مرجع تكوين OmniSCEF

تصف هذه الوثيقة كل معلمة تكوين لـ OmniSCEF. يتم تقسيم التكوين عبر ثلاثة مجالات تطبيقية:

المجال	الغرض
`:diameter_ex`	خدمة **T6a** Diameter: الهوية، المستمعون، التطبيق، والأقران.
`:api_ex`	نقطة نهاية **T8** REST API: TLS، عنوان الربط، وجدول المسارات.
`:omni_scef`	سلوك OmniSCEF: حل الهوية، عضوية المجموعة، والمراقبة.

عند بدء التشغيل، بحيث يمكن للبيئة دفعها Diameter بتقييم معلمات خدمة OmniSCEF تقوم وجدول المسارات ثابتان في وقت البناء T8 (انظر متغيرات البيئة). نقطة النهاية.

جدول المحتويات

- خدمة Diameter (T6a)
- نقطة نهاية T8 API
- إعدادات الهوية والمجموعة
- إعدادات المراقبة
- متغيرات البيئة

خدمة Diameter (T6a)

تقوم OmniSCEF بإنهاء T6a كخادم Diameter. يتصل MME (أو وكيل توجيه Diameter) على المنفذ المكون SCTP و TCP على كل من OmniSCEF بالداخل؛ تستمع.

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

    # المستمعون (على هذا العنوان/المنفذ SCTP و TCP يتم بدء كل من)
    listen_ip: "0.0.0.0",
    listen_port: 3868,

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

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

    # المعالجات الداخلية (ثابتة - لا تغيرها)
    control_module: OmniScef.Control.Diameter,
    processor_module: DiameterEx.Processor,

    # تسجيل تطبيق 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}
        ]
      }
    ],

    # الأقران 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
      }
    ]
  }
```

هوية الخدمة

المعلمة	النوع	مطلوب	الافتراضي	
`service_name`	Atom	نعم	`:omni_scef`	
`host`	String	نعم	`scef01`	
`realm`	String	نعم	`epc.mnc001.mcc001.3gppnetwork.org`	
`product_name`	String	لا	`OmniSCEF`	

المستمعون

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`listen_ip`	String	لا	`0.0.0.0`	عنوان IP للربط من أجل اتصالات Diameter الواردة. استخدم `0.0.0.0` لجميع الواجهات.
`listen_port`	Integer	لا	3868	المنفذ لاتصالات Diameter الواردة. يتم بدء كل من مستمعي SCTP و TCP على هذا المنفذ. 3868 هو المنفذ القياسي لـ Diameter وفقًا لـ RFC 6733.

السلوك

المعلمة	النوع	مطلوب	تراضي
`request_timeout`	Integer	لا	5000
`peer_selection_algorithm`	Atom	لا	`:rando`
`allow_undefined_peers_to_connect`	Boolean	لا	`true`

المعلمة	النوع	مطلوب	تراضي
`log_unauthorized_peer_connection_attempts`	Boolean	لا	`true`

قدرات Diameter

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`vendor_id`	Integer	لا	10415	Vendor-Id المعلن عنه في القدرات. 10415GPP هو 3.
`supported_vendor_ids`	قائمة من الأعداد الصحيحة	لا	`[10415]`	Supported-Vendor-Ids المعلن عنها في القدرات.
`auth_application_ids`	قائمة من الأعداد الصحيحة	لا	`[]`	معرفات تطبيق المصادقة الأساسية (غير محددة للبائع). فارغة لأن T6a مسجلة كتطبيق محدد للبائع (انظر `applications`).
`acct_application_ids`	قائمة من الأعداد الصحيحة	لا	`[]`	معرفات تطبيق المحاسب�� الأساسية. لا تستخدمها OmniSCEF.

المعالجات الداخلية

تقوم هذه بتوصيل كومة Diameter بمنطق OmniSCEF. إنها ثابتة ولا ينبغي تغييرها.

المعلمة	النوع	مطلوب	الافتراضي	ف
`control_module`	Module	نعم	`OmniScef.Control.Diameter`	وحدة التي تقبل لبات واردة زعها على جات NID راقبة
`processor_module`	Module	نعم	`DiameterEx.Processor`	كومة Dia الذي دعي وحدة حكم

تطبيق T6a

تسجل قائمة `applications` تطبيق Diameter T6a. هذا ثابت لـ OmniSCEF.

معلمات إدخال التطبيق:

المعلمة	النوع	مطلوب	الافتراضي
`application_name`	Atom	نعم	`:t6a`
`application_dictionary`	Atom	نعم	`:diameter_gen_3gp`
`vendor_specific_application_ids`	قائمة من الخرائط	نعم	انظر أدناه

معلمات معرف التطبيق المحدد للبائع:

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`vendor_id`	Integer	نعم	10415	معرف بائع 3GPP.
`auth_application_id`	Integer	نعم	16777346	معرف تطبيق T6a.
`acct_application_id`	Integer	لا	`nil`	لا تستخدم لـ T6a.

الأقران

تعلن قائمة `peers` عن الأقران المعروفة لـ Diameter (MME، DRA، و HSS). تكون معلمة `allow_undefined_peers_to_connect` افتراضيًا `true` وعادة ما يبدأ MME الاتصال. يمكنك

بأي شيء خارجي. قم بإدراج نظير OmniSCEF فارغًا (`[]`) في النشر حيث لا يتصل `peers` ترك هنا عندما يجب على OmniSCEF الاتصال، أو لتقييد الأقران التي يمكنها الاتصال **بدء**.

معلمات النظير:

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`host`	String	نعم	-	هوية Diamet للنظير (FQDN جب أن تتطابق تمامًا مع Origi المكون Host للنظير.
`realm`	String	نعم	-	نطاق Diamet للنظير.
`ip`	String	نعم	-	نظير IP عنوان لاتصال TCP/S
`port`	Integer	لا	3868	منفذ Diamet للنظير.
`tls`	Boolean	لا	`false`	ذا كان الاتصال لنظير يستخدم TLS.
`transport`	Atom	لا	`:diameter_sctp`	قل لهذا النظير `:diameter_` أو `:diameter_`
`initiate_connection`	Boolean	لا	`false`	عندما تكون `tr` يتصل OmniS اط بهذا النظير د بدء التشغيل. عندما تكون `false`، ينتظر OmniSCEF ل يتصل النظير لداخل. بالنسبة لنظير هو MME

الوصف	الافتراضي	مطلوب	النوع	المعلمة
SCEF يتصل بـ `fals` اترك هذا				

T8 API نقطة نهاية

تُقدم واجهة برمجة التطبيقات RESTful T8 عبر HTTPS. يتم تركيب جميع المسارات تحت البادئة `/api`، لذا فإن apiRoot الفعلي هو `https://<host>:<port>/api`.

