameter. El MME (o un Agente de Enrutamiento Diameter) se conecta entrante; OmniSCEF escucha tanto en TCP como en SCTP en el puerto configurado.

```
config :diameter_ex,
  diameter: %{
    # Identidad del servicio
    service_name: :omni_scef,
    host: "scef01",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    product_name: "OmniSCEF",

    # Oyentes (TCP y SCTP se inician en esta dirección/puerto)
    listen_ip: "0.0.0.0",
    listen_port: 3868,

    # Comportamiento
    request_timeout: 5000,
    peer_selection_algorithm: :random,
    allow_undefined_peers_to_connect: true,
    log_unauthorized_peer_connection_attempts: true,

    # Capacidades de Diameter
    vendor_id: 10415,
    supported_vendor_ids: [10415],
    auth_application_ids: [],
    acct_application_ids: [],

    # Manejadores internos (fijos - no cambiar)
    control_module: OmniScef.Control.Diameter,
    processor_module: DiameterEx.Processor,

    # Registro de aplicación T6a
    applications: [
      %{
        application_name: :t6a,
        application_dictionary: :diameter_gen_3gpp_t6a,
        vendor_specific_application_ids: [
          %{vendor_id: 10415, auth_application_id: 16_777_346,
acct_application_id: nil}
        ]
      }
    ],

    # Pares MME / DRA / HSS
    peers: [
      %{
```

```
        host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.7.25.185",
        port: 3868,
        tls: false,
        transport: :diameter_sctp,
        initiate_connection: false
      }
    ]
  }
```

Identidad del Servicio

Parámetro	Tipo	Requerido	Predeterminado
`service_name`	Átomo	Sí	`:omni_scef`
`host`	Cadena	Sí	`scef01`
`realm`	Cadena	Sí	`epc.mnc001.mcc001.3gppnetwork.o`
`product_name`	Cadena	No	`OmniSCEF`

Oyentes

Parámetro	Tipo	Requerido	Predeterminado	Descripción
`listen_ip`	Cadena	No	`0.0.0.0`	Dirección IP para enlazar conexiones Diameter entrantes. Use `0.0.0.0` para todas las interfaces.
`listen_port`	Entero	No	3868	Puerto para conexiones Diameter entrantes. Tanto los oyentes TCP como SCTP se inician en este puerto. 3868 es el puerto estándar de Diameter según RFC 6733.

Comportamiento

Parámetro	Tipo	Requerido	P
`request_timeout`	Entero	No	5
`peer_selection_algorithm`	Átomo	No	`:`
`allow_undefined_peers_to_connect`	Booleano	No	`t`

Parámetro	Tipo	Requerido	P
`log_unauthorized_peer_connection_attempts`	Booleano	No	`t`

Capacidades de Diameter

Parámetro	Tipo	Requerido	Predeterminado	Des
`vendor_id`	Entero	No	10415	Vend publi las capa 1041
`supported_vendor_ids`	Lista de Enteros	No	`[10415]`	Supp Vend publi las capa
`auth_application_ids`	Lista de Enteros	No	`[]`	IDs d aplica auter base espe vend Vacío T6a e regist como aplica espe vend `appl`
`acct_application_ids`	Lista de Enteros	No	`[]`	IDs d aplica conta base. utiliz Omni

Manejadores Internos

Estos conectan la pila Diameter a la lógica de OmniSCEF. Son fijos y no deben ser cambiados.

Parámetro	Tipo	Requerido	Predeterminado
`control_module`	Módulo	Sí	`OmniScef.Control.Diameter`
`processor_module`	Módulo	Sí	`DiameterEx.Processor`

Aplicación T6a

La lista `applications` registra la aplicación Diameter T6a. Esto es fijo para OmniSCEF.

Parámetros de entrada de la aplicación:

Parámetro	Tipo	Requerido	Predeterm
`application_name`	Átomo	Sí	`:t6a`
`application_dictionary`	Átomo	Sí	`:diameter_gen`
`vendor_specific_application_ids`	Lista de Mapas	Sí	ver abajo

Parámetros de ID de aplicación específicos del vendedor:

Parámetro	Tipo	Requerido	Predeterminado	Descrip
`vendor_id`	Entero	Sí	10415	ID de vended 3GPP.
`auth_application_id`	Entero	Sí	16777346	El T6a Applica Id.
`acct_application_id`	Entero	No	`nil`	No utiliz para T6

Pares

La lista `peers` declara pares Diameter conocidos (el MME, un DRA y el HSS). El parámetro `allow_undefined_peers_to_connect` tiene como predeterminado `true` y el MME normalmente inicia la conexión. Puede dejar `peers` vacío (`[]`) en implementaciones donde OmniSCEF no marque nada saliente. Liste un par aquí cuando OmniSCEF deba **iniciar** la conexión, o para restringir qué pares pueden conectarse.

Parámetros de pares:

Parámetro	Tipo	Requerido	Predeterminado	De
`host`	Cadena	Sí	-	Ident Diam par (Debe exac con e Host confi par.
`realm`	Cadena	Sí	-	Realr del p
`ip`	Cadena	Sí	-	Direc par p cone TCP/S
`port`	Entero	No	3868	Puert del p
`tls`	Booleano	No	`false`	Si la este TLS.
`transport`	Átomo	No	`:diameter_sctp`	Trans este `:dia` o `:dia`
`initiate_connection`	Booleano	No	`false`	Cuar `true` Omn cone

Parámetro	Tipo	Requerido	Predeterminado	De
				activ este inicio es `fa` Omn espe par s entra un pa un M marc SCEF en `fa`

Punto Final de la API T8

La API RESTful T8 se sirve a través de HTTPS. Todas las rutas están montadas bajo el prefijo `/api`, por lo que el apiRoot efectivo es `https://<host>:<port>/api`.

```
config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "0.0.0.0",
    product_name: "OmniSCEF",
    title: "API T8 - OmniSCEF",
    hostname: "localhost",
    enable_tls: true,
    tls_cert_path: "priv/cert/omnitouch.crt",
    tls_key_path: "priv/cert/omnitouch.pem",
    routes: [ ... ]   # tabla de rutas T8 fija - ver abajo
  }
```

