

Referência de Configuração do OmniSCEF

Este documento descreve todos os parâmetros de configuração para o OmniSCEF. A configuração é dividida em três escopos de aplicação:

Escopo	Propósito
<code>:diameter_ex</code>	O serviço Diameter T6a : identidade, ouvintes, aplicação e pares.
<code>:api_ex</code>	O endpoint da API REST T8 : TLS, endereço de ligação e a tabela de rotas.
<code>:omni_scef</code>	Comportamento do OmniSCEF: resolução de identidade, associação a grupos e monitoramento.

O OmniSCEF avalia os parâmetros do serviço Diameter na inicialização, para que o ambiente possa direcioná-los (veja [Variáveis de Ambiente](#)). O endpoint T8 e a tabela de rotas são fixos na hora da construção.

Índice

- [Serviço Diameter \(T6a\)](#)
- [Endpoint da API T8](#)
- [Configurações de Identidade e Grupo](#)
- [Configurações de Monitoramento](#)
- [Variáveis de Ambiente](#)

Serviço Diameter (T6a)

O OmniSCEF termina o T6a como um servidor Diameter. O MME (ou um Agente de Roteamento Diameter) conecta-se de forma inbound; o OmniSCEF escuta tanto em TCP quanto em SCTP na porta configurada.

```

config :diameter_ex,
  diameter: %{
    # Identidade do serviço
    service_name: :omni_scef,
    host: "scef01",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    product_name: "OmniSCEF",

    # Ouvintes (TCP e SCTP são iniciados neste endereço/porta)
    listen_ip: "0.0.0.0",
    listen_port: 3868,

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

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

    # Manipuladores internos (fixos - não altere)
    control_module: OmniScef.Control.Diameter,
    processor_module: DiameterEx.Processor,

    # Registro da aplicação 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  
  }  
]  
}
```

Identidade do Serviço

Parâmetro	Tipo	Necessário	Padrão
service_name	Atom	Sim	:omni_scef
host	String	Sim	scef01
realm	String	Sim	epc.mnc001.mcc001.3gppnetwork.or
product_name	String	Não	OmniSCEF

Ouvintes

Parâmetro	Tipo	Necessário	Padrão	Descrição
<code>listen_ip</code>	String	Não	<code>0.0.0.0</code>	Endereço IP para vincular conexões Diameter inbound. Use <code>0.0.0.0</code> para todas as interfaces.
<code>listen_port</code>	Integer	Não	3868	Porta para conexões Diameter inbound. Tanto os ouvintes TCP quanto SCTP são iniciados nesta porta. 3868 é a porta Diameter padrão conforme RFC 6733 .

Comportamento

Parâmetro	Tipo	Necessário	P
<code>request_timeout</code>	Integer	Não	5
<code>peer_selection_algorithm</code>	Atom	Não	:
<code>allow_undefined_peers_to_connect</code>	Boolean	Não	t

Parâmetro	Tipo	Necessário	P
log_unauthorized_peer_connection_attempts	Boolean	Não	t

Capacidades Diameter

Parâmetro	Tipo	Necessário	Padrão	Descrição
<code>vendor_id</code>	Integer	Não	10415	Vendor-Id anunciado nas capacidades. 10415 é 3GPP.
<code>supported_vendor_ids</code>	Lista de Integer	Não	<code>[10415]</code>	Supported-Vendor-Ids anunciados na capacidades.
<code>auth_application_ids</code>	Lista de Integer	Não	<code>[]</code>	IDs de aplicação de autenticação base (não específicas do fornecedor). Vazio porque o T6a é registrado como uma aplicação específica do fornecedor (veja <code>applications</code>).
<code>acct_application_ids</code>	Lista de Integer	Não	<code>[]</code>	IDs de aplicação de contabilidade base. Não utilizado pelo OmniSCEF.

Manipuladores Internos

Esses conectam a pilha Diameter à lógica do OmniSCEF. Eles são fixos e não devem ser alterados.

Parâmetro	Tipo	Necessário	Padrão
<code>control_module</code>	Módulo	Sim	<code>OmniScef.Control.Diameter</code>
<code>processor_module</code>	Módulo	Sim	<code>DiameterEx.Processor</code>

Aplicação T6a

A lista `applications` registra a aplicação Diameter T6a. Isso é fixo para o OmniSCEF.

Parâmetros de entrada da aplicação:

Parâmetro	Tipo	Necessário	Padrã
application_name	Atom	Sim	:t6a
application_dictionary	Atom	Sim	:diameter_gen_
vendor_specific_application_ids	Lista de Mapa	Sim	veja abaixo

Parâmetros de ID de aplicação específicos do fornecedor:

Parâmetro	Tipo	Necessário	Padrão	Descrição
<code>vendor_id</code>	Integer	Sim	10415	ID do fornecedor 3GPP.
<code>auth_application_id</code>	Integer	Sim	16777346	O Application-Id do T6a.
<code>acct_application_id</code>	Integer	Não	<code>nil</code>	Não utilizado para T6a.

Pares

A lista `peers` declara pares Diameter conhecidos (o MME, um DRA e o HSS). O parâmetro `allow_undefined_peers_to_connect` tem o padrão `true` e o MME normalmente inicia a conexão. Você pode deixar `peers` vazio (`[]`) em implantações onde o OmniSCEF não disca nada outbound. Liste um par aqui quando o OmniSCEF deve **iniciar** a conexão, ou para restringir quais pares podem se conectar.

Parâmetros do par:

Parâmetro	Tipo	Necessário	Padrão	Descrição
<code>host</code>	String	Sim	-	Identificador do servidor Diameter (FQDN), correspondente ao campo Origin-Host da configuração par.
<code>realm</code>	String	Sim	-	Realm do par.
<code>ip</code>	String	Sim	-	Endereço IP para a conexão TCP/SC.
<code>port</code>	Integer	Não	3868	Porta de destino do par.
<code>tls</code>	Boolean	Não	<code>false</code>	Se a conexão deve ser estabelecida com o servidor usando TLS.
<code>transport</code>	Atom	Não	<code>:diameter_sctp</code>	Transporte de destino para este par. Pode ser <code>:diameter_tcp</code> ou <code>:diameter_sctp</code> .
<code>initiate_connection</code>	Boolean	Não	<code>false</code>	Quando o OmniSwitch se conecta ao servidor, ativa este par.

