Référence de configuration d'OmniSCEF

Ce document décrit chaque paramètre de configuration pour OmniSCEF. La configuration est répartie sur trois portées d'application :

Portée	Objectif
`:diameter_ex`	Le service Diameter **T6a** : identité, écouteurs, application et pairs.
`:api_ex`	Le point de terminaison API REST **T8** : TLS, adresse de liaison et table de routage.
`:omni_scef`	Comportement d'OmniSCEF : résolution d'identité, appartenance à un groupe et surveillance.

OmniSCEF évalue les paramètres du service Diameter au démarrage, de sorte que l'environnement peut les déterminer (voir Variables d'environnement). Le point de terminaison T8 et la table de routage sont fixes au moment de la construction.

Table des matières

- Service Diameter (T6a)
- Point de terminaison API T8
- Paramètres d'identité et de groupe
- Paramètres de surveillance
- Variables d'environnement

Service Diameter (T6a)

OmniSCEF termine T6a en tant que serveur Diameter. Le MME (ou un agent de routage Diameter) se connecte en entrant ; OmniSCEF écoute à la fois sur TCP et SCTP sur le port configuré.

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

    # Écouteurs (TCP et SCTP sont tous deux démarrés sur cette
adresse/port)
    listen_ip: "0.0.0.0",
    listen_port: 3868,

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

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

    # Gestionnaires internes (fixes - ne pas changer)
    control_module: OmniScef.Control.Diameter,
    processor_module: DiameterEx.Processor,

    # Enregistrement de l'application 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}
        ]
      }
    ],

    # Pairs 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
      }
    ]
  }
```

Identité du service

Paramètre	Type	Requis	Par défaut
`service_name`	Atome	Oui	`:omni_scef`
`host`	Chaîne	Oui	`scef01`
`realm`	Chaîne	Oui	`epc.mnc001.mcc001.3gppnetwork.org`
`product_name`	Chaîne	Non	`OmniSCEF`

Écouteurs

Paramètre	Type	Requis	Par défaut	Description
`listen_ip`	Chaîne	Non	`0.0.0.0`	Adresse IP à lier pour les connexions Diameter entrantes. Utilisez `0.0.0.0` pour toutes les interfaces.
`listen_port`	Entier	Non	3868	Port pour les connexions Diameter entrantes. Les écouteurs TCP et SCTP sont démarrés sur ce port. 3868 est le port Diameter standard selon RFC 6733.

Comportement

Paramètre	Type	Requis	Par défau
`request_timeout`	Entier	Non	5000
`peer_selection_algorithm`	Atome	Non	`:rand`

Paramètre	Type	Requis	Par défau
`allow_undefined_peers_to_connect`	Booléen	Non	`true`
`log_unauthorized_peer_connection_attempts`	Booléen	Non	`true`

Capacités Diameter

Paramètre	Type	Requis	Par défaut	Description
`vendor_id`	Entier	Non	10415	Vendor-Id annoncé dans les capacités. 10415 est 3GPP.
`supported_vendor_ids`	Liste d'entiers	Non	`[10415]`	Supported-Vendor-Ids annoncés dans les capacités.
`auth_application_ids`	Liste d'entiers	Non	`[]`	Identifiants d'application d'authentification de base (non spécifiques au fournisseur). Vide car T6a est enregistré en tant qu'application spécifique au fournisseur (voir `applications`).
`acct_application_ids`	Liste d'entiers	Non	`[]`	Identifiants d'application de comptabilité de base. Non utilisé par OmniSCEF.

Gestionnaires internes

Ceux-ci connectent la pile Diameter à la logique d'OmniSCEF. Ils sont fixes et ne doivent pas être modifiés.

Paramètre	Type	Requis	Par défaut	De
`control_module`	Module	Oui	`OmniScef.Control.Diameter`	Le qui req ent les dis aux ges NID sur
`processor_module`	Module	Oui	`DiameterEx.Processor`	Le pro de Dia inv mo cor

Application T6a

La liste `applications` enregistre l'application Diameter T6a. Ceci est fixe pour OmniSCEF.

Paramètres d'entrée de l'application :

Paramètre	Type	Requis	Par défaut
`application_name`	Atome	Oui	`:t6a`
`application_dictionary`	Atome	Oui	`:diameter_gen_3gp`
`vendor_specific_application_ids`	Liste de cartes	Oui	voir ci-dessous

Paramètres d'identifiant d'application spécifique au fournisseur :

Paramètre	Type	Requis	Par défaut	Description
`vendor_id`	Entier	Oui	10415	Identifiant de fournisseur 3GPP.
`auth_application_id`	Entier	Oui	16777346	L'Identifiant d'application T6a.
`acct_application_id`	Entier	Non	`nil`	Non utilisé pour T6a.

Pairs

La liste `peers` déclare les pairs Diameter connus (le MME, un DRA et le HSS). Le paramètre `allow_undefined_peers_to_connect` est par défaut `true` et le MME initie normalement la connexion. Vous pouvez laisser `peers` vide (`[]`) dans les déploiements où OmniSCEF ne compose rien en sortant. Listez un pair ici lorsque OmniSCEF doit **initier** la connexion, ou pour restreindre quels pairs peuvent se connecter.

Paramètres de pair :

Paramètre	Type	Requis	Par défaut	Descripti
`host`	Chaîne	Oui	-	Identité Diameter d pair (FQDN) Doit correspondr exactement l'Origin-Hos configuré d pair.
`realm`	Chaîne	Oui	-	Royaume Diameter d pair.
`ip`	Chaîne	Oui	-	Adresse IP d pair pour la connexion TCP/SCTP.
`port`	Entier	Non	3868	Port Diamet du pair.
`tls`	Booléen	Non	`false`	Indique si la connexion à pair utilise T
`transport`	Atome	Non	`:diameter_sctp`	Transport p ce pair : `:diameter_` ou `:diameter_`
`initiate_connection`	Booléen	Non	`false`	Lorsque `tru` OmniSCEF s connecte

Paramètre	Type	Requis	Par défaut	Descripti
				activement pair au démarrage. Lorsque `fa` OmniSCEF attend que pair se conn en entrant. un pair qui un MME composant SCEF, laisse ceci à `fals`

Point de terminaison API T8

L'API RESTful T8 est servie sur HTTPS. Tous les itinéraires sont montés sous le préfixe `/api`, donc le apiRoot effectif est `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: [ ... ]   # table de routage T8 fixe - voir ci-dessous
  }
```