Parámetros del Punto Final

Parámetro	Tipo	Requerido	Predeterminado	De
`port`	Entero	No	8443	Pue HT la A
`listen_ip`	Cadena	No	`0.0.0.0`	Dir par la A Use par las int
`product_name`	Cadena	No	`OmniSCEF`	No pro util los me de API
`title`	Cadena	No	`API T8 - OmniSCEF`	Títu mo el doc Op ger en de de
`hostname`	Cadena	No	`localhost`	No hos al

Parámetro	Tipo	Requerido	Predeterminado	De
				UR pu
`enable_tls`	Booleano	No	`true`	Cu `tr` pu siv uti cer cor
`tls_cert_path`	Cadena	Sí (si TLS)	`priv/cert/omnitouch.crt`	Rut cer TLS coc PE
`tls_key_path`	Cadena	Sí (si TLS)	`priv/cert/omnitouch.pem`	Rut cla pri coc PE
`routes`	Lista	Sí	fija	La rut Est def de sup la aju el Vea Rut

Tabla de Rutas

Las entradas `routes` definen la superficie de la API T8. Son fijas para OmniSCEF y producen los puntos finales a continuación (todos bajo `/api`). Cada entrada mapea una plantilla de URL a un manejador y el conjunto de acciones que sirve.

Parámetros de entrada de ruta:

Parámetro	Tipo	Descripción
`path`	Cadena	La plantilla de URL. Segmentos como `:scsAsId` son variables de ruta.
`module`	Módulo	El manejador que sirve la ruta.
`parameters`	Cadena o `nil`	El nombre de la variable de ruta de recurso miembro (por ejemplo, `configurationId`), o `nil` para rutas solo de colección.
`actions`	Lista de Átomo	Las acciones HTTP servidas: `:index` (GET colección), `:create` (POST), `:show` (GET miembro), `:update` (PUT/PATCH miembro), `:delete` (DELETE miembro).

Puntos finales resultantes:

Método y Ruta	Prop
`GET /api/status`	Vivacid servici identid
`GET /api/3gpp-nidd/v1/{scsAsId}/configurations`	Listar configu NIDD.
`POST /api/3gpp-nidd/v1/{scsAsId}/configurations`	Crear u configu NIDD.
`GET/PUT/PATCH/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}`	Leer / reempl elimina configu NIDD.
`GET/POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`	Listar / datos d bajada
`GET/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries/{downlinkDataDeliveryId}`	Leer es cancela entrega bajada
`GET/POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`	Listar / suscrip de mon
`GET/PUT/DELETE /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}`	Leer / reempl elimina

Método y Ruta	Prop
	suscrip monito

El documento OpenAPI generado está disponible en `GET /api/schema`, y una interfaz de usuario interactiva de Swagger en `GET /api/docs`.

> **Autenticación opcional con clave compartida.** El punto final T8 admite una verificación opcional de clave compartida en solicitudes entrantes. Está deshabilitado a menos que se agregue una clave `auth` bajo `config :api_ex, :api`. Cuando no está configurado (el predeterminado), no se aplica ninguna verificación de clave compartida y el punto final debe estar protegido por controles de red (por ejemplo, una interconexión privada o un proxy inverso).

Configuraciones de Identidad y Grupo

OmniSCEF resuelve la identidad orientada al AS (Identificador Externo o MSISDN) a la IMSI de la red, y resuelve un identificador de grupo a sus IMSIs miembros. En la primera versión, estos son mapas estáticos del operador.

```
config :omni_scef,
  nidd: %{
    identity_map: %{
      "device01@iot.example.org" => "001010000000001",
      "61400000001" => "001010000000001"
    },
    group_map: %{
      "fleet-a@iot.example.org" => ["001010000000001",
"001010000000002"]
    },
    default_max_packet_size: 255
  }
```

Parámetro	Tipo	Requerido	Predeterminado	
`identity_map`	Mapa	No	`%{}`	Ma Ide Ext (`us` MS de cua una NID o u mo ide pre rec UE
`group_map`	Mapa	No	`%{}`	Ma `ex` la l mie par NID
`default_max_packet_size`	Entero	No	255	El t pre car oct una NID esp `ma` El t lim me 25

> En producción, estos mapas están típicamente respaldados por una búsqueda HSS/UDR en lugar de una configuración estática. El comportamiento orientado al AS no cambia.

Configuraciones de Monitoreo

Opcional. Cuando configura un destino de monitoreo, crear una suscripción de monitoreo activa el evento hacia abajo. OmniSCEF envía una Solicitud de Información de Configuración (CIR) a ese nodo. Cuando no establece un destino, OmniSCEF aún almacena suscripciones y aún entrega informes entrantes. En ese caso, OmniSCEF no envía proactivamente el CIR.

```
config :omni_scef,
  monitoring: %{
    destination: %{
      host: "hss01.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org"
    }
  }
```

Parámetros de `destination`:

Parámetro	Tipo	Requerido	Predeterminado	Descripción
`host`	Cadena	No	-	Identidad Diameter (FQDN) del HSS / nodo de servicio al que se envían las solicitudes de configuración de monitoreo. Cuando se omite, la solicitud se enruta solo por realm.
`realm`	Cadena	Sí (si se establece `destination`)	-	Realm Diameter utilizado como el Destination-Realm del CIR de monitoreo.

Variables de Entorno

La identidad del servicio Diameter y los oyentes pueden ser suministrados desde el entorno al inicio. Estos anulan los valores predeterminados mostrados bajo Servicio Diameter.

Variable	Mapea a	Predeterminado
`SCEF_DIAMETER_LISTEN_IP`	`listen_ip`	`0.0.0.0`
`SCEF_DIAMETER_LISTEN_PORT`	`listen_port`	`3868`
`SCEF_DIAMETER_HOST`	`host`	`scef01`
`SCEF_DIAMETER_REALM`	`realm`	`epc.mnc001.mcc001.3gppnetw`

Monitoreo de Eventos

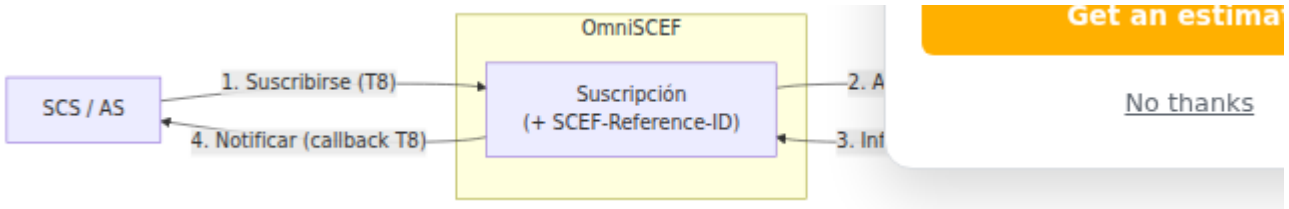
El servicio de Monitoreo de Eventos permite a un Servidor de Aplicaciones suscribirse a eventos de red sobre un dispositivo o grupo: disponibilidad, pérdida de conectividad, ubicación, estado de itinerancia y más. El Servidor de Aplicaciones se suscribe a través de **T8**. OmniSCEF arma el evento en la red a través de **T6a** y entrega cada informe de vuelta al callback del suscriptor.