Parâmetro	Tipo	Necessário	Padrão	Des
				inicializ Quando o Omn aguard se conc inboun um par um MM discan SCEF, c como (

Endpoint da API T8

A API RESTful T8 é servida sobre HTTPS. Todas as rotas são montadas sob o prefixo `/api`, então o apiRoot efetivo é `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: [ ... ] # tabela de rotas T8 fixa - veja abaixo
  }
```

Parâmetros do Endpoint

Parâmetro	Tipo	Necessário	Padrão	Descrição
port	Integer	Não	8443	Porta para o T8.
listen_ip	String	Não	0.0.0.0	Endereço IP para vincular o T8. 0.0.0.0 para todas as interfaces.
product_name	String	Não	OmniSCEF	Nome do produto usado na API.
title	String	Não	API T8 - OmniSCEF	Título do documento OpenAPI do Swagger.
hostname	String	Não	localhost	Nome do host ao qual se conectar.

Parâmetro	Tipo	Necessário	Padrão	Descrição
				URL encodada
<code>enable_tls</code>	Boolean	Não	<code>true</code>	Quando true, o servidor usa certificado abastecido pelo sistema
<code>tls_cert_path</code>	String	Sim (se TLS)	<code>priv/cert/omnitech.crt</code>	Caminho para o certificado TLS codificado em base64
<code>tls_key_path</code>	String	Sim (se TLS)	<code>priv/cert/omnitech.pem</code>	Caminho para o chave privada TLS codificado em base64
<code>routes</code>	Lista	Sim	fixo	A tabela de rotas está definida fixa no servidor API e não pode ser alterada

Parâmetro	Tipo	Necessário	Padrão	De
				Veja de l

Tabela de Rotas

As entradas `routes` definem a superfície da API T8. Elas são fixas para o OmniSCEF e produzem os endpoints abaixo (todos sob `/api`). Cada entrada mapeia um template de URL para um manipulador e o conjunto de ações que ele serve.

Parâmetros de entrada da rota:

Parâmetro	Tipo	Descrição
<code>path</code>	String	O template da URL. Segmentos como <code>:scsAsId</code> são variáveis de caminho.
<code>module</code>	Módulo	O manipulador que serve a rota.
<code>parameters</code>	String ou <code>nil</code>	O nome da variável de caminho de recurso membro (por exemplo, <code>configurationId</code>), ou <code>nil</code> para rotas apenas de coleção.
<code>actions</code>	Lista de Atom	As ações HTTP servidas: <code>:index</code> (GET coleção), <code>:create</code> (POST), <code>:show</code> (GET membro), <code>:update</code> (PUT/PATCH membro), <code>:delete</code> (DELETE membro).

Endpoints resultantes:

Método & Caminho	Propósito
GET /api/status	Verificar o status do sistema e obter a identidade do serviço.
GET /api/3gpp-nidd/v1/{scsAsId}/configurations	Listar as configurações NIDD para um determinado SCS.
POST /api/3gpp-nidd/v1/{scsAsId}/configurations	Criar uma nova configuração NIDD para um determinado SCS.
GET/PUT/PATCH/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}	Ler, atualizar, modificar ou excluir uma configuração NIDD específica.
GET/POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries	Listar ou criar novas entregas de dados de downlink para uma configuração NIDD específica.
GET/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries/{downlinkDataDeliveryId}	Ler o status ou cancelar uma entrega de dados de downlink específica.
GET/POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions	Listar ou criar novas assinaturas de eventos de monitoramento para um determinado SCS.
GET/PUT/DELETE /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}	Ler, atualizar ou excluir uma assinatura de eventos de monitoramento específica.

O documento OpenAPI gerado está disponível em `GET /api/schema`, e uma interface interativa do Swagger em `GET /api/docs`.

Autenticação opcional com chave compartilhada. O endpoint T8 suporta uma verificação opcional de chave compartilhada em solicitações inbound. Ela está desativada, a menos que uma chave `auth` seja adicionada sob `config :api_ex, :api`. Quando não definida (o padrão), nenhuma verificação de chave compartilhada é aplicada e o endpoint deve ser protegido por controles de rede (por exemplo, uma interconexão privada ou proxy reverso).

Configurações de Identidade e Grupo

O OmniSCEF resolve a identidade voltada para o AS (Identificador Externo ou MSISDN) para o IMSI da rede, e resolve um identificador de grupo para seus IMSIs membros. Na primeira versão, esses são mapas de operador estáticos.