Paramètres de point de terminaison

Paramètre	Type	Requis	Par défaut	Descrip
`port`	Entier	Non	8443	Port HTT pour l'AI
`listen_ip`	Chaîne	Non	`0.0.0.0`	Adresse lier pour T8. Utilis `0.0.0.0` pour tou les interface
`product_name`	Chaîne	Non	`OmniSCEF`	Nom du produit utilisé d les métador API/Ope
`title`	Chaîne	Non	`API T8 - OmniSCEF`	Titre affi dans le docume OpenAP généré e l'interfac Swagge
`hostname`	Chaîne	Non	`localhost`	Nom d'h utilisé lo la génér de l'URL point de terminai

Paramètre	Type	Requis	Par défaut	Descrip
`enable_tls`	Booléen	Non	`true`	Lorsque `true`, le point de terminai sert HTT en utilis certifica dessous
`tls_cert_path`	Chaîne	Oui (si TLS)	`priv/cert/omnitouch.crt`	Chemin le certifi TLS enc en PEM.
`tls_key_path`	Chaîne	Oui (si TLS)	`priv/cert/omnitouch.pem`	Chemin la clé pr TLS enc en PEM.
`routes`	Liste	Oui	fixe	La table routage C'est la définitio de la su API et n' pas régl par l'opérate Voir Tabl routage.

Table de routage

Les entrées `routes` définissent la surface API T8. Elles sont fixes pour OmniSCEF et produisent les points de terminaison ci-dessous (tous sous `/api`). Chaque entrée associe un modèle d'URL à un gestionnaire et à l'ensemble d'actions qu'il sert.

Paramètres d'entrée de route :

Paramètre	Type	Description
`path`	Chaîne	Le modèle d'URL. Des segments comme `:scsAsId` sont des variables de chemin.
`module`	Module	Le gestionnaire qui sert la route.
`parameters`	Chaîne ou `nil`	Le nom de la variable de chemin de ressource membre (par exemple, `configurationId`), ou `nil` pour les itinéraires uniquement de collection.
`actions`	Liste d'Atome	Les actions HTTP servies : `:index` (GET collection), `:create` (POST), `:show` (GET membre), `:update` (PUT/PATCH membre), `:delete` (DELETE membre).

Points de terminaison résultants :

Méthode & Chemin	Obj
`GET /api/status`	Vivacit service identit
`GET /api/3gpp-nidd/v1/{scsAsId}/configurations`	Lister l configu NIDD.
`POST /api/3gpp-nidd/v1/{scsAsId}/configurations`	Créer u configu NIDD.
`GET/PUT/PATCH/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}`	Lire / rempla supprir une configu NIDD.
`GET/POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`	Lister / envoye donnée descer
`GET/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries/{downlinkDataDeliveryId}`	Lire l'é annule livraisc descer
`GET/POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`	Lister / des abonne de surveil

Méthode & Chemin	Obj
`GET/PUT/DELETE /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}`	Lire / rempla supprir abonne de surveil

Le document OpenAPI généré est disponible à `GET /api/schema`, et une interface Swagger interactive à `GET /api/docs`.

> **Authentification par clé partagée optionnelle.** Le point de terminaison T8 prend en charge une vérification par clé partagée optionnelle sur les requêtes entrantes. Elle est désactivée à moins qu'une clé `auth` ne soit ajoutée sous `config :api_ex, :api`. Lorsqu'elle n'est pas définie (la valeur par défaut), aucune vérification par clé partagée n'est appliquée et le point de terminaison doit être protégé par des contrôles réseau (par exemple, un interconnexion privée ou un proxy inverse).

Paramètres d'identité et de groupe

OmniSCEF résout l'identité côté AS (Identifiant externe ou MSISDN) vers l'IMSI réseau, et résout un identifiant de groupe vers ses IMSIs membres. Dans la première version, ce sont des cartes d'opérateur statiques.

```
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
  }
```

Paramètre	Type	Requis	Par défaut	Description
`identity_map`	Carte	Non	`%{}`	Mappe un Identifiant externe (`user@domain`) **ou** un MSISDN à un IMSI d'abonné. Utilisé lorsque l'AS crée une configuration NIDD à UE unique ou un abonnement de surveillance. Une identité non présente ici est rejetée comme UE inconnu.
`group_map`	Carte	Non	`%{}`	Mappe un `externalGroupId` la liste des IMSIs membres. Utilisé pour la livraison NIDD de groupe.
`default_max_packet_size`	Entier	Non	255	La taille maximale par défaut de la charge utile Non-IP en octets, appliqué à une configuratio NIDD qui ne spécif pas `maximumPacketSiz` Le transport NAS limite un seul

Paramètre	Type	Requis	Par défaut	Description
				message Non-IP à 255 octets.

> En production, ces cartes sont généralement soutenues par une recherche HSS/UDR plutôt que par une configuration statique. Le comportement côté AS reste inchangé.

Paramètres de surveillance

Optionnel. Lorsque vous configurez une destination de surveillance, la création d'un abonnement de surveillance arme l'événement vers le sud. OmniSCEF envoie une Configuration-Information-Request (CIR) à ce nœud. Lorsque vous ne définissez pas de destination, OmniSCEF stocke toujours les abonnements et livre toujours les rapports entrants. Dans ce cas, OmniSCEF n'envoie pas proactivement le CIR.

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

Paramètres de `destination` :

Paramètre	Type	Requis	Par défaut	Description
`host`	Chaîne	Non	-	Identité Diameter (FQDN) du HSS / nœud de service auquel les demandes de configuration de surveillance sont envoyées. Lorsqu'il est omis, la demande est routée uniquement par royaume.
`realm`	Chaîne	Oui (si `destination` défini)	-	Royaume Diameter utilisé comme Destination-Realm du CIR de surveillance.

Variables d'environnement

L'identité du service Diameter et les écouteurs peuvent être fournis par l'environnement au démarrage. Ceux-ci remplacent les valeurs par défaut indiquées sous Service Diameter.