```
config :api_ex,
  api: %{
    port: 8443,
    listen_ip: "0.0.0.0",
    product_name: "OmniSCEF",
    title: "T8 API - OmniSCEF",
    hostname: "localhost",
    enable_tls: true,
    tls_cert_path: "priv/cert/omnitouch.crt",
    tls_key_path: "priv/cert/omnitouch.pem",
    routes: [ ... ]   # جدول المسارات الثابت T8 - انظر أدناه
  }
```

معلمات نقطة النهاية

المعلمة	النوع	مطلوب	الافتراضي	وصف
`port`	Integer	لا	8443	HTT منفذ جهة برمجة التطبيقات
`listen_ip`	String	لا	`0.0.0.0`	IP ـ عنوان جهة برمجة التطبيقات استخدم `0.0.0.0` لجميع الواجهات.
`product_name`	String	لا	`OmniSCEF`	سم المنتج ستخدم في ت التعريف API/Oper
`title`	String	لا	`T8 API - OmniSCEF`	العنوان عروض في الوثيقة OpenAPI دة وواجهة Swagger
`hostname`	String	لا	`localhost`	م المضيف ستخدم عند شاء عنوان URL قطة النهاية.
`enable_tls`	Boolean	لا	`true`	ندما تكون `true`، دم طة النهاية

المعلمة	النوع	مطلوب	الافتراضي	وصف
				HTTPS باستخدام شهادة أدناه
`tls_cert_path`	String	إذا (نعم كانت TLS)	`priv/cert/omnitouch.crt`	لمسار إلى الشهادة T المشفرة بتنسيق PE
`tls_key_path`	String	إذا (نعم كانت TLS)	`priv/cert/omnitouch.pem`	لمسار إلى تاح الخاص شفر TLS بتنسيق PE
`routes`	قائمة	نعم	ثابت	ل مسارات ذا هو .T8 يف الثابت جهة برمجة التطبيقات وليس قابلًا ل من قبل شغل. انظر جدول المسارات.

جدول المسارات

وتنتج النقاط OmniSCEF إنها ثابتة لـ .T8 سطح واجهة برمجة التطبيقات `routes` تعرف إدخالات بمعالج ومجموعة الإجراءات التي URL كل إدخال يربط قالب (`/api` كل ذلك تحت) النهائية أدناه يخدمها.

معلمات إدخال المسار:

المعلمة	النوع	الوصف
`path`	String	قالب URL. المقاطع مثل `:scsAsId` هي متغيرات مسار.
`module`	Module	المعالج الذي يخدم المسار.
`parameters`	String أو `nil`	اسم متغير مسار المورد العضو (مثل `configurationId`)، أو `nil` للمسارات الخاصة بالمجموعة فقط.
`actions`	قائمة من Atom	الإجراءات HTTP التي يتم تقديمها: `:index` (GET المجموعة)، `:create` (POST)، `:show` (GET العضو)، `:update` (PUT/PATCH العضو)، `:delete` (DELETE العضو).

النقاط النهائية الناتجة:

الطريقة والمسار	غرض
`GET /api/status`	حيوية الخدمة / الهوية.
`GET /api/3gpp-nidd/v1/{scsAsId}/configurations`	قائمة تكوينات NIDD.
`POST /api/3gpp-nidd/v1/{scsAsId}/configurations`	اء تكوين NIDD.
`GET/PUT/PATCH/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}`	قراءة / ستبدال / ف تكوين NIDD.
`GET/POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`	قائمة / ل بيانات الاتجاه الهابط.
`GET/DELETE /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries/{downlinkDataDeliveryId}`	ة الحالة اء تسليم الاتجاه الهابط.
`GET/POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`	قائمة / إنشاء شتراكات المراقبة
`GET/PUT/DELETE /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions/{subscriptionId}`	قراءة / بدال / حذف

الغرض	الطريقة والمسار
اشتراك المراقبة	

واجهة Swagger التفاعلية عند `GET /api/docs`، والوثيقة OpenAPI المولدة متاحة عند `GET /api/schema`.

> **المصادقة الاختيارية باستخدام مفتاح مشترك.** تدعم نقطة نهاية T8 فحص مفتاح مشترك اختياري على الطلبات الواردة. يتم تعطيله ما لم يتم إضافة مفتاح تحت `auth` عندما يكون غير محدد (الافتراضي)، لا يتم تطبيق فحص مفتاح `config :api_ex, :api`. مشترك ويجب حماية نقطة النهاية بواسطة ضوابط الشبكة (مثل اتصال خاص أو وكيل عكسي).

إعدادات الهوية والمجموعة

تقوم OmniSCEF بحل الهوية المواجهة لـ AS (معرف خارجي أو MSISDN) إلى IMSI و الشبكة، تحل معرف المجموعة إلى IMSIs تحل هذه الخرائط ثابتة للمشغل في الإصدار الأول، تكون هذه الخرائط الأعضاء.