```
config :omni_scef,  
  nidd: %{  
    identity_map: %{  
      "device01@iot.example.org" => "0010100000000001",  
      "614000000001" => "0010100000000001"  
    },  
    group_map: %{  
      "fleet-a@iot.example.org" => ["0010100000000001",  
"0010100000000002"]  
    },  
    default_max_packet_size: 255  
  }  
}
```

Parâmetro	Tipo	Necessário	Padrão	Descrição
<code>identity_map</code>	Mapa	Não	<code>%{}</code>	Mapeia um Identificado Externo (user@doma: um MSISDN um IMSI de assinante. L quando o AS uma configu NIDD de úni ou assinatura monitorame Uma identid presente aq rejeitada co UE desconh
<code>group_map</code>	Mapa	Não	<code>%{}</code>	Mapeia um externalGr para a lista membros. U para entreg NIDD em gr
<code>default_max_packet_size</code>	Integer	Não	255	O tamanho padrão de c Não-IP, em c aplicado a u configuraçã que não esp maximumPac O transporte limita uma c mensagem 255 octetos

Em produção, esses mapas são tipicamente suportados por uma consulta HSS/UDR em vez de configuração estática. O comportamento voltado para o AS não é alterado.

Configurações de Monitoramento

Opcional. Quando você configura um destino de monitoramento, criar uma assinatura de monitoramento ativa o evento para o sul. O OmniSCEF envia uma Solicitação de Informação de Configuração (CIR) para esse nó. Quando você não define um destino, o OmniSCEF ainda armazena assinaturas e ainda entrega relatórios inbound. Nesse caso, o OmniSCEF não envia proativamente o CIR.

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

Parâmetros de `destination`:

Parâmetro	Tipo	Necessário	Padrão	Descrição
<code>host</code>	String	Não	-	Identidade Diameter (FQDN) do HSS / nó de serviço para o qual as solicitações de configuração de monitoramento são enviadas. Quando omitido, a solicitação é roteada apenas pelo realm.
<code>realm</code>	String	Sim (se <code>destination</code> definido)	-	Realm Diameter usado como o Destination-Realm do CIR de monitoramento.

Variáveis de Ambiente

A identidade do serviço Diameter e os ouvintes podem ser fornecidos a partir do ambiente na inicialização. Esses substituem os padrões mostrados em [Serviço Diameter](#).

Variável	Mapeia para	Padrão
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

Monitoramento de Eventos

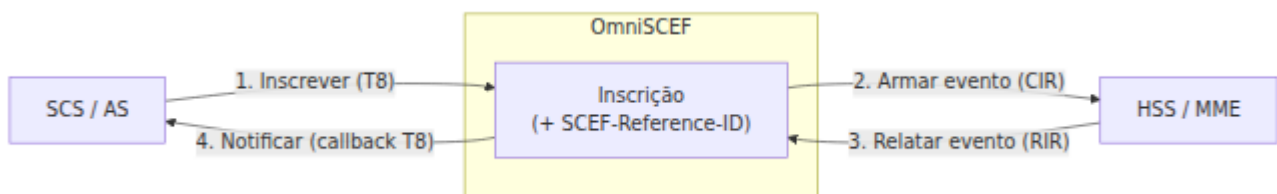
O serviço de Evento de Monitoramento permite que um Servidor de Aplicação se inscreva em eventos de rede sobre um dispositivo ou grupo: acessibilidade, perda de conectividade, localização, status de roaming e mais. O Servidor de Aplicação se inscreve via **T8**. O OmniSCEF arma o evento na rede via **T6a** e entrega cada relatório de volta ao callback do assinante.

Os eventos de monitoramento são definidos na [3GPP TS 23.682 §5.6](#), a API T8 na [TS 29.122 §5.3](#) e os procedimentos Diameter na [TS 29.128](#) / [TS 29.336](#).

Índice

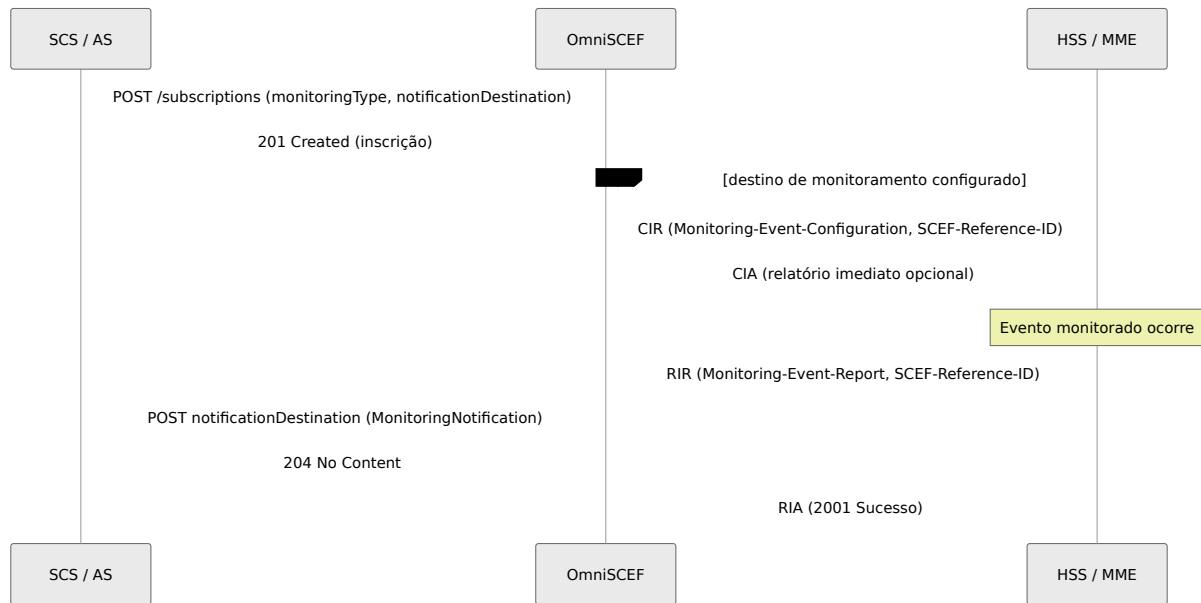
- [Visão Geral](#)
- [Fluxo de Inscrição e Relato](#)
- [Referência de Recursos T8](#)
- [Tipos de Monitoramento](#)
- [Valores de Referência](#)

Visão Geral



O OmniSCEF atribui a cada inscrição um **SCEF-Reference-ID**. Este identificador único vai na configuração de saída, e a rede o ecoa de volta em cada relatório. O OmniSCEF o utiliza para direcionar um relatório de entrada para a inscrição correta e seu callback do Servidor de Aplicação.

Fluxo de Inscrição e Relato



Armar é opcional no SCEF. Quando você configura um **destino de monitoramento**, o OmniSCEF envia o CIR para armar o evento. Quando você não configura um, o OmniSCEF ainda cria a inscrição e ainda entrega quaisquer relatórios de entrada. Nesse caso, o OmniSCEF não envia proativamente o CIR (por exemplo, quando outro caminho arma o evento através do HSS).

Quando o SCEF-Reference-ID de um relatório não corresponde a nenhuma inscrição, o OmniSCEF o reconhece com um RIA, mas não o encaminha.

Referência de Recursos T8

MonitoringEventSubscription