Variable	Correspond à	Par défaut
`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`

Surveillance des Événements

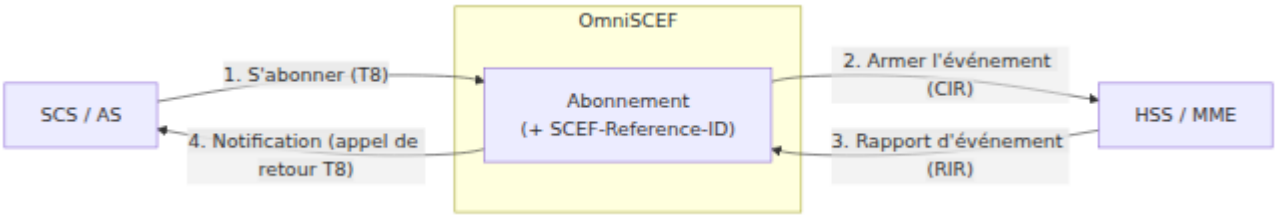
Le service de Surveillance des Événements permet à un Serveur d'Application de s'abonner aux événements réseau concernant un appareil ou un groupe : accessibilité, perte de connectivité, localisation, statut de roaming, et plus encore. Le Serveur d'Application s'abonne via **T8**. OmniSCEF arme l'événement dans le réseau via **T6a** et renvoie chaque rapport au rappel de l'abonné.

Les événements de surveillance sont définis dans 3GPP TS 23.682 §5.6, l'API T8 dans TS 29.122 §5.3, et les procédures Diameter dans TS 29.128 / TS 29.336.

Table des Matières

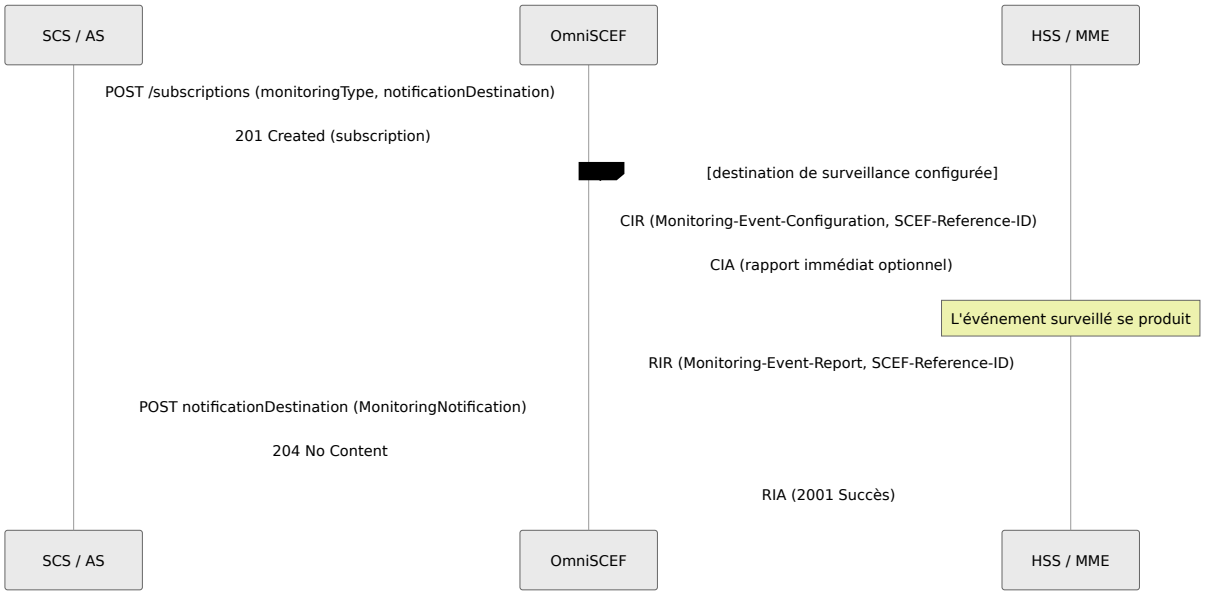
- Aperçu
- Flux d'Abonnement et de Rapport
- Référence des Ressources T8
- Types de Surveillance
- Valeurs de Référence

Aperçu



OmniSCEF attribue à chaque abonnement un **SCEF-Reference-ID**. Cet identifiant unique est utilisé dans la configuration sud et le réseau le renvoie dans chaque rapport. OmniSCEF l'utilise pour acheminer un rapport entrant vers le bon abonnement et son rappel de Serveur d'Application.

Flux d'Abonnement et de Rapport



L'armement est optionnel au SCEF. Lorsque vous configurez une destination de surveillance, OmniSCEF envoie le CIR pour armer l'événement. Lorsque vous n'en configurez pas, OmniSCEF crée toujours l'abonnement et livre tout rapport entrant. Dans ce cas, OmniSCEF n'envoie pas proactivement le CIR (par exemple, lorsque un autre chemin arme l'événement via le HSS).

Lorsque l'SCEF-Reference-ID d'un rapport ne correspond à aucun abonnement, OmniSCEF l'accuse réception avec un RIA mais ne le transfère pas.

Référence des Ressources T8

MonitoringEventSubscription

Créé par `POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`.

Champ	Type	Requis	Description
`notificationDestination`	String (URI)	Oui	Rappel sur lequel le AS reçoit des rapports de surveillance.
`monitoringType`	String (enum)	Oui	L'événement à surveiller. Voir Types de Surveillance.
`externalId`	String	Conditionnel	Identifiant Externe de l'Appareil. Un des `externalId`, `msisdn`, ou `externalGroupId`.
`msisdn`	String	Conditionnel	MSISDN de l'Appareil.
`externalGroupId`	String	Conditionnel	Identifiant de groupe pour la surveillance de groupe.
`maximumNumberOfReports`	Integer	Non	Arrêter après ce nombre de rapports.
`monitoringDuration`	String (date-time)	Non	Arrêter la surveillance ce moment.
`reachabilityType`	String (enum)	Non	Pour `UE_REACHABILITY` `SMS` ou `DATA`.
`maximumDetectionTime`	Integer	Non	Pour `LOSS_OF_CONNECTIVITY` temps de détection en secondes.