```
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
  }
```

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`identity_map`	Map	لا	`%{}`	يط معرف خارجي (`user@domain`) MSISDN إلى IM ك. يستخدم عندما تكوين AS ينشئ N أو اشتراك UE ل ة. يتم رفض الهوية بر الموجودة هنا كـ غير معروف.
`group_map`	Map	لا	`%{}`	يربط `externalGroup` ضاء. IMSIs بقائمة N يستخدم لتسليم الجماعي.
`default_max_packet_size`	Integer	لا	255	الأقصى الافتراضي لحجم الحمولة غير ايت، المطبق على ي لا NIDD تكوين يحدد `maximumPacket` لة NAS تحد كومة ة عند IP 255 غير بايت.

> بدلاً من التكوين HSS/UDR في الإنتاج، عادةً ما تكون هذه الخرائط مدعومة من خلال بحث غير متغير AS الثابت. سلوك المواجهة لـ.

إعدادات المراقبة

اختياري. عند تكوين وجهة للمراقبة، فإن إنشاء اشتراك للمراقبة يجهز الحدث في ��لاتجاه إلى تلك العقدة. عندما لا تحدد وجهة، (CIR) طلب معلومات التكوين OmniSCEF الجنوبي. ترسل

تخزن الاشتراكات ولا تزال تسلم التقارير الواردة. في تلك الحالة، لا ترسل OmniSCEF لا تزال OmniSCEF CIR بشكل استباقي.

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

معلمات `destination`:

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`host`	String	لا	-	هوية Diameter (FQDN) لـ HSS / العقدة الخدمية التي يتم إرسال طلبات تكوين المراقبة إليها. عند الإغفال، يتم توجيه الطلب بواسطة النطاق فقط.
`realm`	String	نعم (إذا تم تعيين `destination`)	-	نطاق Diameter المستخدم كنطاق وجهة لـ CIR المراقبة.

متغيرات البيئة

يمكن تزويد هوية خدمة Diameter والمستمعين من البيئة عند بدء التشغيل. تتجاوز هذه القيم الافتراضية الموضحة تحت Diameter.

المتغير	يتوافق مع	الافتراضي
`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`

مراقبة الأحداث

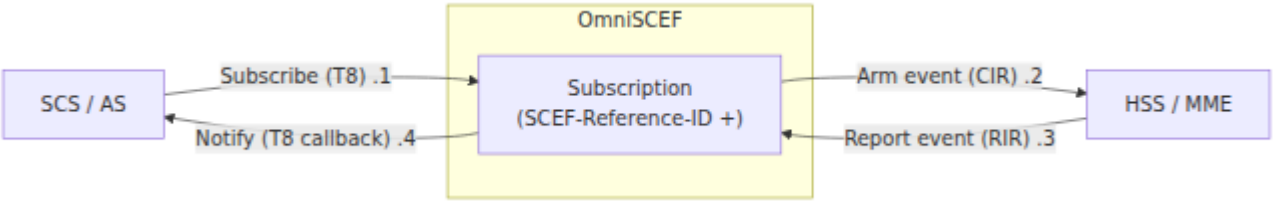
تتيح خدمة مراقبة الأحداث لخادم التطبيق الاشتراك في أحداث الشبكة حول جهاز أو مجموعة: إمكانية الوصول، وفقدان الاتصال، والموقع، وحالة التجوال، والمزيد. يقوم خادم التطبيق بالاشتراك عبر **T8**. يقوم OmniSCEF بتسليح الحدث في الشبكة عبر **T6a** ويقوم بتسليم كل تقرير مرة أخرى إلى رد الاتصال الخاص بالاشتراك.

تم تعريف أحداث المراقبة في 3GPP TS 23.682 §5.6، وواجهة برمجة التطبيقات T8 في TS 29.122 §5.3، وإجراءات Diameter في TS 29.128 / TS 29.336.

جدول المحتويات

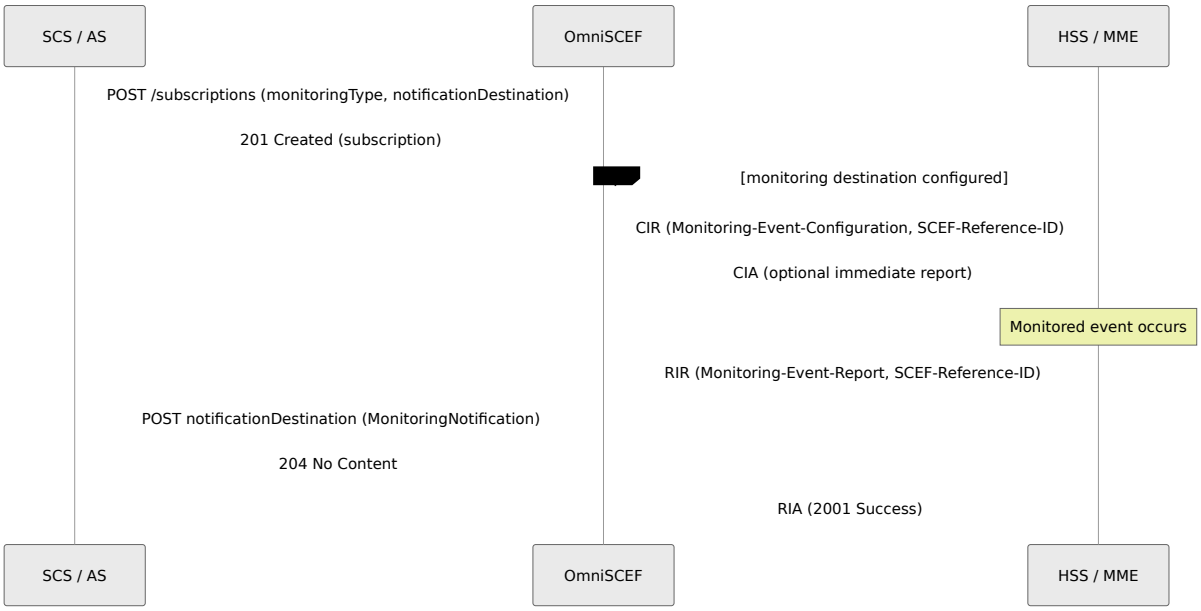
- نظرة عامة
- تدفق الاشتراك والتقارير
- مرجع موارد T8
- أنواع المراقبة
- القيم المرجعية

نظرة عامة



يتم استخدام هذا المعرف الفريد في **SCEF-Reference-ID**. يخصص OmniSCEF لكل اشتراك هذا لتوجيه تقرير وارد OmniSCEF التكوين الجنوبي، وتقوم الشبكة بإعادته في كل تقرير. يستخدم إلى الاشتراك الصحيح ورد الاتصال الخاص بخادم التطبيق.

تدفق الاشتراك والتقارير



التسليح اختياري في SCEF. يقوم، وجهة المراقبة عند تكوين OmniSCEF بإرسال CIR لتسليح ينشئ الاشتراك ويقوم بتسليم أي تقارير OmniSCEF الحدث. عندما لا تقوم بتكوين واحدة، لا يزال على سبيل المثال، عندما) بشكل استباقي CIR بإرسال OmniSCEF واردة. في هذه الحالة، لا يقوم يقوم مسار آخر بتسليح الحدث عبر HSS).

به مع OmniSCEF RIA لتقرير مع أي اشتراك، يعترف SCEF-Reference-ID عندما لا يتطابق ولكنه لا يقوم بإعادة توجيهه.

مرجع موارد T8

MonitoringEventSubscription

تم إنشاؤه بواسطة `POST /api/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`.

الحقل	النوع	مطلوب	الوصف
`notificationDestination`	سلسلة (URI)	نعم	رد الاتصال الذي يتلقى خادم التطبيق تقارير المراقبة عليه.