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

Campo	Tipo	Obrigatório	Descrição
<code>notificationDestination</code>	String (URI)	Sim	Callback que o AS recebe relatórios de monitoramento.
<code>monitoringType</code>	String (enum)	Sim	O evento a ser monitorado. Veja Tipos de Monitoramento .
<code>externalId</code>	String	Condicional	Identificador Externo do Dispositivo. Um de <code>externalId</code> , <code>msisdn</code> ou <code>externalGroupId</code> .
<code>msisdn</code>	String	Condicional	MSISDN do Dispositivo
<code>externalGroupId</code>	String	Condicional	Identificador de grupo para monitoramento do grupo.
<code>maximumNumberOfReports</code>	Integer	Não	Parar após este número de relatórios.
<code>monitoringDuration</code>	String (data-hora)	Não	Parar o monitoramento neste momento.
<code>reachabilityType</code>	String (enum)	Não	Para <code>UE_REACHABILITY</code> <code>SMS</code> ou <code>DATA</code> .
<code>maximumDetectionTime</code>	Integer	Não	Para <code>LOSS_OF_CONNECTIVITY</code> tempo de detecção em segundos.

Campo	Tipo	Obrigatório	Descrição
<code>mtcProviderId</code>	String	Não	Identificador do provedor de serviço MTC.
<code>self</code>	String (URI)	Somente leitura	O URI da própria inscrição.

Exemplo de solicitação de inscrição:

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

MonitoringNotification

O OmniSCEF POSTa um `MonitoringNotification` para o `notificationDestination` da inscrição para cada relatório. Ele faz referência à inscrição de origem e carrega um ou mais relatórios de evento decodificados.

Exemplo de notificação:

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

O Servidor de Aplicação reconhece com `204 No Content`.

Tipos de Monitoramento

O OmniSCEF suporta o conjunto completo de tipos de monitoramento da TS 29.122. Cada um mapeia para o valor correspondente de `Monitoring-Type` na interface Diameter ([TS 29.336 §5.3.9](#)).

monitoringType (T8)	Valor Diameter	Descrição
LOSS_OF_CONNECTIVITY	0	O UE não está mais acessível para dados.
UE_REACHABILITY	1	O UE se tornou acessível para SMS ou dados.
LOCATION_REPORTING	2	A localização do UE (ou uma mudança nela) é relatada.
CHANGE_OF_IMSI_IMEI_ASSOCIATION	3	O IMEI associado ao IMSI mudou.
ROAMING_STATUS	4	O status de roaming do UE (ou uma mudança) é relatado.
COMMUNICATION_FAILURE	5	Um evento de falha de comunicação ocorreu.
AVAILABILITY_AFTER_DDN_FAILURE	6	O UE se tornou disponível após uma falha de notificação de dados de downlink.
NUMBER_OF_UES_IN_AN_AREA	7	Contagem de UEs presentes em uma determinada área.
PDN_CONNECTIVITY_STATUS	8	Conexão PDN estabelecida/liberada.

<code>monitoringType</code> (T8)	Valor Diameter	Descrição
<code>DOWNLINK_DATA_DELIVERY_STATUS</code>	9	Status da entrega de dados de downlink.
<code>API_SUPPORT_CAPABILITY</code>	10	Relato da capacidade de suporte à API.

Uma inscrição com um `monitoringType` não suportado é rejeitada com `400 INVALID_MONITORING_TYPE`.

Valores de Referência

Tipo de Acessibilidade

Valor	Significado
<code>SMS</code>	O UE está acessível para SMS.
<code>DATA</code>	O UE está acessível para dados.

Comandos Diameter Relacionados

Veja as [tabelas de referência do Guia de Operações](#) para os códigos de comando e resultado CIR/CIA e RIR/RIA.

Entrega de Dados Não-IP (NIDD)

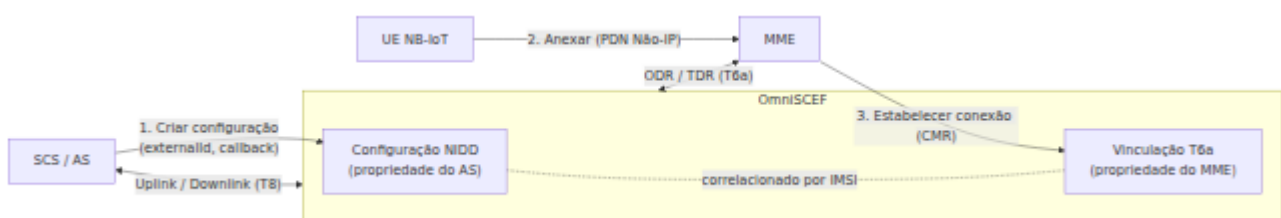
Entrega de Dados Não-IP permite que um dispositivo Cellular-IoT / NB-IoT troque pequenas mensagens **Não-IP** com um Servidor de Aplicação **sem um endereço IP**. Os dados trafegam pelo plano de sinalização NAS (a otimização do Control-Plane Clot EPS) entre o UE e o MME. O MME os retransmite para o OmniSCEF via **T6a**. O OmniSCEF então os expõe ao Servidor de Aplicação via **T8**.

A arquitetura e os procedimentos do NIDD estão definidos em [3GPP TS 23.682 §5.13](#); a interface Diameter T6a em [TS 29.128](#); e a API NIDD T8 em [TS 29.122](#).

Índice

- [Visão Geral](#)
- [Ciclo de Vida da Conexão](#)
