EIR (سجل هوية المعدات)

نظرة عامة

يتضمن HSS EIR (سجل هوية المعدات) مدمج يوفر التحقق من هوية المعدات للأجهزة المحمولة. يقوم EIR بالتحقق من أرقام IMEI (هوية المعدات المحمولة الدولية) لتحديد ما إذا كانت المعدات المحمولة مصرح بها أو مسروقة أو تحت المراقبة قبل السماح بالوصول إلى الشبكة.

القدرات الرئيسية

- **واجهة S13**: التحقق من هوية المعدات عبر بروتوكول Diameter
- **التحقق من IMEI**: التحقق من هوية المعدات باستخدام IMEI/IMEISV
- **مطابقة مرنة**: مطابقة نمطية تعتمد على Regex لـ IMEI و IMEISV و IMSI
- **تصنيف ثلاثي المستويات**: دعم القوائم البيضاء والسوداء والرمادية
- **تقييم مرتب**: يتم تقييم القواعد بترتيب تصاعدي، ويمكن إدراج قاعدة جديدة في أي موضع
- **سياسات قابلة للتكوين**: سلوك قابل للتخصيص للمعدات غير المعروفة
- **REST API**: عمليات CRUD كاملة لإدارة قواعد EIR

الهيكلية

واجهة Diameter

الواجهة	معرف التطبيق	النظير	الغرض
S13	16,777,252	MME/SGSN	التحقق من هوية المعدات

قاعدة بيانات قواعد المعدات

يستخدم EIR نظام مطابقة قائم على القواعد مرن:

EIR_RULE		
uuid	id	PK
string	action	
string	regex	
int	precedence	
timestamp	inserted_at	
timestamp	updated_at	

إجراءات القاعدة:

- `whitelist` - السماح بالمعدات
- `blacklist` - حظر المعدات
- `greylist` - مراقبة المعدات

أنماط Regex: المطابقة ضد IMSI أو IMEISV و IMEI

قيم حالة المعدات

الحالة	الرمز	المعنى	إجراء الشبكة
قائمة بيضاء	0	المعدات معتمدة	السماح بالوصول إلى الشبكة
قائمة سودا��	1	المعدات مسروقة/محظورة	رفض الوصول إلى الشبكة
قائمة رمادية	2	المعدات تحت المراقبة	السماح مع المراقبة

واجهة S13

العمليات المدعومة

إجابة التحقق من هوية المعدات (ECA) / طلب التحقق من هوية المعدات (ECR)

الاتجاه: MME/SGSN → HSS (EIR)

التحفيز: يتحقق MME من هوية المعدات أثناء الاتصال أو تحديث منطقة التتبع

طلب AVPs:

- Session-Id
- Origin-Host, Origin-Realm
- Destination-Realm
- Auth-Session-State
- Terminal-Information
  - IMEI (14 رقم كما هو موجود في AVP IMEI S13؛ مع نسخة البرنامج يشكل IMEISV المكون من 16 رقم. الطول غير مُتحقق منه)
  - Software-Version (رقمان، اختياري)
- User-Name (IMSI، اختياري)
- Vendor-Specific-Application-Id

إجراءات EIR:

1. استخراج IMEI و (إذا كانت موجودة) IMSI ونسخة البرنامج (إذا كانت موجودة)
2. إذا تم توفير IMSI:
   - تحقق من وجود المشترك وتمكينه
   - تحديث حالة المشترك بمعلومات آخر ظهور (`last_seen_realm`, `last_received_diameter_message_type`, `last_seen_imei`, `last_seen_imei_software_version`, `last_seen_imei_timestamp`). يتم تسجيل هوية المعدات بغض النظر عن حالة المعدات المعادة.
3. محاولة البحث عن المعدات بترتيب الأولوية:
   - **مطابقة IMEISV** (IMEI + نسخة البرنامج المدمجة)
   - **مطابقة IMEI** (IMEI فقط)
   - **مطابقة IMSI** (إذا تم توفيرها في الطلب)
   - **سياسة المعدات غير المعروفة** (سلوك افتراضي مُعد مسبقًا)
4. إرجاع حالة المعدات

استجابة AVPs:

- Session-Id (مكرر من الطلب)

- Result-Code: 2001 (نجاح)
- Equipment-Status: 0 (قائمة بيضاء) / 2 (قائمة رمادية) / 1 (قائمة سوداء)

استجابات الخطأ:

- Experimental-Result: 5422 (المعدات/المشترك غير موجود)
- Experimental-Result: 5012 (خطأ عام)

منطق مطابقة المعدات

ترتيب الأولوية

استراتيجية بحث متسلسلة لتعظيم مرونة المطابقة EIR يستخدم:

```
1. IMEISV (IMEI + نسخة البرنامج)
   ↓ (إذا لم يكن هناك تطابق)
2. IMEI فقط
   ↓ (إذا لم يكن هناك تطابق)
3. IMSI (إذا تم ��وفيرها في الطلب)
   ↓ (إذا لم يكن هناك تطابق)
4. سياسة المعدات غير المعروفة
```

خوارزمية المطابقة

الخطوة 1: مطابقة IMEISV

- نسخة البرنامج: `"08" + "35979139461611" =` دمج IMEI + `3597913946161108""`
- اختبار ضد قواعد EIR بترتيب تصاعدي
- إرجاع الإجراء ("قائمة بيضاء"، "قائمة سوداء"، "قائمة رمادية") للقاعدة المطابقة الأولى

الخطوة 2: مطابقة IMEI (استرجاع)

- استخدام IMEI فقط: `35979139461611"`
- اختبار ضد قواعد EIR بترتيب تصاعدي
- إرجاع الإجراء للقاعدة المطابقة الأولى

الخطوة 3: مطابقة IMSI (استرجاع إذا تم توفير IMSI)

- استخدام IMSI من الطلب: `"999999876543210"`
- اختبار ضد قواعد EIR بترتيب تصاعدي
- إرجاع الإجراء للقاعدة المطابقة الأولى
- **حالة الاستخدام**: حظر جميع المعدات لمشترك معين

الخطوة 4: سياسة المعدات غير المعروفة (استرجاع نهائي)

- إعداد التكوين: `eir_unknown_equipment_behaviour`
- الخيارات:
  - `:whitelist` - السماح بالمعدات غير المعروفة (مرن)
  - `:blacklist` - حظر المعدات غير المعروفة (مقيد)
  - `:greylist` - مراقبة المعدات غير المعروفة (معتدل)
  - `:reject_unknown_equipment` - إرجاع خطأ 5422 (صارم)

أولوية القاعدة

لكل قاعدة عدد صحيح `precedence` من 1 إلى 65535. داخل كل خطوة مطابقة، يتم اختبار القواعد بترتيب تصاعدي، وأول تطابق يفوز، لذا يتم تقييم الأرقام الأقل أولاً.

- إنشاء قاعدة بدون أولوية يضيفها بعد أعلى أولوية حالية.
- إنشاء قاعدة بأولوية صريحة يُدرجها في ذلك الموضع. كل قاعدة موجودة بأولوية متساوية أو أعلى تتحرك لأسفل بمقدار واحد، سواء كانت القيمة المطلوبة مستخدمة بالفعل أم لا، لذا لا يتم ملء الفجوات. مع القواعد `a`، `b`، `c` إنشاء عند 1، 2، 3، `d` بأولوية 1 يعطي `d`، `a`، `b`، `c` عند 1، 2، 3، 4.
- تحديث أولوية قاعدة تنقلها إلى ذلك الموضع وتغير فقط القواعد بين مواضعها القديمة والجديدة، لذا يحتفظ بقية القائمة بترتيبها.
- إرسال أولوية القاعدة الحالية، على سبيل المثال GET متبوعًا بـ PUT لنفس الجسم، لا يغير شيئًا.
- حذف قاعدة يترك فجوة في الترقيم. الفجوات غير ضارة لأن الترتيب النسبي فقط هو المهم.
- تحدد الأولوية ترتيب القواعد داخل خطوة المطابقة. لا تغير ترتيب خطوات IMEISV و IMSI أعلاه و IMEI.

بترتيب الإنشاء عند ترحيل N القواعد التي كانت موجودة قبل تقديم الأولوية يتم ترقيمها من 1 إلى قاعدة البيانات. إذا تداخلت أي من تلك القواعد، راجع أولوياتها باستخدام `GET /api/eir/rule`

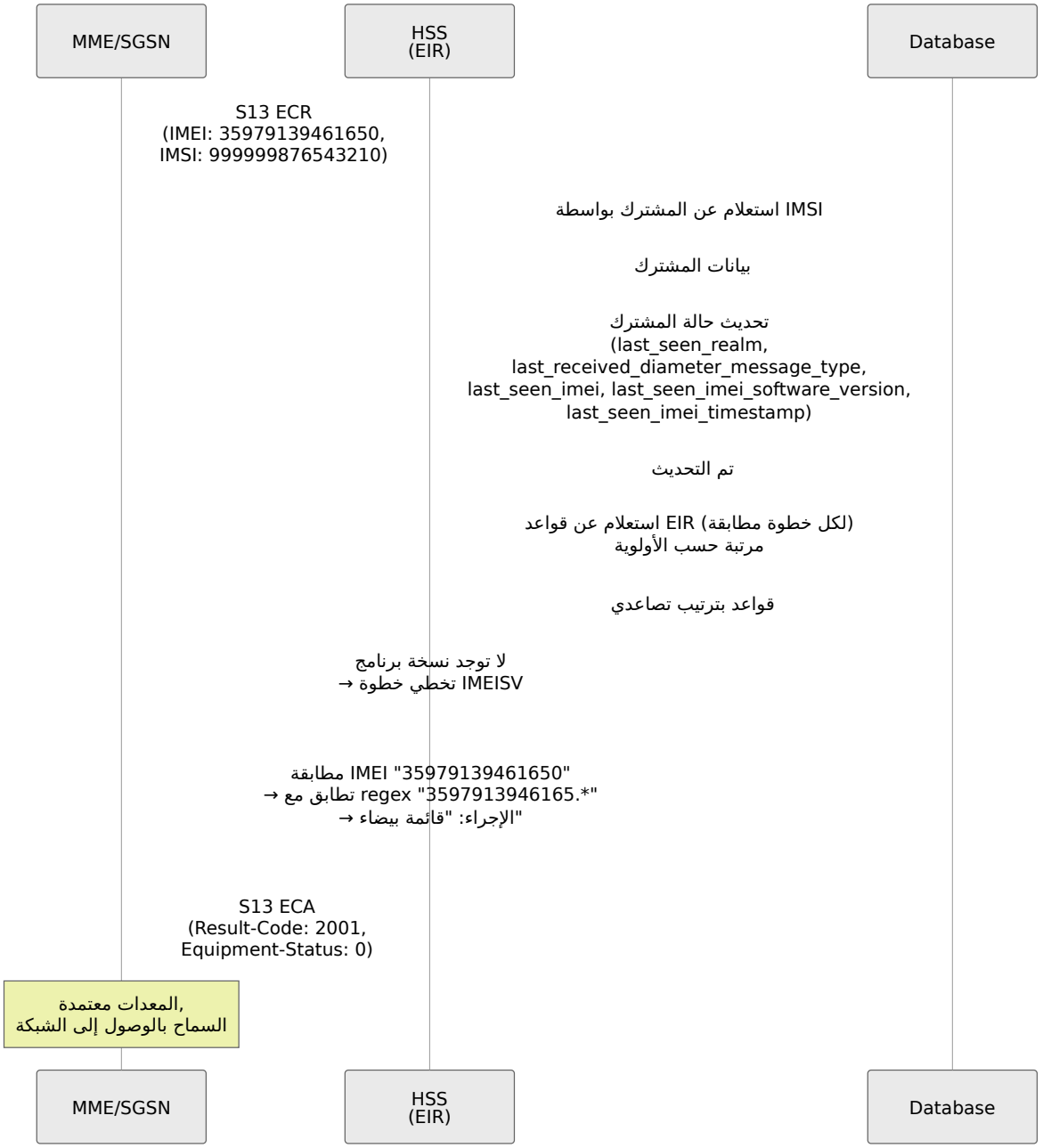
بعد الترقية.

أمثلة على أنماط Regex

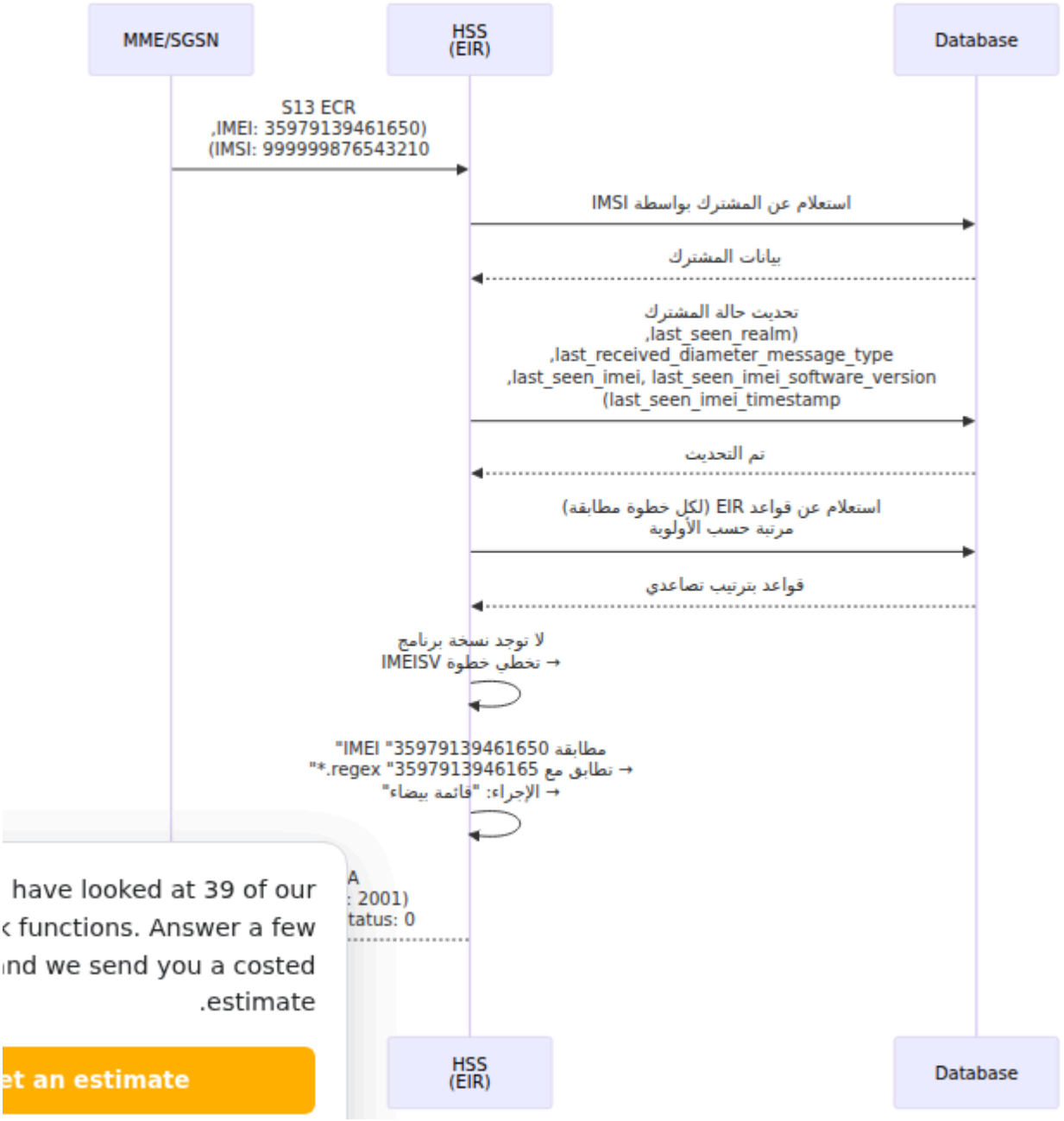
حالة الاستخدام	المطابقات	النمط
قائمة بيضاء/سوداء لجهاز واحد	دقيق IMEI	`"35979139461650"`
نطاق الشركة المصنعة/النموذج	نمط IMEI مع wildcard	`"3597913946165.*"`
جهاز محدد مع نسخة البرنامج	دقيق IMEISV	`"3597913946161108"`
حظر جميع ��لمعدات للمشترك	IMSI	`"999999876543210"`
تخصيص نوع الجهاز بالكامل	نمط TAC مع wildcard	`"359791.*"`

تدفقات الرسائل الشائعة

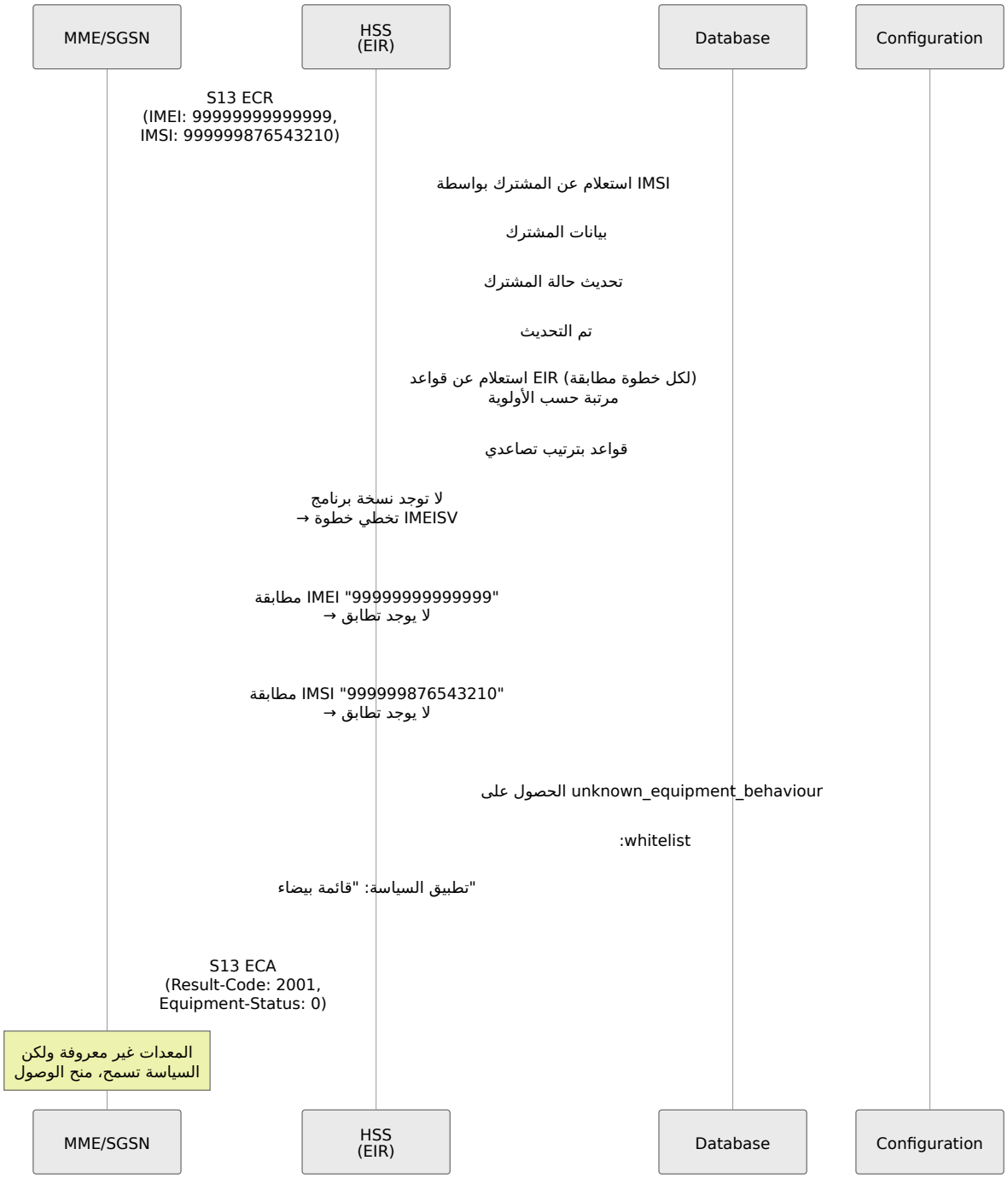
معروف في IMEI - التدفق 1: التحقق من المعدات القائمة البيضاء



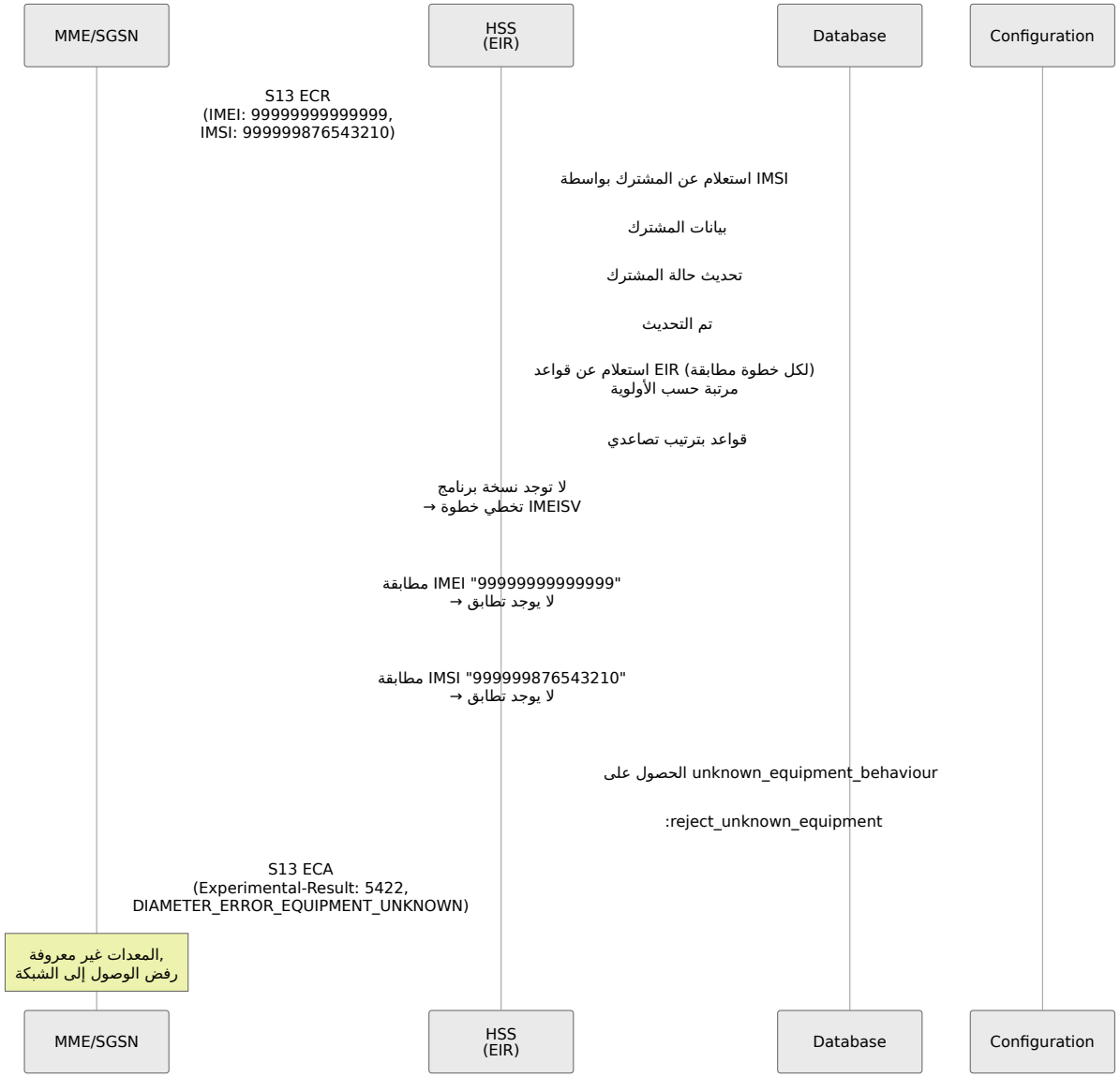
في القائمة IMEI - التدفق 2: التحقق من المعدات السوداء (جهاز مسروق)



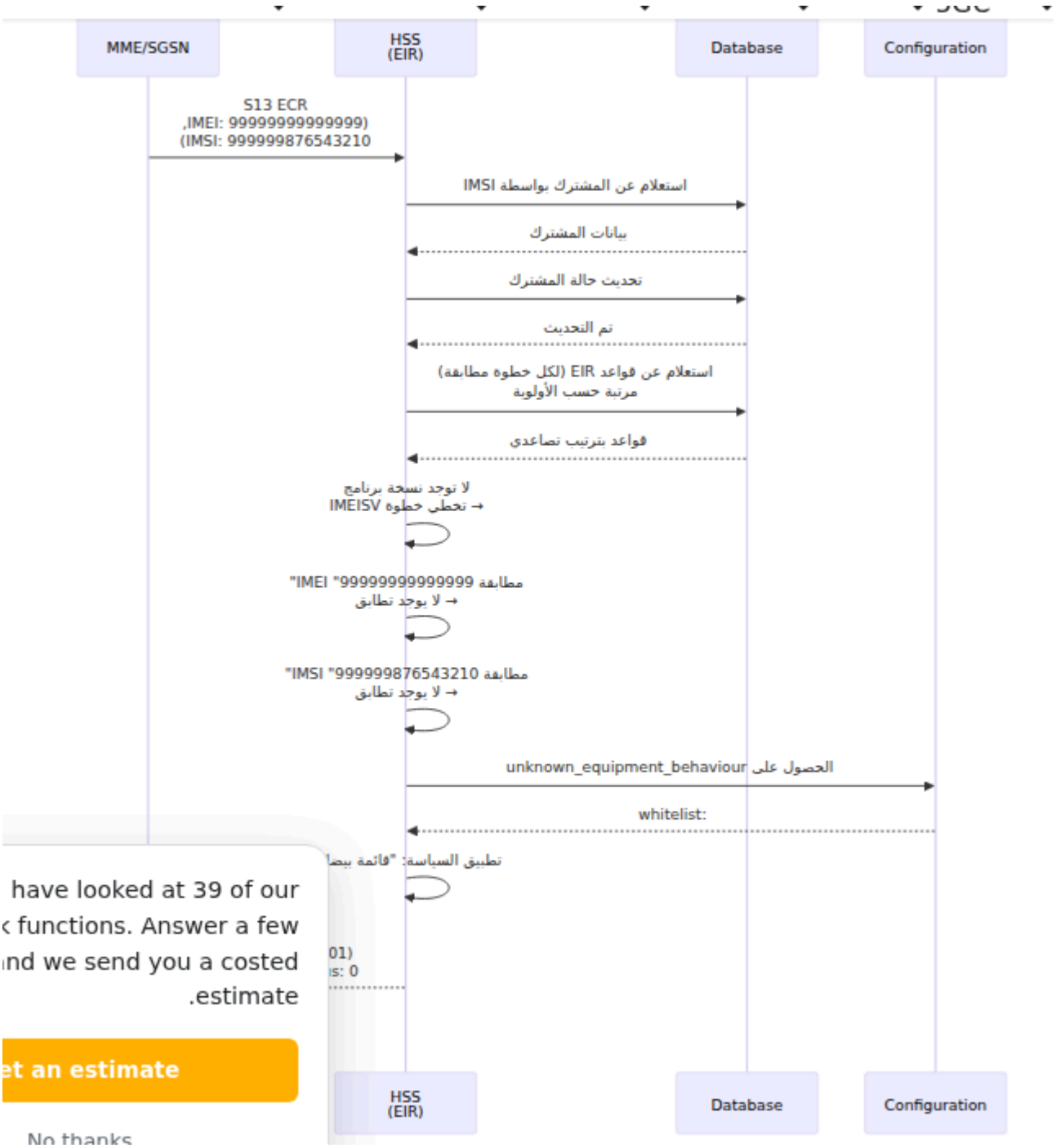
التدفق 3: التحقق من المعدات - معدات غير معروفة (سياسة القائمة البيضاء)



التدفق 4: التحقق من المعدات - معدات غير معروفة (سياسة الرفض)



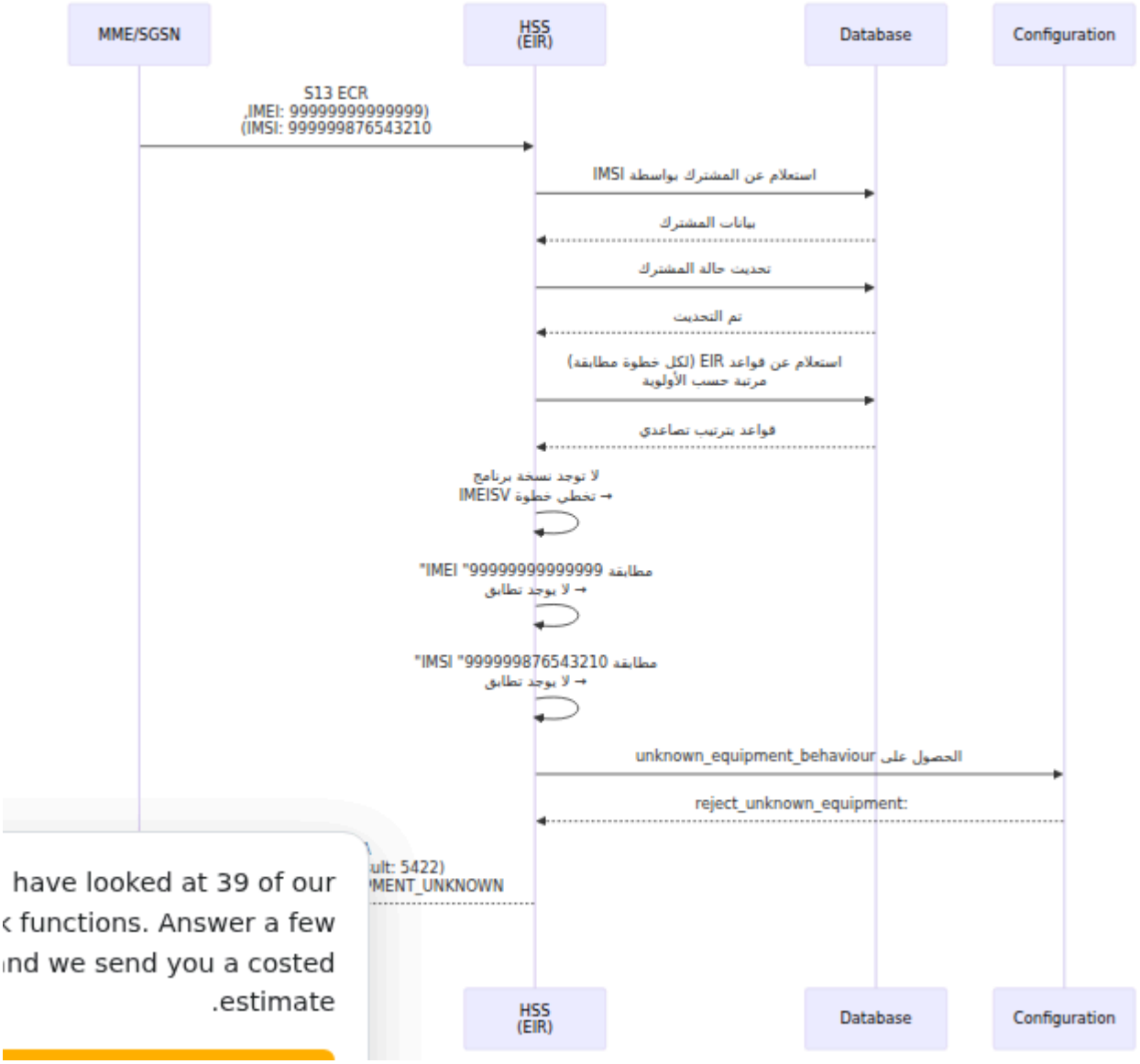
التدفق 5: التحقق من المعدات - مشترك غير معروف أو معطل



IMEISV التدفق 6: التحقق من المعدات - مطابقة



التدفق 7: التحقق من المعدات - حظر IMSI



REST API

إدارة قواعد EIR

مسار القاعدة: `/api/eir/rule`

مسطحة تحتوي على حقول القاعدة في المستوى الأعلى (انظر JSON أجسام الطلب هي كائنات تحمل كل قاعدة. API تنسيق الطلب). تستخدم الاستجابات الغلاف القياسي الموصوف في مرجع `id` و `action` و `regex` و `precedence`.