Champ	Type	Requis	Description
`mtcProviderId`	String	Non	Identifiant du fournisseur de service MTC.
`self`	String (URI)	Lecture seule	L'URI de l'abonnement

Exemple de demande d'abonnement :

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

MonitoringNotification

OmniSCEF POSTe un `MonitoringNotification` à la `notificationDestination` de l'abonnement pour chaque rapport. Il fait référence à l'abonnement d'origine et contient un ou plusieurs rapports d'événements décodés.

Exemple de notification :

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

Le Serveur d'Application accuse réception avec `204 No Content`.

Types de Surveillance

OmniSCEF prend en charge l'ensemble complet des types de surveillance TS 29.122. Chacun correspond à la valeur `Monitoring-Type` correspondante sur l'interface Diameter (TS 29.336 §5.3.9).

`monitoringType` (T8)	Valeur Diameter	Description
`LOSS_OF_CONNECTIVITY`	0	L'UE n'est plus accessible pour les données.
`UE_REACHABILITY`	1	L'UE est devenu accessible pour les SMS ou les données.
`LOCATION_REPORTING`	2	La localisation de l'UE (ou un changement) est rapportée.
`CHANGE_OF_IMSI_IMEI_ASSOCIATION`	3	L'IMEI associé à l'IMSI a changé.
`ROAMING_STATUS`	4	Le statut de roaming de l'UE (ou un changement) est rapporté.
`COMMUNICATION_FAILURE`	5	Un événement de défaillance de communication s'est produit.
`AVAILABILITY_AFTER_DDN_FAILURE`	6	L'UE est devenu disponible après un échec de notification de données descendantes.
`NUMBER_OF_UES_IN_AN_AREA`	7	Compte des UEs présentes dans une zone donnée.

`monitoringType` (T8)	Valeur Diameter	Description
`PDN_CONNECTIVITY_STATUS`	8	Connexion PDN établie/libérée.
`DOWNLINK_DATA_DELIVERY_STATUS`	9	Statut de la livraison de données descendantes.
`API_SUPPORT_CAPABILITY`	10	Rapport sur la capacité de support API.

Un abonnement avec un `monitoringType` non pris en charge est rejeté avec `400 INVALID_MONITORING_TYPE`.

Valeurs de Référence

Type d'Accessibilité

Valeur	Signification
`SMS`	L'UE est accessible pour les SMS.
`DATA`	L'UE est accessible pour les données.

Commandes Diameter Associées

Voir les tables de référence du Guide des Opérations pour les codes de commande et de résultat CIR/CIA et RIR/RIA.

Livraison de données Non-IP (NIDD)

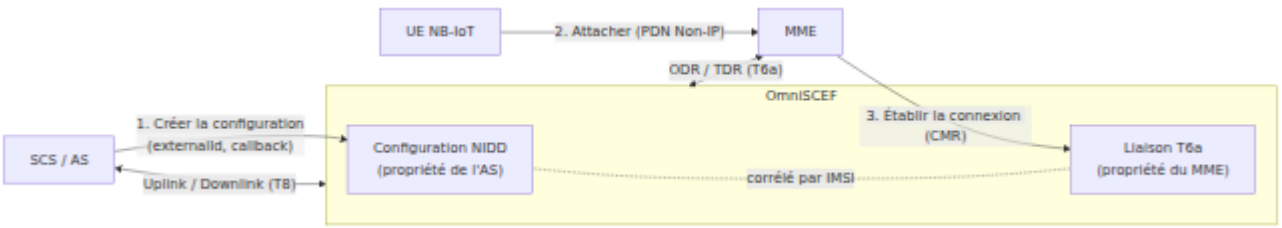
La livraison de données Non-IP permet à un appareil Cellular-IoT / NB-IoT d'échanger de petits messages **Non-IP** avec un serveur d'application **sans adresse IP**. Les données circulent sur le plan de signalisation NAS (l'optimisation CIoT EPS du plan de contrôle) entre l'UE et le MME. Le MME les relaie à OmniSCEF via **T6a**. OmniSCEF les expose ensuite au serveur d'application via **T8**.

L'architecture et les procédures NIDD sont définies dans 3GPP TS 23.682 §5.13; l'interface Diameter T6a dans TS 29.128; et l'API NIDD T8 dans TS 29.122.

Table des matières

- Aperçu
- Cycle de vie de la connexion
- Données d'origine mobile
- Données terminées mobiles
- Groupe NIDD
- Service de données fiable
- Données d'exception MO
- Référence de ressource T8
- Valeurs de référence

Aperçu



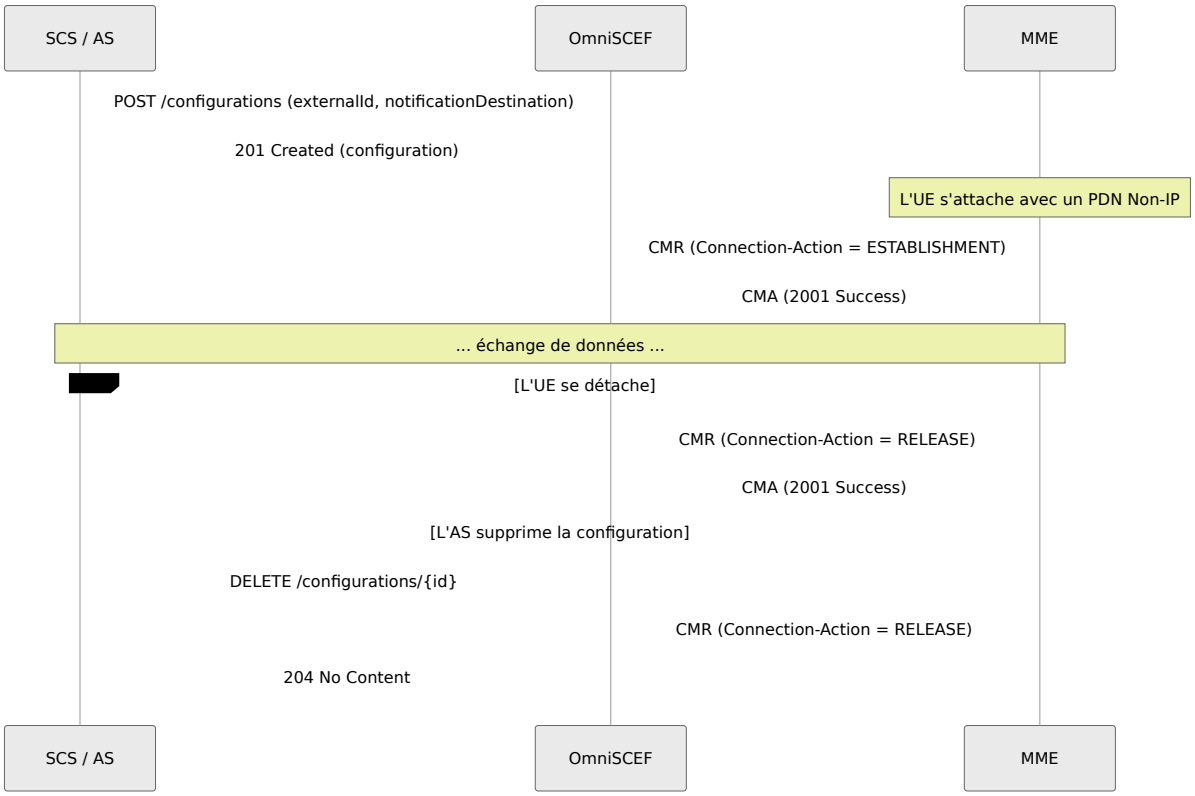
Une session NIDD a deux moitiés corrélées :