- [Dados Originados pelo Móvel](#)
- [Dados Terminados pelo Móvel](#)
- [Grupo NIDD](#)
- [Serviço de Dados Confiável](#)
- [Dados de Exceção MO](#)
- [Referência de Recursos T8](#)
- [Valores de Referência](#)

Visão Geral



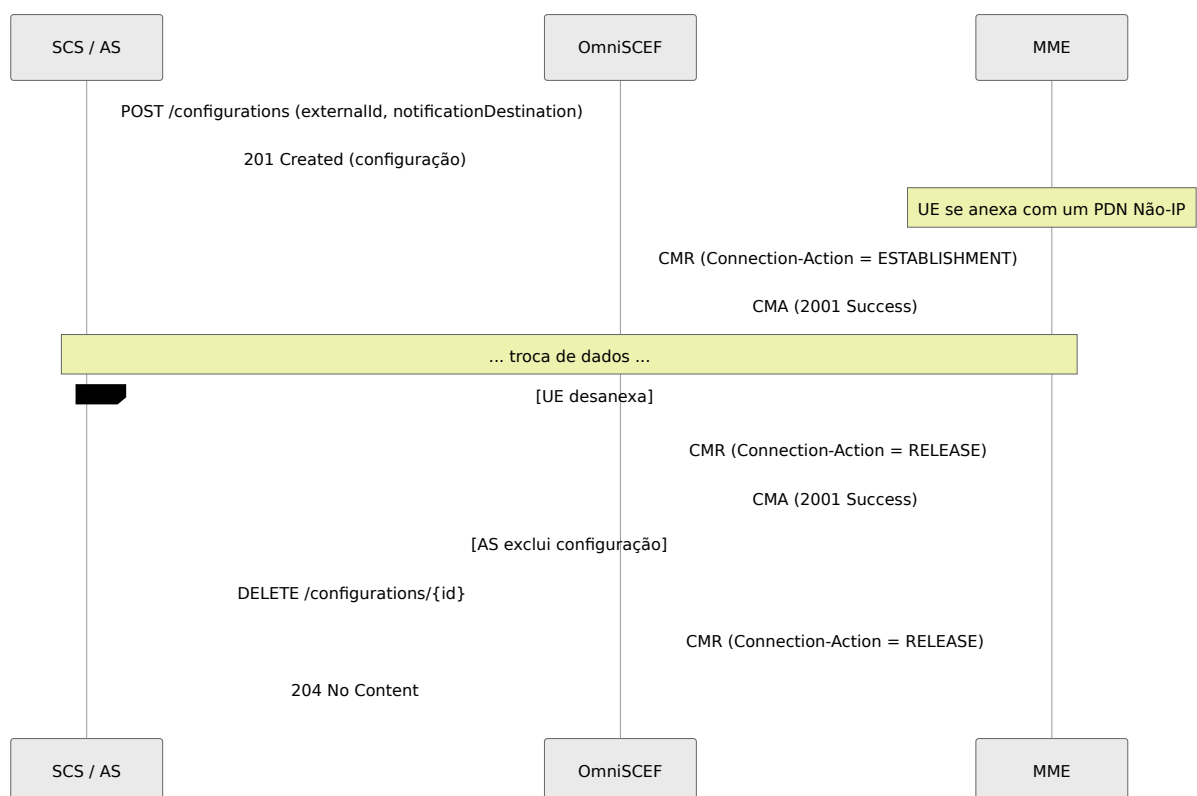
Uma sessão NIDD tem duas metades correlacionadas:

- A **Configuração NIDD** é criada pelo Servidor de Aplicação via T8. Ela nomeia o dispositivo (por Identificador Externo, MSISDN ou grupo), o callback de notificação e as opções NIDD.
- A **Vinculação T6a** é criada quando o MME estabelece a conexão Não-IP para aquele assinante. Ela vincula a sessão Diameter e a identidade do MME ao {IMSI, EBI} usado para alcançar o UE.

O OmniSCEF correlaciona as duas por identidade do assinante, de modo que os dados uplink encontrem o callback correto do AS e os dados downlink encontrem a conexão ativa correta.

Ciclo de Vida da Conexão

O MME gerencia a conexão T6a enquanto o UE se anexa e desanexa. O Servidor de Aplicação também pode encerrar uma conexão excluindo sua configuração NIDD.

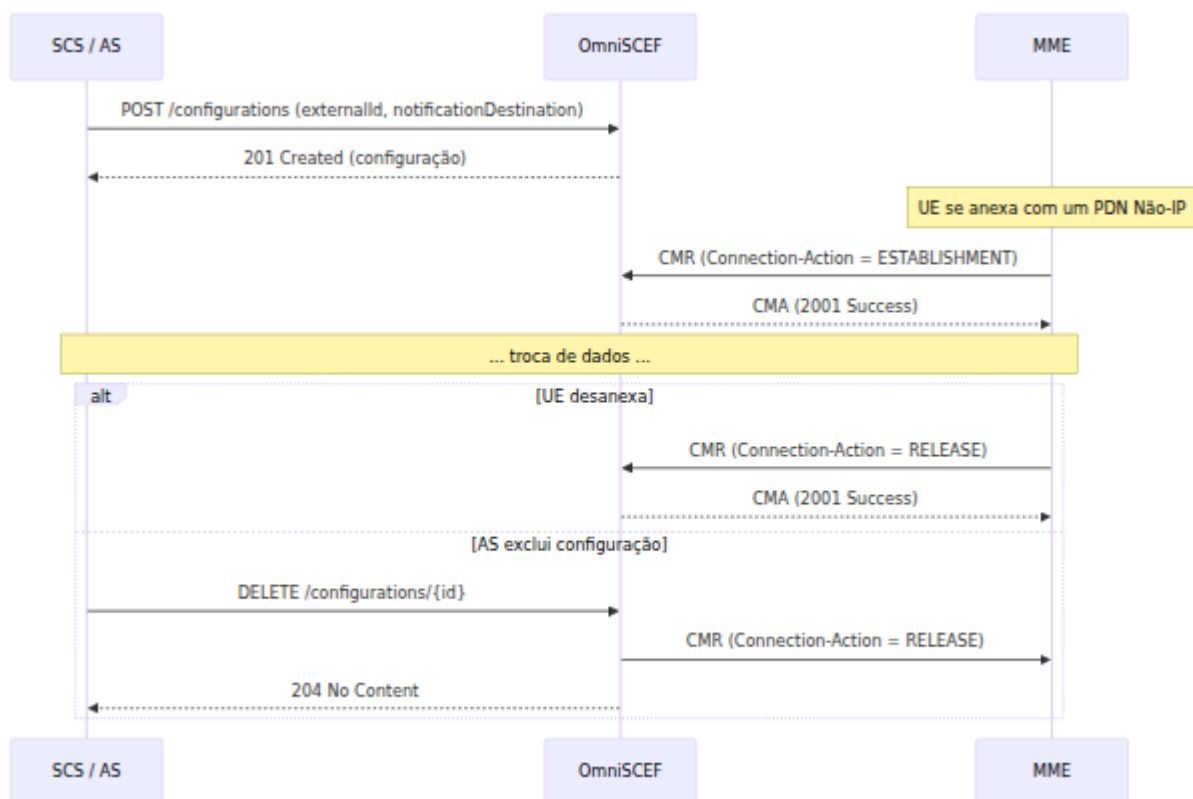


Quando o MME estabelece uma conexão para um assinante que **não** tem configuração NIDD, o OmniSCEF responde ao CMR com

DIAMETER_ERROR_USER_UNKNOWN (5001). O assinante não está provisionado para NIDD.

Dados Originados pelo Móvel (Uplink)

Os dados Não-IP enviados pelo UE chegam ao OmniSCEF como um **MO-Data-Request (ODR)** T6a. O OmniSCEF os entrega ao Servidor de Aplicação fazendo um POST de uma notificação para o callback da configuração, e responde ao MME com um **MO-Data-Answer (ODA)**.



Se o OmniSCEF não conseguir resolver a configuração ou o callback falhar, ele responde ao ODA com `DIAMETER_UNABLE_TO_COMPLY (5012)`.

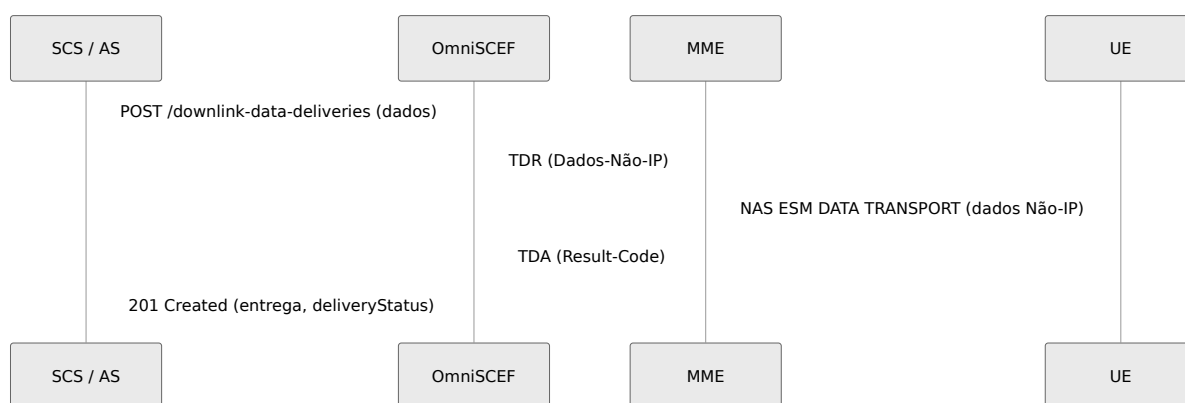
Exemplo de notificação de uplink (POSTada para o callback):

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

Campo	Descrição
<code>externalId</code> / <code>msisdn</code>	A identidade do dispositivo, conforme provisionada na configuração.
<code>data</code>	O payload Não-IP, codificado em base64.
<code>rdsSourcePort</code> / <code>rdsDestinationPort</code>	Presente quando o Serviço de Dados Confiável está habilitado.
<code>moExceptionDataCounter</code>	Presente quando o uplink foi sinalizado como dados de exceção MO .

Dados Terminados pelo Móvel (Downlink)

O Servidor de Aplicação envia dados Não-IP downlink fazendo um POST para a coleção `downlink-data-deliveries` da configuração. O OmniSCEF o encaminha para o MME como um **MT-Data-Request (TDR)** T6a, e registra o resultado (do **MT-Data-Answer, TDA**) em um recurso de entrega individual que o AS pode recuperar.



Quando o UE está ocioso, o MME armazena os dados e faz o paging do UE, respondendo ao TDA com sucesso uma vez que assumiu a responsabilidade pela entrega. O OmniSCEF reflete o resultado no `deliveryStatus` da entrega (veja **Valores de Status de Entrega**).

Exemplo de solicitação de downlink:

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

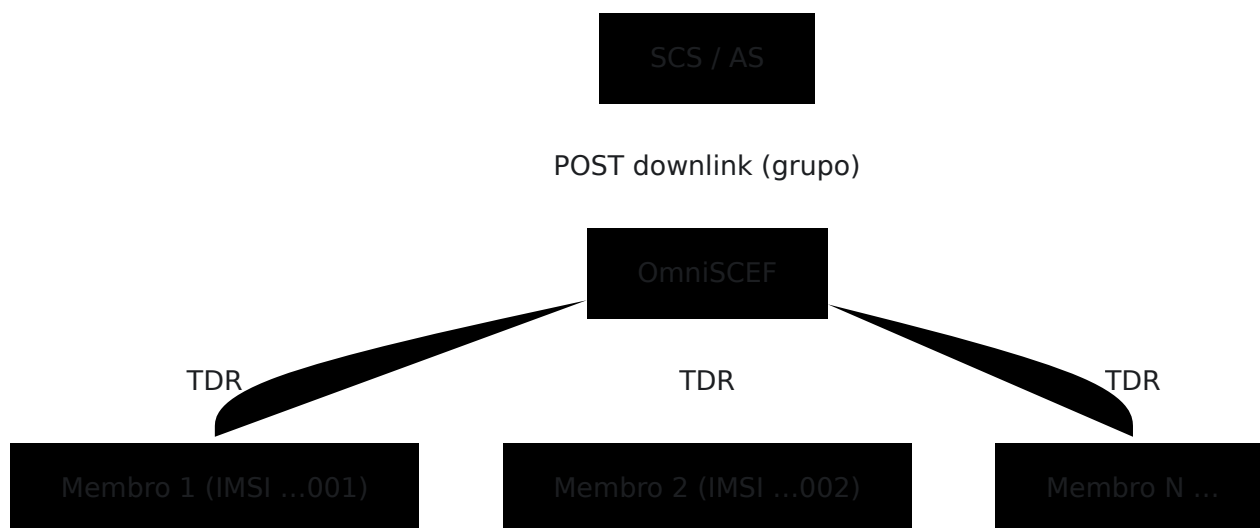
Campo	Descrição
<code>data</code>	O payload Não-IP a ser entregue, codificado em base64. Obrigatório.
<code>maximumLatency</code>	Opcional. Máximo atraso de buffer aceitável, em segundos.
<code>priority</code>	Opcional. Prioridade relativa entre as entregas enfileiradas.
<code>pdnEstablishmentOption</code>	Opcional. Comportamento quando nenhuma conexão existe. Veja Opções de Estabelecimento de PDN .
<code>rdsSourcePort</code> / <code>rdsDestinationPort</code>	Opcional. Portas RDS. Veja Serviço de Dados Confiável .

Exemplo de resposta de downlink:

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

Grupo NIDD

Uma configuração NIDD criada com um `externalGroupId` (em vez de um único `externalId/msisdn`) representa um **grupo** de dispositivos (TS 23.682 §5.13.3A). Uma única entrega downlink para uma configuração de grupo é **distribuída** para cada membro do grupo que tem uma conexão T6a ativa.