Los eventos de monitoreo están definidos en 3GPP TS 23.682 §5.6, la API T8 en TS 29.122 §5.3, y los procedimientos de Diameter en TS 29.128 / TS 29.336.

Tabla de Contenidos

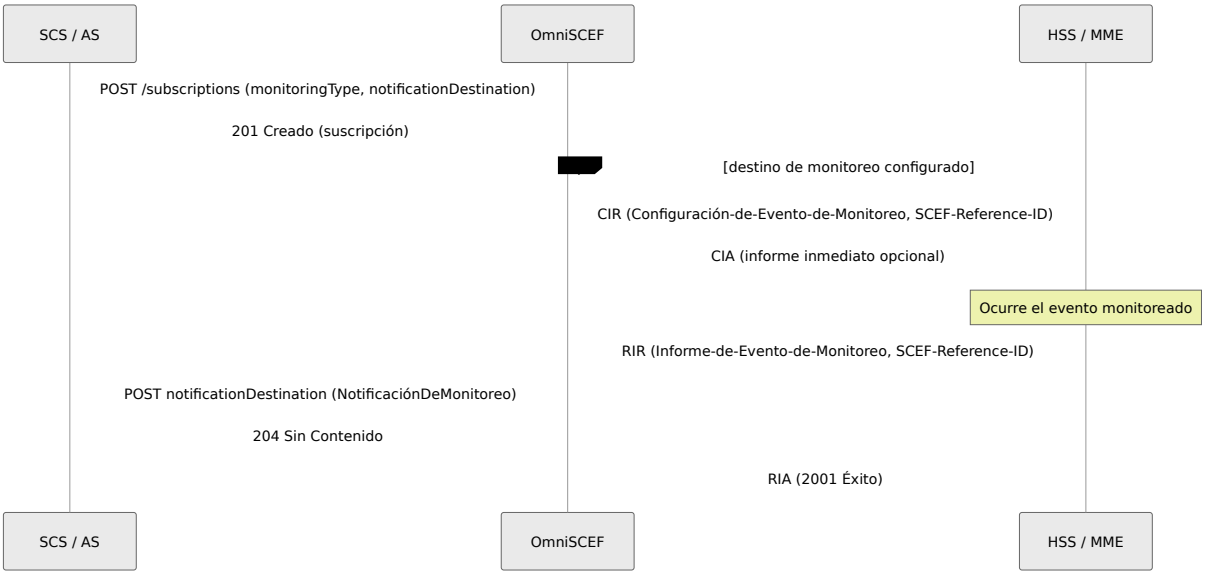
- Descripción General
- Flujo de Suscripción e Informe
- Referencia de Recursos T8
- Tipos de Monitoreo
- Valores de Referencia

Descripción General



OmniSCEF asigna a cada suscripción un **SCEF-Reference-ID**. Este identificador único se incluye en la configuración de salida, y la red lo devuelve en cada informe. OmniSCEF lo utiliza para dirigir un informe entrante a la suscripción correcta y su callback del Servidor de Aplicaciones.

Flujo de Suscripción e Informe



Armar es opcional en el SCEF. Cuando configuras un destino de monitoreo, OmniSCEF envía el CIR para armar el evento. Cuando no configuras uno, OmniSCEF aún crea la suscripción y entrega cualquier informe entrante. En ese caso, OmniSCEF no envía proactivamente el CIR (por ejemplo, cuando otro camino arma el evento a través del HSS).

Cuando el SCEF-Reference-ID de un informe no coincide con ninguna suscripción, OmniSCEF lo reconoce con un RIA pero no lo reenvía.

Referencia de Recursos T8

SuscripciónEventoMonitoreo

Creado por `POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`.

Campo	Tipo	Requerido	Descripción
`notificationDestination`	Cadena (URI)	Sí	Callback en el que el AS recibe informes de monitoreo.
`monitoringType`	Cadena (enum)	Sí	El evento a monitorear. Ver Tipos de Monitoreo.
`externalId`	Cadena	Condicional	Identificador Externo del Dispositivo. Uno de `externalId`, `msisdn` o `externalGroupId`.
`msisdn`	Cadena	Condicional	MSISDN del Dispositivo
`externalGroupId`	Cadena	Condicional	Identificador de grupo para monitoreo de grupo.
`maximumNumberOfReports`	Entero	No	Detener después de este número de informes.
`monitoringDuration`	Cadena (fecha-hora)	No	Detener el monitoreo a esta hora.
`reachabilityType`	Cadena (enum)	No	Para `UE_REACHABILITY`: `SMS` o `DATA`.
`maximumDetectionTime`	Entero	No	Para `LOSS_OF_CONNECTIVITY` tiempo de detección en segundos.

Campo	Tipo	Requerido	Descripción
`mtcProviderId`	Cadena	No	Identificador del proveedor de servicio MTC.
`self`	Cadena (URI)	Solo lectura	La propia URI de la suscripción.

Ejemplo de solicitud de suscripción:

```
{
  "monitoringType": "UE_REACHABILITY",
  "notificationDestination":
"https://as.example.org/monitoring/callback",
  "externalId": "device01@iot.example.org",
  "reachabilityType": "DATA",
  "maximumNumberOfReports": 10
}
```

NotificaciónDeMonitoreo

OmniSCEF POSTea una `NotificaciónDeMonitoreo` al `notificationDestination` de la suscripción para cada informe. Hace referencia a la suscripción de origen y lleva uno o más informes de eventos decodificados.