`monitoringType`	سلسلة (enum)	ن��م	الحدث الذي سيتم مراقبته. انظر أنواع المراقبة.
`externalId`	سلسلة	شرطي	معرف الجهاز الخارجي. واحد من `externalId`، `msisdn`، أو `externalGroupId`.
`msisdn`	سلسلة	شرطي	MSISDN للجهاز.
`externalGroupId`	سلسلة	شرطي	معرف المجموعة لمراقبة المجموعة.
`maximumNumberOfReports`	عدد صحيح	لا	التوقف بعد هذا العدد من التقارير.
`monitoringDuration`	سلسلة (تاريخ-وقت)	لا	التوقف عن المراقبة في هذا الوقت.
`reachabilityType`	سلسلة (enum)	لا	لـ `UE_REACHABILITY`: `SMS` أو `DATA`.
`maximumDetectionTime`	عدد صحيح	لا	لـ `LOSS_OF_CONNECTIVITY`: وقت الكشف بالثواني.
`mtcProviderId`	سلسلة	لا	معرف مزود خدمة MTC.
`self`	سلسلة (URI)	قراءة فقط	URI الخاص بالاشتراك.

مثال على طلب الاشتراك:

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

MonitoringNotification

يقوم OmniSCEF بإرسال `MonitoringNotification` إلى `notificationDestination` للاشتراك لكل تقرير. يشير إلى الاشتراك الأصلي ويحمل تقرير أو أكثر من تقارير الأحداث المفككة.

مثال على الإشعار:

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

`204` يعترف خادم التطبيق بـ `No Content`.

أنواع المراقبة

يدعم OmniSCEF مجموعة أنواع المراقبة الكاملة لـ TS 29.122. كل منها يتطابق مع القيمة المقابلة لـ `Monitoring-Type` على واجهة Diameter (TS 29.336 §5.3.9).

`monitoringType` (T8)	قيمة Diameter	الوصف
`LOSS_OF_CONNECTIVITY`	0	لم يعد UE قابلاً للوصول للبيانات.
`UE_REACHABILITY`	1	أصبح UE قابلاً للوصول لـ SMS أو البيانات.
`LOCATION_REPORTING`	2	يتم الإبلاغ عن موقع UE (أو تغيير فيه).
`CHANGE_OF_IMSI_IMEI_ASSOCIATION`	3	تغير IMEI المرتبط بـ IMSI.
`ROAMING_STATUS`	4	يتم الإبلاغ عن حالة التجوال لـ UE (أو تغيير).
`COMMUNICATION_FAILURE`	5	حدث فشل في الاتصال.
`AVAILABILITY_AFTER_DDN_FAILURE`	6	أصبح UE متاحًا بعد فشل إشعار بيانات التنزيل.
`NUMBER_OF_UES_IN_AN_AREA`	7	عدد UEs الموجودة في منطقة معينة.
`PDN_CONNECTIVITY_STATUS`	8	تم إنشاء/إلغاء اتصال PDN.
`DOWNLINK_DATA_DELIVERY_STATUS`	9	حالة تسليم بيانات التنزيل.
`API_SUPPORT_CAPABILITY`	10	الإبلاغ عن قدرة دعم API.

يتم رفض الاشتراك الذي يحتوي على `monitoringType` غير المدعوم مع `400` `INVALID_MONITORING_TYPE`.

القيم المرجعية

نوع الوصول

القيمة	المعنى
`SMS`	قابل للوصول لـ UE SMS.
`DATA`	قابل للوصول للبيانات UE.

أوامر Diameter ذات الصلة

لأكواد الأوامر والنتائج جداول مرجع دليل العمليات انظر CIR/CIA و RIR/RIA.

تسليم البيانات غير IP (NIDD)

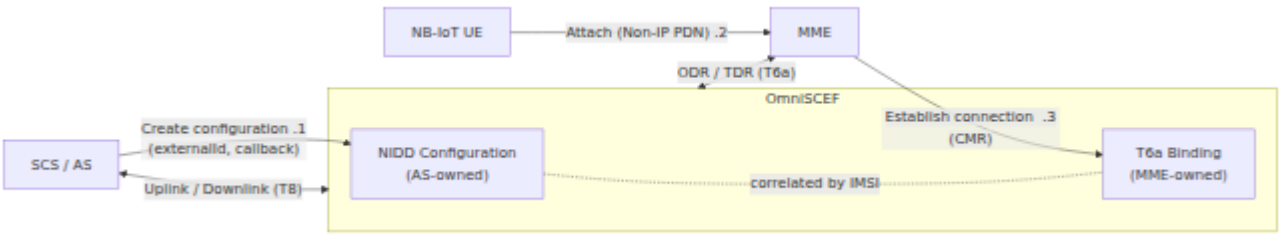
تسليم البيانات غير IP يتيح لجهاز Cellular-IoT / NB-IoT **غير** تبادل رسائل **IP** صغيرة مع خادم التطبيق **بدون عنوان IP**. البيانات تمر عبر طائرة الإشارة NAS (تحسين CIoT EPS في Control-Plane) بين UE وMME. يقوم MME بإعادة توجيهها إلى OmniSCEF عبر **T6a**. ثم تعرض OmniSCEF البيانات على خادم التطبيق عبر **T8**.

تم تعريف معمارية وإجراءات NIDD في 3GPP TS 23.682 §5.13؛ واجهة T6a Diameter في TS 29.128؛ وواجهة T8 NIDD API في TS 29.122.

جدول المحتويات

- نظرة عامة
- دورة حياة الاتصال
- بيانات منشأة من الهاتف المحمول
- بيانات منتهي�ة إلى الهاتف المحمول
- مجموعة NIDD
- خدمة البيانات الموثوقة
- بيانات استثناء MO
- مرجع موارد T8
- القيم المرجعية

نظرة عامة



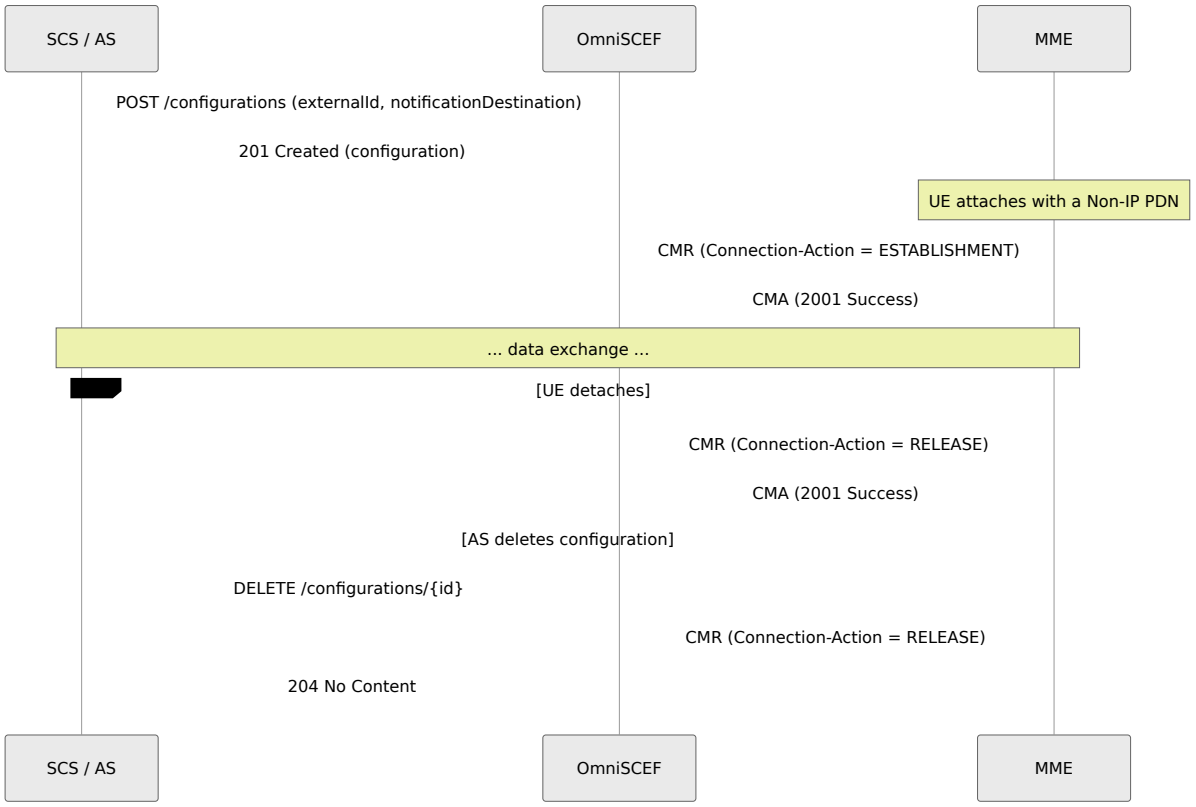
تحتوي جلسة NIDD على نصفين مترابطين:

- **تكوين** **NIDD** يتم إنشاء بواسطة خادم التطبيق عبر T8. يسمي الجهاز (عن طريق رد الاتصال للإشعار، وخيارات، (أو مجموعة MSISDN، معرف خارجي، NIDD.
- **ربط** **T6a** يتم إنشاء بإنشاء الاتصال غير MME عندما يقوم IP لذلك المشترك. يربط `{IMSI, EBI}` بـ MME وهوية Diameter جلسة المستخدمة للوصول إلى UE.

بين الاثنين بواسطة هوية المشترك، بحيث تجد بيانات الرفع رد الاتصال الصحيح OmniSCEF ترتبط لـ AS الصحيح المباشر الاتصال النزول بيانات تجد و.

دورة حياة الاتصال

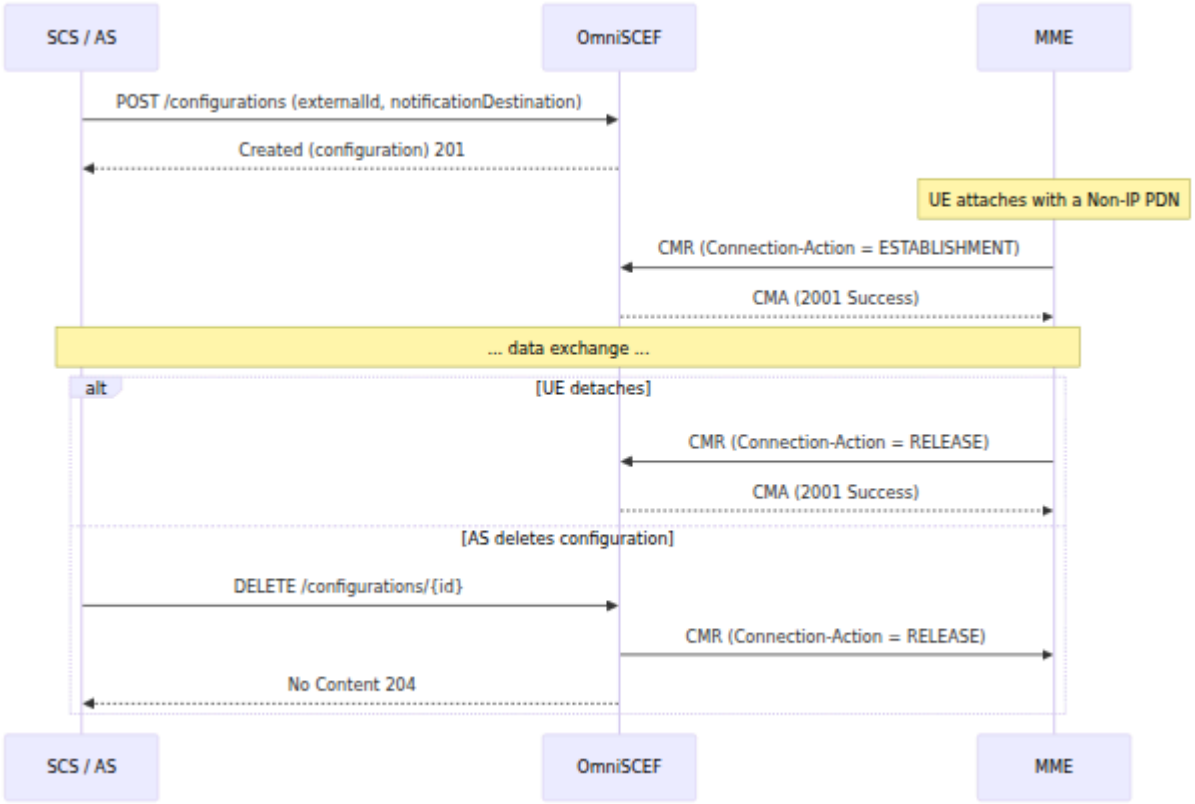
يدير MME اتصال T6a أثناء اتصال UE عن طريق إنهاء الاتصال أيضًا يمكن التطبيق لخادم وفصله. الخاص به NIDD تكوين حذف.



على OmniSCEF ترد، **NIDD** بإنشاء اتصال لمشترك ليس لدي**** **تكوين** MME عندما يقوم بـ CMR `DIAMETER_ERROR_USER_UNKNOWN (5001)`. المشترك غير مهيأ لـ NIDD.

بيانات منشأة من الهاتف المحمول (الرفع)

تصل بيانات Non-IP المرسلة من UE إلى OmniSCEF كطلب بيانات MO **T6a (ODR)**. تقوم OmniSCEF بتسليمها إلى خادم التطبيق عن طريق POSTing إشعار إلى رد الاتصال الخاص بالتكوين، وترد على MME بـ **MO-Data-Answer (ODA)**.



إذا لم تتمكن OmniSCEF من حل التكوين أو فشل رد الاتصال، فإنها ترد على ODA بـ `DIAMETER_UNABLE_TO_COMPLY (5012)`.

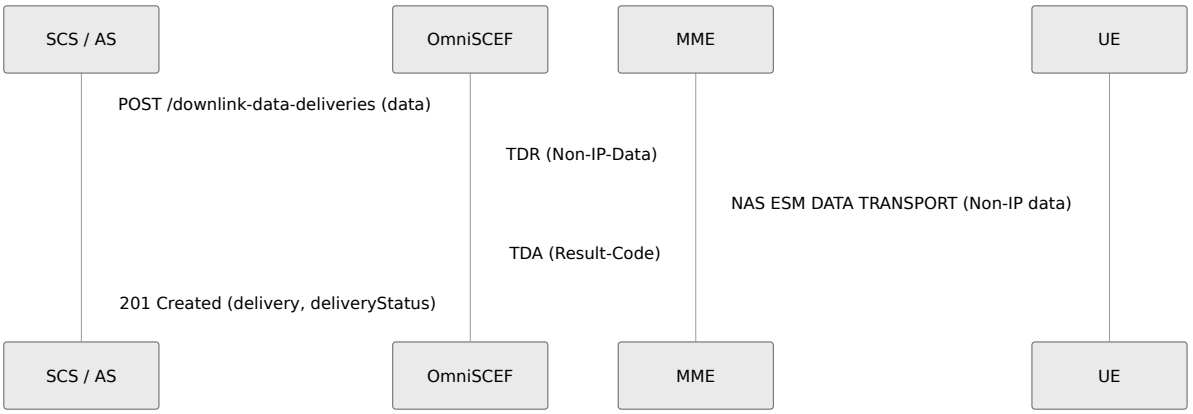
مثال على إشعار الرفع (POSTed إلى رد الاتصال):

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

الحقل	الوصف
`externalId` / `msisdn`	هوية الجهاز، كما هو موفر في التكوين.
`data`	الحمولة غير IP، مشفرة بتنسيق base64.
`rdsSourcePort` / `rdsDestinationPort`	موجود عند تمكين خدمة البيانات الموثوقة.
`moExceptionDataCounter`	موجود عندما يتم تمييز الرفع على أنه بيانات استثناء MO.

بيانات منتهية إلى الهاتف المحمول (النزول)

يرسل خادم التطبيق بيانات Non-IP المنتهية عبر POST إلى مجموعة `downlink-data-deliveries`. تقوم OmniSCEF الخاصة بالتكوين بإعادة توجيهها إلى MME كطلب بيانات MT على موارد تسليم فردية (**MT-Data-Answer, TDA** من) وتقوم بتسجيل النتيجة، **T6a (TDR)**. يمكن لـ AS استرجاعها.



عندما يكون UE في حالة خمول، يقوم MME بصفحة UE، ويجيب على بتخزين البيان��ت ويقوم OmniSCEF بالنجاح بمجرد أن يتحمل المسؤولية عن التسليم. تعكس النتيجة في TDA `deliveryStatus` (انظر قيم حالة التسليم) للتسليم.

مثال على طلب النزول:

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

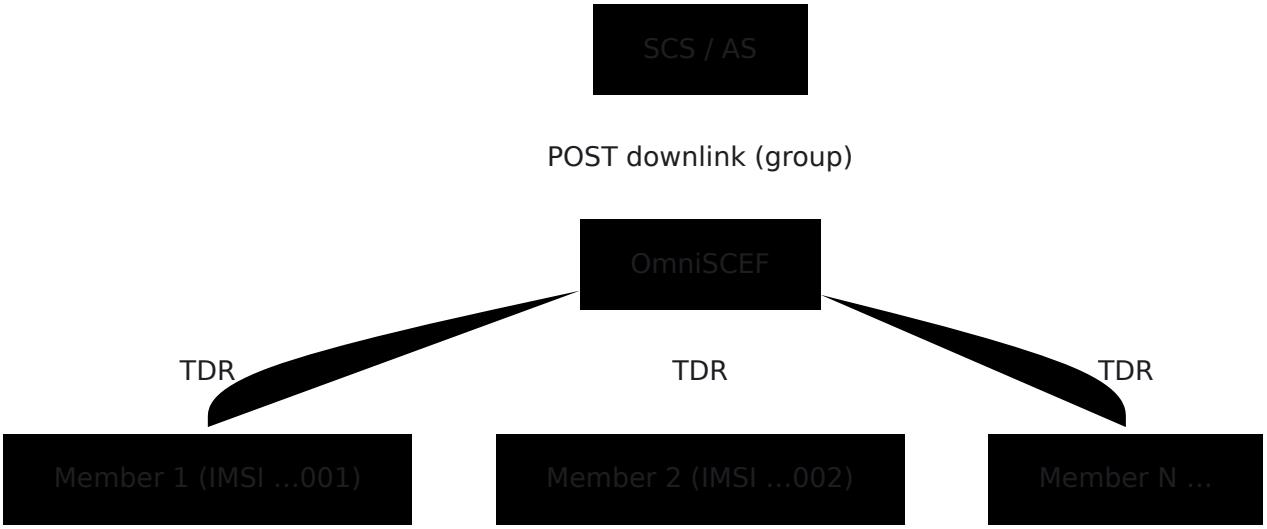
الحقل	الوصف
`data`	للتسليم، مشفرة بتنسيق IP الحمولة غير base64. مطلوب.
`maximumLatency`	اختياري. الحد الأقصى المقبول لتأخير التخزين المؤقت، بالثواني.
`priority`	اختياري. الأولوية النسبية بين التسليمات المتراكمة.
`pdnEstablishmentOption`	اختياري. السلوك عند عدم وجود اتصال. انظر خيارات إنشاء PDN.
`rdsSourcePort` / `rdsDestinationPort`	اختياري. منافذ RDS. انظر خدمة البيانات الموثوقة.

مثال على استجابة النزول:

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

مجموعة NIDD

يمثل تكوين NIDD الذي تم إنشاؤه باستخدام `externalGroupId` (بدلاً من `externalId`/`msisdn` الفردي) من الأجهزة **مجموعة** (TS 23.682 §5.13.3A). يتم **توزيع** تسليم نزول واحد إلى تكوين مجموعة على كل عضو في المجموعة الذي يمتلك اتصال T6a نشط.



الإجمالية للتسليم `deliveryStatus` يتم حل أعضاء المجموعة من خريطة المجموعة. تعكس عندما يتم تقديم كل `SUCCESS` **أسوأ** نتيجة لكل عضو، لذا فإن تسليم المجموعة يبلغ فقط عن عضو يمكن الوصول إليه.