قائمة جميع قواعد EIR

الطلب:

```
GET /api/eir/rule
```

الاستجابة (HTTP 200):

```
{
  "status": "success",
  "response": [
    {
      "id": "e7f6a5b4-c3d2-4e1f-8a9b-0c1d2e3f4a5b",
      "action": "whitelist",
      "regex": "3597913946165.*",
      "precedence": 2
    },
    {
      "id": "f8a7b6c5-d4e3-4f2a-9b0c-1d2e3f4a5b6c",
      "action": "blacklist",
      "regex": "35979139461640",
      "precedence": 1
    }
  ]
}
```

لرؤية ترتيب `precedence` وليس حسب الأولوية. قم بترتيبها حسب `id`، القائمة مرتبة حسب التقييم.

الحصول على قاعدة EIR محددة

الطلب:

```
GET /api/eir/rule/{id}
```

الاستجابة (HTTP 200):

```
{
  "status": "success",
  "response": {
    "id": "e7f6a5b4-c3d2-4e1f-8a9b-0c1d2e3f4a5b",
    "action": "whitelist",
    "regex": "3597913946165.*",
    "precedence": 2
  }
}
```

إنشاء قاعدة EIR

الطلب:

```
POST /api/eir/rule
Content-Type: application/json

{
  "action": "blacklist",
  "regex": "35979139461640",
  "precedence": 1
}
```

التحقق:

- `action`: مطلوب، يجب أن تكون "greylist" أو "blacklist" أو "whitelist"
- `regex`: مطلوب، يجب أن تكون نمط regex صالح
- `precedence`: عدد صحيح اختياري من 1 إلى 65535. اتركه فارغًا لإضافة القاعدة بعد أعلى أولوية حالية. تقديم قيمة يُدرج القاعدة في ذلك الموضع وينقل كل قاعدة بأولوية متساوية أو أعلى لأسفل بمقدار واحد. انظر أولوية القاعدة.

الاستجابة (HTTP 201):

```
{
  "status": "success",
  "response": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "blacklist",
    "regex": "35979139461640",
    "precedence": 1
  }
}
```

استجابة الخطأ (HTTP 422):

```
{
  "status": "error",
  "response": {
    "invalid_fields": {
      "precedence": "must be greater than or equal to 1"
    }
  }
}
```

تحديث قاعدة EIR (جزئي)

الطلب:

```
PATCH /api/eir/rule/{id}
Content-Type: application/json

{
  "action": "greylist"
}
```

الاستجابة (HTTP 200):

```
{
  "status": "success",
  "response": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "greylist",
    "regex": "35979139461640",
    "precedence": 1
  }
}
```

تغيير `precedence` ينقل القاعدة إلى ذلك الموضع ويغير فقط القواعد بين مواضعها القديمة والجديدة. ترك `precedence` فارغًا، أو إرسال قيمتها الحالية، يبقي الترتيب دون تغيير. لا ترسل `null`: فإنه يمسح أولوية القاعدة وتُقيم القاعدة بعد كل قاعدة مرقمة.

تحديث قاعدة EIR (PUT)

الطلب:

```
PUT /api/eir/rule/{id}
Content-Type: application/json

{
  "action": "whitelist",
  "regex": "359791394616.*",
  "precedence": 3
}
```

الاستجابة (HTTP 200):

```
{
  "status": "success",
  "response": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "whitelist",
    "regex": "359791394616.*",
    "precedence": 3
  }
}
```

يطبق PUT الحقول الموجودة في الجسم، مثل PATCH؛ الحقول المفقودة تحتفظ بقيمها الحالية. إلى معرف غير موجود ينشئ القاعدة بذلك المعرف، متبعًا نفس موضع الأولوية كما في PUT POST.

حذف قاعدة EIR

الطلب:

```
DELETE /api/eir/rule/{id}
```

الاستجابة (HTTP 200):

```
{
  "status": "success",
  "response": ""
}
```

حذف قاعدة يترك فجوة في ترقيم الأولوية. تبقى القواعد المتبقية بترتيبها النسبي.

التكوين

إعداد خدمة Diameter

تطبيق S13 (`config/runtime.exs`):

```
%{
  application_name: :s13,
  application_dictionary: :diameter_gen_3gpp_s13,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_252}
  ]
}
```

سلوك المعدات غير المعروفة

قم بتكوين السلوك الافتراضي للمعدات التي لا تتطابق مع أي قواعد في `config/runtime.exs`:

مثال:

```
config :hss, :eir,
  unknown_equipment_behaviour: :whitelist
```

القيم الصالحة:

- `:whitelist` - السماح بالمعدات غير المعروفة (افتراضي، مرن)
- `:blacklist` - حظر المعدات غير المعروفة (مقيد)
- `:greylist` - مراقبة المعدات غير المعروفة (معتدل)
- `:reject_unknown_equipment` - إرجاع خطأ Diameter 5422 (صارم)

حالات الاستخدام:

- **التطوير/الاختبار**: `:whitelist` - السماح لجميع الأجهزة
- **الإنتاج (مرن)**: `:whitelist` - حظر فقط الأجهزة السيئة المعروفة
- **الإنتاج (معتدل)**: `:greylist` - تسجيل الأجهزة غير المعروفة للمراجعة
- **الإنتاج (صارم)**: `:reject_unknown_equipment` - السماح فقط للأجهزة المسجلة

معالجة الأخطاء

رمز النتيجة	النوع	المعنى	السبب
2001	نجاح	DIAMETER_SUCCESS	اكتمل التحقق من المعدات
5422	تجريبي	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	المشترك غير موجود أو المعدات غير المعروفة مرفوضة
5012	تجريبي	DIAMETER_UNABLE_TO_COMPLY	خطأ في المعالجة

حالات الاستخدام

1. إدارة الأجهزة المسروقة

السيناريو: تم الإبلاغ عن جهاز مسروق

الإجراء:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "35979139461640"  # IMEI دقيق
}
```

النتيجة: تم رفض الوصول إلى الشبكة للجهاز في الاتصال التالي

2. قائمة بيضاء للشركة المصنعة

السيناريو: الموافقة مسبقًا على نطاق كامل من طرازات الأجهزة

الإجراء:

```
POST /api/eir/rule
{
  "action": "whitelist",
  "regex": "359791394.*"  # TAC للشركة المصنعة/النموذج
}
```

النتيجة: تمت الموافقة على جميع الأجهزة في نطاق TAC

3. قفل معدات المشترك

السيناريو: حظر جميع المعدات لمشترك معين (قفل SIM)

الإجراء:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "999999876543210"  # IMSI
}
```

النتيجة: يتم حظر أي معدات مستخدمة مع هذه الشريحة

4. قائمة رمادية لمعدات الاختبار

السيناريو: مراقبة معدات الاختبار في الإنتاج

الإجراء:

```
POST /api/eir/rule
{
  "action": "greylist",
  "regex": "35979139.*"  # نطاق TAC لمعدات الاختبار
}
```

النتيجة: يتم السماح بالمعدات ولكن يتم الإشارة إليها للمراقبة

5. التحكم في نسخة البرنامج

السيناريو: حظر إصدار البرنامج الثابت الضعيف المحدد

الإجراء:

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "359791394616.*05"  # نطاق IMEI + 05 نسخة البرنامج
}
```

النتيجة: يتم حظر فقط الأجهزة التي تحتوي على نسخة البرنامج "05" في نطاق IMEI

تفاصيل التنفيذ

المكونات الداخلية

تتم تنفيذ وظيفة EIR باستخدام عدة وحدات داخلية:

- **معالج بروتوكول S13** - معالجة رسائل ECR/ECA
- **محرك مطابقة المعدات** - مطابقة IMEI/IMEISV/IMSI بناءً على Regex بترتيب الأولوية
- **موضع الأولوية** - منطق الإدراج في الموضع الذي يحرك القواعد المجاورة لـ EIR عند إنشاء قاعدة في، أو نقلها إلى، أولوية صريحة. تشترك قواعد الشحن فقط في فحص الحدود من 1 إلى 65535 ولا يتم إعادة ترقيمها
- **قاعدة بيانات قواعد EIR** - تخزين الأنماط والبحث
- **وحدة تحكم REST API** - نقاط نهاية إدارة القواعد

وظيفة البحث عن حالة المعدات

يتبع البحث عن حالة المعدات هذه المنطق المتسلسل:

1. **مطابقة IMEISV**: تحقق من IMEI + إصدار البرمجيات المدموجين
2. **مطابقة IMEI**: تحقق من IMEI فقط
3. **مطابقة IMSI**: تحقق من IMSI (إذا تم توفيره)
4. **معدات غير معروفة**: تطبيق سياسة افتراضية مكونة

النتائج المحتملة:

- `whitelist` - المعدات مسموح بها
- `blacklist` - المعدات محظورة
- `greylist` - المعدات تحت المراقبة
- `reject_unknown_equipment` - رفض صارم

اعتبارات الأمان

خصوصية IMEI

أرقام IMEI هي معرفات حساسة. الـ EIR:

- لا يسجل قيم IMEI بنص عادي بشكل افتراضي
- يقدم واجهة برمجة التطبيقات REST بدون مصادقة ما لم يتم تكوين مصادقة المفتاح المشترك الاختيارية (`config :api_ex, api: %{auth: %{key: "..."}}`، قابلاً `/api/eir/rule` قم بتمكينها أينما كان). يقدمها العملاء في رأس `x-api-key` للوصول من الشبكات غير الموثوقة

ترتيب القواعد

يتم تقييم القواعد بترتيب `precedence` تصاعدي ضمن كل خطوة مطابقة، وأول مطابقة تفوز. عندما تتداخل الأنماط، أعطِ القاعدة المحددة أولوية أقل:

```
Precedence 1: regex "35979139461640" action "blacklist"  (محددة)
Precedence 2: regex "359791.*" action "whitelist"  (عامة)
```

بينما القاعدة العامة بالفعل تحمل أولوية 1 ينقل `"precedence": 1` إنشاء القاعدة المحددة مع القاعدة العامة تلقائيًا إلى 2. انظر أولوية القاعدة لسلوك الترتيب الكامل.

تحديد المعدل

فكر في تنفيذ تحديد المعدل على:

- طلبات S13 ECR من نظراء غير موثوقين
- تعديلات قواعد REST API EIR
- استعلامات بحث IMEI لمنع هجمات التعداد

الوثائق ذات الصلة

- S13 مواصفة بروتوكول - بروتوكولات Diameter
- الوثائق الكاملة لواجهة برمجة التطبيقات - مرجع API
- العمارة العامة لـ HSS - العمارة
- الإجراءات التشغيلية - دليل العمليات

هيكل IMEI الملحق:

تنسيق IMEI (15 رقم)

```
35 9791 394616 1
|  |    |      └─ رقم التحقق (خوارزمية لونه)
|  |    └─ رقم السيريال (6 أرقام)
|  └─ FAC (رمز التجميع النهائي، 4 أرقام)
└─ TAC (رمز تخصيص النوع، 8 أرقام إجمالية بما في ذلك RBI)
   |  └─ RBI (معرف الهيئة المبلغة، 2 رقم)
   └─ الشركة المصنعة/النموذج (6 أرقام)
```

تنسيق IMEISV (16 رقم)

```
35 9791 394616 1 08
|  |    |      | └─ (2 رقم) إصدار البرمجيات
└─ IMEI (15 رقم)
```

أنماط المثال

IMEI/IMEISV	النمط	المطابقات
359791394616108	`3597913946161.*`	جميع الأجهزة التي تحمل TAC+FAC+Serial 359791394616*
359791394616140	`35979139461614.`	جميع أرقام التحقق للسيريال 9-359791394616141
35979139461640	`35979139461640`	مطابقة IMEI دقيقة
3597913946163008	`3597913946163008`	مطابقة IMEISV دقيقة (IMEI + SV)

PCRF (وظيفة قواعد السياسة والفوترة)

نظرة عامة

وظيفة PCRF (وظيفة قواعد السياسة والفوترة) المدمجة التي توفر التحكم في HSS يتضمن في سياسات جودة الخدمة PCRF السياسة وقواعد الفوترة لجلسات البيانات المحمولة. يتحكم وتخصيص النطاق الترددي وقواعد الفوترة لكل من الحاملات الافتراضية والمخصصة في (QoS) شبكات LTE.

القدرات الرئيسية

- **واجهة Gx**: التحكم في السياسة لـ PGW/PCEF (بوابة شبكة البيانات الحزمية / وظيفة تنفيذ السياسة والفوترة)
- **واجهة Rx**: التفويض وجودة الخدمة لتدفقات الوسائط IMS (نظام الوسائط المتعددة IP)
- **واجهة Sy**: التحكم في حد إنفاق المشترك مقابل OCS واجهة - انظر Sy خارجي
- **إدارة السياسة الديناميكية**: تحديثات السياسة في الوقت الحقيقي عبر طلبات إعادة التفويض (RAR)
- **دعم VoLTE**: إنشاء حامل مخصص لمكالمات الصوت مع ضمان جودة الخدمة
- **قواعد الفوترة**: تحديد سلوك الفوترة وملفات السرعة باستخدام قوالب تدفق البيانات (TFTs)
- **REST API**: التحكم البرمجي في تنفيذ السياسة وإدارة القواعد

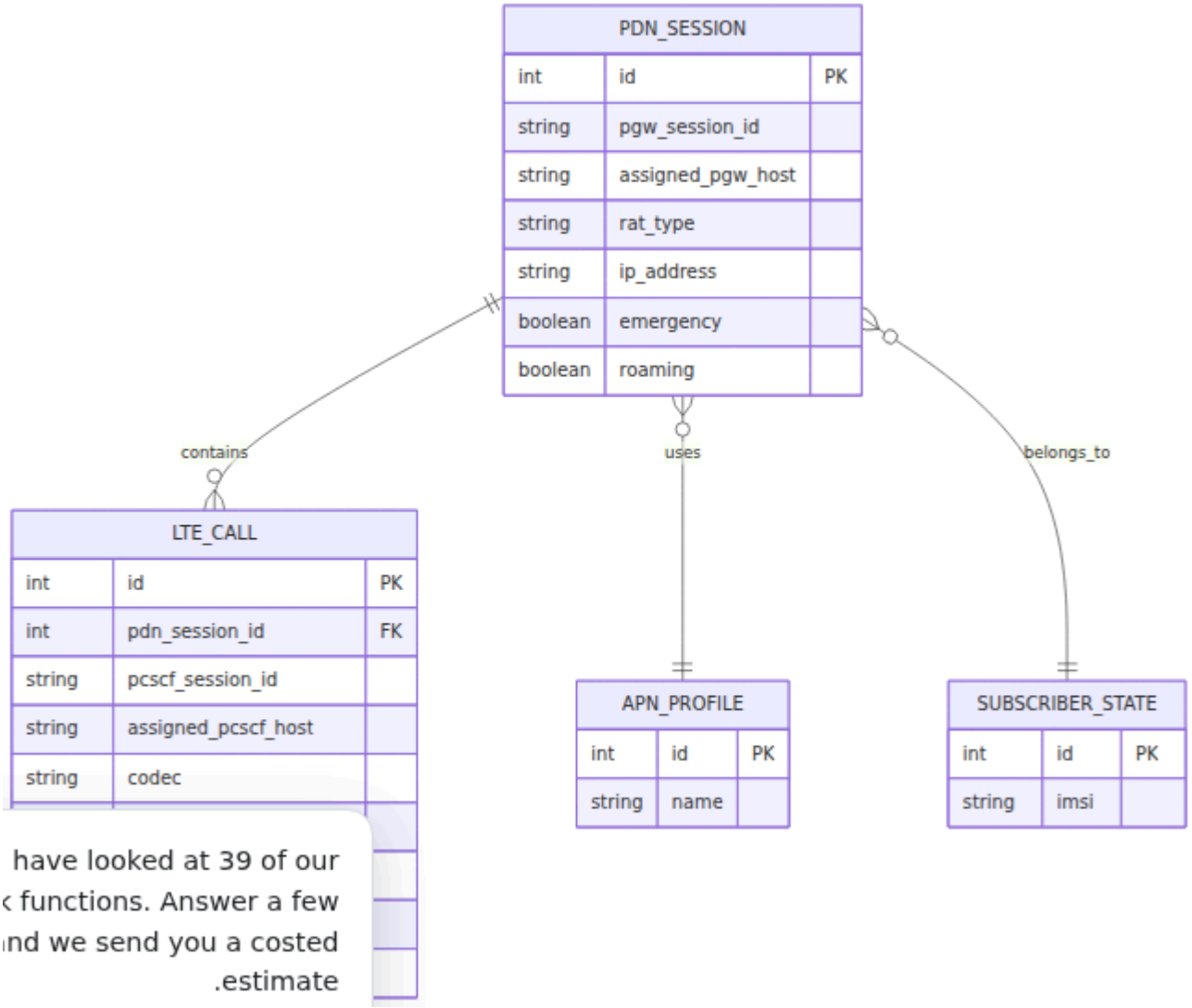
الهيكلية

واجهات القطر

الواجهة	معرف التطبيق	النظير	الغرض
Gx	16,777,238	PGW (PCEF)	إدارة جلسة PDN، تنفيذ QoS، قواعد الفوترة
Rx	16,777,236	P-CSCF (AF)	حجز النطاق الترددي IMS، تفويض الوسائط
Sy	16,777,302	OCS	حالة حد إنفاق المشترك، سياسة مدفوعة بالإنفاق - انظر واجهة Sy

إدارة حالة الجلسة

يحافظ PCRF على حالة الجلسة للاتصالات النشطة PDN ومكالمات VoLTE:



واجهة Gx

العمليات المدعومة

1. طلب التحكم في الائتمان - أولي (CCR-I)

التحفيز: يقوم PGW بإنشاء اتصال PDN جديد للمشترك

طلب AVPs:

- Session-Id
- Origin-Host, Origin-Realm
- Subscription-Id (يحتوي على IMSI)
- Called-Station-Id (اسم APN)

- IP-CAN-Type (نوع شبكة الوصول إلى الاتصال IP)
- RAT-Type (تكنولوجيا الوصول اللاسلكي)
- Framed-IP-Address (عنوان IP للـ UE)

إجراءات PCRF:

1. البحث عن المشترك بواسطة IMSI
2. استرجاع ملف APN وتهيئة QoS
3. إنشاء إدخال تتبع الجلسة
4. بناء سياسات QoS من ملف APN

استجابة AVPs:

- Result-Code: 2001 (DIAMETER_SUCCESS)
- QoS-Information (حدود النطاق الترددي المجمع لـ APN)
- Default-EPS-Bearer-QoS (QCI، ARP، الأولوية)
- Bearer-Control-Mode
- Online / Offline (طريقة الفوترة الافتراضية على مستوى الجلسة - انظر الفوترة على مستوى الجلسة Online/Offline)

2. طلب التحكم في الائتمان - تحديث (CCR-U)

التحفيز: يقوم PGW بالإبلاغ عن تغييرات الجلسة (تغيير الموقع، RAT، إلخ.)

إجراءات PCRF:

1. تحديد موقع الجلسة الحالية بواسطة معرف الجلسة
2. تحديث معلمات الجلسة (نوع RAT، إلخ، الموقع.)
3. إرجاع السياسات المحدثة إذا لزم الأمر

الاستجابة: Result-Code 2001 مع تحديثات سياسة اختيارية

3. طلب التحكم في الائتمان - إنهاء (CCR-T)

التحفيز: يقوم PGW بإنهاء اتصال PDN

إجراءات PCRF:

1. تحديد موقع الجلسة بواسطة معرف الجلسة

2. حذف الجلسة وسجلات المكالمات المرتبطة
3. تأكيد الإنهاء

الاستجابة: Result-Code 2001

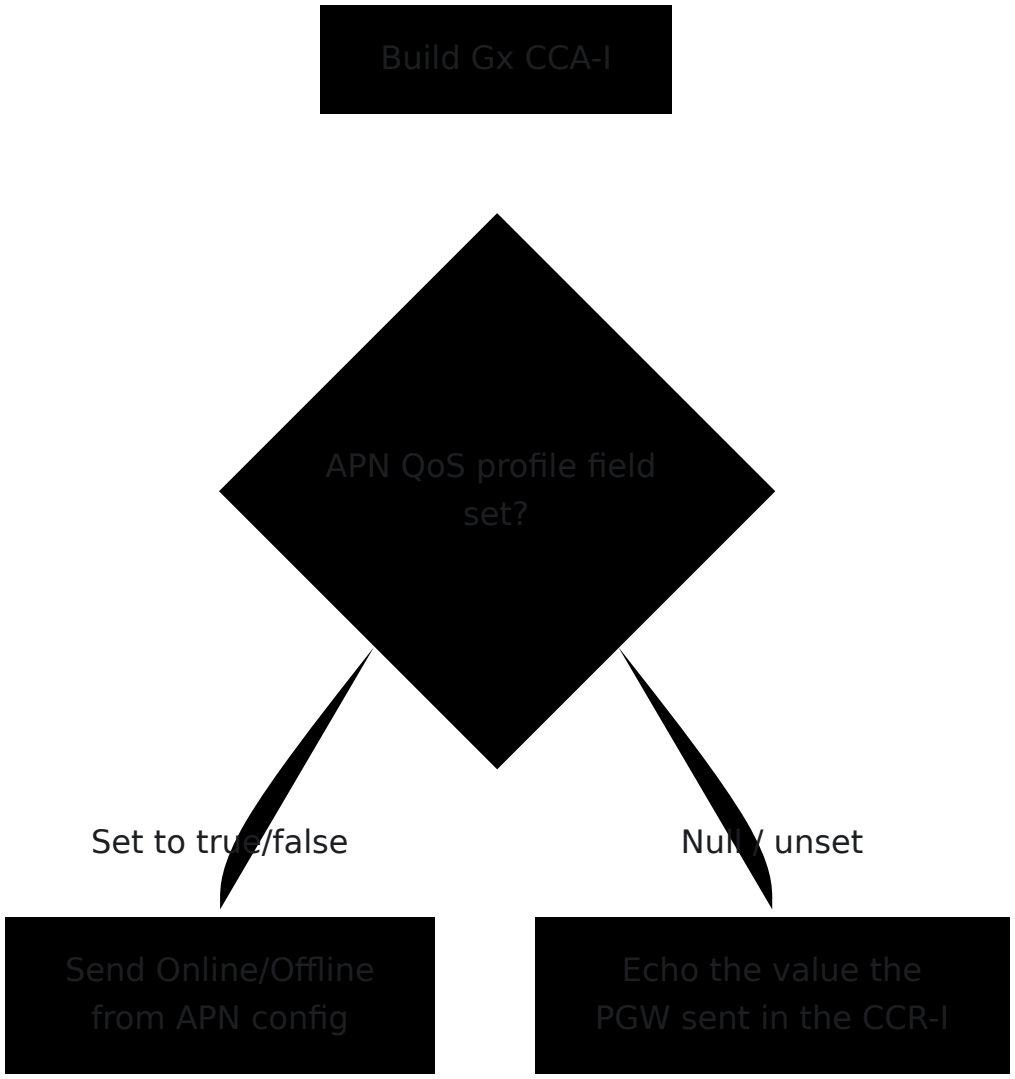
الفوترة على مستوى الجلسة Online/Offline

تحدد AVPs `Online` (AVP 1009) و `Offline` (AVP 1008) المرسلة في أعلى مستوى من **IP-CAN** (الحامل الافتراضي) **طريقة الفوترة الافتراضية لجلسة** Gx CCA-I **بأكملها** لكل `Online`/`Offline`. هذا يختلف عن 3GPP TS 29.212 الافتراضي)، كما هو محدد في قاعدة التي يتم حملها *داخل* تعريف قاعدة الفوترة، والتي تحكم فقط حركة المرور المطابقة لتلك القاعدة المحددة.

يمكن أن **يثبت** ملف CCR-I في PGW/PCEF **بصدى** أي قيم أعلنها PCRF بشكل افتراضي، يقوم طريقة الفوترة على مستوى الجلسة، متجاوزًا الصدى. يتم التحكم في ذلك من APN الخاص بـ QoS خلال حقلين اختياريين على ملف APN الخاص بـ QoS:

الحقل	النوع	AVP	التأثير
`online_charging_enabled`	Boolean	`Online` (1009)	`true` → `ENABLE_ONLINE (1)`، `false` → `DISABLE_ONLINE (0)`
`offline_charging_enabled`	Boolean	`Offline` (1008)	`true` → `ENABLE_OFFLINE (1)`، `false` → `DISABLE_OFFLINE (0)`

يتم حل كل حقل بشكل مستقل:



قيم AVP لطريقة الفوترة (TS 29.212):

AVP	الرمز	القيمة	الاسم	المعنى
`Online`	1009	0	DISABLE_ONLINE	لم يتم تطبيق الفوترة عبر الإنترنت (OCS / Gy) على الجلسة
`Online`	1009	1	ENABLE_ONLINE	تم تطبيق الفوترة عبر الإنترنت - يجب منح الائتمان قبل تدفق حركة المرور
`Offline`	1008	0	DISABLE_OFFLINE	لم يتم تطبيق الفوترة غير المتصلة (CDR / Gz) على الجلسة
`Offline`	1008	1	ENABLE_OFFLINE	تم تطبيق الفوترة غير المتصلة - تم تسجيل الاستخدام للفوترة

كيف يعمل: عندما تُترك `online_charging_enabled`/`offline_charging_enabled` غير محددة (الإعداد الافتراضي لكل ملف موجود)، تظل السلوكيات دون تغيير - يعكس طلب PCRF لذا يتم الحفاظ على موقف الفوترة الحالي للشبكة. يؤدي تعيين أي حقل إلى فرض وضع PGW، الفوترة هذا على كل CCR-I لأي APN يستخدم الملف، بغض النظر عن ما يعلنه PGW.

حالة الاستخدام: تثبيت الفوترة عبر الإنترنت لـ IoT/بعد الدفع APN أو فرض الفوترة غير المتصلة على، (حتى لو طلب الفوترة غير المتصلة OCS استشارة PGW لذا يجب على) مسبق الدفع APN الخاص بـ QoS نظرًا لأن الإعداد موجود على ملف APN، فإنه ينطبق بشكل لضمان توليد CDR. يشير إلى ذلك الملف APN موحد على كل.

> **ملاحظة:** هذا يتحكم في *الإعداد الافتراضي للجلسة* فقط. لا تزال الفوترة لكل حركة مرور تحكمها حقول `online_charging_enabled`/`offline_charging_enabled` على تعريف قاعدة الفوترة AVPs قواعد الفوترة الفردية، والتي تظهر داخل.

4. طلب إعادة التفويض (RAR)

الاتجاه: PCRF → PGW (يبدأ HSS)

التحفيز:

- إعداد مكالمة IMS (ت triggers Rx AAR Gx RAR)

- إنهاء مكالمة IMS (ت triggers Rx STR Gx RAR)
- إعادة التفويض اليدوي عبر REST API

AVPs RAR:

- Session-Id (معرف جلسة PGW)
- Auth-Application-Id: 16,777,238
- Re-Auth-Request-Type (0 = التفويض فقط)
- Charging-Rule-Install/Remove
- QoS-Information (للحاملات المخصصة)

إجراءات PGW: إنشاء/تعديل/حذف الحاملات المخصصة بناءً على قواعد الفوترة

قواعد الفوترة وقوالب تدفق البيانات

يدعم PCRF تعريف قواعد الفوترة باستخدام قوالب تدفق البيانات (TFTs) للتحكم في:

- **الفوترة الخاصة بالخدمة** - معدلات مختلفة للفيديو، الألعاب، وسائل التواصل الاجتماعي، إلخ.
- **ملفات السرعة** - تقييد أو إعطاء الأولوية لحركة المرور المطابقة لأنماط محددة
- **سياسات قائمة على الاستخدام** - تطبيق QoS مختلفة بناءً على نوع حركة المرور أو الوجهة

يمكن أن تكون قواعد الفوترة:

- مثبتة ديناميكيًا عبر Gx RAR بناءً على اكتشاف التطبيق
- محددة مسبقًا ويتم تحفيزها بواسطة ظروف محددة (وقت اليوم، الموقع، الحصة)
- باستخدام قواعد تصفية الحزم TFTs مرتبطة بـ IP (5-tuple: عنوان البروتوكول، منفذ المصدر/الوجهة، المصدر/الوجهة)

حالات الاستخدام الشائعة:

- **التسعير الصفري** - الوصول غير المحدود إلى خدمات معينة (Spotify، WhatsApp، Facebook) دون استهلاك حصة البيانات
- **الوصول بعد الحصة** - السماح ببوابة الرعاية الذاتية ومواقع الدعم حتى بعد استنفاد المشترك لحد البيانات
- **سرعة متدرجة** - سرعة عالية للخدمات المتميزة، مقيدة للمحتوى القياسي

- **سياسات قائمة على الوقت** - دفق غير محدود في أوقات الذروة، إعطاء الأولوية في أوقات الذروة
- **سياسات التجوال** - فوترة مختلفة لاستخدام البيانات الدولية مقابل المحلية
- **SLA للشركات** - ضمان QoS للتطبيقات الحيوية للأعمال

هيكل سياسة QoS

QoS للحامل الافتراضي (من ملف APN):