Os membros do grupo são resolvidos a partir do **mapa de grupos**. O `deliveryStatus` agregado da entrega reflete o **pior** resultado por membro, de modo que uma entrega em grupo só relata `SUCCESS` quando cada membro acessível foi atendido.

Serviço de Dados Confiável

O Serviço de Dados Confiável (RDS) multiplexa múltiplos fluxos de aplicação sobre uma única conexão Não-IP usando **números de porta**, conforme TS 23.682 §4.5.14.3. O RDS é habilitado por configuração ao definir `reliableDataService: true` quando a configuração é criada.

Quando o RDS está habilitado:

- **Downlink:** quando a entrega especifica `rdsDestinationPort` e `rdsSourcePort`, o OmniSCEF estrutura o payload Não-IP com um cabeçalho RDS que carrega essas portas antes de enviar o TDR.
- **Uplink:** o OmniSCEF analisa o cabeçalho RDS do payload ODR. Ele apresenta `rdsSourcePort` e `rdsDestinationPort` na notificação de uplink,

e entrega o payload interno como `data`.

As portas variam de 0 a 255. Quando o RDS não está habilitado, ou uma entrega omite as portas, o payload é transportado sem estrutura.

Dados de Exceção MO

Dispositivos NB-IoT podem sinalizar uma transmissão de uplink como **relato de exceção** (um relatório urgente, fora do padrão) via a causa de estabelecimento RRC, contada no `RRC-Cause-Counter` T6a (TS 23.682 §5.13.4). Quando o OmniSCEF vê essa indicação em um ODR, ele inclui um `moExceptionDataCounter` na notificação de uplink para que o Servidor de Aplicação possa priorizar o manuseio.

Referência de Recursos T8

NiddConfiguration

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

Campo	Tipo	Obrigatório	Descrição
<code>notificationDestination</code>	String (URI)	Sim	Callback que o AS re notificações de uplir status.
<code>externalId</code>	String	Condicional	Identificador Externo Dispositivo (<code>user@domain</code>). Um <code>externalId</code> , <code>msisd</code> <code>externalGroupId</code> .
<code>msisdn</code>	String	Condicional	MSISDN do dispositi
<code>externalGroupId</code>	String	Condicional	Identificador do grup para grupo NIDD .
<code>dnn</code>	String	Não	Nome da Rede de D APN da conexão Não
<code>pdnEstablishmentOption</code>	String (enum)	Não	Comportamento no downlink quando nenhuma conexão e Veja Opções de Estabelecimento de
<code>maximumPacketSize</code>	Inteiro	Não	Tamanho máximo do payload Não-IP em c (padrão para o <code>default_max_packet</code> configurado, 255).
<code>reliableDataService</code>	Booleano	Não	Habilitar Serviço de Confiável .
<code>mtcProviderId</code>	String	Não	Identificador do prov de serviço MTC.

Campo	Tipo	Obrigatório	Descrição
<code>validityTime</code>	String (data-hora)	Não	Quando a configuração expira.
<code>status</code>	String (enum)	Somente leitura	Status do ciclo de vida. Veja Valores de Status de Configuração .
<code>self</code>	String (URI)	Somente leitura	O próprio URI do recurso.

NiddDownlinkDataTransfer

Criado por `POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`. Os campos são descritos em [Dados Terminados pelo Móvel](#). Os campos `deliveryStatus` e `requestedRetransmissionTime` são somente leitura e definidos a partir do TDA.

Notificações

O OmniSCEF POSTa o seguinte para o `notificationDestination` da configuração:

Notificação	Quando
<code>NiddUplinkDataNotification</code>	Dados Não-IP de uplink chegaram (de um ODR).
<code>NiddDownlinkDataDeliveryStatusNotification</code>	O resultado de uma entrega downlink previamente aceita mudou (status assíncrono).

O Servidor de Aplicação reconhece cada notificação com `204 No Content`.

Valores de Referência

Valores de Status de Entrega

Valor	Significado
<code>SUCCESS</code>	O MME entregou os dados (ou assumiu a responsabilidade ao armazenar/paging um UE ocioso).
<code>SENDING</code>	A entrega está em andamento.
<code>BUFFERING</code>	O MME armazenou os dados para um UE ocioso.
<code>FAILURE_UE_NOT_REACHABLE</code>	O UE não pôde ser alcançado.