خدمة البيانات الموثوقة

تقوم خدمة البيانات الموثوقة (RDS) بتعدد تدفقات التطبيقات المتعددة عبر اتصال غير واحد IP لكل تكوين عن RDS يتم تمكين. TS 23.682 §4.5.14.3 باستخدام **أرقام المنافذ**، وفقًا لـ طريق تعيين `reliableDataService: true` عند إنشاء التكوين.

عند تمكين RDS:

- **النزول**: عندما يحدد التسليم `rdsDestinationPort` و `rdsSourcePort`، تقوم يحمل تلك المنافذ قبل أن ترسل RDS مع رأس IP بتأطير الحمولة غير OmniSCEF TDR.
- **الرفع**: تقوم OmniSCEF بتحليل رأس RDS من الحمولة ODR. تظهر على إشعار الرفع، وتقوم بتسليم `rdsSourcePort` و `rdsDestinationPort` الحمولة الداخلية كـ `data`.

أو يتجاهل التسليم المنافذ، يتم حمل الحمولة بدون RDS، المنافذ هي 0–255. عندما لا يتم تمكين تأطير.

بيانات استثناء MO

تمييز نقل الرفع على أنه **تقرير استثناء** (تقرير عاجل، خارج النمط) عبر NB-IoT يمكن لأجهزة سبب إنشاء RRC، الذي يتم عدّه في `RRC-Cause-Counter` لـ T6a (TS 23.682 §5.13.4). عندما ترى OmniSCEF هذه الإشارة على ODR، فإنها تتضمن `moExceptionDataCounter` على إشعار الرفع حتى يتم��ن خادم التطبيق من إعطاء الأولوية في المعالجة.

مرجع موارد T8

NiddConfiguration

تم إنشاؤه بواسطة `POST /api/3gpp-nidd/v1/{scsAsId}/configurations`.

الحقل	النوع	مطلوب	الوصف
`notificationDestination`	سلسلة (URI)	نعم	رد الاتصال الذي يتلقى خادم التطبيق إشعارات الرفع وحالة.
`externalId`	سلسلة	مشروط	معرف الجهاز الخارجي (`user@domain`). واحد من `externalId`، `msisdn`، أو `externalGroupId`.
`msisdn`	سلسلة	مشروط	MSISDN للجهاز.
`externalGroupId`	سلسلة	مشروط	معرف المجموعة لـ مجموعة NIDD.
`dnn`	سلسلة	لا	اسم شبكة البيانات / APN للاتصال غير IP.
`pdnEstablishmentOption`	سلسلة (enum)	لا	السلوك عند النزول عندما لا يوجد اتصال. انظر خيارات إنشاء PDN.
`maximumPacketSize`	عدد صحيح	لا	الحد الأقصى لحجم الحمولة غير IP بالبايت (الافتراضي هو `default_max_packet_size` المكون، 255).
`reliableDataService`	منطق��	لا	تمكين خدمة البيانات الموثوقة.
`mtcProviderId`	سلسلة	لا	معرف مزود خدمة MTC.
`validityTime`	سلسلة (تاريخ-وقت)	لا	متى تنتهي صلاحية التكوين.
`status`	سلسلة (enum)	للقراءة فقط	حالة دورة الحياة. انظر قيم حالة التكوين.

الحقل	النوع	مطلوب	الوصف
`self`	سلسلة (URI)	للقراءة فقط	URI الخاص بالموارد.

NiddDownlinkDataTransfer

تم إنشاؤه بواسطة `POST /api/3gpp-nidd/v1/{scsAsId}/configurations/{configurationId}/downlink-data-deliveries`. الحقول تم وصف الحقول تحت بيانات منتهية إلى الهاتف المحمول. `deliveryStatus` و `requestedRetransmissionTime` هي للقراءة فقط ويتم تعيينها من TDA.

الإشعارات

تقوم OmniSCEF بإرسال POSTs التالية إلى `notificationDestination` الخاصة بالتكوين:

الإشعار	متى
`NiddUplinkDataNotification`	وصلت بيانات Non-IP الرفيعة (من ODR).
`NiddDownlinkDataDeliveryStatusNotification`	تغيرت نتيجة تسليم النزول الذي تم قبوله سابقًا (حالة غير متزامنة).

يقر خادم التطبيق بكل إشعار بـ `204 No Content`.

القيم المرجعية

قيم حالة التسليم

القيمة	المعنى
`SUCCESS`	قام MME بتسليم البيانات (أو تحمل المسؤولية عن طريق التخزين المؤقت / صفحة UE الخاملة).
`SENDING`	التسليم جارٍ.
`BUFFERING`	قام MME بتخزين البيانات لجهاز UE الخامل.
`FAILURE_UE_NOT_REACHABLE`	لم يكن بالإمكان الوصول إلى UE.
`FAILURE_REMOTE_FAILURE`	رفض MME / العقدة الخادمة أو فشلت في الطلب.
`FAILURE`	فشل التسليم لسبب آخر.

خيارات إنشاء PDN

القيمة	السلوك عند عدم وجود اتصال في وقت النزول