Ejemplo de notificación:

```
{
  "subscription": "/3gpp-monitoring-
event/v1/as01/subscriptions/XyZ...",
  "monitoringEventReports": [
    {
      "monitoringType": "UE_REACHABILITY",
      "reachabilityType": "DATA"
    }
  ]
}
```

El Servidor de Aplicaciones reconoce con `204 Sin Contenido`.

Tipos de Monitoreo

OmniSCEF soporta el conjunto completo de tipos de monitoreo de TS 29.122. Cada uno se mapea al valor correspondiente de `Monitoring-Type` en la interfaz Diameter (TS 29.336 §5.3.9).

`monitoringType` (T8)	Valor de Diameter	Descripción
`LOSS_OF_CONNECTIVITY`	0	El UE ya no es alcanzable para datos.
`UE_REACHABILITY`	1	El UE se ha vuelto alcanzable para SMS o datos.
`LOCATION_REPORTING`	2	Se informa la ubicación del UE (o un cambio en ella).
`CHANGE_OF_IMSI_IMEI_ASSOCIATION`	3	El IMEI asociado con el IMSI cambió.
`ROAMING_STATUS`	4	Se informa el estado de itinerancia del UE (o un cambio).
`COMMUNICATION_FAILURE`	5	Ocurrió un evento de falla de comunicación.
`AVAILABILITY_AFTER_DDN_FAILURE`	6	El UE se volvió disponible después de una falla de notificación de datos de enlace descendente.
`NUMBER_OF_UES_IN_AN_AREA`	7	Conteo de UEs presentes en un área dada.
`PDN_CONNECTIVITY_STATUS`	8	Conexión PDN establecida/liberada.

`monitoringType` (T8)	Valor de Diameter	Descripción
`DOWNLINK_DATA_DELIVERY_STATUS`	9	Estado de la entrega de datos de enlace descendente.
`API_SUPPORT_CAPABILITY`	10	Informe de capacidad de soporte de API.

Una suscripción con un `monitoringType` no soportado es rechazada con `400 INVALID_MONITORING_TYPE`.

Valores de Referencia

Tipo de Disponibilidad

Valor	Significado
`SMS`	El UE es alcanzable para SMS.
`DATA`	El UE es alcanzable para datos.

Comandos Diameter Relacionados

Consulta las tablas de referencia de la Guía de Operaciones para los códigos de comando y resultado de CIR/CIA y RIR/RIA.

Entrega de Datos No-IP (NIDD)

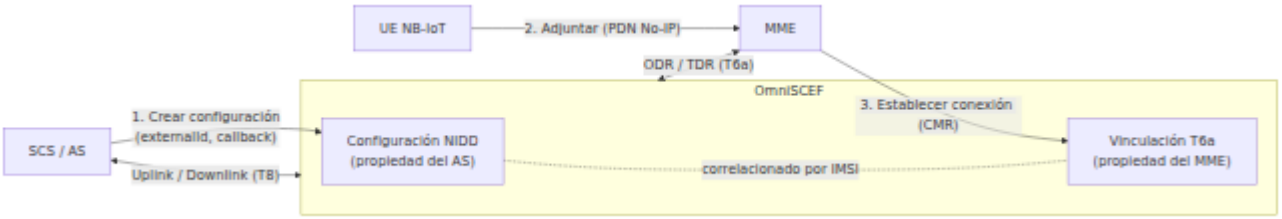
Entrega de Datos No-IP permite que un dispositivo Cellular-IoT / NB-IoT intercambie pequeños mensajes **No-IP** con un Servidor de Aplicaciones **sin una dirección IP**. Los datos viajan por el plano de señalización NAS (la optimización del plano de control CIoT EPS) entre el UE y el MME. El MME lo reenvía a OmniSCEF a través de **T6a**. OmniSCEF luego lo expone al Servidor de Aplicaciones a través de **T8**.

La arquitectura y los procedimientos de NIDD están definidos en 3GPP TS 23.682 §5.13; la interfaz Diameter T6a en TS 29.128; y la API NIDD T8 en TS 29.122.

Tabla de Contenidos

- Descripción General
- Ciclo de Vida de la Conexión
- Datos Originados en el Móvil
- Datos Terminados en el Móvil
- NIDD de Grupo
- Servicio de Datos Fiable
- Datos de Excepción MO
- Referencia de Recursos T8
- Valores de Referencia

Descripción General



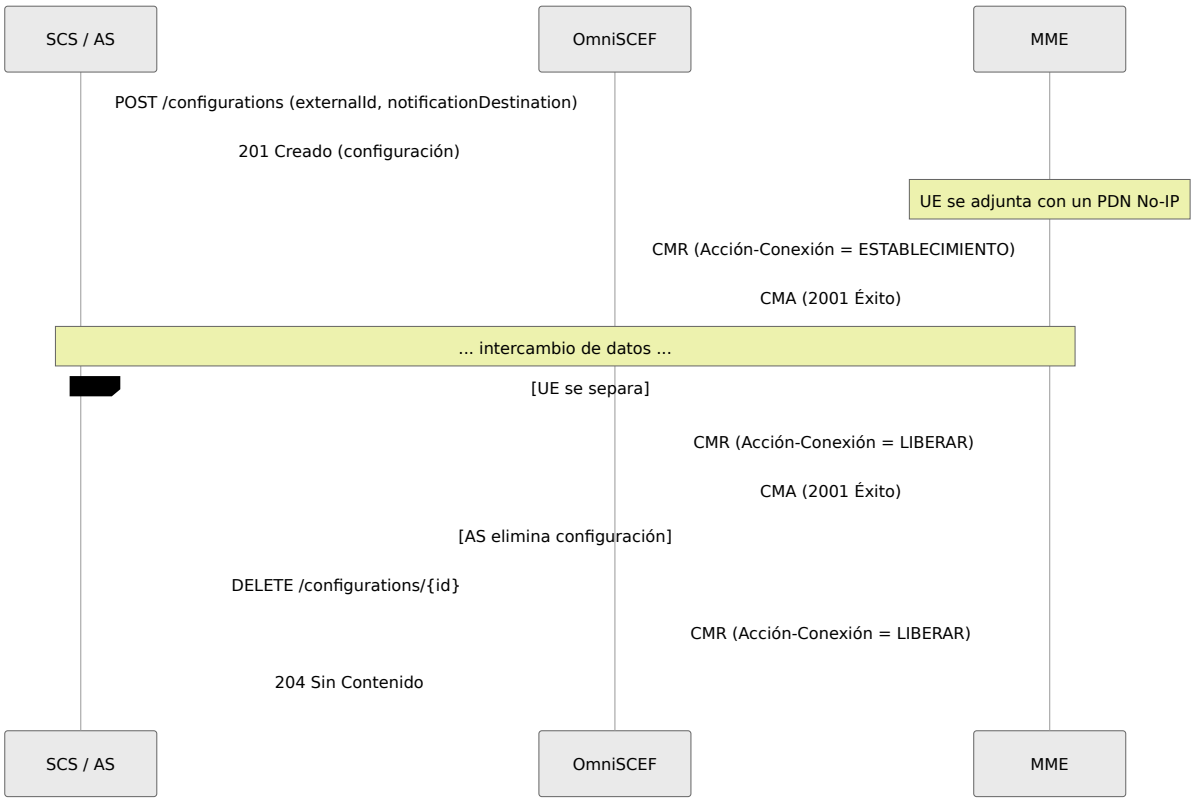
Una sesión NIDD tiene dos mitades correlacionadas:

- La **Configuración NIDD** es creada por el Servidor de Aplicaciones a través de T8. Nombra el dispositivo (por Identificador Externo, MSISDN o grupo), el callback de notificación y las opciones de NIDD.
- La **Vinculación T6a** se crea cuando el MME establece la conexión No-IP para ese suscriptor. Une la sesión Diameter y la identidad del MME al `{IMSI, EBI}` utilizado para alcanzar el UE.

OmniSCEF correlaciona las dos por la identidad del suscriptor, de modo que los datos de uplink encuentran el callback correcto del AS y los datos de downlink encuentran la conexión activa correcta.

Ciclo de Vida de la Conexión

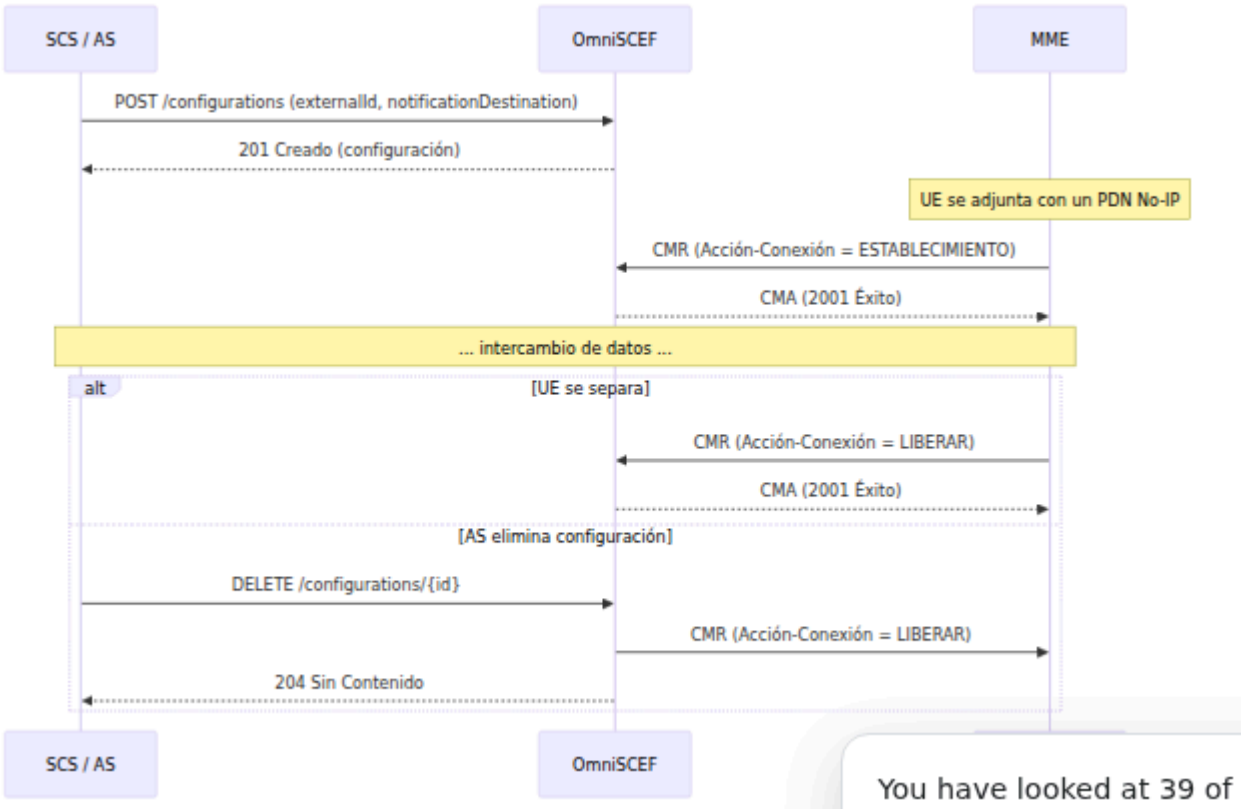
El MME gestiona la conexión T6a a medida que el UE se adjunta y se separa. El Servidor de Aplicaciones también puede finalizar una conexión eliminando su configuración NIDD.



Cuando el MME establece una conexión para un suscriptor que **no** tiene configuración NIDD, OmniSCEF responde al CMR con `DIAMETER_ERROR_USER_UNKNOWN (5001)`. El suscriptor no está provisionado para NIDD.

Datos Originados en el Móvil (Uplink)

Los datos No-IP de uplink enviados por el UE llegan a OmniSCEF como un **MO-Data-Request (ODR)** T6a. OmniSCEF los entrega al Servidor de Aplicaciones enviando una notificación a la callback de la configuración, y responde al MME con un **MO-Data-Answer (ODA)**.



You have looked at 39 of

Si OmniSCEF no puede resolver la configuración o el callback falla, responde al ODA con `DIAMETER_UNABLE_TO_COMPLY (5012)`.