- La **Configuration NIDD** est créée par le serveur d'application via T8. Elle nomme l'appareil (par Identifiant Externe, MSISDN ou groupe), le callback de notification et les options NIDD.
- La **Liaison T6a** est créée lorsque le MME établit la connexion Non-IP pour cet abonné. Elle lie la session Diameter et l'identité du MME au `{IMSI, EBI}` utilisé pour atteindre l'UE.

OmniSCEF corrèle les deux par l'identité de l'abonné, de sorte que les données uplink trouvent le bon callback de l'AS et que les données downlink trouvent la bonne connexion active.

Cycle de vie de la connexion

Le MME gère la connexion T6a lorsque l'UE s'attache et se détache. Le serveur d'application peut également mettre fin à une connexion en supprimant sa configuration NIDD.

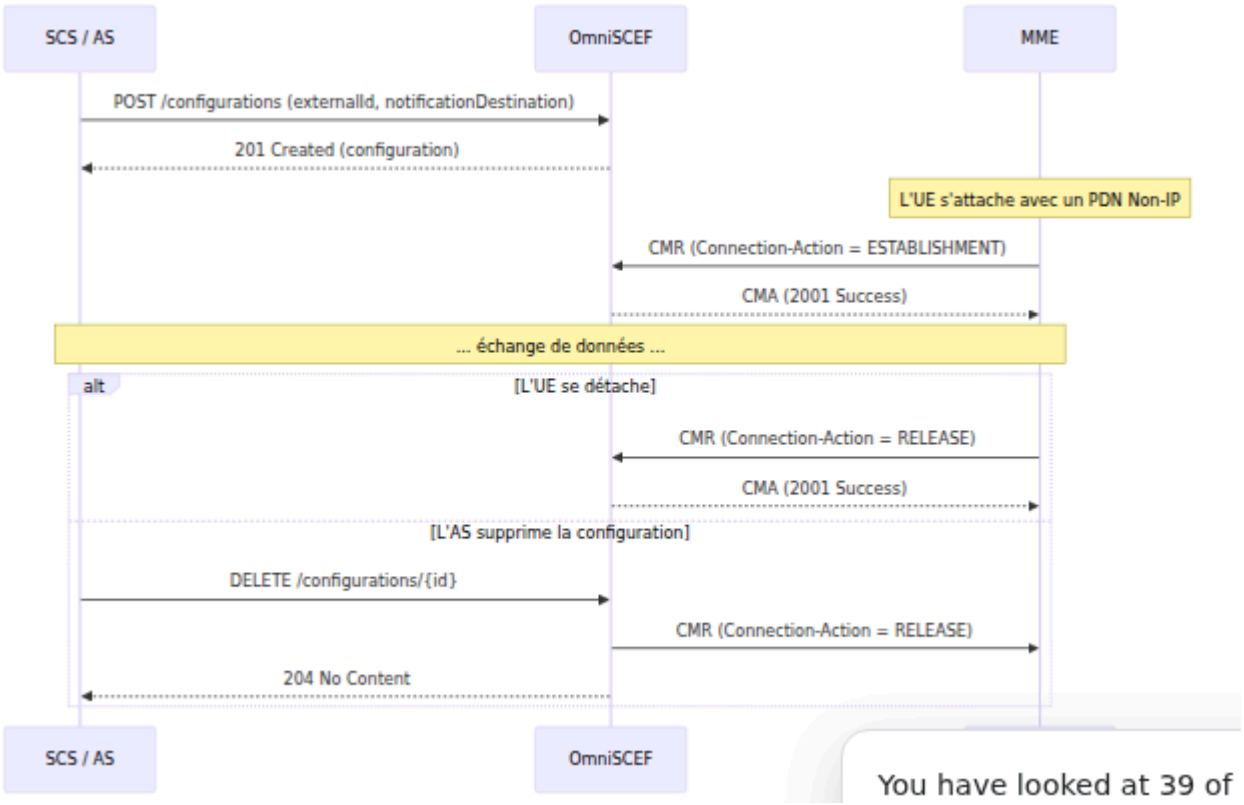


Lorsque le MME établit une connexion pour un abonné qui **n'a pas** de configuration NIDD, OmniSCEF répond au CMR avec

`DIAMETER_ERROR_USER_UNKNOWN (5001)`. L'abonné n'est pas provisionné pour NIDD.

Données d'origine mobile (Uplink)

Les données Non-IP uplink envoyées par l'UE arrivent à OmniSCEF sous la forme d'une **MO-Data-Request (ODR)** T6a. OmniSCEF les livre au serveur d'application en POSTant une notification au callback de la configuration, et répond au MME avec un **MO-Data-Answer (ODA)**.



Si OmniSCEF ne peut pas résoudre la configuration ou si le callback échoue, il répond à l'ODA avec `DIAMETER_UNABLE_TO_COMPLY (5012)`.