<code>FAILURE_REMOTE_FAILURE</code>	O MME / nó de serviço rejeitou ou falhou na solicitação.
<code>FAILURE</code>	A entrega falhou por outro motivo.

Opções de Estabelecimento de PDN

Valor	Comportamento quando nenhuma conexão existe no momento do downlink
WAIT_FOR_UE	Armazenar até que o UE estabeleça a conexão.
INDICATE_ERROR	Rejeitar a entrega imediatamente.
ESTABLISH_PDN_CONNECTION	Acionar o UE para estabelecer a conexão Não-IP.

Valores de Status de Configuração

Valor	Significado
ACTIVE	A configuração está autorizada e utilizável.
TERMINATED_UE_NOT_AUTHORIZED	O assinante não está autorizado para NIDD.
TERMINATED	A configuração expirou ou foi removida.

Solução de Problemas do OmniSCEF

Orientações sobre problemas operacionais comuns do OmniSCEF e suas resoluções. Para os fluxos subjacentes, consulte [NIDD](#) e [Eventos de Monitoramento](#); para parâmetros, veja a [Referência de Configuração](#).

Índice

- [MME Não Consegue Conectar Via T6a](#)
- [Conexão Rejeitada Com USER_UNKNOWN \(5001\)](#)
- [Falha na Entrega de Downlink](#)
- [Dados de Uplink Não Chegando ao Servidor de Aplicação](#)
- [Downlink de Grupo Não Alcança Dispositivos](#)
- [Relatórios de Monitoramento Não Entregues](#)
- [API T8 Retorna 404 para um Endpoint Válido](#)
- [Endpoint T8 Não Inicia](#)

MME Não Consegue Conectar Via T6a

Sintomas: O MME não consegue estabelecer uma conexão Diameter com o OmniSCEF; nenhuma troca de capacidades é concluída.

Causas possíveis:

- Firewall bloqueando a porta Diameter (padrão 3868).
- Incompatibilidade de transporte: o MME usa SCTP enquanto apenas TCP está acessível, ou vice-versa.
- A autorização do par está restrita e o MME não é um par configurado.

- Incompatibilidade de Origin-Host / realm entre o que o MME espera e o que o OmniSCEF anuncia.

Resolução:

1. Confirme se o firewall permite o `listen_port` configurado tanto em TCP quanto em SCTP. O OmniSCEF escuta em ambos. Veja [Listeners](#).
2. Verifique se o transporte configurado do MME corresponde. Os listeners de TCP e SCTP são sempre iniciados.
3. Se `allow_undefined_peers_to_connect` for `false`, adicione o MME a `peers` com seu exato Origin-Host. Veja [Peers](#).
4. Confirme se o `host` e o `realm` do OmniSCEF correspondem ao que o MME está provisionado para se comunicar. Verifique a saída de log `log_unauthorized_peer_connection_attempts` para tentativas rejeitadas.

Conexão Rejeitada Com USER_UNKNOWN (5001)

Sintomas: O MME estabelece a conexão Diameter, mas uma solicitação de conexão NIDD (CMR) é respondida com `DIAMETER_ERROR_USER_UNKNOWN (5001)`.

Causas possíveis:

- Nenhuma configuração NIDD existe para o IMSI desse assinante.
- O Servidor de Aplicação criou uma configuração usando uma identidade externa que não resolve para o IMSI do assinante.

Resolução:

1. Confirme se o Servidor de Aplicação criou uma configuração NIDD para o dispositivo antes de o UE se conectar.
2. Verifique se o `externalId/msisdn` do dispositivo resolve para o IMSI correto no [mapa de identidade](#).
3. Confirme se o IMSI no mapa de identidade corresponde ao IMSI que o MME apresenta no CMR.

Falha na Entrega de Downlink

Sintomas: Um `POST` para `downlink-data-deliveries` retorna uma entrega cujo `deliveryStatus` é um valor `FAILURE_*`, ou um `404`.

Causas possíveis:

- Nenhuma conexão T6a ativa existe para o dispositivo (`404 NIDD_CONFIGURATION_NOT_AVAILABLE`). O UE não se conectou, ou o OmniSCEF liberou sua conexão.
- O UE está inacessível (`FAILURE_UE_NOT_REACHABLE`).
- O MME / nó de serviço rejeitou a solicitação (`FAILURE_REMOTE_FAILURE`).
- O campo `data` está ausente ou não é um base64 válido (`400 DATA_MISSING`).

Resolução:

1. Confirme se o dispositivo está conectado e sua conexão está estabelecida (um CMR anterior foi aceito).
2. Verifique se o campo `data` está presente e codificado em base64.