```
{
  "QoS-Class-Identifier": 9,          // QCI (9 = الحامل الافتراضي)
  "APN-Aggregate-Max-Bitrate-UL": 50000,  // كيلوبت في الثانية
  "APN-Aggregate-Max-Bitrate-DL": 100000, // كيلوبت في الثانية
  "Allocation-Retention-Priority": {
    "Priority-Level": 8,
    "Pre-emption-Capability": 1,      // قد يتم استباقه
    "Pre-emption-Vulnerability": 1    // قد يتم استباقه
  }
}
```

QoS للحامل المخصص (VoLTE):

```
{
  "QoS-Class-Identifier": 1,          // QCI 1 = الصوت المحادثة
  "Max-Requested-Bandwidth-UL": 128000,   // بت في الثانية
  "Max-Requested-Bandwidth-DL": 128000,   // بت في الثانية
  "Guaranteed-Bitrate-UL": 128000,
  "Guaranteed-Bitrate-DL": 128000
}
```

واجهة Rx

العمليات المدعومة

1. طلب AA (AAR) / إجابة AA (AAA)

التحفيز: يطلب P-CSCF التفويض لجلسة الوسائط IMS (إعداد مكالمة VoLTE)

طلب AVPs:

- Session-Id (معرف جلسة P-CSCF)
- Subscription-Id (IMSI أو SIP URI)
- Media-Component-Description
  - Media-Type (صوت، فيديو)
  - Max-Requested-Bandwidth-UL/DL
  - Codec-Data
  - Flow-Description (5 قواعد تصفية الحزم-tuple)
- AF-Application-Identifier

إجراءات PCRF:

1. البحث عن المشترك بواس��ة IMSI أو SIP URI
2. العثور على جلسة IMS النشطة
3. استخراج معلمات الوسائط (ترميز، عرض النطاق الترددي، قواعد التدفق)
4. إنشاء إدخال تتبع المكالمة
5. **تحفيز Gx RAR إلى PGW** لإنشاء حامل مخصص
6. الانتظار لاستجابة Gx RAA
7. إرجاع Rx AAA مع نتيجة التفويض

استجابة AVPs:

- Result-Code: 2001 (نجاح) أو 5063 (الخدمة غير مفوضة)

مكالمات الطوارئ (SOS)، بدون / بما في ذلك المتصلين غير المصرح لهم SIM

حتى عندما لا يكون المتصل مشتركًا (`urn:service:sos`) تتم الموافقة على مكالمات الطوارئ معروفًا (جهاز بدون SIM، أو مشترك تجوال بدون بيانات اعتماد في السجل). هذا مطلوب حتى تحصل مكالمات الطوارئ دائمًا على QoS الصحيح (TS 23.167).

كيف يتعرف PCRF على AAR ويوافق عليه الطوارئ:

1. **كشف الطوارئ.** يتم اعتبار الطلب طارئًا إذا كان `Subscription-Id` هو SIP URI يحتوي على `sos`، **أو** إذا كان `Framed-IP-Address` لـ AAR يحل إلى جلسة Gx الطوارئ طارئ بواسطة PDN تم إنشاؤها بالفعل كـ PDN (Gx CCR-I يحدد جانب المسار الثاني هو ما). `sos` الذي يحتوي على `Called-Station-Id` / APN بواسطة يسمح لـ INVITE (بدون هوية قابلة للاستخدام) بأن يتم الموافقة عليه **مجهول** طارئ.

2. **حل المشترك.** يتم البحث عنه بواسطة `Subscription-Id`، أو بواسطة `Framed-IP-Address`. لا يحتوي PDN **اليتيم** الطارئ (الذي تم إنشاؤه بواسطة Gx لمشترك على مشترك (غير معروف (`subscriber_state_id: nil`)؛ تأخذ AAR بعد ذلك المسار اليتيم بدلاً من مسار المشترك العادي.
3. **ملف APN الطارئ.** يتم أخذ QoS للحامل المخصص من ملف APN الطارئ (انظر الطارئ الافتراضي المدمج" أدناه "ملف APN).
4. يقوم Gx RAR بتثبيت الحامل الصوتي المخصص (QCI 1) على PDN (اليتيم)، وتعيد AAA `2001`.

> ملاحظة: لا يؤدي `Framed-IP-Address` إلى التفويض إلا إذا كان يتوافق مع PDN الذي أنشأه Gx من طارئ AAR). يتم رفض طلب غير الطوارئ من UE غير المسجل عند P-CSCF (لا يصل أبدًا إلى PCRF كـ **كطوارئ**.

ملف APN الطارئ الافتراضي المدمج.** لم يعد يعتمد التفويض الطارئ على وجود مشغل الطارئ APN بحل ملف PCRF في قاعدة البيانات. يقوم APN `sos` قد قام مسبقًا بتوفير ملف على النحو التالي:

- إذا كان `sos`، الخاص به هو APN محدد من قبل المشغل يكون معرف ملف APN موجودًا؛ خلاف ذلك
- **ملف APN الطارئ الافتراضي** المدمج الذي توفره OmniHSS.

`apn_profile_id: nil`، لا يوجد صف في قاعدة البيانات) الافتراضي المدمج هو ملف عابر الطارئ QoS مع (اليتيم - العمود قابل للإلغاء على PDN:

القيمة	المعلمة
5	الحامل الطارئ الافتراضي QCI
1 (أولوية ARP 2)	الحامل الصوتي المخصص QCI
1	أولوية الاحتفاظ بالتخصيص
مفعل	قدرة الاستباق
معطل	قابلية الاستباق
10000 كيلوبت في الثانية	APN-AMBR UL/DL

قم بإنشاء ملف APN، (PCRF أو لتعيين قواعد الفوترة لكل مشغل عبر ملف) لتجاوز هذه القيم في قاعدة البيانات - فإنه يأخذ الأولوية على الافتر��ضي المدمج `sos`.

2. طلب إنهاء الجلسة (STR) / إجابة إنهاء الجلسة (STA)

التحفيز: يقوم P-CSCF بإنهاء جلسة IMS (إنهاء المكالمة)

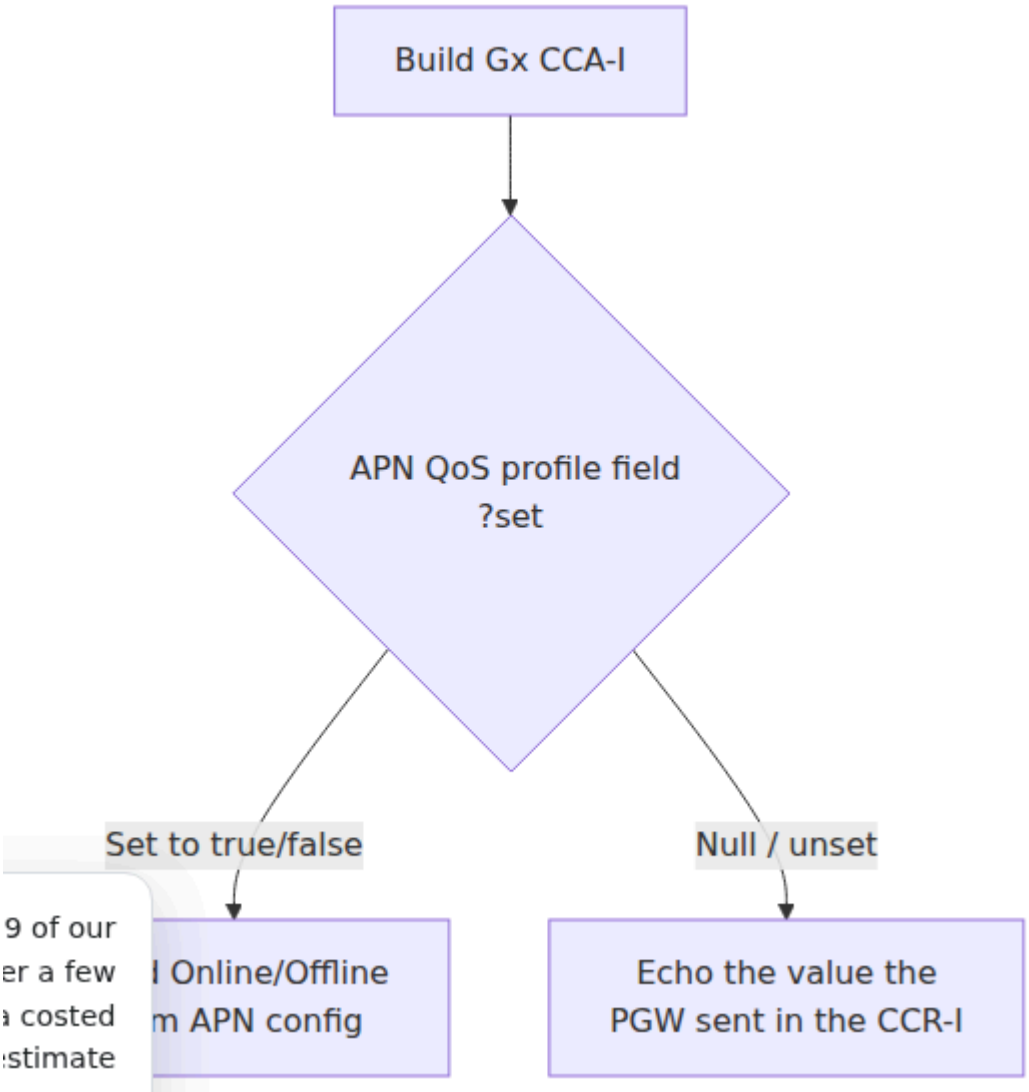
إجراءات PCRF:

1. تحديد موقع جلسة المكالمة بواسطة معرف جلسة P-CSCF
2. **تحفيز Gx RAR إلى PGW** لإزالة الحامل المخصص
3. حذف إدخال تتبع المكالمة
4. إرجاع تأكيد STA

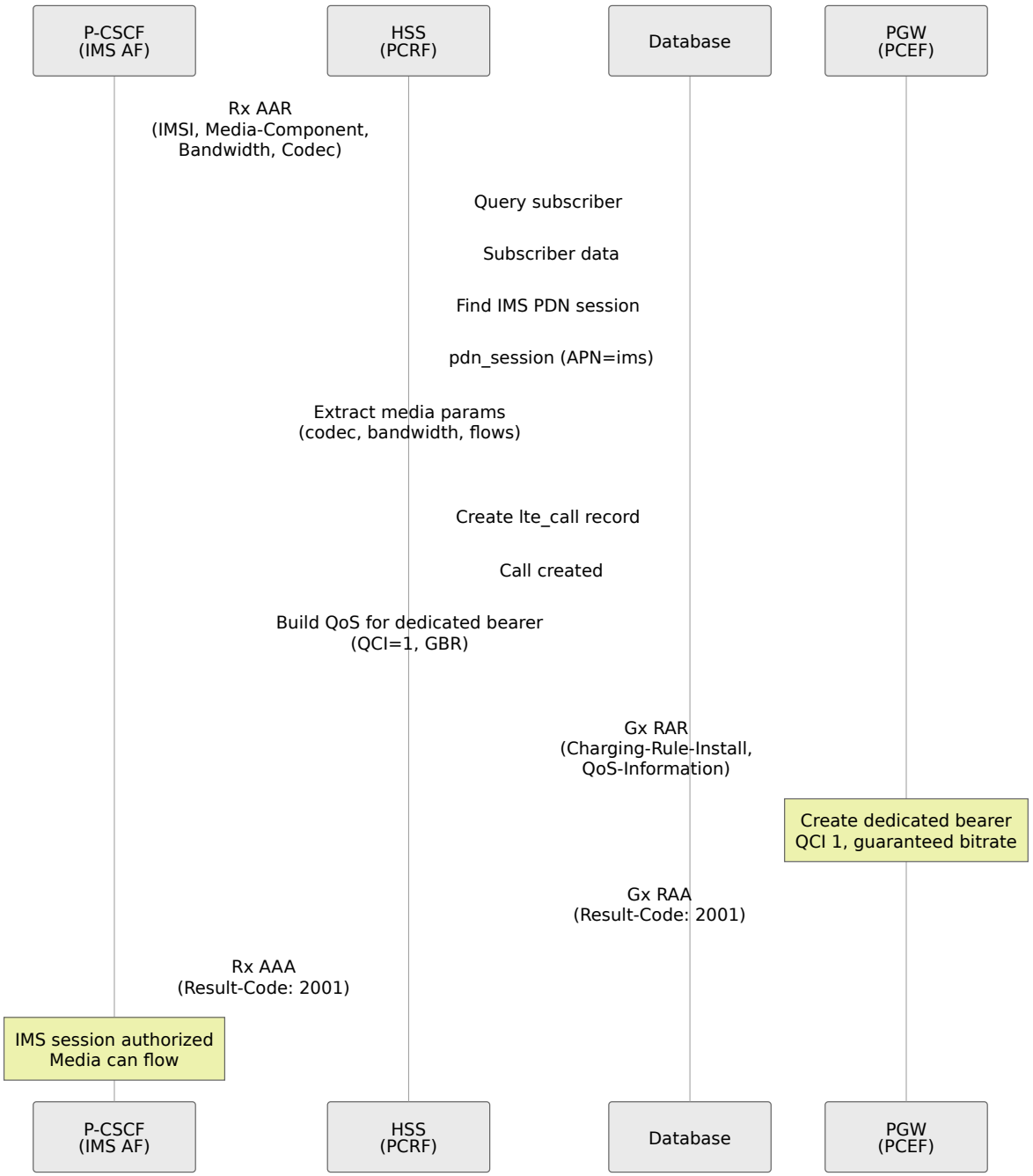
الاستجابة: Result-Code 2001

تدفقات الرسائل الشائعة

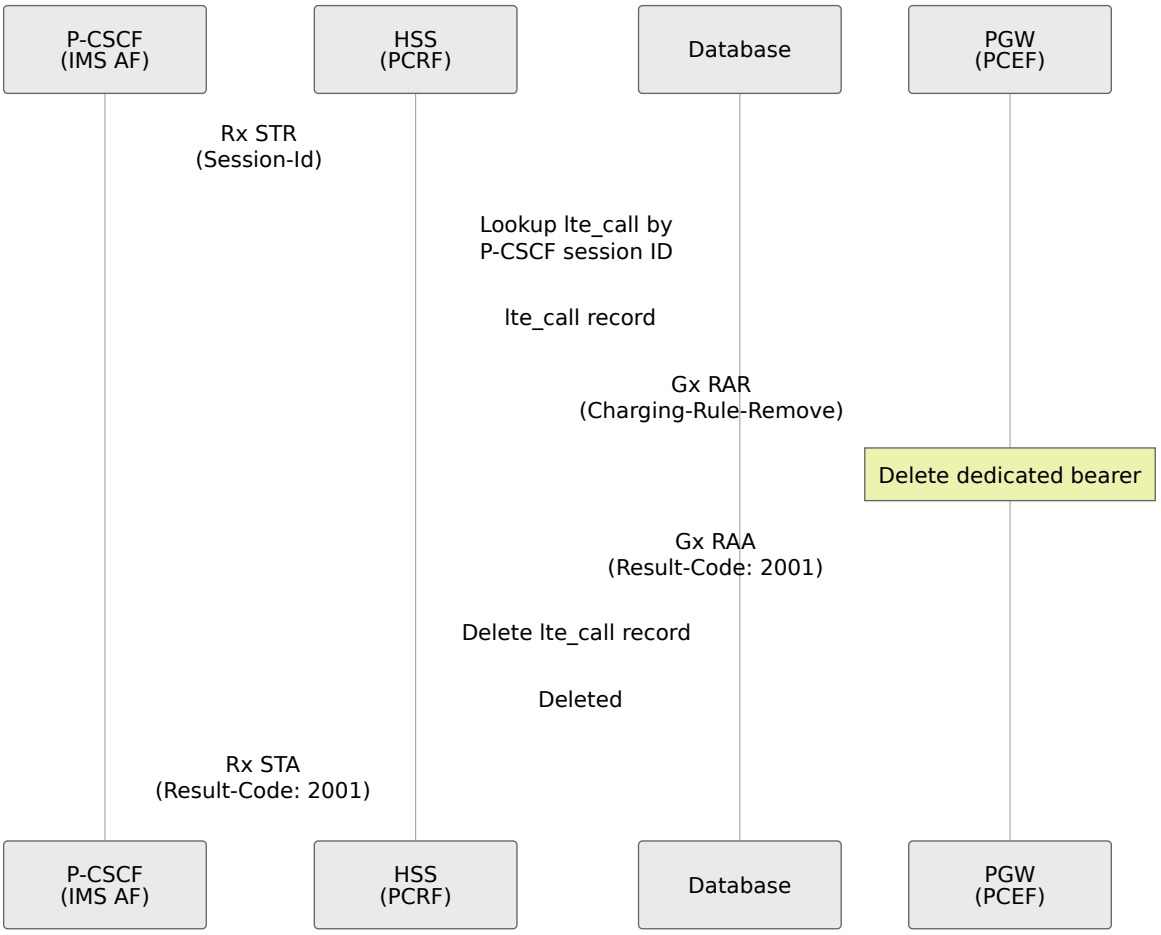
التدفق 1: إنشاء جلسة PDN



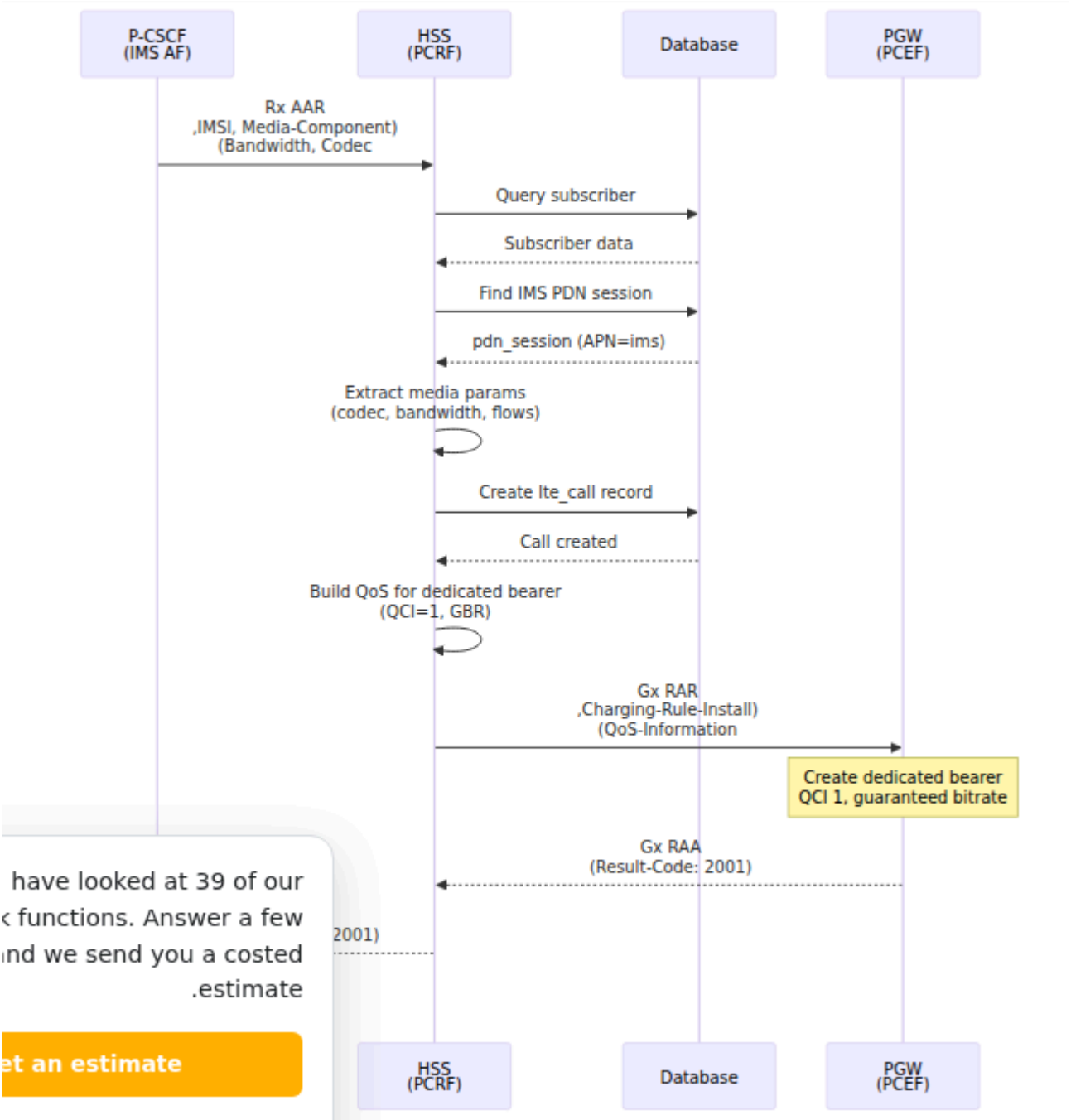
التدفق 2: إعداد مكالمة VoLTE (Rx AAR → Gx RAR)



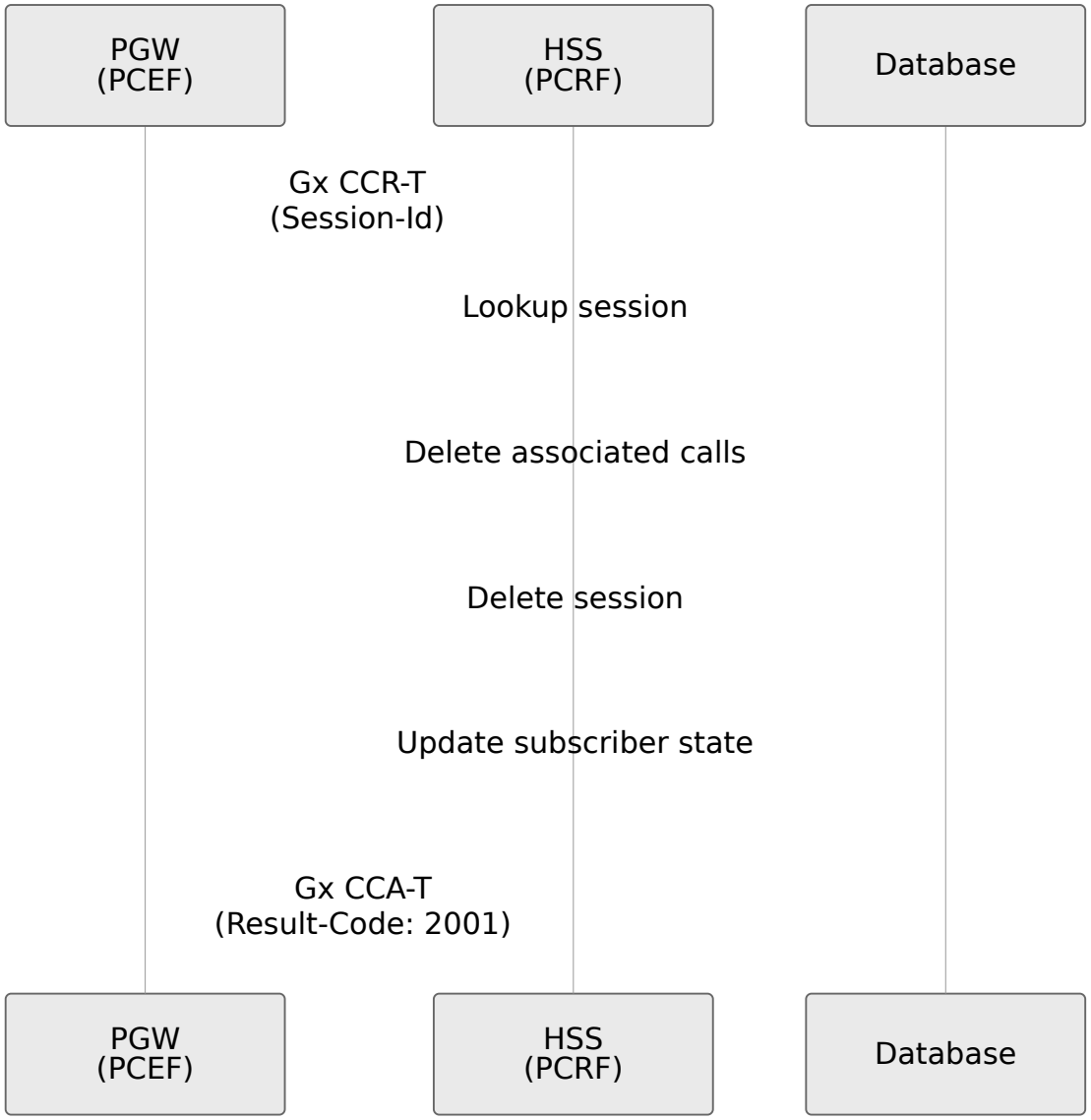
التدفق 3: إنهاء مكالمة VoLTE (Rx STR → Gx RAR)



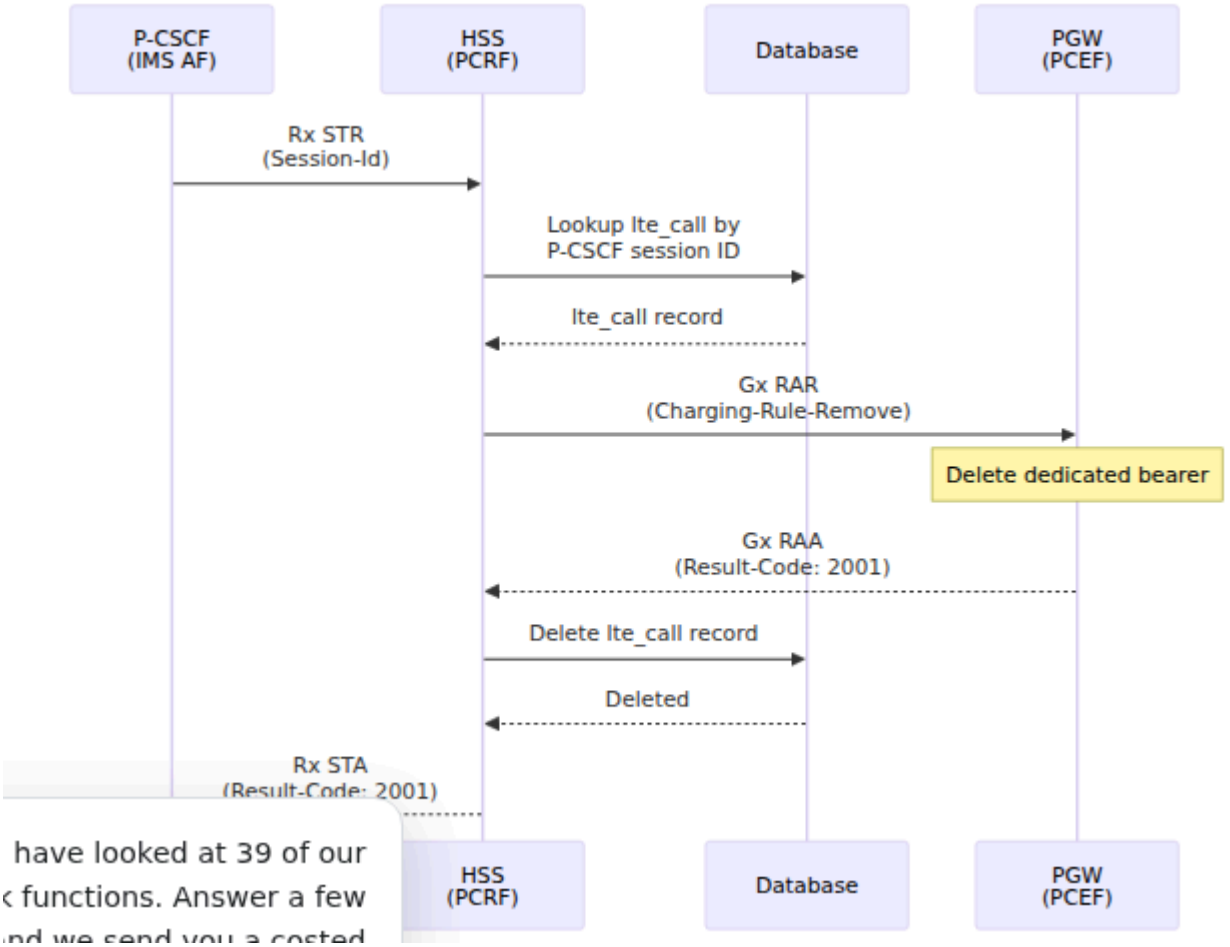
تحديث جلسة 4: التدفق PDN



التدفق 5: إنهاء جلسة PDN



التدفق 6: إعادة التفويض اليدوي عبر REST API



REST API

نقطة نهاية إعادة التفويض PCRF

نقطة النهاية: `POST /api/operation/pcrf_re_auth`

الغرض: تحفيز يدوي لطلب إعادة التفويض لتحديث السياسات Gx

متى تستخدم: تُستخدم هذه النقطة اليدوية عادةً لأغراض استكشاف الأخطاء وإصلاحها أو لفرض تغيير ملفات QoS لـ) تحديث السياسة على مشتركين محددين. بالنسبة لتحديثات السياسة الروتينية يقوم النظ��م تلقائيًا بتحفيز إعادة التفويض لجميع الجلسات المتأثرة - لا حاجة لإجراء، APN) يدوي.

جسم الطلب:

```
{
  "imsi": "999999876543210",
  "apn": "ims"
}
```

استجابة النجاح (HTTP 200):