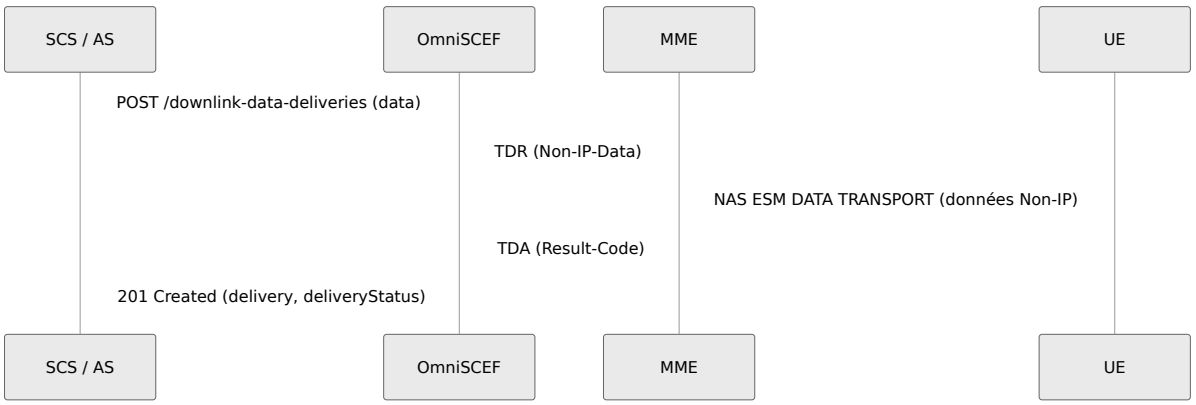
Exemple de notification uplink (POSTée au callback) :

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

Champ	Description
`externalId` / `msisdn`	L'identité de l'appareil, telle que provisionnée dans la configuration.
`data`	La charge utile Non-IP, encodée en base64.
`rdsSourcePort` / `rdsDestinationPort`	Présent lorsque le Service de données fiable est activé.
`moExceptionDataCounter`	Présent lorsque l'uplink a été signalé comme données d'exception MO.

Données terminées mobiles (Downlink)

Le serveur d'application envoie des données Non-IP downlink en POSTant à la collection `downlink-data-deliveries` de la configuration. OmniSCEF les transfère au MME sous la forme d'une **MT-Data-Request (TDR)** T6a, et enregistre le résultat (provenant de la **MT-Data-Answer, TDA**) sur une ressource de livraison individuelle que l'AS peut récupérer.



Lorsque l'UE est inactif, le MME met en mémoire tampon les données et page l'UE, répondant au TDA avec succès une fois qu'il a pris la responsabilité de la livraison. OmniSCEF reflète le résultat dans le `deliveryStatus` de la livraison (voir Valeurs de statut de livraison).

Exemple de demande downlink :

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

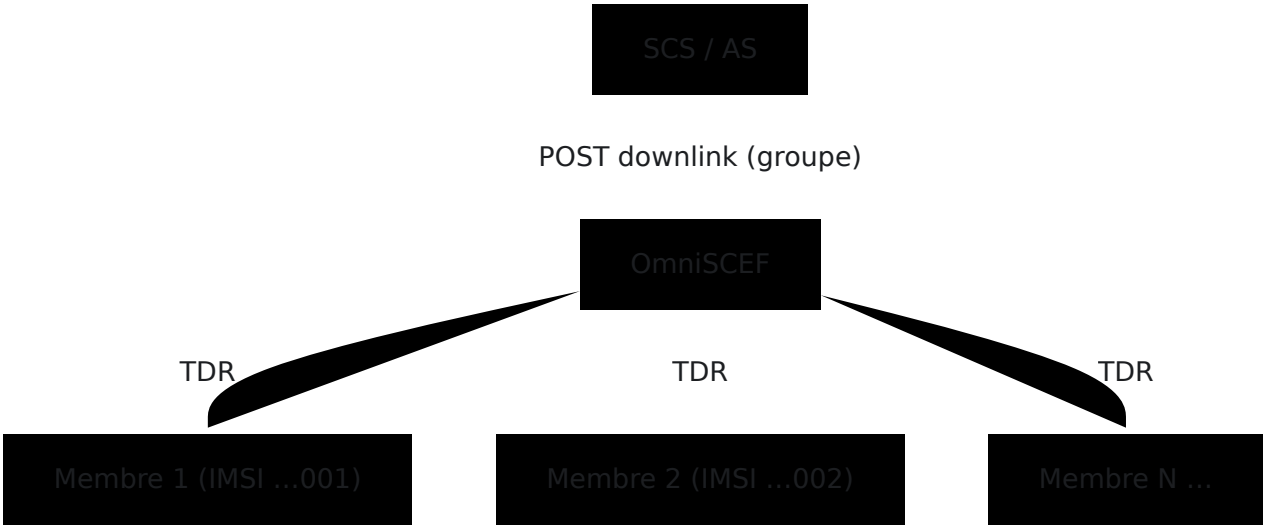
Champ	Description
`data`	La charge utile Non-IP à livrer, encodée en base64. Requis.
`maximumLatency`	Optionnel. Délai de mise en mémoire tampon maximal acceptable, en secondes.
`priority`	Optionnel. Priorité relative parmi les livraisons en attente.
`pdnEstablishmentOption`	Optionnel. Comportement lorsque aucune connexion n'existe. Voir Options d'établissement PDN.
`rdsSourcePort` / `rdsDestinationPort`	Optionnel. Ports RDS. Voir Service de données fiable.

Exemple de réponse downlink :

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

Groupe NIDD

Une configuration NIDD créée avec un `externalGroupId` (au lieu d'un seul `externalId`/`msisdn`) représente un **groupe** d'appareils (TS 23.682 §5.13.3A). Une seule livraison downlink à une configuration de groupe est **répartie** à chaque membre du groupe qui a une connexion T6a active.



Les membres du groupe sont résolus à partir de la carte de groupe. Le `deliveryStatus` agrégé de la livraison reflète le **pire** résultat par membre, donc une livraison de groupe ne rapporte `SUCCESS` que lorsque chaque membre accessible a été servi.

Service de données fiable

Le Service de données fiable (RDS) multiplexe plusieurs flux d'application sur une seule connexion Non-IP en utilisant **des numéros de port**, selon TS 23.682 §4.5.14.3. Le RDS est activé par configuration en définissant `reliableDataService: true` lors de la création de la configuration.