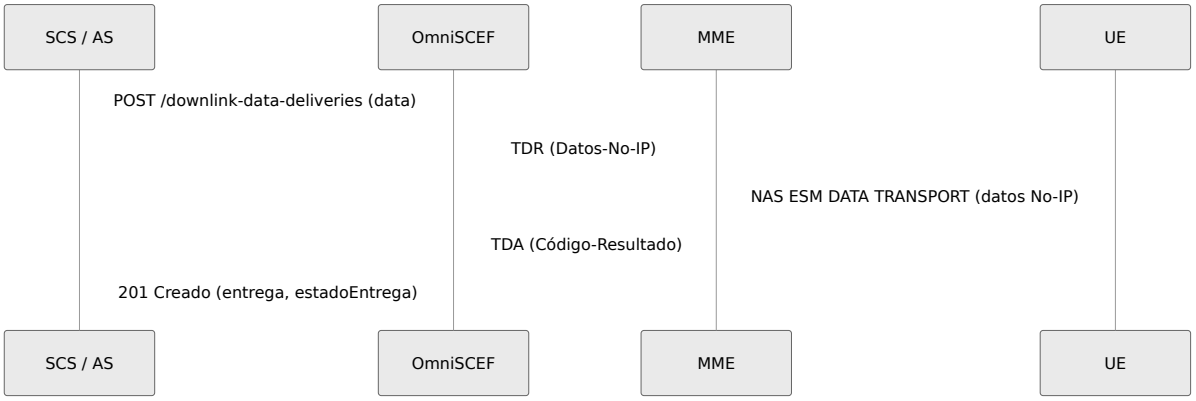
Ejemplo de notificación de uplink (enviada a la callback):

```
{
  "externalId": "device01@iot.example.org",
  "data": "AQIDBA=="
}
```

Campo	Descripción
`externalId` / `msisdn`	La identidad del dispositivo, según lo provisionado en la configuración.
`data`	La carga útil No-IP, codificada en base64.
`rdsSourcePort` / `rdsDestinationPort`	Presente cuando el Servicio de Datos Fiable está habilitado.
`moExceptionDataCounter`	Presente cuando el uplink fue marcado como datos de excepción MO.

Datos Terminados en el Móvil (Downlink)

El Servidor de Aplicaciones envía datos No-IP de downlink enviando un POST a la colección `downlink-data-deliveries` de la configuración. OmniSCEF lo reenvía al MME como un **MT-Data-Request (TDR)** T6a, y registra el resultado (del **MT-Data-Answer, TDA**) en un recurso de entrega individual que el AS puede recuperar.



Cuando el UE está inactivo, el MME almacena los datos y busca al UE, respondiendo al TDA con éxito una vez que ha asumido la responsabilidad de la entrega. OmniSCEF refleja el resultado en el `estadoEntrega` de la entrega (ver Valores de Estado de Entrega).

Ejemplo de solicitud de downlink:

```
{
  "data": "SGVsbG8=",
  "maximumLatency": 3600,
  "priority": 5
}
```

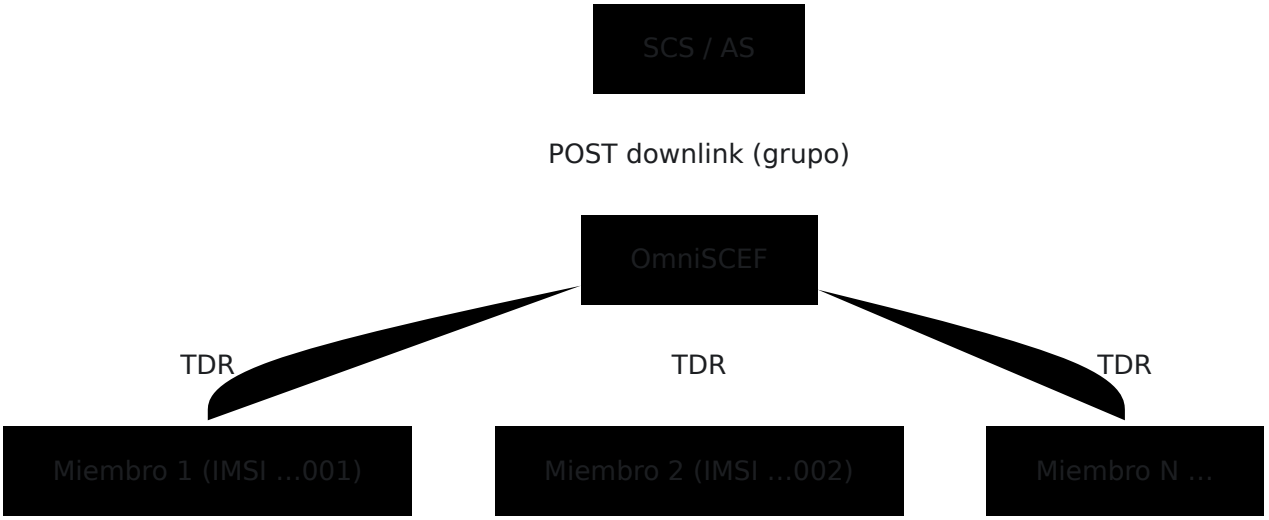
Campo	Descripción
`data`	La carga útil No-IP a entregar, codificada en base64. Requerido.
`maximumLatency`	Opcional. Máximo retraso de almacenamiento aceptable, en segundos.
`priority`	Opcional. Prioridad relativa entre las entregas en cola.
`pdnEstablishmentOption`	Opcional. Comportamiento cuando no existe conexión. Ver Opciones de Establecimiento de PDN.
`rdsSourcePort` / `rdsDestinationPort`	Opcional. Puertos RDS. Ver Servicio de Datos Fiable.

Ejemplo de respuesta de downlink:

```
{
  "self": "https://scef01:8443/api/3gpp-
nidd/v1/as01/configurations/AbC.../downlink-data-
deliveries/XyZ...",
  "data": "SGVsbG8=",
  "deliveryStatus": "SUCCESS"
}
```

NIDD de Grupo

Una configuración NIDD creada con un `externalGroupId` (en lugar de un único `externalId`/`msisdn`) representa un **grupo** de dispositivos (TS 23.682 §5.13.3A). Una única entrega de downlink a una configuración de grupo se **distribuye** a cada miembro del grupo que tiene una conexión T6a activa.



Los miembros del grupo se resuelven a partir del mapa de grupo. El `estadoEntrega` agregado de la entrega refleja el **peor** resultado por miembro, por lo que una entrega de grupo solo informa `SUCCESS` cuando cada miembro alcanzable fue atendido.