`WAIT_FOR_UE`	التخزين المؤقت حتى يقوم UE بإنشاء الاتصال.
`INDICATE_ERROR`	رفض التسليم على الفور.
`ESTABLISH_PDN_CONNECTION`	تحفيز UE لإنشاء الاتصال غير IP.

قيم حالة التكوين

القيمة	المعنى
`ACTIVE`	التكوين مفوض ��قابل للاستخدام.
`TERMINATED_UE_NOT_AUTHORIZED`	المشترك غير مفوض لـ NIDD.
`TERMINATED`	انتهت صلاحية التكوين أو تم إزالته.

استكشاف أخطاء OmniSCEF وإصلاحها

إرشادات حول المشكلات التشغيلية الشائعة في OmniSCEF. لمزيد من المعلومات حول التدفقات الأساسية، راجع مرجع التكوين NIDD؛ لمعلمات التكوين، راجع مراقبة الأحداث.

جدول المحتويات

- لا يمكنه الاتصال عبر T6a MME
- تم رفض الاتصال مع USER_UNKNOWN (5001)
- فشل تسليم البيانات الهابطة
- بيانات الرفع لا تصل إلى خادم التطبيق
- تسليم البيانات الجماعية لا يصل إلى أي أجهزة
- تقارير المراقبة لم يتم تسليمها
- لنقطة نهاية صالحة T8 404 تُرجع واجهة برمجة التطبيقات
- لن تبدأ T8 نقطة نهاية

لا يمكنه الاتصال عبر T6a MME

الأعراض: لا يمكن لـ MME إنشاء اتصال Diameter بـ OmniSCEF؛ لا تكتمل تبادلات القدرات.

الأسباب المحتملة:

- جدار الحماية يحظر منفذ Diameter (3868 الافتراضي).
- عدم تطابق في النقل: يستخدم MME SCTP بينما يمكن الوصول فقط إلى TCP، أو العكس.
- تم تقييد تفويض النظير و MME ليس نظيرًا مُكونًا.
- عدم تطابق Origin-Host / realm بين ما يتوقعه MME وما تعلنه OmniSCEF.

الحل:

1. تأكد من أن جدار الحماية يسمح بـ `listen_port` المُكون على كل من TCP وSCTP. تستمع OmniSCEF على كلاهما. راجع المستمعون.
2. تحقق من تطابق النقل المُكون لـ MME. يتم دائمًا بدء كل من مستمعي TCP وSCTP.
3. إذا كانت `allow_undefined_peers_to_connect` تساوي `false`، أضف MME إلى `peers` مع Origin-Host الخاص به بالضبط. راجع الأقران.
4. تأكد من أن `host` و`realm` لـ OmniSCEF تتطابق مع ما تم تزويد MME للـ حدث إليه. تحقق من مخرجات سجل `log_unauthorized_peer_connection_attempts` لمحاولات الرفض.

تم رفض الاتصال مع USER_UNKNOWN (5001)

الأعراض: يقوم MME بإنشاء اتصال Diameter، لكن طلب اتصال NIDD (CMR) يتم الرد عليه بـ `DIAMETER_ERROR_USER_UNKNOWN (5001)`.

الأسباب المحتملة:

- لا توجد تكوينات NIDD موجودة لـ IMSI هذا المشترك.
- أنشأ خادم التطبيق تكوينًا باستخدام هوية خارجية لا تحل إلى IMSI المشترك.

الحل:

1. تأكد من أن خادم التطبيق قد أنشأ تكوين NIDD للجهاز قبل أن يتصل UE.
2. تحقق من أن `externalId`/`msisdn` للجهاز تحل إلى IMSI الصحيح في خريطة الهوية.
3. تأكد من أن IMSI في CMR الذي يقدمه MME يتطابق مع IMSI في خريطة الهوية.

فشل تسليم البيانات الهابطة

الأعراض: يُرجع `POST` إلى `downlink-data-deliveries` تسليمًا يكون فيه `deliveryStatus` قيمة `FAILURE_*`، `404` أو.

الأسباب المحتملة:

- لا يوجد اتصال T6a نشط للجهاز (`404 NIDD_CONFIGURATION_NOT_AVAILABLE`). لم يتصل UE، أو أصدرت OmniSCEF اتصالها.

- UE غير قابل للوصول (`FAILURE_UE_NOT_REACHABLE`).
- رفض MME / عقدة الخدمة الطلب (`FAILURE_REMOTE_FAILURE`).
- الحقل `data` مفقود أو غير صالح base64 (`400 DATA_MISSING`).

الحل:

1. تأكد من أن الجهاز متصل وأن اتصاله قد تم إنشاؤه (سابق CMR تم قبول).
2. تحقق من أن الحقل `data` موجود ومشفر بتنسيق base64.
3. بالتخزين المؤقت والصفحة؛ تقارير MME غير النشط، توقع أن يقوم UE بالنسبة لـ المسؤولية. راجع البيانات المنتهية إلى الهاتف التسليم النجاح بمجرد أن يتحمل MME المحمول.
4. بالنسبة لـ `FAILURE_REMOTE_FAILURE`، تحقق من جانب MME/عقدة الخدمة لمعرفة سبب الرفض.