Lorsque le RDS est activé :

- **Downlink** : lorsque la livraison spécifie `rdsDestinationPort` et `rdsSourcePort`, OmniSCEF encadre la charge utile Non-IP avec un en-tête RDS qui porte ces ports avant d'envoyer le TDR.
- **Uplink** : OmniSCEF analyse l'en-tête RDS à partir de la charge utile ODR. Il fait remonter `rdsSourcePort` et `rdsDestinationPort` sur la notification

uplink, et livre la charge utile interne en tant que `data`.

Les ports sont de 0 à 255. Lorsque le RDS n'est pas activé, ou qu'une livraison omet les ports, la charge utile est transportée sans encadrement.

Données d'exception MO

Les appareils NB-IoT peuvent signaler une transmission uplink comme **rapport d'exception** (un rapport urgent, hors norme) via la cause d'établissement RRC, comptée dans le `RRC-Cause-Counter` T6a (TS 23.682 §5.13.4). Lorsque OmniSCEF voit cette indication sur un ODR, il inclut un `moExceptionDataCounter` sur la notification uplink afin que le serveur d'application puisse prioriser le traitement.

Référence de ressource T8

NiddConfiguration

Créée par `POST /api/3gpp-nidd/v1/{scsAsId}/configurations`.

Champ	Type	Requis	Description
`notificationDestination`	String (URI)	Oui	Callback sur lequel l'A reçoit les notifications uplink et de statut.
`externalId`	String	Conditionnel	Identifiant Externe de l'appareil (`user@domai` Un des `externalId`, `msisdn`, ou `externalGroupId`.
`msisdn`	String	Conditionnel	MSISDN de l'appareil.
`externalGroupId`	String	Conditionnel	Identifiant de groupe groupe NIDD.
`dnn`	String	Non	Nom de réseau de données / APN de la connexion Non-IP.
`pdnEstablishmentOption`	String (enum)	Non	Comportement en downlink lorsque aucu connexion n'existe. Vo Options d'établisseme PDN.
`maximumPacketSize`	Integer	Non	Taille maximale de la charge utile Non-IP en octets (par défaut à la `default_max_packet_` configurée, 255).
`reliableDataService`	Boolean	Non	Activer le Service de données fiable.

Champ	Type	Requis	Description
`mtcProviderId`	String	Non	Identifiant du fourniss de service MTC.
`validityTime`	String (date-heure)	Non	Quand la configuratio expire.
`status`	String (enum)	Lecture seule	Statut du cycle de vie Valeurs de statut de configuration.
`self`	String (URI)	Lecture seule	L'URI de la ressource même.

NiddDownlinkDataTransfer

Créé par `POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`. Les champs sont décrits sous Données terminées mobiles. Les champs `deliveryStatus` et `requestedRetransmissionTime` sont en lecture seule et définis à partir du TDA.

Notifications

OmniSCEF POSTe les éléments suivants à `notificationDestination` de la configuration :

Notification	Quand
`NiddUplinkDataNotification`	Des données Non-IP uplink sont arrivées (d'un ODR).
`NiddDownlinkDataDeliveryStatusNotification`	Le résultat d'une livraison downlink précédemment acceptée a changé (statut asynchrone).

Le serveur d'application accuse réception de chaque notification avec `204 No Content`.

Valeurs de référence

Valeurs de statut de livraison

Valeur	Signification
`SUCCESS`	Le MME a livré les données (ou a pris la responsabilité en mettant en mémoire tampon/pagant un UE inactif).
`SENDING`	La livraison est en cours.
`BUFFERING`	Le MME a mis en mémoire tampon les données pour un UE inactif.
`FAILURE_UE_NOT_REACHABLE`	L'UE n'a pas pu être atteint.
`FAILURE_REMOTE_FAILURE`	Le MME / nœud de service a rejeté ou échoué à la demande.
`FAILURE`	La livraison a échoué pour une autre raison.

Options d'établissement PDN

Valeur	Comportement lorsque aucune connexion n'existe au moment du downlink
`WAIT_FOR_UE`	Mettre en mémoire tampon jusqu'à ce que l'UE établisse la connexion.
`INDICATE_ERROR`	Rejeter immédiatement la livraison.
`ESTABLISH_PDN_CONNECTION`	Déclencher l'UE pour établir la connexion Non-IP.

Valeurs de statut de configuration

Valeur	Signification
`ACTIVE`	La configuration est autorisée et utilisable.
`TERMINATED_UE_NOT_AUTHORIZED`	L'abonné n'est pas autorisé pour NIDD.
`TERMINATED`	La configuration a expiré ou a été supprimée.

Dépannage d'OmniSCEF

Guide de résolution des problèmes pour les problèmes opérationnels courants d'OmniSCEF. Pour les flux sous-jacents, voir NIDD et Événements de surveillance ; pour les paramètres, voir la Référence de configuration.

Table des matières

- MME ne peut pas se connecter via T6a
- Connexion rejetée avec USER_UNKNOWN (5001)
- Échec de la livraison descendante
- Les données montantes n'atteignent pas le serveur d'application
- Le groupe descendant n'atteint aucun appareil
- Les rapports de surveillance ne sont pas livrés
- L'API T8 renvoie 404 pour un point de terminaison valide
- Le point de terminaison T8 ne démarre pas

MME ne peut pas se connecter via T6a

Symptômes : Le MME ne peut pas établir une connexion Diameter avec OmniSCEF ; aucun échange de capacités n'est terminé.

Causes possibles :

- Pare-feu bloquant le port Diameter (par défaut 3868).
- Incompatibilité de transport : le MME utilise SCTP tandis que seul TCP est accessible, ou vice versa.
- L'autorisation du pair est restreinte et le MME n'est pas un pair configuré.

- Mismatch entre l'Origin-Host / le domaine attendu par le MME et ce qu'OmniSCEF annonce.

Résolution :

1. Confirmer que le pare-feu autorise le `listen_port` configuré à la fois sur TCP et SCTP. OmniSCEF écoute sur les deux. Voir Listeners.
2. Vérifier que le transport configuré du MME correspond. Les écouteurs TCP et SCTP sont toujours démarrés.
3. Si `allow_undefined_peers_to_connect` est `false`, ajouter le MME à `peers` avec son exact Origin-Host. Voir Peers.
4. Confirmer que `host` et `realm` d'OmniSCEF correspondent à ce que le MME est provisionné pour communiquer. Vérifier la sortie du journal `log_unauthorized_peer_connection_attempts` pour les tentatives rejetées.