Servicio de Datos Fiable

El Servicio de Datos Fiable (RDS) multiplexa múltiples flujos de aplicación sobre una única conexión No-IP utilizando **números de puerto**, según TS 23.682 §4.5.14.3. RDS se habilita por configuración estableciendo `reliableDataService: true` cuando se crea la configuración.

Cuando RDS está habilitado:

- **Downlink**: cuando la entrega especifica `rdsDestinationPort` y `rdsSourcePort`, OmniSCEF enmarca la carga útil No-IP con un encabezado RDS que lleva esos puertos antes de enviar el TDR.
- **Uplink**: OmniSCEF analiza el encabezado RDS de la carga útil ODR. Superficies `rdsSourcePort` y `rdsDestinationPort` en la notificación de

uplink, y entrega la carga útil interna como `data`.

Los puertos son 0–255. Cuando RDS no está habilitado, o una entrega omite los puertos, la carga útil se transporta sin enmarcar.

Datos de Excepción MO

Los dispositivos NB-IoT pueden marcar una transmisión de uplink como **informe de excepción** (un informe urgente, fuera de patrón) a través de la causa de establecimiento RRC, contada en el `RRC-Cause-Counter` T6a (TS 23.682 §5.13.4). Cuando OmniSCEF ve esta indicación en un ODR, incluye un `moExceptionDataCounter` en la notificación de uplink para que el Servidor de Aplicaciones pueda priorizar el manejo.

Referencia de Recursos T8

NiddConfiguration

Creado por `POST /api/3gpp-nidd/v1/{scsAsId}/configurations`.

Campo	Tipo	Requerido	Descripción
`notificationDestination`	String (URI)	Sí	Callback en el que el A recibe notificaciones d uplink y estado.
`externalId`	String	Condicional	Identificador Externo d Dispositivo (`user@domain`). Uno de `externalId`, `msisdn`, o `externalGroupId`.
`msisdn`	String	Condicional	MSISDN del dispositivo
`externalGroupId`	String	Condicional	Identificador de grupo para NIDD de grupo.
`dnn`	String	No	Nombre de Red de Dat APN de la conexión No
`pdnEstablishmentOption`	String (enum)	No	Comportamiento en downlink cuando no ex conexión. Ver Opciones Establecimiento de PD
`maximumPacketSize`	Integer	No	Tamaño máximo de ca útil No-IP en octetos (predeterminado al `default_max_packet_s` configurado, 255).
`reliableDataService`	Boolean	No	Habilitar Servicio de Da Fiable.
`mtcProviderId`	String	No	Identificador del proveedor de servicio MTC.

Campo	Tipo	Requerido	Descripción
`validityTime`	String (date-time)	No	Cuándo expira la configuración.
`status`	String (enum)	Solo lectura	Estado del ciclo de vid Ver Valores de Estado Configuración.
`self`	String (URI)	Solo lectura	La URI propia del recur

NiddDownlinkDataTransfer

Creado por `POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`. Los campos se describen en Datos Terminados en el Móvil. Los campos `deliveryStatus` y `requestedRetransmissionTime` son de solo lectura y se establecen desde el TDA.

Notificaciones

OmniSCEF envía POST a la `notificationDestination` de la configuración:

Notificación	Cuándo
`NiddUplinkDataNotification`	Llegaron datos No-IP de uplink (de un ODR).
`NiddDownlinkDataDeliveryStatusNotification`	El resultado de una entrega de downlink previamente aceptada cambió (estado asincrónico).

El Servidor de Aplicaciones reconoce cada notificación con `204 Sin Contenido`.

Valores de Referencia

Valores de Estado de Entrega

Valor	Significado
`SUCCESS`	El MME entregó los datos (o asumió la responsabilidad al almacenar/paginar un UE inactivo).
`SENDING`	La entrega está en progreso.
`BUFFERING`	El MME almacenó los datos para un UE inactivo.
`FAILURE_UE_NOT_REACHABLE`	No se pudo alcanzar el UE.
`FAILURE_REMOTE_FAILURE`	El MME / nodo de servicio rechazó o falló la solicitud.
`FAILURE`	La entrega falló por otra razón.

Opciones de Establecimiento de PDN

Valor	Comportamiento cuando no existe conexión en el momento de downlink
`WAIT_FOR_UE`	Almacenar hasta que el UE establezca la conexión.
`INDICATE_ERROR`	Rechazar la entrega inmediatamente.
`ESTABLISH_PDN_CONNECTION`	Activar al UE para establecer la conexión No-IP.

Valores de Estado de Configuración

Valor	Significado
`ACTIVE`	La configuración está autorizada y es utilizable.
`TERMINATED_UE_NOT_AUTHORIZED`	El suscriptor no está autorizado para NIDD.
`TERMINATED`	La configuración ha expirado o ha sido eliminada.

Solución de Problemas de OmniSCEF

Orientación sobre problemas operativos comunes de OmniSCEF y sus resoluciones. Para los flujos subyacentes, consulte NIDD y Monitoreo de Eventos; para parámetros, consulte la Referencia de Configuración.

Tabla de Contenidos

- El MME No Puede Conectarse a Través de T6a
- Conexión Rechazada Con USER_UNKNOWN (5001)
- La Entrega de Downlink Falla
- Los Datos de Uplink No Alcanzan el Servidor de Aplicaciones
- El Downlink de Grupo No Llega a Dispositivos
- Informes de Monitoreo No Entregados
- La API T8 Devuelve 404 para un Endpoint Válido
- El Endpoint T8 No Se Inicia

El MME No Puede Conectarse a Través de T6a

Síntomas: El MME no puede establecer una conexión Diameter con OmniSCEF; no se completa el intercambio de capacidades.

Causas posibles:

- El firewall bloquea el puerto Diameter (por defecto 3868).
- Desajuste de transporte: el MME usa SCTP mientras que solo TCP es accesible, o viceversa.
- La autorización del par está restringida y el MME no es un par configurado.

- Desajuste de Origin-Host / realm entre lo que el MME espera y lo que OmniSCEF anuncia.

Resolución:

1. Confirme que el firewall permite el `listen_port` configurado tanto en TCP como en SCTP. OmniSCEF escucha en ambos. Consulte Listeners.
2. Verifique que el transporte configurado del MME coincida. Ambos oyentes TCP y SCTP siempre se inician.
3. Si `allow_undefined_peers_to_connect` es `false`, agregue el MME a `peers` con su exacto Origin-Host. Consulte Peers.
4. Confirme que `host` y `realm` de OmniSCEF coincidan con lo que el MME está provisionado para comunicarse. Verifique la salida del registro `log_unauthorized_peer_connection_attempts` para intentos rechazados.