3. Para um UE ocioso, espere que o MME faça buffer e pagine; a entrega relata sucesso uma vez que o MME assume a responsabilidade. Veja [Dados Terminados em Móvel](#).
4. Para `FAILURE_REMOTE_FAILURE`, inspecione o lado do MME/nó de serviço para a causa da rejeição.

Dados de Uplink Não Chegando ao Servidor de Aplicação

Sintomas: O UE envia dados de uplink, mas o callback do Servidor de Aplicação não é invocado.

Causas possíveis:

- O dispositivo não possui configuração NIDD (portanto, nenhum callback é conhecido).

- A URL `notificationDestination` é inacessível a partir do OmniSCEF, ou retorna um status não 2xx.
- Nenhum binding ativo existe para o `{IMSI, EBI}` apresentado no uplink.

Resolução:

1. Confirme se uma configuração NIDD existe para o dispositivo e possui um `notificationDestination` acessível.
2. Verifique a conectividade de rede do OmniSCEF para a URL de callback, incluindo a confiança TLS se for HTTPS.
3. Confirme se o callback retorna um status 2xx; um não 2xx é tratado como uma falha de entrega.
4. Confirme se o dispositivo se conectou (um CMR foi aceito) antes de enviar dados de uplink.

Downlink de Grupo Não Alcança Dispositivos

Sintomas: Um downlink para uma configuração de grupo retorna `404 NIDD_CONFIGURATION_NOT_AVAILABLE`, ou alcança menos dispositivos do que o esperado.

Causas possíveis:

- O `externalGroupId` não está presente no mapa de grupo, ou não mapeia para membros.
- Nenhum membro do grupo atualmente possui uma conexão T6a ativa.

Resolução:

1. Confirme se o `externalGroupId` está definido no **mapa de grupo** e lista os IMSIs dos membros esperados.
2. Confirme se pelo menos um dispositivo membro está conectado. Apenas membros com uma conexão ativa recebem a entrega. O status agregado reflete o pior resultado por membro. Veja **Grupo NIDD**.

Relatórios de Monitoramento Não Entregues

Sintomas: Uma assinatura de monitoramento é criada, mas o Servidor de Aplicação não recebe notificações.

Causas possíveis:

- O evento nunca foi armado na rede (nenhum destino de monitoramento configurado, e nenhum outro caminho o armou).
- O SCEF-Reference-ID do relatório não corresponde a uma assinatura ativa. Isso pode acontecer após uma reinicialização, porque o estado da assinatura está na memória.
- O `notificationDestination` da assinatura é inacessível.

Resolução:

1. Se o OmniSCEF deve armar o evento, configure um **destino de monitoramento** para que o CIR seja enviado.
2. Recrie assinaturas após uma reinicialização do OmniSCEF. O estado da assinatura e do reference-ID é volátil e não sobrevive a uma reinicialização.
3. Verifique a conectividade do OmniSCEF para o callback da assinatura.

API T8 Retorna 404 para um Endpoint Válido

Sintomas: Uma solicitação para um caminho T8 documentado retorna `404`, e o endpoint não aparece no documento OpenAPI em `/api/schema`.

Causas possíveis:

- A tabela de rotas foi alterada, mas a camada da API não foi recompilada, então a nova rota não está registrada.
- A solicitação omite o prefixo `/api` que todas as rotas T8 estão montadas.

Resolução:

1. Confirme se o caminho da solicitação inclui o prefixo `/api` (por exemplo, `/api/3gpp-nidd/v1/{scsAsId}/configurations`).
2. Se a **tabela de rotas** foi modificada, a dependência da API deve ser recompilada para que as novas rotas sejam registradas (`mix deps.compile api_ex --force`), e então o serviço deve ser reiniciado.

Endpoint T8 Não Inicia

Sintomas: O OmniSCEF falha ao iniciar o endpoint HTTPS T8.

Causas possíveis:

- O arquivo de certificado ou chave TLS está ausente ou ilegível.
- A `port` configurada já está em uso.

Resolução:

1. Confirme se `tls_cert_path` e `tls_key_path` apontam para arquivos PEM válidos e legíveis. Veja **Endpoint da API T8**.
2. Confirme se nada mais está vinculado à `port` configurada na interface `listen_ip`.
3. Para executar sem TLS em um ambiente controlado, defina `enable_tls: false`. Implementações de produção devem sempre encerrar o TLS em ou antes do OmniSCEF.