بيانات الرفع لا تصل إلى خادم التطبيق

الأعراض: يرسل UE استدعاؤه لا يتم الخاص بخادم التطبيق الاتصال رد يُعرف لا (لذا NIDD تكوين الجهاز لدى ليس (بيانات الرفع، لكن رد الاتصال.

الأسباب المحتملة:

- NIDD تكوين الجهاز لدى ليس (لذا لا يُعرف رد الاتصال).
- `notificationDestination` غير قابل للوصول من عنوان URL ل OmniSCEF، 2 أو يُرجع حالة غير xx.
- `{IMSI, EBI}` لا يوجد ربط نشط لـ الرفع على المعروض.

الحل:

1. تأكد من وجود تكوين NIDD للجهاز ويحمل `notificationDestination` قابل للوصول.
2. تحقق من الاتصال الشبكي من OmniSCEF إلى عنوان URL الخاص برد الاتصال، بما في ذلك ثقة TLS إذا كان HTTPS.
3. تأكد من أن رد الاتصال يُرجع حالة غير 2xx؛ يتم اعتبار حالة 2xx كفشل في التسليم.
4. تأكد من أن الجهاز متصل (تم قبول CMR) قبل إرسال بيانات الرفع.

تسليم البيانات الجماعية لا يصل إلى أي أجهزة

الأعراض: يُرجع تسليم هابط إلى تكوين جماعي `404 NIDD_CONFIGURATION_NOT_AVAILABLE`، أو يصل إلى عدد أقل من الأجهزة مما هو متوقع.

الأسباب المحتملة:

- `externalGroupId` غير موجود في خريطة المجموعة، أو لا يطابق أي أعضاء.
- لا يوجد عضو في المجموعة لديه اتصال T6a نشط حاليًا.

الحل:

1. تأكد من تعريف `externalGroupId` وتدرج الأعضاء IMSIs في خريطة المجموعة المتوقعة.
2. تأكد من أن جهاز عضو واحد على الأقل متصل. فقط الأعضاء الذين لديهم اتصال نشط يتلقون التسليم. تعكس الحالة الإجمالية أسوأ نتيجة لكل عضو. راجع NIDD الجماعي.

تقارير المراقبة لم يتم تسليمها

الأعراض: تم إنشاء اشتراك للمراقبة، لكن خادم التطبيق لا يتلقى أي إشعارات.

الأسباب المحتملة:

- لم يتم تسليح الحدث أبدًا في الشبكة (لا يوجد وجهة مراقبة مُكونة، ولا يوجد مسار آخر يسليحه).
- لا يتطابق SCEF-Reference-ID بعد هذا للتقرير مع اشتراك نشط. يمكن أن يحدث إعادة التشغيل، لأن حالة الاشتراك في الذاكرة.
- `notificationDestination` للاشتراك غير قابل للوصول.

الحل:

1. إذا كان يجب على OmniSCEF تسليح الحدث، قم بتكوين وجهة المراقبة حتى يتم إرسال CIR.
2. أعد إنشاء الاشتراكات بعد إعادة تشغيل OmniSCEF. ومرجع SCEF-Reference-ID حالة الاشتراك متقلبة ولا تبقى بعد إعادة التشغيل.
3. تحقق من الاتصال من OmniSCEF إلى رد الاتصال للاشتراك.

T8 404 تُرجع واجهة برمجة التطبيقات لنقطة نهاية صالحة

الأعراض: يُرجع طلب إلى مسار `/api/schema` موثق في OpenAPI `404`، ولا تظهر نقطة النهاية في وثيقة T8.

الأسباب المحتملة:

- تم تغيير جدول المسارات ولكن لم يتم إعادة تجميع طبقة API، لذا فإن المسار الجديد غير مسجل.
- يفتقر الطلب إلى البادئة `/api` التي يتم تركيب جميع مسارات T8 تحتها.

الحل:

1. تأكد من أن مسار الطلب يتضمن بادئة `/api` (على سبيل المثال، `/api/3gpp-nidd/v1/{scsAsId}/configurations`).
2. إذا تم تعديل جدول المسارات، يجب إعادة تجميع اعتماد API حتى يتم تسجيل المسارات الجديدة (`mix deps.compile api_ex --force`)، ثم إعادة تشغيل الخدمة.

T8 لن تبدأ نقطة نهاية

الأعراض: تفشل OmniSCEF في بدء نقطة نهاية HTTPS لـ T8.

الأسباب المحتملة:

- ملف شهادة TLS أو مفتاح مفقود أو غير قابل للقراءة.
- المنفذ المُكون قيد الاستخدام بالفعل.

الحل:

1. تأكد من أن `tls_cert_path` و`tls_key_path` تشير إلى ملفات PEM صالحة وقابلة للقراءة. راجع نقطة نهاية واجهة برمجة التطبيقات T8.
2. تأكد من عدم ارتباط أي شيء آخر بالمنفذ المُكون على واجهة `listen_ip`.
3. في بيئة خاضعة للرقابة، قم بتعيين `enable_tls: false` لتشغيل بدون TLS. يجب عند أو قبل TLS دائمًا إنهاء عمليات النشر في الإنتاج OmniSCEF.