Conexión Rechazada Con USER_UNKNOWN (5001)

Síntomas: El MME establece la conexión Diameter, pero una solicitud de conexión NIDD (CMR) es respondida con `DIAMETER_ERROR_USER_UNKNOWN (5001)`.

Causas posibles:

- No existe configuración NIDD para el IMSI de ese suscriptor.
- El Servidor de Aplicaciones creó una configuración utilizando una identidad externa que no se resuelve al IMSI del suscriptor.

Resolución:

1. Confirme que el Servidor de Aplicaciones ha creado una configuración NIDD para el dispositivo antes de que el UE se adjunte.
2. Verifique que el `externalId`/`msisdn` del dispositivo se resuelva al IMSI correcto en el mapa de identidades.
3. Confirme que el IMSI en el mapa de identidades coincida con el IMSI que el MME presenta en el CMR.

La Entrega de Downlink Falla

Síntomas: Un `POST` a `downlink-data-deliveries` devuelve una entrega cuyo `deliveryStatus` es un valor `FAILURE_*`, o un `404`.

Causas posibles:

- No existe una conexión T6a activa para el dispositivo (`404 NIDD_CONFIGURATION_NOT_AVAILABLE`). El UE no se ha adjuntado, o OmniSCEF liberó su conexión.
- El UE es inalcanzable (`FAILURE_UE_NOT_REACHABLE`).
- El MME / nodo de servicio rechazó la solicitud (`FAILURE_REMOTE_FAILURE`).
- El campo `data` falta o no es un base64 válido (`400 DATA_MISSING`).

Resolución:

1. Confirme que el dispositivo esté adjunto y su conexión esté establecida (se aceptó un CMR anterior).
2. Verifique que el campo `data` esté presente y codificado en base64.
3. Para un UE inactivo, espere que el MME almacene en búfer y pagine; la entrega informa éxito una vez que el MME asume la responsabilidad. Consulte Datos Terminados en Móvil.
4. Para `FAILURE_REMOTE_FAILURE`, inspeccione el lado del MME/nodo de servicio para la causa del rechazo.

Los Datos de Uplink No Alcanzan el Servidor de Aplicaciones

Síntomas: El UE envía datos de uplink, pero el callback del Servidor de Aplicaciones no se invoca.

Causas posibles:

- El dispositivo no tiene configuración NIDD (por lo que no se conoce ningún callback).

- La URL `notificationDestination` es inalcanzable desde OmniSCEF, o devuelve un estado no 2xx.
- No existe un enlace activo para el `{IMSI, EBI}` presentado en el uplink.

Resolución:

1. Confirme que existe una configuración NIDD para el dispositivo y que lleva un `notificationDestination` accesible.
2. Verifique la conectividad de red desde OmniSCEF a la URL del callback, incluyendo la confianza TLS si es HTTPS.
3. Confirme que el callback devuelve un estado 2xx; un estado no 2xx se trata como un fallo de entrega.
4. Confirme que el dispositivo se adjuntó (se aceptó un CMR) antes de enviar datos de uplink.

El Downlink de Grupo No Llega a Dispositivos

Síntomas: Un downlink a una configuración de grupo devuelve `404 NIDD_CONFIGURATION_NOT_AVAILABLE`, o llega a menos dispositivos de los esperados.

Causas posibles:

- El `externalGroupId` no está presente en el mapa de grupos, o no mapea a ningún miembro.
- Ningún miembro del grupo tiene actualmente una conexión T6a activa.

Resolución:

1. Confirme que el `externalGroupId` esté definido en el mapa de grupos y liste los IMSIs de miembros esperados.
2. Confirme que al menos un dispositivo miembro esté adjunto. Solo los miembros con una conexión activa reciben la entrega. El estado agregado refleja el peor resultado por miembro. Consulte NIDD de Grupo.

Informes de Monitoreo No Entregados

Síntomas: Se crea una suscripción de monitoreo, pero el Servidor de Aplicaciones no recibe notificaciones.

Causas posibles:

- El evento nunca fue armado en la red (no se configuró ningún destino de monitoreo, y ningún otro camino lo armó).
- El SCEF-Reference-ID del informe no coincide con una suscripción activa. Esto puede suceder después de un reinicio, porque el estado de la suscripción está en memoria.
- El `notificationDestination` de la suscripción es inalcanzable.

Resolución:

1. Si OmniSCEF debe armar el evento, configure un destino de monitoreo para que el CIR se envíe.
2. Recree las suscripciones después de un reinicio de OmniSCEF. El estado de la suscripción y el ID de referencia es volátil y no sobrevive a un reinicio.
3. Verifique la conectividad desde OmniSCEF hasta el callback de la suscripción.

La API T8 Devuelve 404 para un Endpoint Válido

Síntomas: Una solicitud a un camino T8 documentado devuelve `404`, y el endpoint no aparece en el documento OpenAPI en `/api/schema`.

Causas posibles:

- La tabla de rutas fue cambiada pero la capa API no fue recompilada, por lo que la nueva ruta no está registrada.
- La solicitud omite el prefijo `/api` bajo el cual están montadas todas las rutas T8.

Resolución:

1. Confirme que la ruta de la solicitud incluya el prefijo `/api` (por ejemplo, `/api/3gpp-nidd/v1/{scsAsId}/configurations`).
2. Si la tabla de rutas fue modificada, la dependencia de la API debe ser recompilada para que las nuevas rutas se registren (`mix deps.compile api_ex --force`), luego el servicio debe reiniciarse.

El Endpoint T8 No Se Inicia

Síntomas: OmniSCEF no puede iniciar el endpoint HTTPS T8.

Causas posibles:

- El certificado TLS o el archivo de clave están ausentes o no son legibles.
- El `port` configurado ya está en uso.

Resolución:

1. Confirme que `tls_cert_path` y `tls_key_path` apunten a archivos PEM válidos y legibles. Consulte Endpoint de API T8.
2. Confirme que nada más esté vinculado al `port` configurado en la interfaz `listen_ip`.
3. Para ejecutar sin TLS en un entorno controlado, establezca `enable_tls: false`. Las implementaciones en producción siempre deben terminar TLS en o antes de OmniSCEF.