```
{
  "data": "Gx Re-Auth Request for 999999876543210 sent to
pgw.epc.mnc999.mcc999.3gppnetwork.org, Result-Code: 2001"
}
```

استجابة الخطأ (HTTP 400):

```
{
  "error": "Unable to send Re-Auth Request for 999999876543210 on
APN ims, no active PDN Session found"
}
```

واجهة تكوين السياسة API

يسترجع PCRF سياسات QoS من تكوينات APN المخزنة في قاعدة البيانات. يمكن إنشاء هذه السياسات وإدارتها عبر REST API.

تنفيذ السياسة التلقائي: عند تحديث ملف QoS لـ APN (على سبيل المثال، تغيير حدود النطاق الترددي أو QCI)، يرسل النظام تلقائيًا طلبات إعادة التفويض Gx (RAR) إلى جميع PGWs مع جلسات PDN النشطة التي تستخدم ذلك APN. يضمن ذلك تطبيق تغييرات السياسة على الفور على جميع المشتركين المتصلين دون تدخل يدوي.

هيكل السياسة

يتم تعريف السياسات من خلال هيكل ثلاثي المستويات:

```
معرف APN → ملف QoS لـــ APN → ملف APN
     ↓                  ↓                ↓
  "internet"      QCI, AMBR, ARP    يربط بين الاثنين
```

1. إنشاء معرف APN

حدد اسم APN ودعم إصدار IP.

نقطة النهاية: `POST /api/apn/identifier`

جسم الطلب:

```
{
  "apn_identifier": {
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

خيارات إصدار IP:

- `"ipv4"` - IPv4 فقط
- `"ipv6"` - IPv6 فقط
- `"ipv4v6"` - كومة مزدوجة (كلا من IPv4 و IPv6)
- `"ipv4_or_ipv6"` - الشبكة تقرر (إما IPv4 أو IPv6)

الاستجابة (HTTP 201):

```
{
  "data": {
    "id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

التحقق:

- `apn`: مطلوب، 1-254 حرف، فريد
- `ip_version`: مطلوب، يجب أن يكون واحدًا من الخيارات الأربعة أعلاه

قائمة معرفات APN: `GET /api/apn/identifier`

2. إنشاء ملف QoS لـ APN

حدد معلمات QoS (الأولوية، QCI، النطاق الترددي).

نقطة النهاية: `POST /api/apn/qos_profile`

جسم الطلب:

```
{
  "apn_qos_profile": {
    "name": "أفضل جهد إنترنت",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true,
    "online_charging_enabled": false,
    "offline_charging_enabled": true
  }
}
```

معلمات QoS:

الحقل	النوع	النطاق	الوصف
`name`	string	1-254 حرف	اسم الملف (فريد)
`qci`	integer	1-254	معرف فئة QoS (1-4 = GBR، 5-9 = غير GBR)
`allocation_retention_priority`	integer	1-15	مستوى ARP (1 = أعلى أولوية)
`apn_ambr_dl_kbps`	integer	1-4,294,967,293	معدل البت الأقصى المجمع لـ APN في الاتجاه الهابط (كيلوبت في الثانية)
`apn_ambr_ul_kbps`	integer	1-4,294,967,293	معدل البت الأقصى المجمع لـ APN في الاتجاه الصاعد (كيلوبت في الثانية)
`pre_emption_capability`	boolean	true/false	يمكن أن يستبق الحاملات ذات الأولوية المنخفضة
`pre_emption_vulnerability`	boolean	true/false	يمكن أن يتم استباقه بواسطة الحاملات ذات الأولوية الأعلى

الحقل	النوع	النطاق	الوصف
`online_charging_enabled`	boolean	true/false/null	AVP `Online` على مستوى الجلسة لـ Gx CCA-I. `null` (افتراضي) يعكس قيمة لخاصة بـ CCR-I PGW. انظر الفوترة على مستوى الجلسة Online/Offline
`offline_charging_enabled`	boolean	true/false/null	AVP `Offline` على مستوى الجلسة لـ Gx CCA-I. `null` (افتراضي) يعكس قيمة لخاصة بـ CCR-I PGW. انظر الفوترة على مستوى الجلسة Online/Offline

قيم QCI الشائعة:

- `1` - الصوت المحادثة (VoLTE) - GBR، ميزانية تأخير 100 مللي ثانية
- `2` - الفيديو المحادثة - GBR، ميزانية تأخير 150 مللي ثانية
- `5` - إشارات IMS - غير GBR، ميزانية تأخير 100 مللي ثانية
- `9` - غير - (الإنترنت) الحامل الافتراضي GBR، ميزانية تأخير 300 مللي ثانية

الاستجابة (HTTP 201):

```
{
  "data": {
    "id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793",
    "name": "أفضل جهد إنترنت",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true,
    "online_charging_enabled": false,
    "offline_charging_enabled": true
  }
}
```

قائمة ملفات QoS: `GET /api/apn/qos_profile`

3. إنشاء ملف APN

ربط معرف APN بملف QoS.

نقطة النهاية: `POST /api/apn/profile`

جسم الطلب:

```
{
  "apn_profile": {
    "name": "ملف APN للإنترنت",
    "apn_identifier_id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
    "apn_qos_profile_id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793"
  }
}
```

الحقول:

- `name`: اسم الملف (فريد)، يستخدم كمرجع
- `apn_identifier_id`: معرف من إنشاء معرف APN
- `apn_qos_profile_id`: معرف من إنشاء ملف QoS لـ APN

الاستجابة (HTTP 201):

```
{
  "data": {
    "id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "name": "ملف APN للإنترنت",
    "apn_identifier_id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
    "apn_qos_profile_id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793"
  }
}
```

القيود:

- يجب أن يشير `apn_identifier_id` و `apn_qos_profile_id` إلى سجلات موجودة
- يجب أن تكون كل مجموعة من معرف APN وملف QoS فريدة

قائمة ملفات APN: `GET /api/apn/profile`

مثال كامل لتكوين السياسة

الخطوة 1: إنشاء سياسة APN IMS (VoLTE)

```
# 1. إنشاء معرف APN
curl -X POST https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "ims",
      "ip_version": "ipv4v6"
    }
  }'
# الاستجابة: {"data": {"id": "2c3e4f5a-6b7c-4d8e-9f0a-
1b2c3d4e5f6a", ...}}

# 2. إنشاء ملف QoS (إشارات IMS)
curl -X POST https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "name": "QoS لإشارات IMS",
      "qci": 5,
      "allocation_retention_priority": 2,
      "apn_ambr_dl_kbps": 5000,
      "apn_ambr_ul_kbps": 5000,
      "pre_emption_capability": true,
      "pre_emption_vulnerability": false
    }
  }'
# الاستجابة: {"data": {"id": "7b44a3e0-27cc-4b21-8d7a-
3f19e5c2b8d4", ...}}

# 3. إنشاء ملف APN
curl -X POST https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_profile": {
      "name": "APN IMS",
      "apn_identifier_id": "2c3e4f5a-6b7c-4d8e-9f0a-1b2c3d4e5f6a",
      "apn_qos_profile_id": "7b44a3e0-27cc-4b21-8d7a-3f19e5c2b8d4"
    }
  }'
# الاستجابة: {"data": {"id": "91c2f3a4-5d6e-4f7a-8b9c-
0d1e2f3a4b5c", ...}}
```

الخطوة 2: تعيين إلى المشترك

بمجرد الإنشاء، يتم تعيين ملف APN إلى المشتركين عبر ملفات EPC. انظر مرجع API لربط ملفات APN بالمشتركين.

تحديث السياسة والحذف

تحديث ملف QoS:

```
PATCH /api/apn/qos_profile/{id}
PUT /api/apn/qos_profile/{id}
```

مثال - زيادة النطاق الترددي لجميع المستخدمين:

```
# تحديث ملف QoS لزيادة النطاق الترددي
curl -X PATCH
https://hss.example.com:8443/api/apn/qos_profile/8d8ac610-566d-
4ef0-9c22-186b2a5ed793 \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "apn_ambr_dl_kbps": 150000,
      "apn_ambr_ul_kbps": 75000
    }
  }'
```

ما يحدث تلقائيًا:

1. يتم تحديث ملف QoS في قاعدة البيانات
2. يحدد النظام جميع جلسات PDN النشطة التي تستخدم APNs المرتبطة بهذا الملف QoS
3. لكل جلسة نشطة، يتم إرسال RAR Gx إلى PGW المقابل
4. تقوم PGWs بتحديث QoS للحامل لتعكس حدود النطاق الترددي الجديدة
5. يتلقى جميع المشتركين المتصلين السياسة المحدثة على الفور

سيناريو المثال: إذا كان 100 مشترك متصلين حاليًا على APN "الإنترنت" باستخدام هذا الملف QoS، فسيتم تحديث حدود النطاق الترددي الخاصة بهم إلى 150 ميجابت في الثانية في الاتجاه الهابط / 75 ميجابت في الثانية في الاتجاه الصاعد خلال ثوانٍ من اكتمال استدعاء API.

يقوم النظام **بتحفيز إعادة التفويض تلقائيًا** لجميع APN، لـ QoS **ملاحظة**: عند تحديث ملف جلسات PDN النشطة التي تستخدم ذلك APN، مما يطبق السياسات الجديدة على الفور على المشتركين المتصلين. لا حاجة لإعادة التفويض اليدوي.

حذف الموارد:

```
DELETE /api/apn/identifier/{id}
DELETE /api/apn/qos_profile/{id}
DELETE /api/apn/profile/{id}
```

قيود الحذف:

- لا يمكن حذف معرفات APN أو ملفات QoS المشار إليها بواسطة ملفات APN
- لا يمكن حذف ملفات APN نشطين لمشتركين المعينة

قوالب السياسة

إنترنت عالي السرعة (100 ميجابت في الثانية في الاتجاه الهابط / 50 ميجابت في الثانية في الاتجاه الصاعد):

```
{
  "apn_qos_profile": {
    "name": "إنترنت عالي السرعة",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

إنترنت متميز (500 ميجابت في الثانية في الاتجاه الهابط / 100 ميجابت في الثانية في الاتجاه الصاعد):

```
{
  "apn_qos_profile": {
    "name": "إنترنت متميز",
    "qci": 8,
    "allocation_retention_priority": 5,
    "apn_ambr_dl_kbps": 500000,
    "apn_ambr_ul_kbps": 100000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

IoT/M2M (نطاق ترددي منخفض):

```
{
  "apn_qos_profile": {
    "name": "IoT M2M",
    "qci": 9,
    "allocation_retention_priority": 10,
    "apn_ambr_dl_kbps": 1024,
    "apn_ambr_ul_kbps": 512,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

خدمات الطوارئ (أعلى أولوية):

```
{
  "apn_qos_profile": {
    "name": "APN الطوارئ",
    "qci": 5,
    "allocation_retention_priority": 1,
    "apn_ambr_dl_kbps": 10000,
    "apn_ambr_ul_kbps": 10000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

التكوين

إعداد خدمة القطر

تطبيق Gx (`config/runtime.exs`):

```
%{
  application_name: :gx,
  application_dictionary: :diameter_gen_3gpp_gx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_238}
  ]
}
```

تطبيق Rx (`config/runtime.exs`):

```
%{
  application_name: :rx,
  application_dictionary: :diameter_gen_3gpp_rx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_236}
  ]
}
```

معلمات QoS

تستمد معلمات QoS من:

- في قاعدة البيانات APN **الحامل الافتراضي**: تكوين ملف
  - `apn_qos_profile.qci` (معرف فئة QoS)
  - `apn_qos_profile.apn_ambr_ul_kbps` (معدل البت الأقصى المجمع في الاتجاه الصاعد)
  - `apn_qos_profile.apn_ambr_dl_kbps` (معدل البت الأقصى المجمع في الاتجاه الهابط)
  - `apn_qos_profile.priority_level` (أولوية الاحتفاظ بالتخصيص)

- Rx AAR **الحامل المخصص**: مستخرج من وصف مكون الوسائط
    - QCI: 1 (الصوت المحادثة)
    - معدل البت المضمون: من AVPs Max-Requested-Bandwidth
    - مرشحات التدفق: من AVPs Flow-Description

معالجة الأخطاء

رمز النتيجة	النوع	المعنى	السبب
2001	نجاح	DIAMETER_SUCCESS	تم معالجة الطلب بنجاح
5001	تجريبي	المستخدم غير موجود	IMSI غير موجود في قاعدة بيانات المشتركين
5002	تجريبي	الجلسة غير موجودة	لا توجد جلسة PDN للتحديث/الإنهاء
5063	تجريبي	الخدمة غير مفوضة	تم رفض تفويض الوسائط IMS

تفاصيل التنفيذ

إدارة الجلسة

يتعقب PCRF:

- **جلسات PDN النشطة** - واحدة لكل APN، لكل مشترك
- **مكالمات VoLTE** - مكالمات متعددة لكل جلسة IMS (تدعم المكالمات الجماعية)
- **سياسات QoS** - تطبق ديناميكيًا بناءً على تكوين APN
- **قواعد الفوترة** - قوالب تدفق الحركة والسياسات الخاصة بالخدمة

ميزات السياسة المتقدمة

يدعم PCRF التحكم المتقدم في السياسة بما في ذلك:

- تثبيت/**إزالة قواعد الفوترة** عبر واجهة Gx
- **مطابقة قوالب تدفق الحركة (TFT)** لتفريق الخدمات
- **ملفات السرعة الديناميكية** بناءً على التطبيق أو نوع الحركة
- **سياسات واعية للخدمة** يتم تحفيزها بواسطة ظروف الشبكة أو سلوك المشترك

اتصل بمدير النظام لديك للحصول على معلومات حول تكوين قواعد الفوترة المتقدمة والسياسات المعتمدة على TFT.

الوثائق ذات الصلة

- واجهة Sy - التحكم في حد إنفاق المشترك مقابل OCS خارجي
- بروتوكولات القطر - مواصفات البروتوكول التفصيلية
- مرجع API - الوثائق الكاملة لـ API
- الهيكلية HSS - الهيكل العام لـ
- تعيين البيانات - تعيين قاعدة البيانات إلى القطر AVP

معالجة أخطاء API

← العودة إلى مرجع API

جدول المحتويات

- استجابات الأخطاء الشائعة
- تدفق معالجة الأخطاء

استجابات الأخطاء الشائعة

400 طلب غير صالح

```
{
  "error": "Invalid JSON format"
}
```

الأسباب:

- JSON غير صحيح
- الحقول المطلوبة مفقودة
- أنواع بيانات غير صالحة

404 غير موجود

```
{
  "error": "Resource not found"
}
```

الأسباب:

- المشترك/الملف الشخصي/الكيان غير موجود
- معرف غير صحيح في URL

422 كيان غير قابل للمعالجة

```
{
  "errors": {
    "imsi": ["has already been taken"],
    "key_set_id": ["does not exist"]
  }
}
```

الأسباب:

- فشل ال��حقق
- انتهاك قيود قاعدة البيانات
- مراجع المفتاح الخارجي غير موجودة

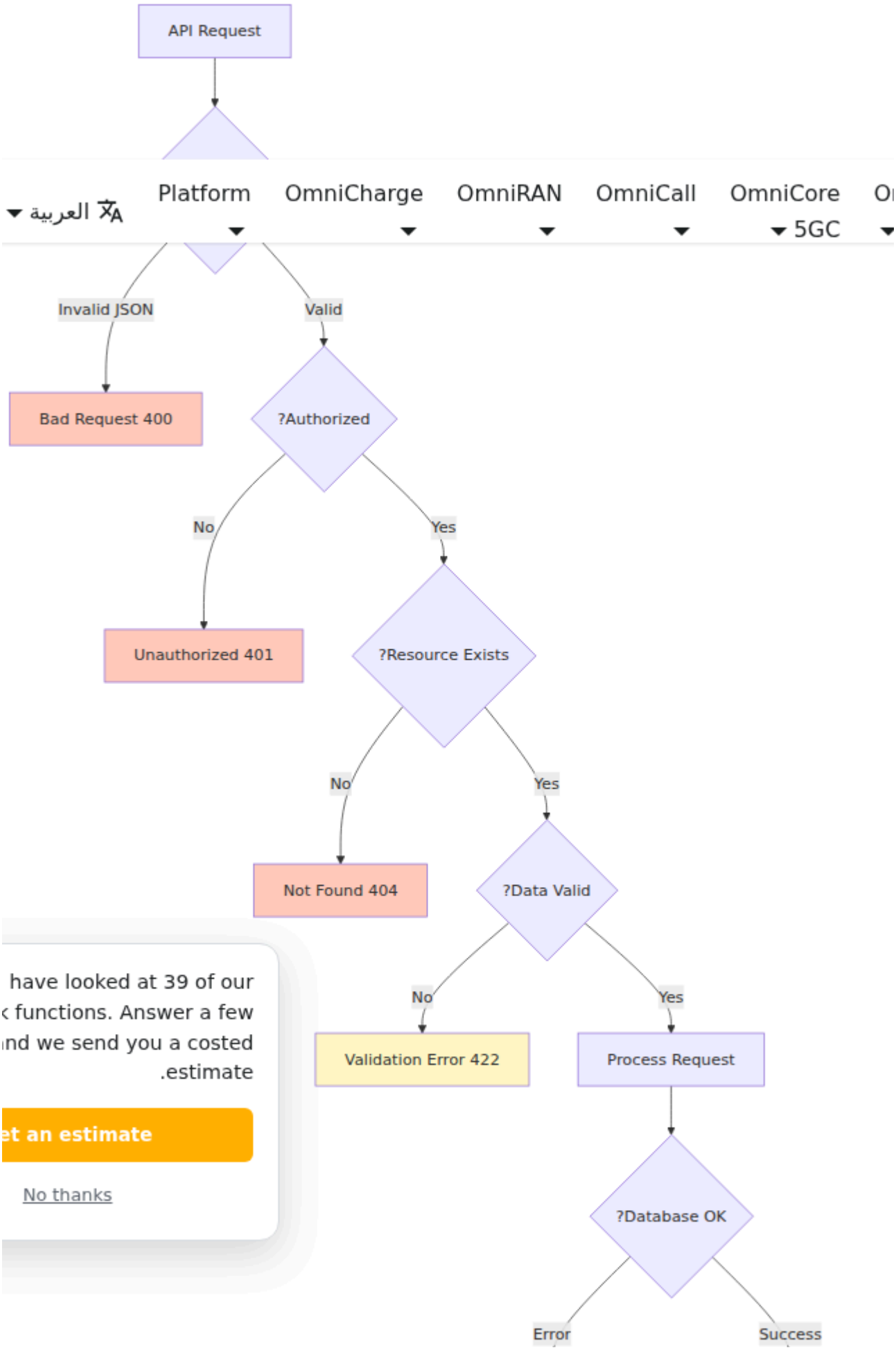
500 خطأ داخلي في الخادم

```
{
  "error": "Internal server error"
}
```

الأسباب:

- مشاكل في الاتصال بقاعدة البيانات
- أخطاء غير متوقعة في التطبيق

تدفق معالجة الأخطاء



have looked at 39 of our
k functions. Answer a few
nd we send you a costed
.estimate

et an estimate

No thanks



← العودة إلى مرجع API

أمثلة على استخدام API

← العودة إلى مرجع API

جدول المحتويات

- توفير المشترك الكامل
- توفير المشترك الخامل مسبقًا
- توفير IP ثابت كامل

توفير المشترك الكامل

هذا المثال يوضح سير العمل الكامل لتوفير مشترك جديد من الصفر. تتضمن العملية إنشاء جميع الملفات الشخصية والمكونات المطلوبة قبل إنشاء المشترك.

يستخدم هذا المثال **المتطلبات المسبقة:** `jq` لتحليل JSON. قم بتثبيته باستخدام `apt-get install jq` أو `brew install jq`.

الأقسام ذات الصلة:

- إدارة مجموعة المفاتيح
- ملفات تعريف APN
- ملفات تعريف EPC
- إدارة المشتركين

```
# 1. إنشاء مجموعة المفاتيح
KEY_SET_ID=$(curl -k -X POST
https://hss.example.com:8443/api/key_set \
  -H "Content-Type: application/json" \
  -d '{
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "authentication_algorithm": "milenage",
    "amf": "8000",
    "sqn": 0
  }' | jq -r '.response.id')

# 2. إنشاء ملف تعريف جودة الخدمة APN
APN_QOS_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "name": "Default Internet QoS",
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 50000,
    "apn_ambr_ul_kbps": 25000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": true,
    "qci": 9
  }' | jq -r '.response.id')

# 3. إنشاء معرف APN
APN_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn": "internet",
    "ip_version": "ipv4v6"
  }' | jq -r '.response.id')

# 4. إنشاء ملف تعريف APN
APN_PROFILE_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_identifier_id\": \"$APN_ID\",
    \"apn_qos_profile_id\": \"$APN_QOS_ID\",
    \"name\": \"Internet APN\"
```

```
  }" | jq -r '.response.id')

# 5. إنشاء ملف تعريف EPC
EPC_PROFILE_ID=$(curl -k -X POST
https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profiles\": [$APN_PROFILE_ID],
    \"name\": \"Standard Data Plan\",
    \"network_access_mode\": \"packet_only\",
    \"tracking_area_update_interval_seconds\": 600,
    \"ue_ambr_dl_kbps\": 100000,
    \"ue_ambr_ul_kbps\": 50000
  }" | jq -r '.response.id')

# 6. إنشاء مشترك
SUBSCRIBER_ID=$(curl -k -X POST
https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"imsi\": \"001001123456789\",
    \"key_set_id\": \"$KEY_SET_ID\",
    \"epc_profile_id\": \"$EPC_PROFILE_ID\"
  }" | jq -r '.response.id')

echo "تم توفير المشترك بنجاح مع المعرف: $SUBSCRIBER_ID"
```

ما الذي يتم إنشاؤه:

تقوم هذه العملية بتوفير مشترك كامل مع:

1. **مفاتيح تشفير** (مجموعة المفاتيح) - من أجل المصادقة
2. **ملف تعريف خدمة البيانات** (ملف تعريف EPC) - إعدادات عرض النطاق الترددي والوصول إلى الشبكة
3. **تكوين APN** (ملف تعريف APN) - نقطة وصول مع جودة الخدمة
4. **سجل المشترك** (المشترك) - الكيان الفعلي للمشترك

الخطوات التالية:

- إضافة أرقام الهواتف MSISDN: انظر إدارة
- تمكين خدمات الصوت IMS: إنشاء وتعيين ملف تعريف

- تكوين التجوال: إنشاء وتعيين ملف تعريف التجوال
- ربط SIM الفعلية: إنشاء وتعيين SIM

انظر أيضًا:

- تعيين أرقام هواتف متعددة - Multi-MSISDN وثائق
- تكوين متقدم للملف الشخصي - وثائق الملفات الشخصية

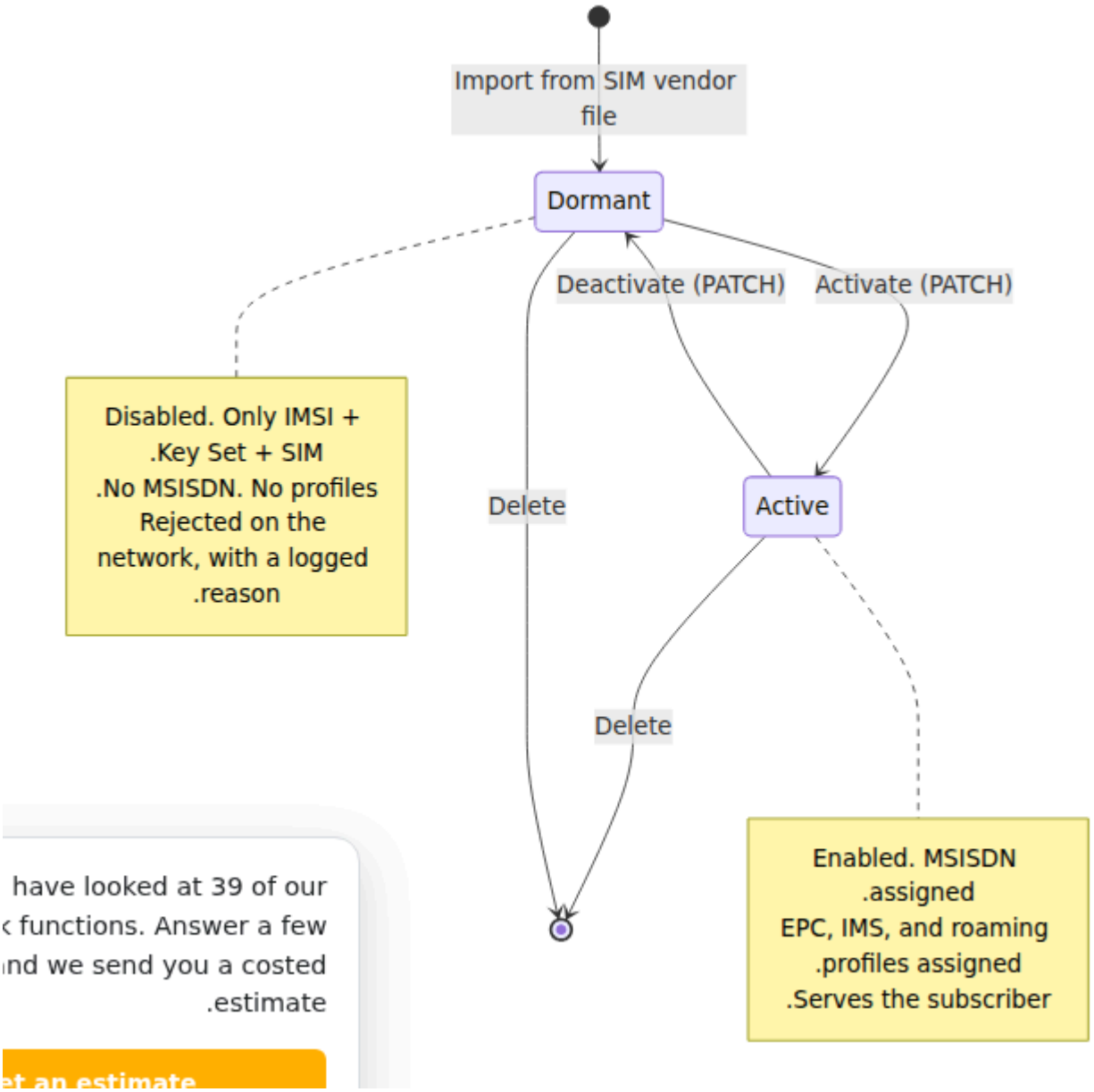
توفير المشترك الخامل مسبقًا

استخدم هذا سير العمل لتحميل المش��ركين بكميات كبيرة من ملف مخرج بائع SIM، ولتفعيل كل مشترك لاحقًا. هذا هو النموذج الموصى به لمعظم المشغلين.

يمتلك المشترك الخامل هويته فقط ومفاتيح المصادقة الخاصة به. تقوم بإضافة رقم الهاتف وملفات التعريف الخدمية عند التفعيل. يتطابق هذا مع البيانات التي يرسلها بائع SIM إليك. يحتوي ملف بائع SIM على ICCID، ورمز PIN، ورمز PUK، ورموز ADM، ومفاتيح المصادقة (Ki، OPc). لا يحتوي الملف على رقم هاتف أو خطة خدمة.

تحتاج قاعدة البيانات فقط إلى IMSI ومجموعة المفاتيح لإدراج مشترك. هذا ما يجعل السجل الخامل ممكنًا. لا يعني ذلك أن الكائنات الأخرى اختيارية للخدمة. كل كائن مطلوب لخدمته الخاصة: ملف تعريف EPC للمصادقة. لا يعمل SIM للصوت، و MSISDN و IMS للبيانات، وملف تعريف المشترك الخامل على الشبكة حتى تقوم بتعيين الكائن المطابق. تقوم بتعيين هذه الكائنات عندما يقوم العميل بتفعيل الخدمة. بسبب ن�ومجموعة المفاتيح والمشترك هي كائنات منفصلة، SIM انظر مجموعة المفاتيح و SIM والمشترك.

دورة حياة التوفير



الخطوة 1: الاستيراد (إنشاء SIM ومجموعة المفاتيح ومشترك معطل)

قم بإنشاء مجموعة مفاتيح واحدة، ومشترك معطل واحد لكل صف في ملف بائع SIM واحدة، و SIM. يستخدم هذا المثال `jq` لقراءة المعرف المعاد من كل استجابة.

```
# 1. إنشاء مجموعة المفاتيح من ملف بائع SIM (Ki، OPc)
KEY_SET_ID=$(curl -k -X POST
https://hss.example.com:8443/api/key_set \
  -H "Content-Type: application/json" \
  -d '{
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "authentication_algorithm": "milenage",
    "amf": "8000",
    "sqn": 0
  }' | jq -r '.response.id')

# 2. إنشاء SIM من ملف بائع SIM (ICCID، PIN/PUK/ADM)
SIM_ID=$(curl -k -X POST https://hss.example.com:8443/api/sim \
  -H "Content-Type: application/json" \
  -d '{
    "iccid": "8944000000000000001",
    "is_esim": false,
    "ind_length": 5
  }' | jq -r '.response.id')

# 3. إنشاء المشترك في حالة معطلة.
#    imsi و key_set_id ربط .مطلوبان SIM. إضافة لا MSISDN ولا ملفات
تعريف.
SUBSCRIBER_ID=$(curl -k -X POST
https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"imsi\": \"001010000000001\",
    \"key_set_id\": \"$KEY_SET_ID\",
    \"sim_id\": \"$SIM_ID\",
    \"enabled\": false,
    \"ims_enabled\": false
  }" | jq -r '.response.id')
```

يعتبر المشترك الخامل آمنًا للاحتفاظ به في قاعدة البيانات. لا يقوم المشترك بالاتصال أو المصادقة يرفض الطلب. انظر HSS أو التسجيل أثناء تعطيله. إذا استفسرت الشبكة عن مشترك خامل، فإن سلوك المشترك الخامل على الشبكة.

الخطوة 2: التفعيل (تعيين الرقم والملفات التعريفية، ثم التمكين)

عيّن الملفات التعريفية، واضبط MSISDN، واحد. أضف `PATCH` لتفعيل مشترك، أرسل طلب `enabled` على `true`.