Connexion rejetée avec USER_UNKNOWN (5001)

Symptômes : Le MME établit la connexion Diameter, mais une demande de connexion NIDD (CMR) est répondue par `DIAMETER_ERROR_USER_UNKNOWN (5001)`.

Causes possibles :

- Aucune configuration NIDD n'existe pour l'IMSI de cet abonné.
- Le serveur d'application a créé une configuration utilisant une identité externe qui ne correspond pas à l'IMSI de l'abonné.

Résolution :

1. Confirmer que le serveur d'application a créé une configuration NIDD pour l'appareil avant que l'UE ne s'attache.
2. Vérifier que `externalId`/`msisdn` de l'appareil correspond à l'IMSI correct dans la carte d'identité.
3. Confirmer que l'IMSI dans la carte d'identité correspond à l'IMSI que le MME présente dans le CMR.

Échec de la livraison descendante

Symptômes : Un `POST` à `downlink-data-deliveries` renvoie une livraison dont le `deliveryStatus` est un valeur `FAILURE_*`, ou un `404`.

Causes possibles :

- Aucune connexion T6a active n'existe pour l'appareil (`404 NIDD_CONFIGURATION_NOT_AVAILABLE`). L'UE ne s'est pas attachée, ou OmniSCEF a libéré sa connexion.
- L'UE est injoignable (`FAILURE_UE_NOT_REACHABLE`).
- Le MME / nœud de service a rejeté la demande (`FAILURE_REMOTE_FAILURE`).
- Le champ `data` est manquant ou non valide base64 (`400 DATA_MISSING`).

Résolution :

1. Confirmer que l'appareil est attaché et que sa connexion est établie (un CMR précédent a été accepté).
2. Vérifier que le champ `data` est présent et encodé en base64.
3. Pour une UE inactive, s'attendre à ce que le MME tamponne et page ; la livraison rapporte le succès une fois que le MME prend la responsabilité. Voir Données mobiles terminées.
4. Pour `FAILURE_REMOTE_FAILURE`, inspecter le côté MME/nœud de service pour la cause du rejet.

Les données montantes n'atteignent pas le serveur d'application

Symptômes : L'UE envoie des données montantes, mais le rappel du serveur d'application n'est pas invoqué.

Causes possibles :

- L'appareil n'a pas de configuration NIDD (donc aucun rappel n'est connu).

- L'URL `notificationDestination` est injoignable depuis OmniSCEF, ou renvoie un statut non-2xx.
- Aucune liaison active n'existe pour le `{IMSI, EBI}` présenté sur le lien montant.

Résolution :

1. Confirmer qu'une configuration NIDD existe pour l'appareil et contient un `notificationDestination` accessible.
2. Vérifier la connectivité réseau d'OmniSCEF à l'URL de rappel, y compris la confiance TLS si c'est HTTPS.
3. Confirmer que le rappel renvoie un statut 2xx ; un non-2xx est traité comme un échec de livraison.
4. Confirmer que l'appareil s'est attaché (un CMR a été accepté) avant d'envoyer des données montantes.

Le groupe descendant n'atteint aucun appareil

Symptômes : Une livraison descendante à une configuration de groupe renvoie `404 NIDD_CONFIGURATION_NOT_AVAILABLE`, ou atteint moins d'appareils que prévu.

Causes possibles :

- L'`externalGroupId` n'est pas présent dans la carte de groupe, ou ne correspond à aucun membre.
- Aucun membre du groupe n'a actuellement une connexion T6a active.

Résolution :

1. Confirmer que l'`externalGroupId` est défini dans la carte de groupe et liste les IMSI des membres attendus.
2. Confirmer qu'au moins un appareil membre est attaché. Seuls les membres avec une connexion active reçoivent la livraison. L'état agrégé reflète le pire résultat par membre. Voir Groupe NIDD.

Les rapports de surveillance ne sont pas livrés

Symptômes : Une souscription de surveillance est créée, mais le serveur d'application ne reçoit aucune notification.

Causes possibles :

- L'événement n'a jamais été armé dans le réseau (aucune destination de surveillance configurée, et aucun autre chemin ne l'a armé).
- L'ID de référence SCEF du rapport ne correspond pas à une souscription active. Cela peut se produire après un redémarrage, car l'état de la souscription est en mémoire.
- La `notificationDestination` de la souscription est injoignable.

Résolution :

1. Si OmniSCEF doit armer l'événement, configurer une destination de surveillance afin que le CIR soit envoyé.
2. Recréer les souscriptions après un redémarrage d'OmniSCEF. L'état de la souscription et de l'ID de référence est volatile et ne survit pas à un redémarrage.
3. Vérifier la connectivité d'OmniSCEF au rappel de souscription.

L'API T8 renvoie 404 pour un point de terminaison valide

Symptômes : Une demande à un chemin T8 documenté renvoie `404`, et le point de terminaison n'apparaît pas dans le document OpenAPI à `/api/schema`.

Causes possibles :

- La table de routage a été modifiée mais la couche API n'a pas été recompilée, donc le nouveau chemin n'est pas enregistré.
- La demande omet le préfixe `/api` sous lequel toutes les routes T8 sont montées.

Résolution :

1. Confirmer que le chemin de la demande inclut le préfixe `/api` (par exemple, `/api/3gpp-nidd/v1/{scsAsId}/configurations`).
2. Si la table de routage a été modifi��e, la dépendance API doit être recompilée afin que les nouveaux chemins s'enregistrent (`mix deps.compile api_ex --force`), puis le service redémarré.

Le point de terminaison T8 ne démarre pas

Symptômes : OmniSCEF échoue à démarrer le point de terminaison HTTPS T8.

Causes possibles :

- Le certificat TLS ou le fichier de clé est manquant ou illisible.
- Le `port` configuré est déjà utilisé.

Résolution :

1. Confirmer que `tls_cert_path` et `tls_key_path` pointent vers des fichiers PEM valides et lisibles. Voir Point de terminaison API T8.
2. Confirmer que rien d'autre n'est lié au `port` configuré sur l'interface `listen_ip`.
3. Pour fonctionner sans TLS dans un environnement contrôlé, définir `enable_tls: false`. Les déploiements en production doivent toujours terminer TLS à ou avant OmniSCEF.