```
curl -k -X PATCH
https://hss.example.com:8443/api/subscriber/$SUBSCRIBER_ID \
  -H "Content-Type: application/json" \
  -d "{
    \"enabled\": true,
    \"ims_enabled\": true,
    \"msisdns\": [\"$MSISDN_ID\"],
    \"epc_profile_id\": \"$EPC_PROFILE_ID\",
    \"ims_profile_id\": \"$IMS_PROFILE_ID\",
    \"roaming_profile_id\": \"$ROAMING_PROFILE_ID\"
  }"
```

يغير طلب `PATCH` فقط الحقول التي ترسلها. تبقى IMSI و مجموعة المفاتيح وSIM كما هي. قم بإنشاء MSISDN والملفات التعريفية أولاً، أو أعد استخدام المعرفات الموجودة. انظر توفير المشترك الكامل لمعرفة كيفية إنشاء الملفات التعريفية.

الخطوة 3: التعطيل (تعطيل المشترك)

لتعطيل مشترك، ضبط `enabled` على `false`. يبقى سجل المشترك وبياناته في قاعدة البيانات.

```
curl -k -X PATCH
https://hss.example.com:8443/api/subscriber/$SUBSCRIBER_ID \
  -H "Content-Type: application/json" \
  -d '{
    "enabled": false,
    "ims_enabled": false
  }'
```

لإزالة الصوت IMS، اضبط `ims_enabled` على `false` واترك `enabled` كما هو `true`.

سلوك المشترك الخامل على الشبكة

الطلب على واجهة الشبكة. كما HSS يفشل المشترك في الإغلاق بينما هو خامل أو معطل. يرفض يسجل HSS تحذيرًا مع السبب الدقيق. السبب هو أحد ما يلي:

- المشترك معطل (`enabled` هو `false`).
- IMS معطل للمشترك (`ims_enabled` هو `false`).
- لم يتم تعيين كائن مطلوب بعد. على سبيل المثال، لا يوجد ملف تعريف EPC للاتصال LTE، أو لا يوجد ملف تعريف IMS لتسجيل IMS.

يستخدم الرفض رمز نتيجة تجريبي `DIAMETER_ERROR_USER_UNKNOWN (5001)` على واجهات S6a و Cx، وفقًا لـ 3GPP TS 29.272 3 و3GPP TS 29.229. يسمي سجل التحذير IMSI والسبب غير المعروف IMSI الدقيق. يسمح لك السجل بالتفريق بين المشترك الخامل و.

توفير IP ثابت كامل

هذا المثال يوضح توفير مشترك بعنوان IP ثابت من الصفر.

السيناريو: توفير مشترك جهاز IoT يحتاج إلى عنوان IPv4 ثابت على APN "internet".

```
# المتطلبات المسبقة: يجب تثبيت jq (apt-get install jq أو brew
install jq)

# 1. إنشاء مجموعة المفاتيح
KEY_SET_ID=$(curl -k -X POST
https://hss.example.com:8443/api/key_set \
  -H "Content-Type: application/json" \
  -d '{
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "authentication_algorithm": "milenage",
    "amf": "8000",
    "sqn": 0
  }' | jq -r '.response.id')

# 2. إنشاء ملف تعريف جودة الخدمة APN
APN_QOS_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "name": "IoT Best Effort",
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 10000,
    "apn_ambr_ul_kbps": 5000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": false,
    "qci": 9
  }' | jq -r '.response.id')

# 3. إنشاء معرف APN
APN_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn": "internet",
    "ip_version": "ipv4"
  }' | jq -r '.response.id')

# 4. إنشاء ملف تعريف APN
APN_PROFILE_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d "{
```

```
    \"apn_identifier_id\": \"$APN_ID\",
    \"apn_qos_profile_id\": \"$APN_QOS_ID\",
    \"name\": \"IoT Internet APN\"
  }" | jq -r '.response.id')

# 5. إنشاء IP ثابت لـــ APN
STATIC_IP_ID=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile_id\": \"$APN_PROFILE_ID\",
    \"ipv4_static_ip\": \"100.64.1.100\"
  }" | jq -r '.response.id')

# 6. إنشاء ملف تعريف EPC
EPC_PROFILE_ID=$(curl -k -X POST
https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profiles\": [$APN_PROFILE_ID],
    \"name\": \"IoT Data Plan\",
    \"network_access_mode\": \"packet_only\",
    \"tracking_area_update_interval_seconds\": 600,
    \"ue_ambr_dl_kbps\": 10000,
    \"ue_ambr_ul_kbps\": 5000
  }" | jq -r '.response.id')

# 7. إنشاء MSISDN (رقم الهاتف)
MSISDN_ID=$(curl -k -X POST
https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{
    "msisdn": "14155551000"
  }' | jq -r '.response.id')

# 8. إنشاء مشترك مع IP ثابت
SUBSCRIBER_ID=$(curl -k -X POST
https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"imsi\": \"001001999999999\",
    \"key_set_id\": \"$KEY_SET_ID\",
    \"epc_profile_id\": \"$EPC_PROFILE_ID\",
    \"msisdns\": [$MSISDN_ID],
```

```
    \"static_ips\": [$STATIC_IP_ID]
  }" | jq -r '.response.id')

echo "تم توفير مشترك IoT بنجاح!"
echo "  معرف المشترك: $SUBSCRIBER_ID"
echo "  IMSI: 001001999999999"
echo "  MSISDN: 14155551000"
echo "  IPv4 100.64.1.100 :ثابت (على APN 'internet')"
```

ما الذي يتم إنشاؤه:

تقوم هذه العملية بتوفير مشترك IoT كامل مع:

1. **مفاتيح تشفير** (مجموعة المفاتيح) - من أجل المصادقة
2. **تكوين APN** (ملف تعريف APN) - نقطة وصول "internet"
3. **تعيين IP ثابت** (IP ثابت) - عنوان IPv4 100.64.1.100 ثابت
4. **ملف تعريف خدمة البيانات** (ملف تعريف EPC) - حدود عرض النطاق الترددي المحسّنة لـ IoT
5. **رقم الهاتف** (MSISDN) - لتحديد الجهاز
6. **سجل المشترك** (المشترك) - الكيان الكامل للمشترك

النتيجة:

عندما يتصل هذا المشترك بالشبكة ويتصل بـ APN "internet"، سيتلقى عنوان IP الثابت `100.64.1.100` بدلاً من عنوان DHCP الديناميكي.

الخطوات التالية:

- كرر الخطوات 2-5 لكل IPs إضافية مع APNs إضافة ثابتة APN
- تمكين خدمات الصوت: إنشاء وتعيين ملف تعريف IMS
- تكوين التجوال: إنشاء وتعيين ملف تعريف التجوال
- ربط SIM الفعلية: إنشاء وتعيين SIM

انظر أيضًا:

- إدارة IP الثابت - وثائق مفصلة حول IP الثابت
- توفير المشترك الكامل - التوفير الأساسي بدون IP ثابت
- وثائق Multi-MSISDN - تعيين أرقام هواتف متعددة

← العودة إلى مرجع API

التحكم في الوصول إلى واجهة برمجة التطبيقات (RBAC)

توضح هذه الصفحة كيفية التحكم في الوصول إلى واجهة برمجة التطبيقات الخاصة بـ REST. تشرح مفاتيح واجهة برمجة التطبيقات والأدوار والأذونات. كما تقدم أدوار مقترحة OmniHSS. للأنظمة التي تستخدم واجهة برمجة التطبيقات، مثل OmniHLR وOmniWeb وOmniCRM وأدوات المراقبة.

العودة إلى دليل العمليات. للحصول على نقاط نهاية واجهة برمجة التطبيقات، راجع مرجع واجهة برمجة التطبيقات.

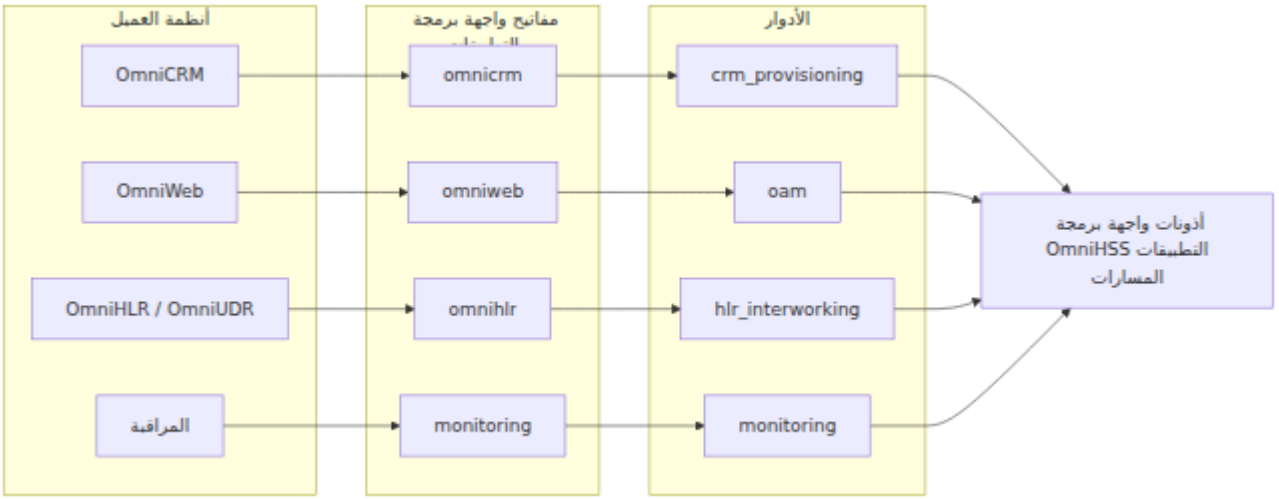
جدول المحتويات

- نظرة عامة
- أنماط المصادقة
- كيف تقوم OmniHSS بتفويض الطلب
- التكوين
- الأذونات
- فهرس أذونات OmniHSS
- الأدوار المقترحة
- مثال كامل على التكوين
- المستخدم الفاعل
- استدعاء واجهة برمجة التطبيقات بمفتاح
- تفعيل RBAC على نظام قيد التشغيل
- تدوير مفتاح
- التسجيل والتدقيق
- استكشاف الأخطاء وإصلاحها

نظرة عامة

يمكن لواجهة برمجة التطبيقات OmniHSS، وأرقام الهواتف، تغيير بيانات اعتماد المشتركين، وملفات تعريف الخدمة. يمكنها أيضًا إرسال عمليات الشبكة، على سبيل المثال، طلب إلغاء الموقع إلى MME. وبالتالي، يجب أن يحصل كل نظام عميل على الوصول الذي يحتاجه فقط.

يمنح كل نظام عميل مفتاح **واجهة برمجة التطبيقات** خاص به. يحتوي كل مفتاح على دور واحد أو أكثر. كل دور هو قائمة من **أنماط الأذونات**. تحتوي كل مسار واجهة برمجة التطبيقات على **إذن** واحد بالضبط. تسمح **التحكم في الوصول القائم على الأدوار (RBAC)** بطلب فقط إذا تطابق دور المفتاح مع إذن المسار. يتم رفض جميع الطلبات الأخرى. OmniHSS هذه هي "الرفض الافتراضي".



مفاتيح واجهة برمجة التطبيقات. (وغيرها Rx وGx وSh وCx وS6a) Diameter لا تستخدم واجهات Diameter. راجع تكوين Diameter من خلال قائمة الأقران في تكوين Diameter يتم التحكم في نظراء Diameter.

أنماط المصادقة

تحتوي واجهة برمجة التطبيقات على ثلاثة أنماط للمصادقة. يأتي النمط من كتلة `config` في `runtime.exs`. `:api_ex, :auth` يعتمد النمط على المفاتيح الموجودة في تلك الكتلة.

`config :api_ex, :auth`	النمط	السلوك
غير محدد	معطل	تقدم واجهة برمجة التطبيقات كل مسار لكل متصل بدون مفتاح. يتم كتابة تحذير في السجل عند بدء التشغيل.
يحتوي على `key` وليس `api_keys`	قديم	مفتاح مشترك واحد يمنح الوصول الكامل إلى جميع المسارات.
يحتوي على `api_keys`	RBAC	لكل عميل مفتاح مسمى مع أدوار. يتم رفض الطلبات التي لا يسمح بها أي دور.

> **تحذير:** لا تشغل OmniHSS في وضع معطل في الإنتاج. إذا لم يتم تعيين كتلة `config :api_ex, :auth`، يمكن لأي مضيف يصل إلى المنفذ 8443 قراءة وتغيير جميع بيانات المشتركين.

استخدم وضع RBAC لجميع أنظمة الإنتاج. استخدم وضع القديم فقط كخطوة قصيرة أثناء الترحيل.

قواعد النمط:

- `key: ""` هو خطأ في التكو��ن. ثم تجيب واجهة برمجة التطبيقات على كل طلب بـ `503`، القيمة الفارغة لا تعطل المصادقة. على سبيل المثال.
- تحدد OmniHSS النمط عند بدء التشغيل. إذا تغير التكوين إلى نمط أدنى أثناء تشغيل الخدمة، فإن واجهة برمجة التطبيقات تجيب على كل طلب بـ `503`. أعد تشغيل الخدمة لاستخدام نمط أدنى.
- في وضع RBAC، يتوقف التكوين غير الصالح واجهة برمجة التطبيقات عند بدء التشغيل. يوفر السجل قائمة مرقمة بكل مشكلة. لا تبدأ واجهة برمجة التطبيقات أبدًا بدون حماية.

بتفويض الطلب OmniHSS كيف تقوم



تتخذ OmniHSS أو `403` أو `401` على الذي يحصل المتصل الطلب. جسم أقرأ أن قبل القرار `503`. طلب جسم يقرأ الخادم جعل يمكنه لا

التكوين

ضع كتلة `config :api_ex, :auth` في ملف تكوين وقت التشغيل `runtime.exs`. على أعد تشغيل OmniHSS `/etc/omnihss/runtime.exs` مضيف تم نشره، يكون هذا الملف هو

بعد تغيير الكتلة.

هيكل التكوين

```
# runtime.exs
config :api_ex, :auth,
  header: "x-omnihss-key",
  user_header: "x-omnihss-user",
  public: ["status/api:read"],
  roles: %{
    admin: ["*"],
    monitoring: ["status/**:read", "subscriber/**:read"]
  },
  api_keys: [
    %{
      name: "monitoring",
      roles: [:monitoring],
      secrets: ["REPLACE-WITH-A-64-CHARACTER-RANDOM-HEX-SECRET-
FROM-OPENSSL-RAND"]
    },
    %{
      name: "break-glass",
      roles: [:admin],
      secrets: ["REPLACE-WITH-A-DIFFERENT-64-CHARACTER-RANDOM-HEX-
SECRET-VALUE"]
    }
  ],
  log: [deny: :warning, unauthenticated: :info, allow: false,
not_found: false]
```

معلمات المصادقة

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`header`	سلسلة	لا	`"x-api-key"`	رأس HTTP الذي يحمل مفتاح واجهة برمجة التطبيقات. الاسم غير حساس لحالة الأحرف. استخدم `"x-omnihss-key"`. لا تستخدم الافتراضي `"x-api-key"`، لأن OmniWeb يستخدم `X-API-Key` لمفاتيحه الخاصة. راجع OmniWeb.
`user_header`	سلسلة	لا	غير محدد	رأس HTTP الذي يسمي المستخدم البشري الذي يتصرف من أجله العميل. يجب أن يكون مختلفًا عن `header`. راجع المستخدم الفاعل.
`public`	قائمة من السلاسل	لا	`[]`	أنماط الأذونات التي يمكن للمتصلين استخدامها بدون مفتاح. استخدم هذا فقط لعمليات التحقق من الصحة. احتفظ بأنماط العامة للقراءة فقط.
`roles`	خريطة	نعم (RBAC)	-	أسماء الأدوار وأنماط الأذونات الخاصة بها. كل مفتاح في الخريطة هو اسم دور. ك�� قيمة هي قائمة بأنماط. راجع الأذونات.
`api_keys`	قائمة من الخرائط	نعم (RBAC)	-	مفاتيح واجهة برمجة التطبيقات. وجود هذه المعلمة يحدد وضع RBAC. راجع

المعلمة	النوع	مطلوب	الافتراضي	الوصف
				معلمات مفتاح واجهة برمجة التطبيقات.
`log`	قائمة كلمات رئيسية	لا	انظر الوصف	مستوى السجل لكل نوع من القرارات. راجع معلمات السجل.
`key`	سلسلة	قديم فقط	-	المفتاح المشترك الوحيد في وضع القديم. لا تقم بتعيين `key` و `api_keys` معًا. أزل `key` عند الانتقال إلى RBAC.

معلمات مفتاح واجهة برمجة التطبيقات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`name`	سلسلة	نعم	-	اسم فريد للمفتاح. استخدم اسم نظام العميل، على سبيل المثال `"omnicrm"`. يظهر الاسم في السجلات. لا يظهر السر أبدًا في السجلات.
`roles`	قائمة من الذرات	نعم	-	أدوار المفتاح. يجب تعريف كل دور في `roles`. يحصل ال��فتاح على أذونات جميع أدواره.
`secrets`	قائمة من السلاسل	نعم	-	سر واحد أو أكثر للمفتاح. يرسل العميل أحد هذه الأسرار في رأس المفتاح. يسمح وجود سرين بتدوير المفتاح بدون توقف. راجع تدوير مفتاح. يجب أن يكون كل سر فريد عبر جميع المفاتيح.
`may_assert_user`	بولياني	لا	`false`	إذا كان `true`، يمكن للمفتاح تسمية مستخدم بشري في `user_header`. قم بتعيين هذا فقط للأنظمة التي لديها تسجيل دخول خاص بها، مثل OmniWeb وOmniCRM.

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`metadata`	خريطة	لا	`%{}`	بيانات حرة الشكل حول المفتاح، مثل مالك أو رقم تذكرة. لا تستخدم OmniHSS هذه البيانات لاتخاذ قرارات.

قواعد السر:

- استخدم سرًا عشوائيًا طويلًا. أنشئ سرًا باستخدام الأمر `openssl rand -hex 32`. هذا يعطي 64 حرفًا سداسيًا.
- تحذيرًا عند بدء التشغيل لسر أقصر من 16 بايت. ستة عشر بايت هو OmniHSS تكتب الحد الأدنى، وليس توصية.
- أعط كل نظام عميل مفتاحه الخا��. لا تشارك مفتاحًا بين نظامين. إذا شاركت مفتاحًا، لا يمكنك إزالة الوصول من نظام واحد فقط، ولا يمكن للسجلات تمييز النظامين.

معلمات السجل

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`deny`	مستوى السجل أو `false`	لا	`:warning`	مستوى السجل لطلب لا تسمح به أدوار المفتاح (`403`).
`unauthenticated`	مستوى السجل أو `false`	لا	`:info`	مستوى السجل لطلب بدون مفتاح أو مفتاح خاطئ (`401`).
`allow`	مستوى السجل أو `false`	لا	`false`	مستوى السجل لطلب مسموح به. قم بتعيين `:info` لتسجيل كل استدعاء واجهة برمجة التطبيقات المسموح به.
`not_found`	مستوى السجل أو `false`	لا	`false`	مستوى السجل لطلب من مفتاح معروف إلى مسار غير موجود (`404`).

مستوى السجل هو `:debug` أو `:info` أو `:warning` أو `:error`. القيمة `false` تعطل خط السجل لذلك القرار.

الأذونات

تنسيق الإذن

كل مسار له إذن وا��د بتنسيق `resource:verb`.

- وبدون معلمات المسار. `/api` **المورد** هو مسار واجهة برمجة التطبيقات بدون بادئة على سبيل المثال، يحتوي المسار `GET /api/subscriber/imsi/:imsi` على المورد `subscriber/imsi`.
- **الفعل** يأتي من طريقة HTTP.

الفعل	طريقة HTTP
`read`	`GET` (قائمة وسجل فردي)
`write`	`POST`
`write`	`PUT`, `PATCH`
`delete`	`DELETE`

لذا، يحتوي `POST /api/operation/s6a/clr` على الإذن `operation/s6a/clr:write`، و`DELETE /api/subscriber/:id` يحتوي على الإذن `subscriber:delete`.

تنسيق النمط

الدور هو قائمة من الأنماط. يحتوي النمط على نفس تنسيق `resource:verb`، ويمكن أن يحتوي على أحرف بدل.

حرف بدل	الموضع	المطابقات
`*` (نمط كامل)	بمفرده	جميع الأذونات.
`*` (جزء المورد)	أي جزء	جزء واحد بالضبط. في نهاية المورد، يتطابق مع جزء أو أكثر.
`**`	الجزء الأخير فقط	صفر أو أكثر من الأجزاء.
`*` (الفعل)	بعد `:`	جميع الأفع��ل.

ليس نمطًا صالحًا `sub*`، الجزء هو النص بين حرفي `/`. `*` ليس تطابق بادئة. على سبيل المثال.

أمثلة على الأنماط

تقدم أحرف البديل `*` و`**` نتائج مختلفة. استخدم هذا الجدول عند كتابة دور.

النمط	`subscriber:read`	`subscriber/imsi:read`	`subscr`
`subscriber:read`	نعم	لا	لا
`subscriber:*`	نعم	لا	نعم
`subscriber/*:read`	لا	نعم	لا
`subscriber/**:read`	نعم	نعم	لا
`subscriber/**:*`	نعم	نعم	نعم
`*:read`	نعم	نعم	لا
`*`	نعم	نعم	نعم

نقاط رئيسية:

- `subscriber/*:read` يعطي مسارات البحث (`subscriber/imsi` و`subscriber/msisdn` وغيرها)، ولكن ليس قائمة `subscriber`.
- `subscriber/**:read` يعطي مسارات `subscriber` وجميع المسارات أدناه `subscriber`.
- تضيف الأدوار الأذونات فقط. لا يوجد نمط "رفض". لإزالة إذن من دور، اكتب الدور بق��ئمة أصغر من الأنماط.

فهرس أذونات OmniHSS

توضح هذه الجدول كل إذن من واجهة برمجة التطبيقات OmniHSS. للحصول على تنسيق الطلب والاستجابة لكل مسار، راجع مرجع واجهة برمجة التطبيقات.

الحالة والتوثيق

الإذن	المسارات	الملاحظات
`status/api:read`	`GET /api/status/api`	صحة واجهة برمجة التطبيقات. مرشح جيد لـ `public`.
`status/license:read`	`GET /api/status/license`	حالة الترخيص.
`status/database:read`	`GET /api/status/database`	صحة قاعدة البيانات.
`docs:read`	`GET /api/docs`، `GET /docs`	واجهة Swagger.
`schema:read`	`GET /api/schema`، `GET /schema`	وثيقة OpenAPI.
`version:read`	`GET /version`	إصدار البرنامج والبناء.

بيانات المشتركين

المسارات	الإذن
`GET /api/subscriber`, `GET /api/subscriber/:id`	`subscriber:read`
`POST /api/subscriber`, `PUT` و`PATCH /api/subscriber/:id`	`subscriber:write`
`DELETE /api/subscriber/:id`	`subscriber:delete`
`GET /api/subscriber/imsi/:imsi`	`subscriber/imsi:read`
`GET /api/subscriber/iccid/:iccid`	`subscriber/iccid:read`
`GET /api/subscriber/msisdn/:msisc`	`subscriber/msisdn:read`
`GET /api/subscriber/ip/:ip_addres`	`subscriber/ip:read`
`GET /api/subscriber/repository_data/:`	`subscriber/repository_data:read`

الإذن	المسارات
`subscriber/repository_data:write`	`PUT` و`PATCH` `/api/subscriber/repository_data/:`
`subscriber/repository_data:delete`	`DELETE` `/api/subscriber/repository_data/:`
`msisdn:read`	`GET /api/msisdn`، `GET /api/msisdn/`
`msisdn:write`	`POST /api/msisdn`، `PUT` و`PATCH` `/api/msisdn/:id`
`msisdn:delete`	`DELETE /api/msisdn/:id`
`msisdn/digits:read`	`GET /api/msisdn/digits/:digits`
`ims_subscription:read`، `:write`، `:delete`	`/api/ims_subscription`
`epc/static_ip:read`، `:write`، `:delete`	`/api/epc/static_ip`

بيانات الاعتماد

الإذن	المسارات	الملاحظات
`key_set:read`	`GET /api/key_set`, `GET /api/key_set/:id`	لا تحتوي الاستجابة على Ki أو OPc أو OP أو PSK أو DES أو كلمة مرور SIP. يتم إزالة هذه الحقول من كل قراءة.
`key_set:write`	`POST /api/key_set`, `PUT` و`PATCH /api/key_set/:id`	**حساس.** يمكن للمتصل الذي لديه هذا الإذن تعيين أو استبدال مفاتيح المصادقة لمشترك.
`key_set:delete`	`DELETE /api/key_set/:id`	**حساس.**
`sim:read`	`GET /api/sim`, `GET /api/sim/:id`	لا تحتوي الاستجابة على Klc أو KID أو ADM1.
`sim:write`	`POST /api/sim`, `PUT` و`PATCH /api/sim/:id`	
`sim:delete`	`DELETE /api/sim/:id`	
`sim/iccid:read`	`GET /api/sim/iccid/:iccid`	البحث حسب ICCID.

الملفات الشخصية والقواعد

المسارات هي `GET` و`write` و`read` كل مورد في هذه الجدول لديه الأذونات الثلاثة `delete`. على المسار. يمكن أن يؤدي تغيير ملف تعريف إلى تغيير خدمة `DELETE` و`PATCH` و`PUT` و`POST` و العديد من المشتركين في نفس الوقت.

وصف	المسار	الم��رد
ملفات تعريف APN. راجع إدارة لملفات شخصية	`/api/apn/profile`	`apn/profile`
أسماء APN.	`/api/apn/identifier`	`apn/identifier`
جودة خدمة APN.	`/api/apn/qos_profile`	`apn/qos_profile`
ملفات تعريف EPC لبيانات)	`/api/epc/profile`	`epc/profile`
ملفات تعريف IMS لصوت)	`/api/ims/profile`	`ims/profile`
ملفات تعريف لتجوال. راجع التحكم في التجوال	`/api/roaming/profile`	`roaming/profile`
قواعد التجوال	`/api/roaming/rule`	`roaming/rule`

الم��رد	المسار	وصف
`eir/rule`	`/api/eir/rule`	قواعد EIR. جع EIR.
`pcrf/profile`	`/api/pcrf/profile`	ملفات تعريف PCRF. راجع PCRF.
`pcrf/charging_rule`	`/api/pcrf/charging_rule`	قواعد تحصيل PCRF.
`pcrf/flow_information_rule`	`/api/pcrf/flow_information_rule`	قواعد تدفق PCRF.

التداخل مع HLR

المسارات	الإذن
`POST /api/hlr/generate_auth_`	`hlr/generate_auth_vectors:write`
`POST /api/hlr/generate_eutran_aut`	`hlr/generate_eutran_auth_vectors:write`
`PUT`، `PATCH`، `DELETE /api/hlr/circuit_session/:im`	`hlr/circuit_session:write`، `:delete`
`PUT` و`PATCH /api/hlr/subscriber_state/:i`	`hlr/subscriber_state:write`
`POST`، `PUT`، `PATCH`، `DELETE /api/hlr/pdn_session`	`hlr/pdn_session:write`، `:delete`

عمليات الشبكة

الإذن	المسارات	ملاحظات
`operation/count:read`	`GET /api/operation/count/:type`	عدادات السجلات.
`operation/s6a/clr:write`	`POST /api/operation/s6a/clr`	رسل طلب غاء الموقع إلى MME. ينفصل المشترك. راجع تدفقات البروتوكول
`operation/s6a/idr:write`	`POST /api/operation/s6a/idr`	رسل طلب دراج بيانات المشترك إلى MME.
`operation/pcrf/re_auth:write`	`POST /api/operation/pcrf/re_auth`	رسل طلب إعادة المصادقة Gx إلى PGW. راجع PCRF.

الأدوار المقترحة

تمنح هذه الأدوار كل نظام عميل المسارات التي يستخدمها، ولا شيء أكثر. ابدأ بهذه الأدوار. ثم اجعل كل دور أصغر إذا لم يستخدم العميل ميزة.

الدور	أنظمة العميل	الوصول
`admin`	مفتاح كسر الزجاج للحالات الطارئة	جميع المسارات.
`crm_provisioning`	OmniCRM	توفير المشتركين و SIMو MSISDN ومجموعات المفاتيح. قراءة فقط للملفات الشخصية.
`oam`	OmniWeb	جميع بيانات المشتركين، والملفات الشخصية، وعمليات الشبكة. لا توجد حالة جلسة HLR.
`hlr_interworking`	OmniHLR (OmniSS7)، OmniUDR	عمليات البحث عن المشتركين، متجهات المصادقة، حالة الدائرة المعتمدة.
`monitoring`	المصدرون، لوحات المعلومات، السكربتات التي تقرأ فقط	عمليات البحث عن المشتركين وحالة القراءة فقط.
`eir_lookup`	OmniEIR	قراءة قواعد EIR فقط.

المسؤول (كسر الزجاج)

```
admin: ["*"]
```

كيف يعمل: يمكن للمفتاح استخدام كل مسار، بما في ذلك المسارات الجديدة في الإصدارات اللاحقة.

حالة الاستخدام: الوصول الطارئ من قبل مشغل. احتفظ بالسر في خزنة كلمات المرور. لا تقم بتكوين نظام عميل مع هذا المفتاح. تحقق من السجلات لكل استخدام لهذا المفتاح.

OmniCRM (التوفير)

```
crm_provisioning: [
  "subscriber:*",
  "subscriber/*:read",
  "msisdn/**:*",
  "sim/**:read",
  "sim:write",
  "key_set:write",
  "status/**:read"
]
```

كيف يعمل: يقوم OmniCRM بإنشاء وتغيير وحذف المشتركين و MSISDNs. ينشئ SIMs ومجموعات مفاتيح عند توفير خدمة جديدة. يبحث عن المشتركين حسب IMSI وعنوان IP للـ UE. لا يمكنه تغيير الملفات الشخصية أو القواعد أو عمليات الشبكة. لا يمكنه حذف مجموعات المفاتيح أو SIMs.

حالة الاستخدام: يوفر CRM الخدمات للعملاء. قم بتعيين `may_assert_user: true` على مفتاح OmniCRM بحيث يمكن لـ CRM تسمية عضو الطاقم الذي أجرى التغيير. راجع المستخدم الفاعل.

إذا كان يجب على CRM إرسال طلب إلغاء الموقع بعد تبديل SIM، أضف `"operation/s6a/clr:write"`.

OmniWeb (OAM)

```
oam: [
  "*:read",
  "subscriber/**:*",
  "msisdn/**:*",
  "sim/**:*",
  "key_set:*",
  "ims_subscription:*",
  "apn/**:*",
  "epc/**:*",
  "ims/**:*",
  "roaming/**:*",
  "eir/**:*",
  "pcrf/**:*",
  "operation/**:write",
  "hlr/subscriber_state:write",
  "hlr/generate_auth_vectors:write",
  "hlr/generate_eutran_auth_vectors:write"
]
```

كيف يعمل: يدير OmniWeb جميع بيانات المشتركين والملفات الشخصية والقواعد. يرسل Gx Re-Auth و IDR و CLR). عمليات الشبكة). لا يمكنه يمكنه توليد متجهات المصادقة للاختبار. تغيير حالة الدائرة المعتمدة أو حالة جلسة PDN التي يمتلكها HLR.

حالة الاستخدام: OmniWeb هو نظام OAM. يحتوي OmniWeb على مستخدمين خاصين به الخاص به قبل إرسال طلب إلى RBAC من OmniWeb خاص به لكل عنصر. يتحقق RBAC و كل ميزة تظهرها OmniWeb الخاص بـ OmniHSS وبالتالي، يجب أن يغطي مفتاح OmniHSS. ب��يث يمكن لـ OmniWeb على مفتاح `may_assert_user: true` قم بتعيين OmniWeb. تسجيل مستخدم OmniHSS OmniWeb.

> **تحذير:** لا تستخدم `x-api-key` كعنوان مفتاح OmniHSS. يستخدم OmniWeb `X-API-Key` قم بتعيين OmniHSS. هذا العنوان إلى OmniWeb لمفاتيحه الشخصية، ويرسل وكيل `header: "x-omnihss-key"`، حتى لا تتعارض المفاتيح.

OmniHLR و OmniUDR (التفاعل بين HLR)

```
hlr_interworking: [
  "subscriber/imsi:read",
  "subscriber/msisdn:read",
  "key_set:read",
  "hlr/generate_auth_vectors:write",
  "hlr/generate_eutran_auth_vectors:write",
  "hlr/circuit_session:*",
  "status/api:read"
]
```

كيف يعمل: يقوم UDR و HLR بالبحث عن المشتركين، وطلب متجهات المصادقة، وتحديث الموقع الدائري. لا يمكنهم تغيير بيانات أو ملفات تعريف المشتركين.

حالة الاستخدام: OmniHLR (OmniSS7) للجيل الثاني/الثالث، و OmniUDR للجيل الخامس. تتلقى هذه الأنظمة متجهات تحتوي على IK و CK. لا تعطي هذه المفاتيح لأي نظام آخر.

المراقبة (للقراءة فقط)

```
monitoring: [
  "status/**:read",
  "subscriber/**:read",
  "operation/count:read"
]
```

كيف يعمل: يمكن للمفتاح قراءة الحالة، والبحث عن المشتركين، وعدد السجلات. لا يمكنه تغيير البيانات.

حالة الاستخدام: المصدرون، لوحات المعلومات، والتقارير. تحتوي قراءات المشتركين على MSISDNs، وهي بيانات شخصية. إذا كانت الأداة تحتاج فقط إلى الحالة، استخدم IMSIs و `"status/**:read"` بمفرده.

OmniEIR (بحث EIR)

```
eir_lookup: ["eir/rule:read"]
```

يمكن للمفتاح قراءة قواعد **كيف يعمل:** EIR فقط.

يقرأ **حالة الاستخدام:** OmniEIR القواعد التي يخزنها OmniHSS.

أدوات المختبر والاختبار

تقوم أدوات الاختبار، مثل محاكي RAN، في المختبر، بإنشاء وحذف المشتركين وملفات التعريف. لا تقم بتثبيت مفاتيح أدوات الاختبار على أنظمة الإنتاج. أعطِ كل أداة اختبار مفتاحها الخاص مع دور `admin`.

مثال كامل على التكوين

يستخدم هذا المثال جميع الأدوار المقترحة. يتم شرح كل معلمة في التكوين.

```
# runtime.exs
config :api_ex, :auth,
  # لا تستخدم x-api-key: يرسل OmniWeb عنوان X-API-Key الخاص به عبر
وكيله
  header: "x-omnihss-key",
  user_header: "x-omnihss-user",

  # فحص الصحة بدون مفتاح
  public: ["status/api:read"],

  roles: %{
    admin: ["*"],
    crm_provisioning: [
      "subscriber:*",
      "subscriber/*:read",
      "msisdn/**:*",
      "sim/**:read",
      "sim:write",
      "key_set:write",
      "status/**:read"
    ],
    oam: [
      "*:read",
      "subscriber/**:*",
      "msisdn/**:*",
      "sim/**:*",
      "key_set:*",
      "ims_subscription:*",
      "apn/**:*",
      "epc/**:*",
      "ims/**:*",
      "roaming/**:*",
      "eir/**:*",
      "pcrf/**:*",
      "operation/**:write",
      "hlr/subscriber_state:write",
      "hlr/generate_auth_vectors:write",
      "hlr/generate_eutran_auth_vectors:write"
    ],
    hlr_interworking: [
      "subscriber/imsi:read",
      "subscriber/msisdn:read",
      "key_set:read",
```

```
      "hlr/generate_auth_vectors:write",
      "hlr/generate_eutran_auth_vectors:write",
      "hlr/circuit_session:*",
      "status/api:read"
    ],
    monitoring: ["status/**:read", "subscriber/**:read",
"operation/count:read"],
    eir_lookup: ["eir/rule:read"]
  },

  api_keys: [
    %{
      name: "omnicrm",
      roles: [:crm_provisioning],
      may_assert_user: true,
      secrets: ["REPLACE-WITH-OPENSSL-RAND-HEX-32-OUTPUT-FOR-THE-
OMNICRM-KEY-00"]
    },
    %{
      name: "omniweb",
      roles: [:oam],
      may_assert_user: true,
      secrets: ["REPLACE-WITH-OPENSSL-RAND-HEX-32-OUTPUT-FOR-THE-
OMNIWEB-KEY-00"]
    },
    %{
      name: "omnihlr",
      roles: [:hlr_interworking],
      secrets: ["REPLACE-WITH-OPENSSL-RAND-HEX-32-OUTPUT-FOR-THE-
OMNIHLR-KEY-00"]
    },
    %{
      name: "omniudr",
      roles: [:hlr_interworking],
      secrets: ["REPLACE-WITH-OPENSSL-RAND-HEX-32-OUTPUT-FOR-THE-
OMNIUDR-KEY-00"]
    },
    %{
      name: "monitoring",
      roles: [:monitoring],
      secrets: ["REPLACE-WITH-OPENSSL-RAND-HEX-32-OUTPUT-FOR-THE-
MONITOR-KEY-00"]
    },
    %{
```

```
      name: "break-glass",
      roles: [:admin],
      metadata: %{owner: "NOC", vault: "omnihss/break-glass"},
      secrets: ["REPLACE-WITH-OPENSSL-RAND-HEX-32-OUTPUT-FOR-
BREAK-GLASS-KEY-00"]
    }
  ],

  log: [deny: :warning, unauthenticated: :info, allow: false,
not_found: false]
```

كيف يعمل: يبدأ OmniHSS في وضع RBAC، لأن `api_keys` موجود. كل نظام عميل لديه مفتاحه الخاص. يمكن لموازين التحميل التحقق من `GET /api/status/api` بدون مفتاح. تحتاج جميع المسارات الأخرى إلى مفتاح، ويحتاج المفتاح إلى دور يتطابق مع المسار.

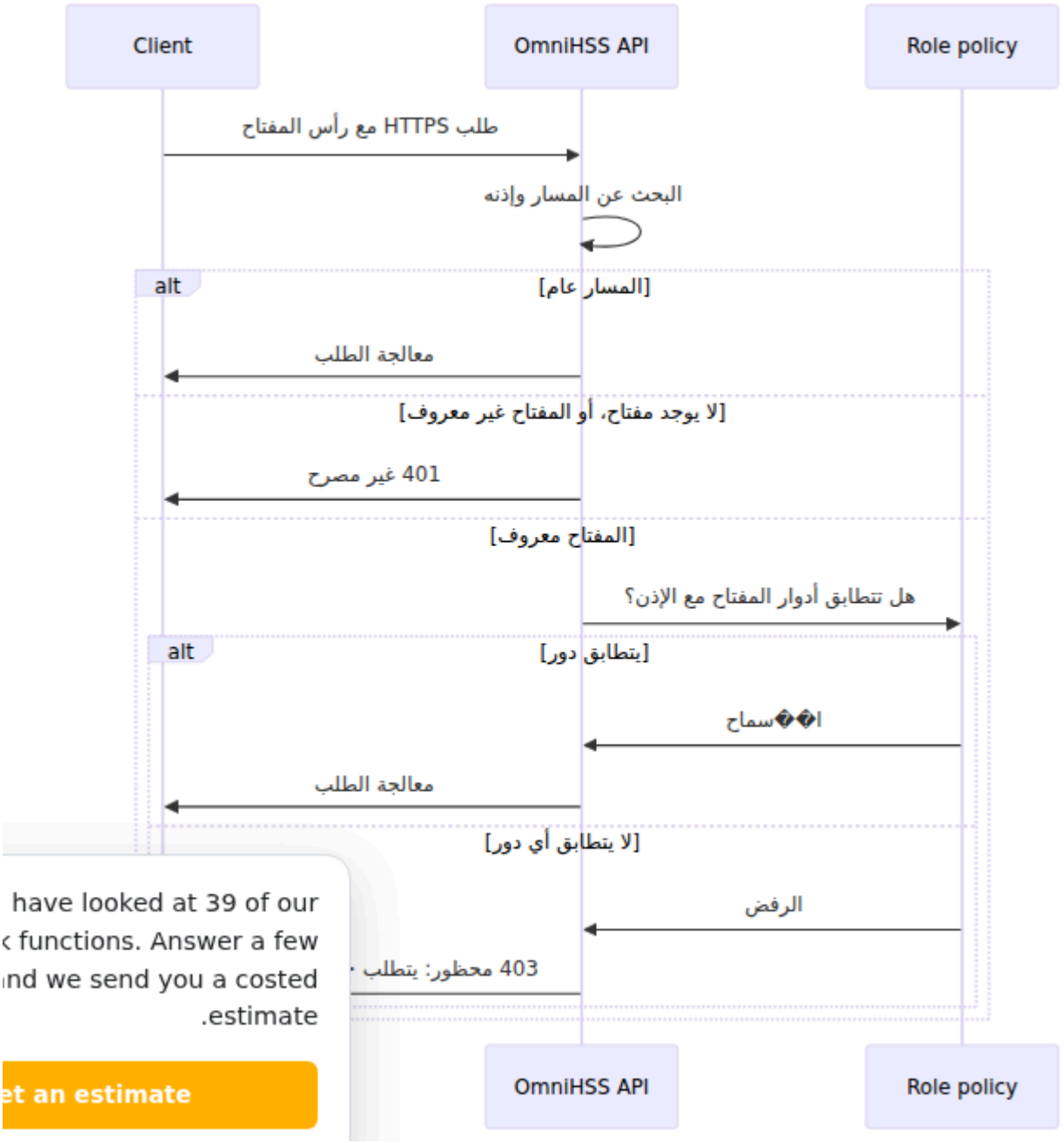
عند بدء الخدمة، يظهر السجل سطر ملخص واحد. يعطي السطر الوضع، وأسماء العناوين، وأسماء المفاتيح، والأدوار، وعدد التحذيرات. لا يظهر أبدًا سرًا. على سبيل المثال:

```
[info] ApiEx: تم تمكين مصادقة المفتاح المشترك (الوضع: rbac،
العنوان: x-omnihss-key، user_header: x-omnihss-user، skip_paths:
[])
  keys: omnicrm [crm_provisioning، يؤكد المستخدم]، omniweb [oam،
يؤكد المستخدم]، omnihlr [hlr_interworking]، ...
```

أو تحذيرًا حول تعطيل `mode: legacy` تحقق من هذا السطر بعد كل تغيير. إذا أظهر السطر المصادقة، فإن معلمة `api_keys` غير محملة.

المستخدم الفاعل

يمكن لنظام العميل أن يتصرف نيابة عن مستخدم بشري. على سبيل المثال، يقوم مستخدم OmniWeb بتغيير مشترك، ويرسل OmniWeb اسم المستخدم في `user_header`.



القواعد:

- اسم المستخدم فقط إذا كان المفتاح يحتوي على OmniHSS يقبل `may_assert_user: true`. بالنسبة للمفاتيح الأخرى، يتجاهل OmniHSS العنوان.
- وأقصى حد 256 بايت، ولا يحتوي، UTF-8 يجب أن يكون اسم المستخدم صالحًا بتشفير على أي أحرف تحكم.
- في نظام OmniHSS المستخدم الفاعل هو سجل تدقيق. إنه ليس تسجيل دخول. يثق `may_assert_user: true` العميل لإرسال اسم المستخدم الصحيح. لذلك، قم بتعيين فقط للأنظمة التي لديها تسجيل دخول خاص بها.

استدعاء واجهة برمجة التطبيقات باستخدام مفتاح

أرسل المفتاح في العنوان المكون. أرسل العنوان مرة واحدة فقط. إذا كان الطلب يحتوي على نسختين من العنوان، يرفض OmniHSS الطلب.

```
curl -k
https://hss.example.com:8443/api/subscriber/imsi/001010000000001 \
  -H "x-omnihss-key: <سر>"
```

انقر على **تفويض** والصق السر. ثم ترسل واجهة Swagger (`/api/docs`)، في واجهة Swagger. يحتاج المفتاح إلى `schema:read` و `docs:read` لفتح المفتاح مع كل طلب "جربه". يحتوي النمط `*:read` على كلاهما. واجهة Swagger.

رموز الاستجابة

تستخدم جميع الأخطاء تنسيق واجهة برمجة التطبيقات المعتاد `{"status":"error","response":"..."}`.

الحالة	`response`	السبب
`401`	`unauthorized`	لا يوجد مفتاح، مفتاح خاطئ، أو نسختين من عنوان المفتاح.
`403`	`forbidden: requires <permission>`	لا تتطاب�ق أدوار المفتاح مع إذن المسار. يذكر الاستجابة الإذن.
`403`	`forbidden: acting user required`	يحتاج المسار إلى مستخدم فاعل، ولم يذكر الطلب واحدًا.
`503`	`authentication misconfigured`	التكوين غير صالح، أو تغير إلى وضع أقل أثناء تشغيل الخدمة.
`404`	`Not Found`	طلب مفتاح معروف مسارًا غير موجود.

تمكين RBAC على نظام قيد التشغيل

يحصل كل عميل لا يرسل مفتاحًا صالحًا على `401`. لذلك، قم بتحضير جميع العملاء قبل إعادة تشغيل OmniHSS، عند تمكين RBAC.

1. في هذا الموقع OmniHSS قم بعمل قائمة بكل نظام يستدعي واجهة برمجة تطبيقات.
2. اختر دورًا من الأدوار المقترحة لكل نظام.
3. اصنع سرًا واحدًا لكل نظام باستخدام `openssl rand -hex 32`.
4. قم بتكوين كل نظام عميل لإرسال سره في العنوان `x-omnihss-key`.
5. أضف كتلة `config :api_ex, :auth` إلى `runtime.exs` على كل مضيف OmniHSS.
6. أعد تشغيل OmniHSS على مضيف واحد.
7. تحقق من سطر سجل بدء التشغيل. ت��كد من أنه يظهر `mode: rbac` وأسماء المفاتيح الصحيحة.
8. ابحث عن أسطر `403` و `401` في السجل. كل سطر `403` يذكر المفتاح والإذن الذي يحتاجه.
9. إذا كان العميل يحتاج إلى إذن ليس لديه دوره، أضف النمط إلى الدور. ثم أعد تشغيل OmniHSS.
10. كرر الخطوات من 6 إلى 9 لكل مضيف آخر من مضيفي OmniHSS.

إذا كان نظام العميل لا يمكنه إرسال عنوان مفتاح بعد، فلا تقم بتمكين RBAC على المضيفات التي يستخدمها العميل. يحصل ذلك العميل على `401` لكل طلب.

في نشر متعدد المواقع، استخدم نفس كتلة `config :api_ex, :auth` على جميع مضيفي OmniHSS. يمكن للعميل بعد ذلك استخدام نفس المفتاح في كل موقع.

تدوير مفتاح

يمكن أن يحتوي المفتاح على أكثر من سر واحد. استخدم هذا لتغيير سر بدون توقف.

1. اصنع سرًا جديدًا باستخدام `openssl rand -hex 32`.
2. أضف السر الجديد إلى قائمة `secrets` في الخاصة بالمفتاح. احتفظ بالسر القديم في القائمة.
3. أعد تشغيل OmniHSS. كلا السرين يعملان الآن.

4. غيّر نظام العميل لإرسال السر الجديد.
5. أزل السر القديم من قائمة `secrets`.
6. أعد تشغيل OmniHSS. يعمل فقط السر الجديد.

```
%{
  name: "omnicrm",
  roles: [:crm_provisioning],
  may_assert_user: true,
  secrets: [
    "REPLACE-WITH-THE-OLD-OMNICRM-SECRET-UNTIL-THE-CRM-USES-THE-
NEW-1",
    "REPLACE-WITH-THE-NEW-OMNICRM-SECRET-FROM-OPENSSL-RAND-HEX-32-
002"
  ]
}
```

لإزالة جميع الوصول لنظام، قم بإزالة مفتاحه من `api_keys`. ثم أعد تشغيل OmniHSS.

السجل والتدقيق

- يحتوي كل سطر سجل يكتبه OmniHSS بعد تحديد مفتاح على `api_ex_principal=<اسم المفتاح>`. استخدم هذا للعثور على النظام الذي أجرى تغييرًا.
- يعطي سطر `403` اسم المفتاح، ونمط المسار، والإذن الذي يحتاجه المفتاح. يعطي السطر نمط المسار، على سبيل المثال `/api/subscriber/:imsi`، وليس المسار الكامل.
- لا تظهر الأسرار أبدًا في أسطر السجل أو في استجابات الأخطاء.
- هذ`log: [allow: :info]`. يعطي لتسجيل كل طلب مسموح به، قم بتعيين أثر تدقيق لجميع تغييرات واجهة برمجة التطبيقات، ولكنه يضيف سطر سجل واحد لكل طلب.

استكشاف الأخطاء وإصلاحها

جميع العملاء يحصلون على 401 بعد إعادة التشغيل

الأعراض: يحصل كل عميل على `401` `unauthorized`.

الأسباب المحتملة:

- لا ترسل العملاء عنوان المفتاح.
- ترسل العملاء المفتاح في عنوان مختلف، مثل `x-api-key`.
- الأسرار في العملاء لا تتطابق مع الأسرار في `runtime.exs`.

الحل:

1. تحقق من سطر سجل بدء التشغيل لاسم العنوان المكون.
2. تأكد من أن كل عميل يرسل مفتاحه في ذلك العنوان.
3. قارن السر في تكوين العميل مع السر في `api_keys`.

عميل يحصل على 403

الأعراض: يحصل عميل على `403` `forbidden: requires <permission>`.

الأسباب المحتملة:

- لا يحتوي دور المفتاح على نمط لذلك الإذن.
- يستخدم النمط `*` حيث يكون `**` ضروريًا. انظر أمثلة النمط.

الحل:

1. ابحث عن الإذن في الاستجابة أو في سطر السجل.
2. ابحث عن المسار في كتالوج أذونات OmniHSS.
3. إذا كان يجب على العميل استخدام المسار، أضف نمطًا للإذن إلى دور المفتاح.
4. أعد تشغيل OmniHSS.

واجهة برمجة التطبيقات تجيب 503 على كل طلب

الأعراض: يحصل كل طلب على `503` `authentication misconfigured`.

الأسباب المحتملة:

- تحتوي معلمة `key` القديمة على قيمة فارغة.
- تغير التكوين إلى وضع أقل أثناء تشغيل الخدمة.

الحل:

1. ابحث في السجل عن السطر الذي يسرد مشاكل التكوين.
2. صحح كتلة `config :api_ex, :auth`.
3. أعد تشغيل OmniHSS.

لا يبدأ OmniHSS بعد التغيير

الأعراض: يتوقف OmniHSS عند بدء التشغيل. يظهر السجل `ApiEx: invalid RBAC configuration`.

الأسباب المحتملة:

- يستخدم مفتاح دورًا غير معرف في `roles`.
- يحتوي مفتاحان على نفس `name`.
- يتشارك مفتاحان سرًا.
- `user_header` هو نفسه `header`.
- ليس لدى مفتاح سر.

الحل:

1. اقرأ قائمة المشاكل المرقمة تحت سطر السجل.
2. صحح كل مشكلة في `runtime.exs`.
3. أعد تشغيل OmniHSS.

يظهر سجل بدء التشغيل تحذيرًا

الأعراض: يحتوي سجل بدء التشغيل على أسطر `ApiEx auth warning:`.

الأسباب المحتملة:

- يكون السر أقصر من 16 بايت.
- يتطابق نمط دور مع أي مسار. عادةً ما تكون هذه خطأ إملائيًا في النمط.

- يفتح نمط `public` مسارًا يمكنه تغيير البيانات.

الحل:

1. اقرأ كل سطر تحذير.
2. اصنع أسرارًا طويلة باستخدام `openssl rand -hex 32`.
3. صحح إملاء النمط. قارنها مع كتالوج أذونات OmniHSS.
4. احتفظ بأنماط `public` للقراءة فقط.

مرجع واجهة برمجة التطبيقات OmniHSS

← العودة إلى دليل العمليات

جدول المحتويات

- نظرة عامة على واجهة برمجة التطبيقات
- المصادقة والتحكم في الوصول
- إدارة مجموعة المفاتيح
- إدارة المشتركين
- بيانات مستودع Sh (البيانات الشفافة)
- إدارة MSISDN
- إدارة اشتراكات IMS
- إدارة SIM
- إدارة مجموعة المفاتيح
- إدارة الملفات الشخصية
- إدارة IP الثابت
- إدارة التجوال
- إدارة EIR
- الحالة والصحة
- معالجة الأخطاء
- أمثلة على استخدام واجهة برمجة التطبيقات

نظرة عامة على واجهة برمجة التطبيقات

عنوان URL الأساسي

```
https://[hostname]:8443/api
```

المصادقة

يجب أن تحمل كل طلب مفتاح واجهة برمجة التطبيقات في رأس المفتاح المكون، على سبيل المثال `x-omnihss-key`. لمزيد من المعلومات حول التكوين، وإذن كل مسار، والأدوار المقترحة لكل نظام عميل، انظر التحكم في الوصول إلى واجهة برمجة التطبيقات (RBAC).

تنسيق الطلب

- **Content-Type:** `application/json`
- **البروتوكول:** HTTPS فقط
- **المنفذ:** 8443 (قابل للتكوين)

مهم: تتوقع جميع نقاط نهاية واجهة برمجة التطبيقات "حمولات JSON "بدون كائنات مسطحة" تغليف.

التنسيق الصحيح:

```
{
  "name": "value",
  "field": "value"
}
```

التنسيق غير الصحيح (لا تستخدمه):

```
{
  "subscriber": {
    "name": "value",
    "field": "value"
  }
}
```

مثال:

```
# ✓ صحيح
curl -X POST https://hss.example.com:8443/api/ims/profile \
  -H "Content-Type: application/json" \
  -d '{"name": "default", "ifc_template": "..."}'

# ✗ غير صحيح
curl -X POST https://hss.example.com:8443/api/ims/profile \
  -H "Content-Type: application/json" \
  -d '{"ims_profile": {"name": "default", "ifc_template": "..."}}'
```

تنسيق الاستجابة

جميع الاستجابات هي JSON بالهيكل التالي:

استجابة النجاح:

```
{
  "status": "success",
  "response": { ... }
}
```

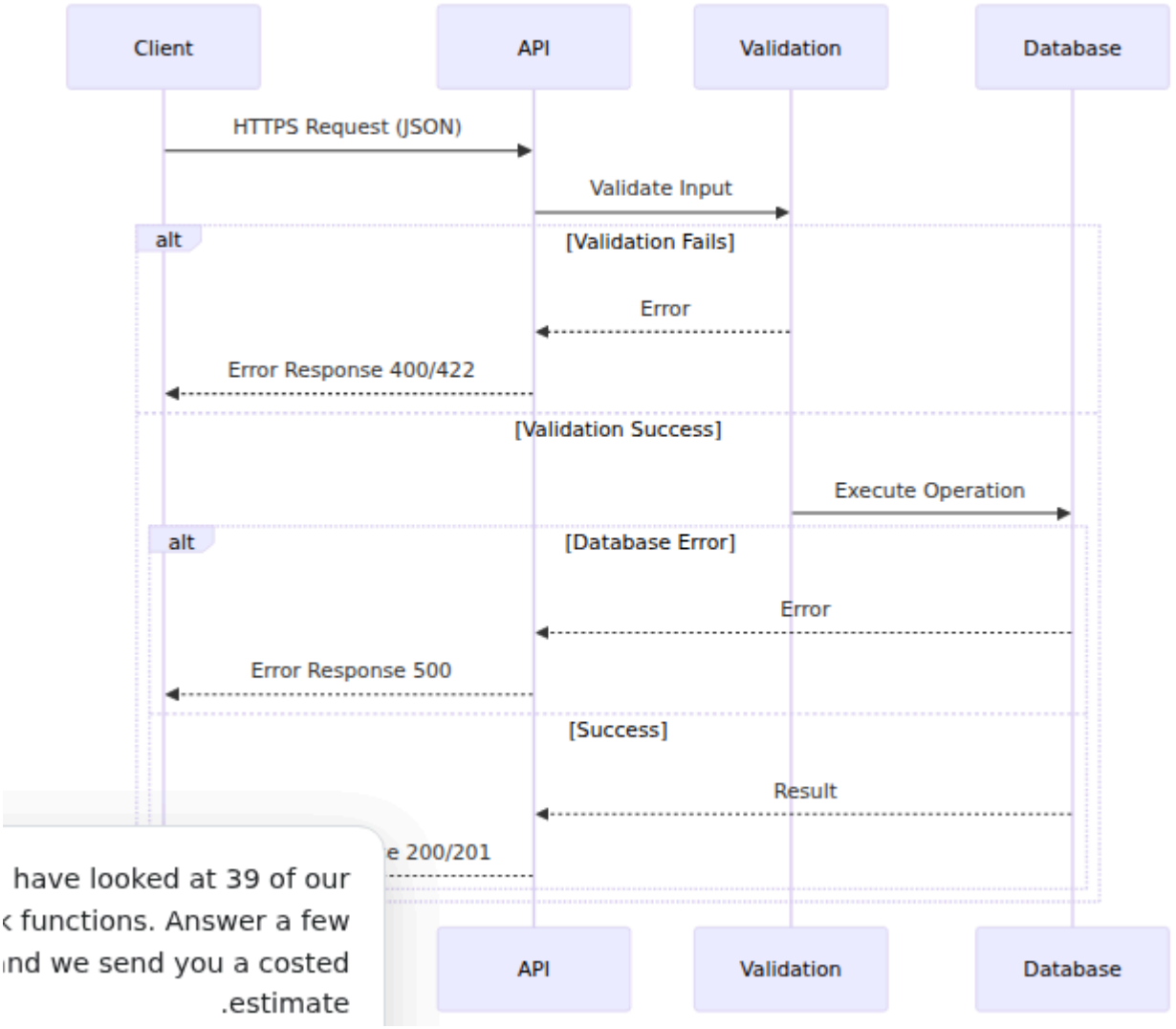
استجابة الخطأ:

```
{
  "status": "error",
  "response": {
    "invalid_fields": {
      "field_name": "error message"
    }
  }
}
```

رموز حالة HTTP

الرمز	المعنى	حالة الاستخدام
200	OK	GET، PUT، DELETE ناجح
201	تم الإنشاء	POST ناجح
400	طلب غير صحيح	بيانات إدخال غير صالحة
401	غير مصرح	لا يوجد مفتاح واجهة برمجة التطبيقات، أو المفتاح غير معروف. انظر التحكم في الوصول إلى واجهة برمجة التطبيقات
403	محظور	أدوار المفتاح لا تسمح بالمسار. انظر التحكم ��ي الوصول إلى واجهة برمجة التطبيقات
404	غير موجود	المورد غير موجود
422	كيان غير قابل للمعالجة	خطأ في التحقق
500	خطأ في الخادم الداخلي	خطأ من جانب الخادم
503	الخدمة غير متاحة	تكوين التحكم في الوصول إلى واجهة برمجة التطبيقات غير صالح. انظر التحكم في الوصول إلى واجهة برمجة التطبيقات

تدفق طلب واجهة برمجة التطبيقات



إدارة المشتركين

قائمة المشتركين

استرجع جميع الم��تركين أو قم بتصفية حسب المعايير.

نقطة النهاية: `GET /api/subscriber`

معلمات الاستعلام:

المعلمة	النوع	الوصف
`enabled`	boolean	تصفية حسب حالة التمكين
`ims_enabled`	boolean	تصفية حسب حالة تمكين IMS

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/subscriber
```

مثال على الاستجابة:

```
{
  "data": [
    {
      "id": "d290f1ee-6c54-4b01-90e6-d701748f0851",
      "imsi": "001001123456789",
      "enabled": true,
      "ims_enabled": true,
      "sim_id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
      "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
      "ims_profile_id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
      "roaming_profile_id": "9c858901-8a57-4791-81fe-
4c455b099bc9",
      "custom_attributes": {},
      "inserted_at": "2025-10-15T10:30:00Z",
      "updated_at": "2025-10-15T10:30:00Z"
    }
  ]
}
```

الحصول على مشترك بواسطة ID

استرجع مشتركًا محددًا بواسطة ID. قاعدة البيانات.

نقطة النهاي��: `GET /api/subscriber/:id`

معلمات المسار:

المعلمة	النوع	الوصف
`id`	string (UUID)	ID قاعدة بيانات المشترك

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-90e6-d701748f0851
```

الحصول على مشترك بواسطة IMSI

استرجع مشتركًا بواسطة IMSI الخاص به.

نقطة النهاية: `GET /api/subscriber/imsi/:imsi`

معلمات المسار:

المعلمة	النوع	الوصف	التنسيق
`imsi`	string	هوية المشترك الدولي للهاتف المحمول	رقم 15-14

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/subscriber/imsi/001001123456789
```

حالة الاستخدام: استكشاف مشترك محدد بواسطة IMSI الخاص به.

الحصول على مشترك بواسطة MSISDN

استرجع مشتركًا بواسطة رقم هاتفه.

نقطة النهاية: `GET /api/subscriber/msisdn/:msisdn`

معلمات المسار:

المعلمة	النوع	الوصف	التنسيق
`msisdn`	string	رقم ISDN لمحطة الهاتف المحمول	رقم 1-15 (E.164)

مثال على الطلب:

```
curl -k
https://hss.example.com:8443/api/subscriber/msisdn/14155551234
```

حالة الاستخدام: البحث عن معلومات المشترك عندما يكون لديك رقم هاتفه فقط.

إنشاء مشترك

توفير مشترك جديد.

نقطة النهاية: `POST /api/subscriber`

جسم الطلب:

```
{
  "subscriber": {
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "sim_id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
    "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
    "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
    "ims_profile_id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
    "roaming_profile_id": "9c858901-8a57-4791-81fe-4c455b099bc9",
    "custom_attributes": {
      "note": "مشترك تجريبي"
    }
  }
}
```

الحقول المطلوبة:

- `imsi` - يجب أن يكون 14-15 رقم، فريد
- `key_set_id` - يجب أن يشير إلى مجموعة المفاتيح الموجودة
- `epc_profile_id` - يجب أن يشير إلى ملف EPC الموجود

الحقول الاختيارية:

- `enabled` - الافتراضي: true
- `ims_enabled` - الافتراضي: true
- `sim_id` - مرجع إلى بطاقة SIM
- `ims_profile_id` - مرجع إلى ملف IMS (مطلوب لخدمات IMS)
- `roaming_profile_id` - مرجع إلى ملف التجوال (مطلوب للتحكم في التجوال)
- `msisdns` - مصفوفة من معرفات MSISDN (أرقام الهواتف)
- `static_ips` - مصفوفة من معرفات IP لتعيينات الثابت APN
- `ims_subscription_id` - مرجع إلى اشتراك IMS لتجميع عدة مشتركين تحت هوية S-CSCF عامة مشتركة واحدة و
- `custom_attributes` - أزواج مفتاح-قيمة مخصصة

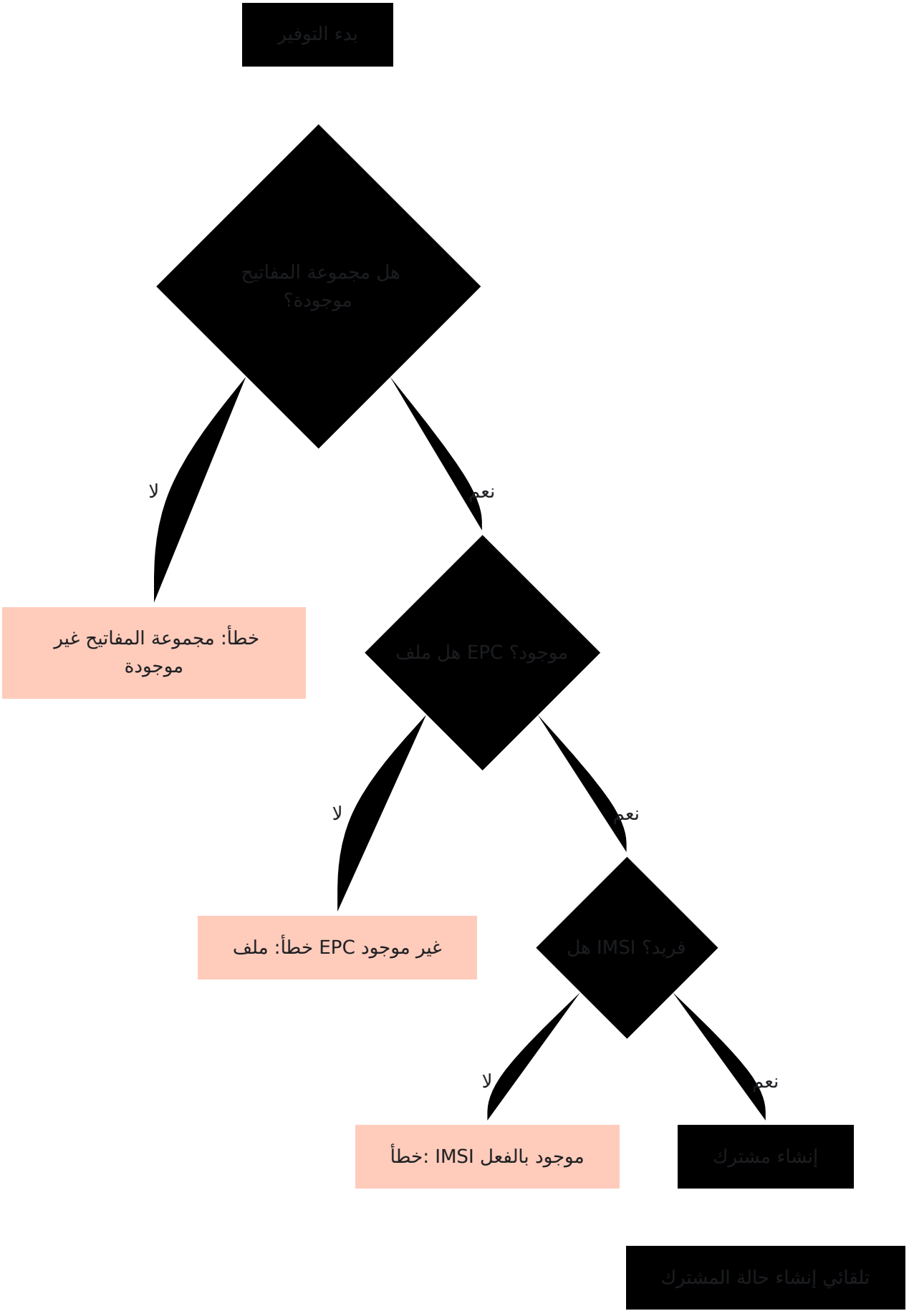
انظر أيضًا:

- مثال كامل على توفير المشترك - سير العمل من البداية إلى النهاية
- وثائق Multi-MSISDN - تعيين أرقام الهواتف للمشتركين
- إدارة IP - تعيين الثابت IP لـ APNs الثابت

مثال على الطلب:

```
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3"
    }
  }'
```

تدفق التوفير:


بدء التوفير
هل مجموعة المفاتيح موجودة؟
لا
نعم
خطأ: مجموعة المفاتيح غير موجودة
هل ملف EPC موجود؟
لا
نعم
خطأ: ملف EPC غير موجود
هل IMSI فريد؟
لا
نعم
خطأ: IMSI موجود بالفعل
إنشاء مشترك
تلقائي إنشاء حالة المشترك

تم الإنشاء 201

تحديث المشترك

تعديل مشترك موجود.

نقطة النهاية: `PUT /api/subscriber/:id`

معلمات المسار:

المعلمة	النوع	الوصف
`id`	string (UUID)	قاعدة بيانات المشترك ID

جسم الطلب:

```
{
  "subscriber": {
    "enabled": false,
    "ims_enabled": false,
    "epc_profile_id": "f47ac10b-58cc-4372-a567-0e02b2c3d479",
    "custom_attributes": {
      "note": "معطل مؤقتًا"
    }
  }
}
```

الحقول القابلة للتحديث:

- `enabled` - تمكين/تعطيل جميع الخدمات
- `ims_enabled` - تمكين/تعطيل خدمات IMS
- `sim_id` - تغيير تعيين بطاقة SIM
- `key_set_id` - تغيير المفاتيح التشفيرية (كن حذرًا!)
- `epc_profile_id` - تغيير ملف خدمة البيانات
- `ims_profile_id` - تغيير ملف خدمة الصوت
- `roaming_profile_id` - تغيير سياسة التجوال
- `msisdns` - تحديث أرقام الهواتف المعينة للمشترك (`[]` يزيل الكل)

- `static_ips` - تحديث تعيينات IP الثابت لـ APNs (`[]` يزيل الكل)
- `custom_attributes` - تحديث البيانات المخصصة

غير قابلة للتحديث:

- `imsi` - لا يمكن تغيير IMSI (احذف وأعد الإنشاء بدلاً من ذلك)
- `subscriber_state` - حالة وقت التشغيل المكتوبة بواسطة HSS؛ لا يمكن تعيينها باستخدام `PATCH /api/hlr/subscriber_state/:imsi` من خلال هذه النقطة النهائية. قم بتعيين أو مسح `assigned_scscf`

انظر أيضًا:

- إدارة ملفات الخدمات - إدارة الملفات الشخصية

مثال على الطلب:

```
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "enabled": false
    }
  }'
```

حالات الاستخدام:

- تعطيل المشترك مؤقتًا: `{"enabled": false}`
- تعطيل خدمات الصوت فقط: `{"ims_enabled": false}`
- تغيير ملف الخدمة: `{"epc_profile_id": "f47ac10b-58cc-4372-a567-0e02b2c3d479"}` (انظر ملفات EPC)
- تحديث سياسة التجوال: `{"roaming_profile_id": "1b671a64-40d5-491e-99b0-da01ff1f3341"}` (انظر إدارة التجوال)

حذف المشترك

إزالة مشترك من النظام.

نقطة النهاية: `DELETE /api/subscriber/:id`

معلمات المسار:

المعلمة	النوع	الوصف
`id`	string (UUID)	قاعدة بيانات المشترك ID

مثال على الطلب:

```
curl -k -X DELETE
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851
```

تحذير: هذا يحذف المشترك بشكل دائم وجميع بيانات الحالة المرتبطة (جلسات PDN، المكالمات، إلخ). يمكن إعادة استخدام IMSI بعد الحذف.

ملاحظة: حذف مشترك لا يحذف:

- مجموعة المفاتيح - يمكن إعادة استخدامها لمشتركين آخرين
- SIM - يمكن إعادة تعيينها لمشترك جديد
- الملفات الشخصية - موارد مشتركة تستخدمها عدة مشتركين
- MSISDNs - يجب حذفها بشكل منفصل إذا رغبت في ذلك

إلغاء طلب الموقع (فصل قسري)

إرسال طلب إلغاء الموقع (CLR) لفصل مشترك من MME المسجل حاليًا.

نقطة النهاية: `POST /api/subscriber/cancel_location`

جسم الطلب:

```
{
  "imsi": "001001123456789"
}
```

المعلمات:

المعلمة	النوع	مطلوب	الوصف
`imsi`	string	نعم	IMSI (14-15 رقم) للمشترك لفصله

مثال على الطلب:

```
curl -k -X POST
https://hss.example.com:8443/api/subscriber/cancel_location \
  -H "Content-Type: application/json" \
  -d '{"imsi": "001001123456789"}'
```

استجابة النجاح (200 OK):

```
{
  "data": {
    "message": "تم إرسال طلب إلغاء الموقع بنجاح",
    "imsi": "001001123456789",
    "destination_host": "mme01.operator.com",
    "destination_realm": "epc.operator.com"
  }
}
```

استجابة الخطأ (404 غير موجود):

```
{
  "error": "المشترك غير موجود أو غير مسجل حاليًا في أي MME"
}
```

السلوك:

- يرسل S6a CLR إلى MME حيث المشترك مسجل حاليًا (`subscriber_state.last_seen_mme`)
- يستخدم `Cancellation-Type: subscription_withdrawal` (يفصل بالكامل)
- يحدد `CLR-Flags: {s6a_indicator: 1, reattach_required: 1}` (يجب إعادة المصادقة على UE)
- يعود 404 إذا لم يسجل المشترك أبدًا أو إذا كان `last_seen_mme` فارغًا

- **يؤثر على جميع MSISDNs** المرتبطة بـ IMSI (نفس الجهاز/SIM)

حالات الاستخدام:

- **منع الاحتيال:** فصل مشترك مشبوه على الفور
- **إنهاء الاشتراك:** فرض تسجيل الخروج عند تعطيل الحساب
- **استكشاف الأخطاء:** مسح تسجيل MME القديم لأغراض التصحيح
- **الهجرة:** فرض إعادة المصادقة لتطبيق إعدادات الملف الشخصي الجديدة
- **الأمان:** فصل مشترك مخترق على الفور

اعتبارات متعددة IMSI:

عند استخدام CLR مع سيناريوهات متعددة MSISDN:

1. **عدة MSISDNs، IMSI واحد:**

```
// المشترك لديه IMSI 001001123456789 مع MSISDNs
["+1234567890", "+9876543210"]
POST /api/subscriber/cancel_location
{"imsi": "001001123456789"}

// تأثرا (نفس الجهاز) MSISDNs واحد، كلا CLR النتيجة: تم إرسال
```

2. **IMSI (أجهزة مختلفة) مختلفة:**

```
// سيناريو نقل الرقم) مختلفة IMSIs ولكن MSISDN مشتركين اثنين بنفس
// المشترك A: IMSI 001001111111111، MSISDN "+1234567890"
// المشترك B: IMSI 001001222222222، MSISDN "+1234567890"

POST /api/subscriber/cancel_location
{"imsi": "001001111111111"}

// لم يتأثر B فقط، المشترك A النتيجة: تم فصل المشترك
```

ملاحظات هامة:

- **استنادًا إلى IMSI:** يتم دائمًا إرسال CLR لكل IMSI، وليس لكل MSISDN

- CLR بشكل غير متزامن؛ تعني استجابة النجاح أن CLR **غير م��زامن:** يتم إرسال عالجه MME تم إرساله، وليس أن
- **لا تحقق من حالة MME:** غير قابل للوصول MME حتى لو كان CLR يتم إرسال (القياسي HSS سلوك)
- IMSI **آمن:** من الآمن استدعاءه عدة مرات لنفس

الوثائق ذات الصلة:

- تدفق بروتوكول طلب إلغاء الموقع
- IMSI سيناريوهات متعددة
- S6a معمارية واجهة

Sh بيانات مستودع (البيانات الشفافة)

توفير الوصول إلى مستندات Sh الشفافة لمشترك (خدمات MMTEL، معلومات IMS-ODB، وغيرها). هذه هي نفس المستندات غير الشفافة التي يقرأها ويكتبها خادم التطبيق عبر واجهة Sh Diameter. الوصول يكون عبر `GET`/`PUT`/`DELETE` `/api/subscriber/repository_data/:imsi`.

لنموذج البيانات، وتدفقات الرسائل، انظر Sh (البيانات الشفافة) بيانات مستودع وقواعد التزام تسلسل الأرقام، والمرجع الكامل لواجهة برمجة التطبيقات REST.

MSISDN إدارة

يمكن تعيين MSISDNs (أرقام الهواتف) للمشتركين لتمكين خدمات الصوت. انظر وثائق Multi-MSISDN للحصول على تفاصيل حول تعيين أرقام متعددة لمشترك واحد.

علامة `shared`

تتضمن الاستجابات التي تحمل MSISDN قيمة `shared` تكون `true` محسوبة، للقراءة فقط. على IMSI، رقم مشترك متعدد) عندما يتم الاحتفاظ بالرقم بواسطة **أكثر من مشترك واحد** بخلاف ذلك. تظهر على كيان `false` و، (منفصلة SIMs سبيل المثال هاتف وساعة ذكية على MSISDN (`GET /api/msisdn` و `GET /api/msisdn/:id`)، على كل رقم مضمن في مشترك (`GET /api/subscriber/:id`)، وعلى أرقام المشتركين التي تم إرجاعها بواسطة

`GET /api/subscriber/msisdn/:msisdn` بحسابها. HSS لا يتم قبولها أبدًا في الكتابة؛ يقوم .
انظر حل MSISDN عبر الواجهات.

قائمة MSISDNs

استرجع جميع أرقام الهواتف.

نقطة النهاية: `GET /api/msisdn`

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/msisdn
```

الحصول على MSISDN

استر��ع رقم هاتف محدد.

نقطة النهاية: `GET /api/msisdn/:id`

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/msisdn/16fd2706-8baf-
433b-82eb-8c7fada847da
```

مثال على الاستجابة:

```
{
  "status": "success",
  "response": {
    "id": "16fd2706-8baf-433b-82eb-8c7fada847da",
    "msisdn": "14155551234",
    "shared": false
  }
}
```

إنشاء MSISDN

إنشاء رقم هاتف جديد.

نقطة النهاية: `POST /api/msisdn`

جسم الطلب:

```
{
  "msisdn": {
    "msisdn": "14155551234"
  }
}
```

التحقق:

- يجب أن يكون 1-15 رقم
- يجب أن يكون فريدًا
- يجب أن يتبع تنسيق E.164 (التنسيق الدولي بدون علامة +)

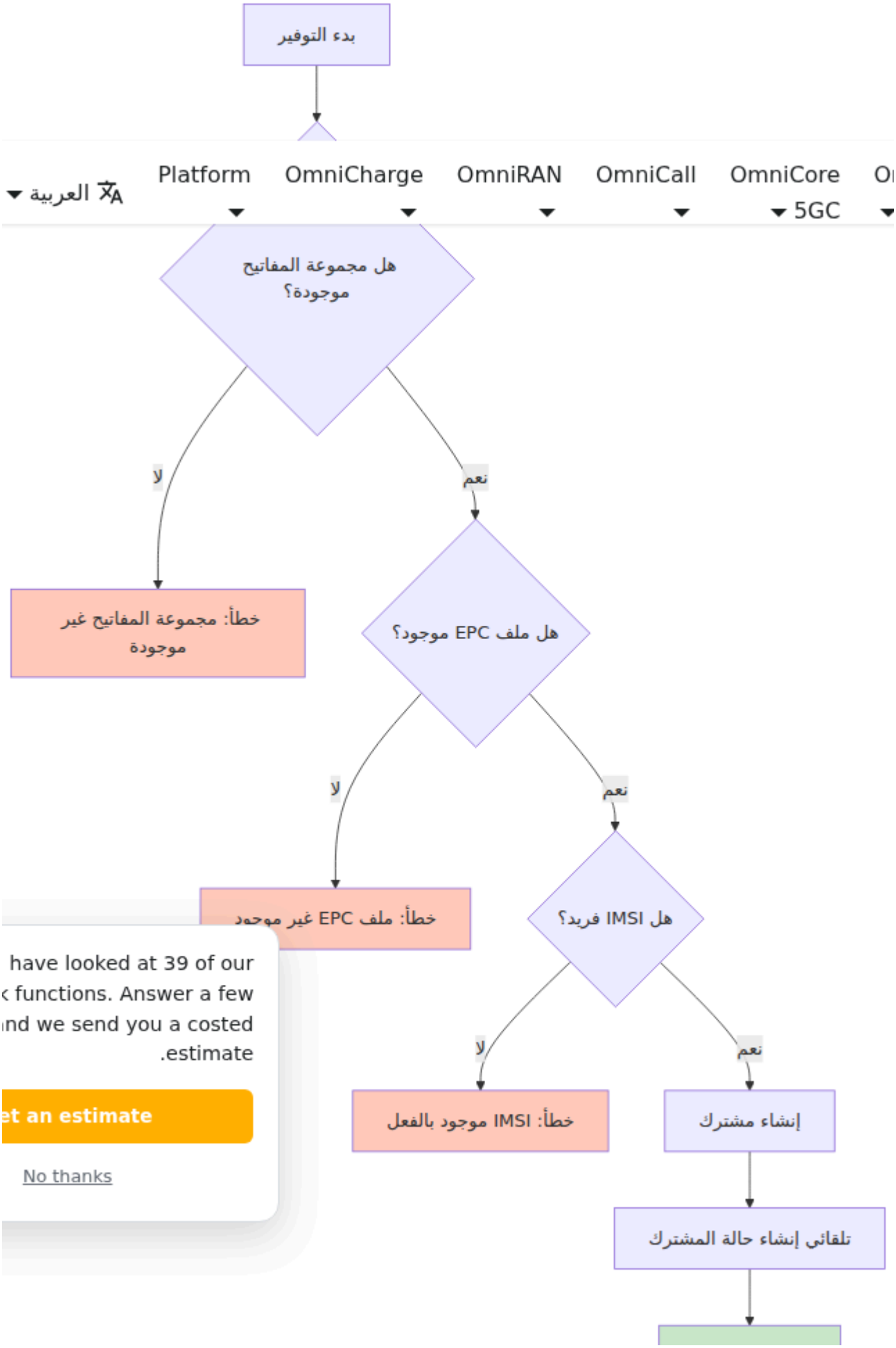
مثال على الطلب:

```
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{
    "msisdn": {
      "msisdn": "14155551234"
    }
  }'
```

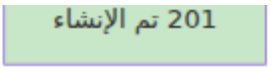
تعيين MSISDN لمشترك

لتعيين رقم هاتف لمشترك، تحتاج إلى إنشاء سجل ارتباط. يتم ذلك عادةً من خلال نقطة تحديث المشترك أو عبر التلاعب المباشر بقاعدة البيانات.

نمط Multi-MSISDN:



have looked at 39 of our
k functions. Answer a few
nd we send you a costed
.estimate
et an estimate
No thanks



للاستخدام التفصيلي Multi-IMSI و Multi-MSISDN انظر ميزات.

حذف MSISDN

إزالة رقم هاتف.

نقطة النهاية: `DELETE /api/msisdn/:id`

مثال على الطلب:

```
curl -k -X DELETE
https://hss.example.com:8443/api/msisdn/16fd2706-8baf-433b-82eb-
8c7fada847da
```

إدارة اشتراكات IMS

تجمع اشتراك IMS عدة مشتركين (IMSIs / IMPIs) في اشتراك IMS و واحد يشارك هوية عامة S-CSCF واحد. انظر هوية المستخدم العامة المشتركة.

قائمة اشتراكات IMS

نقطة النهاية: `GET /api/ims_subscription`

```
curl -k https://hss.example.com:8443/api/ims_subscription
```

الحصول على اشتراك IMS

نقطة النهاية: `GET /api/ims_subscription/:id`

```
curl -k
https://hss.example.com:8443/api/ims_subscription/16fd2706-8baf-
433b-82eb-8c7fada847da
```

إنشاء اشتراك IMS

نقطة النهاية: `POST /api/ims_subscription`

```
curl -k -X POST https://hss.example.com:8443/api/ims_subscription
\
  -H "Content-Type: application/json" \
  -d '{"name": "عائلة سميث - رقم مشترك"}'
```

الحقول:

- `name` - اسم قابل للقراءة البشرية (مطلوب، فريد)
- `ims_profile_id` - ملف IMS مشترك اختياري لهويات المجموعة المشتركة

`assigned_scscf` و `last_seen_scscf_timestamp` هي حالة وقت التشغيل المكتوبة بواسطة HSS وليست محددة بواسطة العميل.

تحديث اشتراك IMS

نقطة النهاية: `PATCH /api/ims_subscription/:id`

حذف اشتراك IMS

نقطة النهاية: `DELETE /api/ims_subscription/:id`

لا يؤدي حذف اشتراك IMS إلى حذف مشتركيه؛ يتم مسح `ims_subscription_id` الخاص بهم. على المشترك (انظر تحديث `ims_subscription_id` لإضافة مشترك إلى مجموعة، قم بتعيين المشترك).

إدارة SIM

تخزن سجلات بطاقة SIM معلومات بطاقة SIM الفعلية بما في ذلك ICCID، رموز تفاصيل البائع، PIN/PUK، ومفاتيح OTA. يمكن ربط سجلات SIM اختياريًا بـ المشتركين.

انظر أيضًا:

- وثائق Multi-IMSI - عدة مشتركين على بطاقة SIM واحدة

قائمة بطاقات SIM

استرجاع جميع بطاقات SIM.

نقطة النهاية: `GET /api/sim`

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/sim
```

الحصول على SIM

استرجاع بطاقة SIM معينة. `adm1`-`adm10`، `kic` و `kid` هي للكتابة فقط: يتم إرجاعها فقط في الاستجابة لطلب الإنشاء أو التحديث الذي تم تعيينها فيه، ولا يتم إرجاعها أبدًا في أي استجابة API أخرى.

نقطة النهاية: `GET /api/sim/:id`

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/sim/3f2504e0-4f89-41d3-9a0c-0305e82c3301
```

إنشاء SIM

إنشاء سجل بطاقة SIM جديدة.

نقطة النهاية: `POST /api/sim`

جسم الطلب:

```
{
  "sim": {
    "iccid": "8991101200003204510",
    "sim_vendor": "Gemalto",
    "batch_name": "2025-Q1-Batch-01",
    "is_esim": false,
    "pin1": "1234",
    "pin2": "5678",
    "puk1": "12345678",
    "puk2": "87654321",
    "adm1": "admin-code-1",
    "kic": "0123456789ABCDEF0123456789ABCDEF",
    "kid": "FEDCBA9876543210FEDCBA9876543210"
  }
}
```

الحقول المطلوبة:

- `iccid` - 19-20 رقمًا، فريد

الحقول الاختيارية ولكن المهمة:

- `sim_vendor` - اسم الشركة المصنعة
- `batch_name` - للتتبع
- `is_esim` - علم بولياني لـ eSIM
- `pin1`، `pin2` - رموز PIN للمستخدم النهائي
- `puk1`، `puk2` - رموز فتح PIN
- `adm1-adm10` - رموز إدارية
- `kic`، `kid` - مفاتيح أمان OTA (سلسلة سداسية)

مثال على الطلب:

```
curl -k -X POST https://hss.example.com:8443/api/sim \
  -H "Content-Type: application/json" \
  -d '{
    "sim": {
      "iccid": "89911012000003204510",
      "sim_vendor": "Gemalto"
    }
  }'
```

تحديث SIM

تعديل بيانات بطاقة SIM.

نقطة النهاية: `PUT /api/sim/:id`

مثال على الطلب:

```
curl -k -X PUT https://hss.example.com:8443/api/sim/3f2504e0-4f89-
41d3-9a0c-0305e82c3301 \
  -H "Content-Type: application/json" \
  -d '{
    "sim": {
      "batch_name": "Updated-Batch-Name"
    }
  }'
```

حذف SIM

إزالة سجل بطاقة SIM.

نقطة النهاية: `DELETE /api/sim/:id`

تحذير: تأكد من عدم وجود مشتركين يشيرون إلى هذه SIM قبل الحذف.

إدارة مجموعات المفاتيح

تحتوي مجموعات المفاتيح على المواد التشفيرية (Ki، OPC/OP، AMF، SQN) المستخدمة في مصادقة المشتركين عبر خوارزمية Milenage. يجب أن تشير كل مشترك إلى مجموعة مفاتيح.

انظر أيضًا:

- تدفقات البروتوكول - إجراءات المصادقة باستخدام مجموعات المفاتيح

قائمة مجموعات المفاتيح

استرجاع جميع مجموعات المفاتيح التشفيرية.

نقطة النهاية: `GET /api/key_set`

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/key_set
```

الحصول على مجموعة مفاتيح

استرجاع مجموعة مفاتيح معينة. `ki`، `opc`، `op`، `psk`، `des` و `sip_password` هي للكتابة فقط: يتم إرجاعها فقط في الاستجابة لطلب الإنشاء أو التحديث الذي تم تعيينها فيه، ولا يتم إرجاعها أبدًا في أي استجابة API أخرى.

نقطة النهاية: `GET /api/key_set/:id`

مثال على الطلب:

```
curl -k https://hss.example.com:8443/api/key_set/6ba7b810-9dad-
41d1-80b4-00c04fd430c8
```

مثال على الاستجابة:

```
{
  "data": {
    "id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenage",
    "ota_counter": 0
  }
}
```

إنشاء مجموعة مفاتيح

إنشاء مجموعة مفاتيح تشفيرية جديدة.

نقطة النهاية: `POST /api/key_set`

جسم الطلب:

```
{
  "key_set": {
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenage"
  }
}
```

الحقول المطلوبة:

- `ki` - مفتاح 128 بت (32 حرف سداسي)
- إما `opc` أو `op` (يمكن اشتقاق OPC من OP)
- `authentication_algorithm` - حاليًا "milenage" فقط

الحقول الاختيارية:

- `amf` - الافتراضي: "8000"
- `sqn` - الافتراضي: 0

- `ota_counter` - 0 :الافتراضي

تنسيق المفتاح:

- جميع المفاتيح هي سلاسل سداسية
- Ki، OPC، OP: 32 (128 بت) حرف سداسي
- AMF: 4 (16 بت) أحرف سداسية

مثال على الطلب:

```
curl -k -X POST https://hss.example.com:8443/api/key_set \
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }'
```

API **تحذير أمني:** تحتوي مجموعات المفاتيح على مواد تشفير حساسة للغاية. احمِ الوصول إلى وفقًا لذلك.

تحديث مجموعة مفاتيح

تعديل مجموعة مفاتيح موجودة.

نقطة النهاية: `PUT /api/key_set/:id`

تحذير: تغيير المفاتيح لمشترك نشط سيؤدي إلى فشل المصادقة. قم بتحديث المفاتيح فقط خلال نوافذ الصيانة أو للمشتركين الجدد.

الأثر: تؤثر التحديثات على جميع المشتركين الذين يستخدمون مجموعة المفاتيح هذه على الفور. سيفشل المشتركون النشطون في المصادقة في محاولة الارتباط التالية.

حذف مجموعة مفاتيح

إزالة مجموعة مفاتيح.

نقطة النهاية: `DELETE /api/key_set/:id`

تحذير: تأكد من عدم وجود مشتركين يشيرون إلى مجموعة المفاتيح هذه قبل الحذف. استفسر عن المشتركين أولاً للتحقق من المراجع.

إدارة الملفات الشخصية

ملفات تعريف EPC

تحدد ملفات تعريف EPC (نواة الحزمة المتطورة) معلمات خدمة البيانات للمشتركين. يتم الإشارة إلى هذه الملفات الشخصية عند إنشاء مشتركين.

قائمة ملفات تعريف EPC

نقطة النهاية: `GET /api/epc/profile`

الحصول على ملف تعريف EPC

نقطة النهاية: `GET /api/epc/profile/:id`

إنشاء ملف تعريف EPC

نقطة النهاية: `POST /api/epc/profile`

جسم الطلب:

```
{
  "apn_profiles": [],
  "name": "Standard Data Plan",
  "network_access_mode": "packet_only",
  "tracking_area_update_interval_seconds": 600,
  "ue_ambr_dl_kbps": 100000,
  "ue_ambr_ul_kbps": 50000
}
```

الحقول:

الحقل	وصف ا�ا	الوحدات	وذجية
`name`	اسم الملف الشخصي	نص	عرف فريد
`ue_ambr_dl_kbps`	حد عرض النطاق الترددي للتنزيل	كيلوبت في الثانية	10000-1
`ue_ambr_ul_kbps`	حد عرض النطاق الترددي للرفع	كيلوبت في الثانية	5000-50
`network_access_mode`	نوع الوصول	سلسلة	"packet "packet
`tracking_area_update_interval_seconds`	مؤقت TAU	ثواني	جي) 600
`apn_profiles`	قائمة بمعرفات ملفات تعريف APN	مصفوفة	[] [3 ،2

مثال على الطلب:

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_profiles": [],
    "name": "Premium 100Mbps",
    "network_access_mode": "packet_only",
    "tracking_area_update_interval_seconds": 600,
    "ue_ambr_dl_kbps": 100000,
    "ue_ambr_ul_kbps": 50000
  }'
```

انظر أيضًا:

- وثائق الملفات الشخصية - دليل تفصيلي لتكوين الملفات الشخصية
- توفير المشتركين الكامل - استخدام ملفات تعريف EPC في التوفير

تحديث ملف تعريف EPC

نقطة النهاية: `PUT /api/epc/profile/:id`

ملاحظة: تؤثر التغييرات على ملفات تعريف EPC هذا على جميع المشتركين الذين يستخدمون الملف الشخصي. قد تحتاج الجلسات النشطة إلى إعادة التأسيس.

حذف ملف تعريف EPC

نقطة النهاية: `DELETE /api/epc/profile/:id`

تحذير: تأكد من عدم وجود مشتركين يشيرون إلى هذا الملف الشخصي قبل الحذف.

ملفات تعريف IMS

تحدد ملفات تعريف IMS (نظام الوسائط المتعددة IP) معلمات خدمة الصوت ومعايير التصفية للمشتركين. يتم الإشارة إلى هذه الملفات الشخصية عند إنشاء مشتركين مع خدمات الأولية (IFC) مفعلة IMS.

قائمة ملفات تعريف IMS

نقطة النهاية: `GET /api/ims/profile`

إنشاء ملف تعريف IMS

نقطة النهاية: `POST /api/ims/profile`

جسم الطلب:

```
{
  "name": "Standard VoLTE",
  "ifc_template": "<IMS-XML-Template-Here>"
}
```

الحقول المطلوبة:

- `name` - اسم الملف الشخصي (يجب أن يكون فريدًا)
- `ifc_template` - قالب IFC (معايير التصفية الأولية) XML مع متغيرات قالب Liquid

متغيرات قالب IFC:

يدعم قالب IFC المتغيرات التالية من قالب Liquid ديناميكيًا التي يتم استبدالها:

المتغير	الوصف	قيمة المثال
`{{ imsi }}`	IMSI المشترك	`001001123456789`
`{{ msisdns }}`	مصفوفة من MSISDNs (للحلقات)	`["14155551234", "14155555678"]`
`{{ mcc }}`	رمز الدولة المحمول	`001`
`{{ mnc }}`	رمز الشبكة المحمولة	`001`

كيف تعمل عملية عرض القالب:

يتم تخزين قالب IFC كـ **قالب Liquid** (مماثل لـ Jinja2) ويتم عرضه **ديناميكيًا** خلال عمليات IMS:

1. **التخزين**: عند إنشاء ملف تعريف IMS، يتم تخزين القالب كما هو مع المتغيرات مثل `{{ imsi }}` و `{% for msisdn in msisdns %}`
2. **التحقق**: يتحقق API من صحة القالب عن طريق عرضه ببيانات اختبار لضمان صحة بناء جملة XML
3. **عر�ض وقت التشغيل**: عندما يقوم مشترك بتسجيل IMS (MAA/SAA)، يقوم HSS:
   - باسترجاع ملف تعريف IMS الخاص بالمشترك
   - عرض القالب ببيانات المشترك الفعلية:
     - `{{ imsi }}` → IMSI المشترك
     - `{{ msisdns }}` → أرقام هواتف المشترك
     - `{{ mcc }}` → رمز الدولة المحمول المكون
     - `{{ mnc }}` → رمز الشبكة المحمولة المكون
   - إرجاع XML المعروض إلى S-CSCF عبر Cx/Diameter

بناء جملة القالب:

```
<!-- استبدال المتغيرات البسيطة -->
{{ imsi }}

<!-- حلقات for على المصفوفات -->
{% for msisdn in msisdns %}
  <MSISDN>{{ msisdn }}</MSISDN>
{% endfor %}

<!-- دمج المتغيرات -->
{{ imsi }}@ims.mnc{{ mnc }}.mcc{{ mcc }}.3gppnetwork.org
```

مثال على قالب IFC:

```
<?xml version="1.0" encoding="UTF-8"?>
<IMSSubscription>
<PrivateID>{{ imsi }}@ims.mnc{{ mnc }}.mcc{{ mcc
}}.3gppnetwork.org</PrivateID>
<ServiceProfile>
{% for msisdn in msisdns %}
<PublicIdentity>
<Identity>sip:{{ msisdn }}@ims.mnc{{ mnc }}.mcc{{ mcc
}}.3gppnetwork.org</Identity>
<Extension>
<IdentityType>0</IdentityType>
</Extension>
</PublicIdentity>
<PublicIdentity>
<Identity>tel:{{ msisdn }}</Identity>
<Extension>
<IdentityType>0</IdentityType>
</Extension>
</PublicIdentity>
{% endfor %}
<InitialFilterCriteria>
<Priority>10</Priority>
<TriggerPoint>
<ConditionTypeCNF>0</ConditionTypeCNF>
<SPT>
<ConditionNegated>0</ConditionNegated>
<Group>0</Group>
<Method>REGISTER</Method>
</SPT>
</TriggerPoint>
<ApplicationServer>
<ServerName>sip:as.ims.mnc{{ mnc }}.mcc{{ mcc
}}.3gppnetwork.org</ServerName>
<DefaultHandling>0</DefaultHandling>
</ApplicationServer>
</InitialFilterCriteria>
</ServiceProfile>
</IMSSubscription>
```

مثال على الطلب (curl):

```
curl -k -X POST https://hss.example.com:8443/api/ims/profile \
  -H "Content-Type: application/json" \
  -d '{
    "name": "default",
    "ifc_template": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>
<IMSSubscription><ServiceProfile>...</ServiceProfile>
</IMSSubscription>"
  }'
```

مثال على الطلب (Python):

```
import requests

response = requests.post(
    "https://hss.example.com:8443/api/ims/profile",
    json={
        "name": "default",
        "ifc_template": ifc_template_string
    },
    verify=False  # للشهادات الموقعة ذاتيًا
)
```

استجابة النجاح (201 تم الإنشاء):

```
{
  "status": "success",
  "response": {
    "id": "0f8fad5b-d9cb-469f-a165-70867728950e",
    "name": "default",
    "ifc_template": "<?xml version=\"1.0\" encoding=\"UTF-8\"?
>..."
  }
}
```

التحقق:

- يتحقق API من أن قالب IFC هو XML صالح
- يتم عرض متغيرات القالب ببيانات اختبار للتحقق من بناء الجملة
- يجب أن يكون حقل `name` فريدًا وغير فارغ

انظر أيضًا:

- وثائق الملفات الشخصية IFC والأمثلة - تفاصيل قالب
- تدفقات البروتوكول IMS وتدفقات المكالمات - تسجيل
- قالب IFC الافتراضي - تنفيذ مرجعي

ملفات تعريف APN

تتكون ملفات تعريف APN (اسم نقطة الوصول) من ثلاثة مكونات تعمل معًا:

1. **معرف APN** - يحدد اسم APN وإصدار IP
2. **ملف تعريف QoS لـ APN** - يحدد معلمات جودة الخدمة
3. **ملف تعريف APN** - يجمع بين المعرف و QoS، مرتبط بـ ملفات تعريف EPC

انظر وثائق PCRF لتكوين السياسة التفصيلية، وإدارة QoS، وإعادة المصادقة التلقائية. انظر أيضًا وثائق الملفات الشخصية لأمثلة تكوين APN.

قائمة معرفات APN

نقطة النهاية: `GET /api/apn/identifier`

إنشاء معرف APN

نقطة النهاية: `POST /api/apn/identifier`

جسم الطلب:

```
{
  "apn": "internet",
  "ip_version": "ipv4v6"
}
```

قيم إصدار IP:

- `"ipv4"` - IPv4 فقط
- `"ipv6"` - IPv6 فقط
- `"ipv4v6"` - IPv4v6 (ثنائي)
- `"ipv4_or_ipv6"` - IPv4 أو IPv6 (اختيار الشبكة)

قائمة ملفات تعريف QoS لـ APN

نقطة النهاية: `GET /api/apn/qos_profile`

إنشاء ملف تعريف QoS لـ APN

نقطة النهاية: `POST /api/apn/qos_profile`

جسم الطلب:

```
{
  "name": "Best Effort Internet",
  "allocation_retention_priority": 8,
  "apn_ambr_dl_kbps": 50000,
  "apn_ambr_ul_kbps": 25000,
  "pre_emption_capability": false,
  "pre_emption_vulnerability": true,
  "qci": 9
}
```

قائمة ملفات تعريف APN

نقطة النهاية: `GET /api/apn/profile`

إنشاء ملف تعريف APN

نقطة النهاية: `POST /api/apn/profile`

جسم الطلب:

```
{
  "apn_identifier_id": "4fa85f64-5717-4562-b3fc-2c963f66afa6",
  "apn_qos_profile_id": "8d8ac610-566d-4ef0-9c22-186b2a5ed793",
  "name": "Internet APN"
}
```

الحقول المطلوبة:

- `apn_identifier_id` - يجب أن تشير إلى معرف APN موجود
- `apn_qos_profile_id` - يجب أن تشير إلى ملف تعريف QoS لـ APN موجود

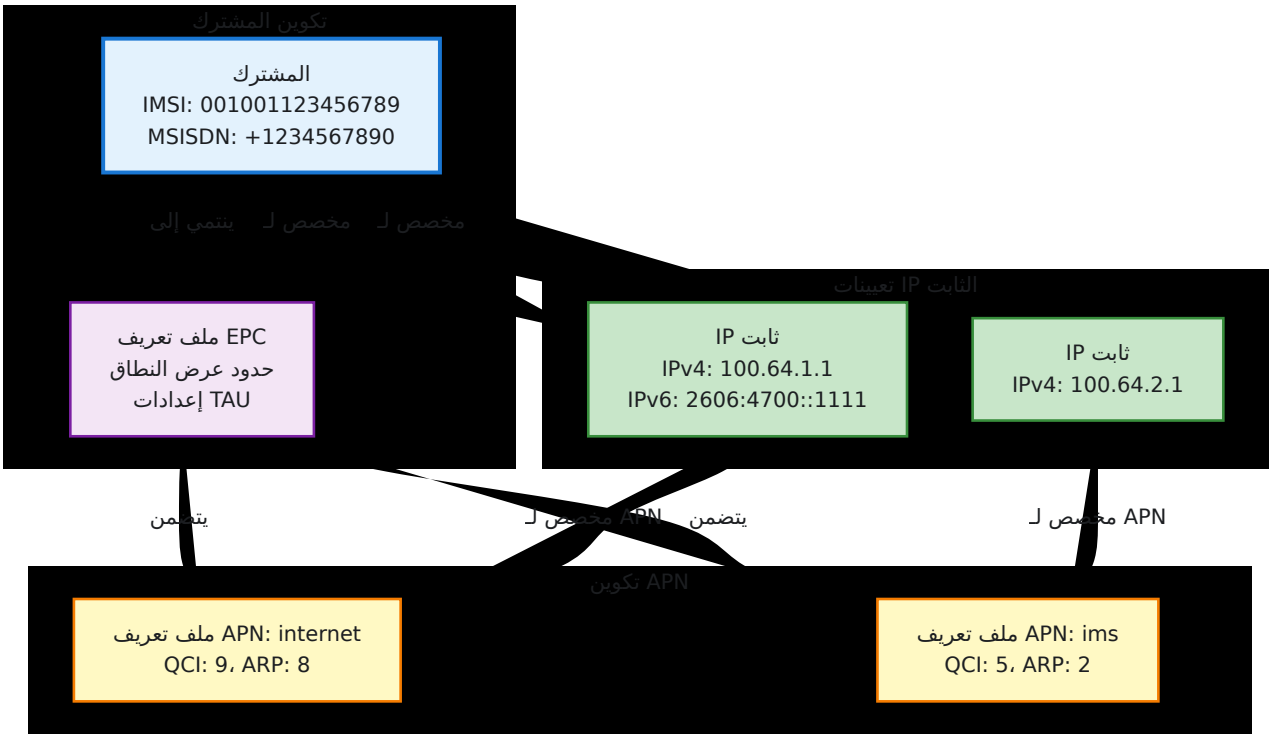
انظر أيضًا:

- APN توفير المشتركين الكامل - مثال كامل بما في ذلك إعداد
- EPC ملفات تعريف - ترتبط ملفات تعريف APN بملفات تعريف EPC

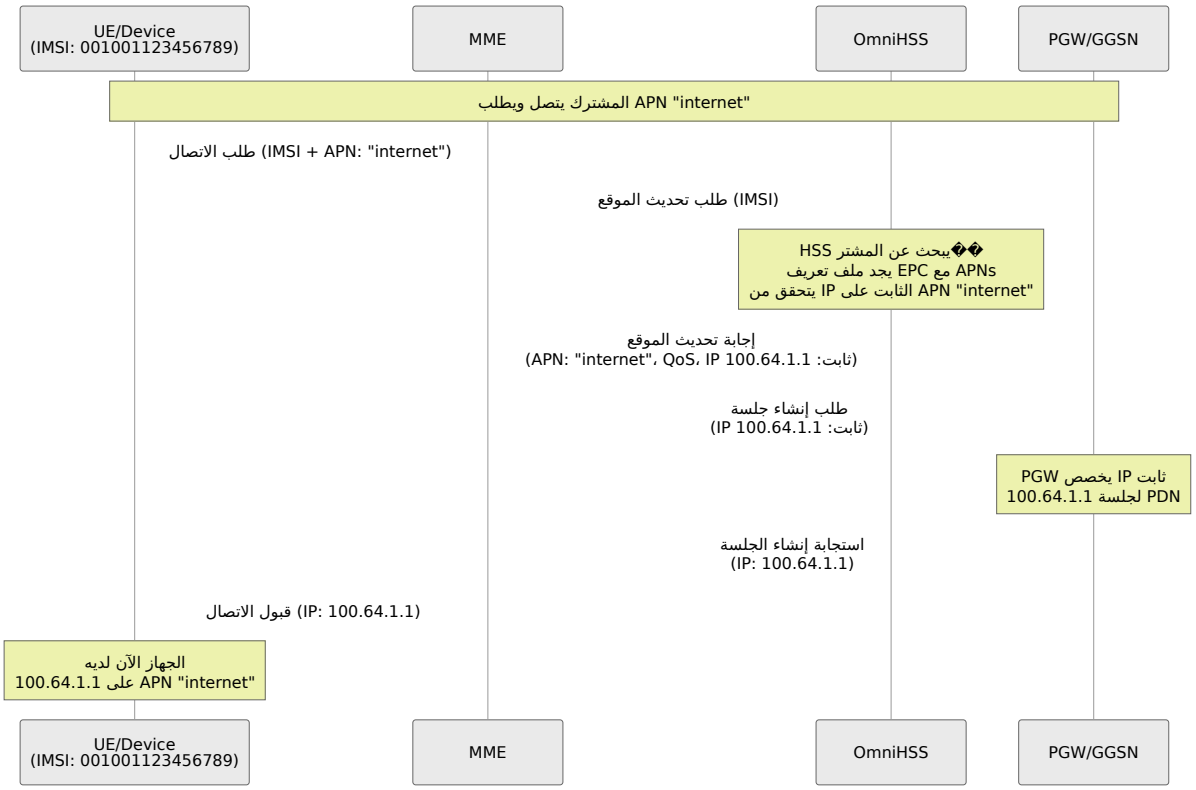
إدارة IP الثابت

يمكن تعيين عناوين IP الثابتة إلى APNs معينة لمشتركين فرديين. يسمح ذلك للمشتركين بتلقي عنوان IPv4 و/أو IPv6 محدد مسبقًا عند الاتصال بـ APN من تلقي عنوان ديناميكي من مجموعة DHCP.

العمارة:

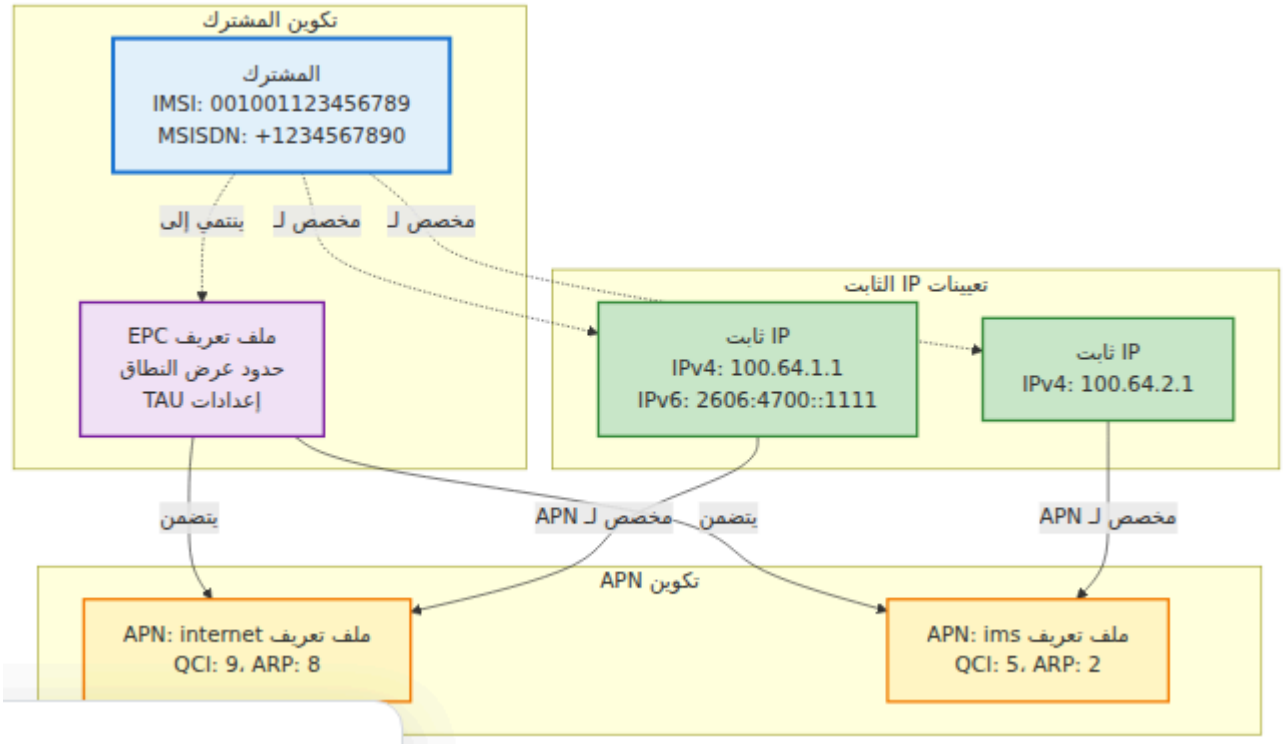


تدفق البيانات عند اتصال المشترك:



إجابة تحديث الموقع - رسم بيانات تكوين APN:

يوضح هذا الرسم البياني بالضبط من أين تأتي كل حقل في S6a Update Location Answer من قاعدة البيانات APN-Configuration AVP:



المفاهيم الأساسية:

- **تعيين لكل APN**: كل عنوان IP ثابت مرتبط بملف APN محدد
- **لكل مشترك**: يمكن أن يكون لدى المشترك تعيين **APN واحد لكل IP عنوان** ثابت واحد فقط لكل IP عنوان APN
- **دعم IPv4 و IPv6**: يمكن أن تكون عناوين IP الثابتة إما IPv4 فقط، أو IPv6 فقط، أو مزدوجة
- **فريدة على مستوى العالم**: يجب أن يكون كل عنوان IP **جميع** فريدًا عالميًا عبر سجلات IP في النظام الثابتة
  - لا يمكن تعيين نفس عنوان IPv4 أو IPv6 لمشتركين متعددين (حتى على APNs مختلفة)
  - يمنع هذا تعارضات التوجيه وغموض عنوان IP
  - يتم فرض ذلك بواسطة فهارس فريدة في قاعدة البيانات على حقول `ipv4_static_ip` و `ipv6_static_ip`
- **علاقة متعددة إلى متعددة**: يتم ربط المشتركين وعناوين IP الثابتة عبر جدول انضمام

حالات الاستخدام:

- عناوين IP ثابتة لأجهزة IoT
- استضافة الخوادم على الأجهزة المحمولة (عنوان IP ثابت للاتصالات الواردة تتطلب)
- التطبيقات القديمة التي تتطلب عناوين IP محددة
- توجيه سياسة الشبكة بناءً على عنوان IP المصدر
- الامتثال التنظيمي الذي يتطلب تتبع عنوان IP

قائمة عناوين IP الثابتة

استرجاع جميع تعيينات عناوين IP الثابتة.

نقطة النهاية: `GET /api/epc/static_ip`

طلب مثال:

```
curl -k https://hss.example.com:8443/api/epc/static_ip
```

استجابة مثال:

```
{
  "data": [
    {
      "id": "c56a4180-65aa-42ec-a945-5fd21dec0538",
      "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111",
      "apn_profile": {
        "id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
        "name": "APN الإنترنت",
        "apn_identifier": {
          "apn": "internet",
          "ip_version": "ipv4v6"
        }
      },
      "inserted_at": "2025-11-15T10:30:00Z",
      "updated_at": "2025-11-15T10:30:00Z"
    }
  ]
}
```


الحصول على عنوان IP ثابت

استرجاع تعيين عنوان IP ثابت محدد.

نقطة النهاية: `GET /api/epc/static_ip/:id`

معلمات المسار:

المعلمة	النوع	الوصف
`id`	سلسلة (UUID)	معرف قاعدة بيانات عنوان IP الثابت

طلب مثال:

```
curl -k https://hss.example.com:8443/api/epc/static_ip/c56a4180-65aa-42ec-a945-5fd21dec0538
```

إنشاء عنوان IP ثابت

إنشاء تعيين عنوان IP ثابت جديد لـ APN.

نقطة النهاية: `POST /api/epc/static_ip`

جسم الطلب:

```
{
  "static_ip": {
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
}
```

الحقول المطلوبة:

- `apn_profile_id` - يجب أن تشير إلى ملف APN موجود
- يجب تحديد واحد على الأقل من `ipv4_static_ip` أو `ipv6_static_ip`

الحقول الاختيارية:

- `ipv4_static_ip` - عنوان IPv4 (صيغة عشرية منقطة)
- `ipv6_static_ip` - عنوان IPv6 (صيغة قياسية)

التحقق من تنسي IP:

- IPv4: صيغة عشرية منقطة قياسية (مثل `100.64.1.1`)
- IPv6: صيغة سداسية عشرية مفصولة بنقطتين قياسية (مثل: `1111::2606:4700:4700`)
- يجب أن تكون كل من عناوين IPv4 و IPv6 **فريدة عالميًا عبر جميع سجلات IP الثابتة**
  - يمنع هذا تعارضات عنوان IP في الشبكة
  - لا يمكن تعيين نفس IP على، حتى APNs مختلفة لمشتركين متعددين
  - هذا قيد على مستوى قاعدة البيانات يتم فرضه بواسطة فهارس فريدة

خيارات التكوين:

التكوين	IPv4	IPv6	مثال
IPv4 فقط	✓	-	`{"ipv4_static_ip": "100.64.1.1"}`
IPv6 فقط	-	✓	`{"ipv6_static_ip": "2606:4700:4700::1111"}`
مزدوج	✓	✓	تم تحديد كلا الحقلين

طلبات مثال:

عنوان IP ثابت IPv4 فقط:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
      "ipv4_static_ip": "100.64.1.1"
    }
  }'
```

عنوان IP ثابت IPv6 فقط:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": "b2c3d4e5-f6a7-4b1c-9d2e-3f4a5b6c7d8e",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }'
```

عنوان IP ثابت مزدوج:

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }'
```

استجابة النجاح (201 تم الإنشاء):

```
{
  "data": {
    "id": "c56a4180-65aa-42ec-a945-5fd21dec0538",
    "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111",
    "inserted_at": "2025-11-15T10:30:00Z",
    "updated_at": "2025-11-15T10:30:00Z"
  }
}
```

انظر أيضًا:

- ثابت للمشترك - كيفية ربط هذا بمشترك تعيين عنوان IP
- ملفات APN - إدارة تكوينات APN

تحديث عنوان IP ثابت

تعديل تعيين عنوان IP ثابت موجود.

نقطة النهاية: `PUT /api/epc/static_ip/:id`

معلمات المسار:

المعلمة	النوع	الوصف
`id`	سلسلة (UUID)	معرف قاعدة بيانات عنوان IP الثابت

جسم الطلب:

```
{
  "static_ip": {
    "ipv4_static_ip": "100.64.1.2",
    "ipv6_static_ip": "2606:4700:4700::1112"
  }
}
```

الحقول القابلة للتحديث:

- `ipv4_static_ip` - تغيير عنوان IPv4
- `ipv6_static_ip` - تغيير عنوان IPv6
- `apn_profile_id` - تغيير تعيين APN

غير القابلة للتحديث:

- `id` - المفتاح الأساسي (للقراءة فقط)

تحذير: تغيير عنوان IP لمشترك نشط سيؤثر على اتصال PDN. ستستمر جلسات PDN التالي له في استخدام عنوان IP القديم حتى يتم قطع الاتصال وإعادة الاتصال.

طلب مثال:

```
curl -k -X PUT
https://hss.example.com:8443/api/epc/static_ip/c56a4180-65aa-42ec-
a945-5fd21dec0538 \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "ipv4_static_ip": "100.64.1.2"
    }
  }'
```

حذف عنوان IP ثابت

إزالة تعيين عنوان IP ثابت.

نقطة النهاية: `DELETE /api/epc/static_ip/:id`

معلمات المسار:

المعلمة	النوع	الوصف
`id`	سلسلة (UUID)	معرف قاعدة بيانات عنوان IP الثابت

طلب مثال:

```
curl -k -X DELETE
https://hss.example.com:8443/api/epc/static_ip/c56a4180-65aa-42ec-
a945-5fd21dec0538
```

السلوك:

- يزيل تعيين عنوان IP الثابت
- لا يؤثر على ملف APN (يظل APN متاحًا لمشتركين آخرين)
- سيحصل المشتركون الذين يستخدمون هذا العنوان IP الثابت على عناوين IP ديناميكية في الاتصال التالي
- يصبح عنوان IP متاحًا لإعادة الاستخدام بعد الحذف

تحذير: إذا كان المشترك يستخدم هذا العنوان IP الثابت بنشاط، فإن حذفه سيؤدي إلى حصوله على عنوان IP ديناميكي في اتصال PDN التالي له. تأكد من أن المشتركون غير متصلين أو أرسل طلب إلغاء الموقع قبل الحذف.

تعيين عنوان IP ثابت لمشترك

لتعيين عنوان IP الثابت لمشترك، تحتاج إلى ربط سجل عنوان IP ثابت بـ المشترك أثناء الإنشاء أو التحديث.

نمط التعيين:

1. **إنشاء عنوان IP الثابت** (انظر إنشاء عنوان IP ثابت)
2. **تعيينه للمشترك** باستخدام حقل `static_ips`

إنشاء مشترك مع عنوان IP ثابت:

```
# الخطوة 1: إنشاء عنوان IP ثابت لـ APN "الإنترنت"
STATIC_IP_ID=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }' | jq -r '.data.id')

# الخطوة 2: إنشاء مشترك مع عنوان IP ثابت معين
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": \"6ba7b810-9dad-41d1-80b4-00c04fd430c8\",
      \"epc_profile_id\": \"e58ed763-928c-4155-bee9-
fdbaaadc15f3\",
      \"static_ips\": [$STATIC_IP_ID]
    }
  }"
```

تحديث مشترك موجود مع عنوان IP ثابت:

```
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "static_ips": ["c56a4180-65aa-42ec-a945-5fd21dec0538",
"5a8f9c3e-2d4b-4e6f-8a1b-3c5d7e9f0a2b"]
    }
  }'
```

عناوين IP ثابتة متعددة (APNs مختلفة):

مختلف APN ثابتة متعددة طالما أن كل منها مخصص لـ IP يمكن أن يكون لدى المشترك عناوين:

```
# إنشاء عنوان IP ثابت لـ APN "الإنترنت"
INTERNET_IP=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": "a1b2c3d4-e5f6-4a3b-8c2d-1e0f9a8b7c6d",
      "ipv4_static_ip": "100.64.1.1"
    }
  }' | jq -r '.data.id')

# إنشاء عنوان IP ثابت لـ APN "ims"
IMS_IP=$(curl -k -X POST
https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": "b2c3d4e5-f6a7-4b1c-9d2e-3f4a5b6c7d8e",
      "ipv4_static_ip": "100.64.2.1"
    }
  }' | jq -r '.data.id')

# تعيين كلاهما للمشترك
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": \"6ba7b810-9dad-41d1-80b4-00c04fd430c8\",
      \"epc_profile_id\": \"e58ed763-928c-4155-bee9-
fdbaaadc15f3\",
      \"static_ips\": [$INTERNET_IP, $IMS_IP]
    }
  }"
```

قواعد التحقق:

- ✓ عناوين: **مسموح** IP ثابتة متعددة لـ APNs مختلفة
- ✗ عناوين: **مرفوض** IP ثابتة متعددة لنفس APN

مثال خطأ - APN مكرر:

```
# تشير إلى نفس IP سيفشل هذا إذا كانت كلا عنواني APN
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "static_ips": ["c56a4180-65aa-42ec-a945-5fd21dec0538",
"5a8f9c3e-2d4b-4e6f-8a1b-3c5d7e9f0a2b"]
    }
  }'

# استجابة الخطأ:
{
  "errors": {
    "static_ips": [
      "يجب أن تكون عناوين IP الثابتة لكل APN على لكل مشترك فريدة. مثال: لا يمكن تعيين عنوان IP ثابت 100.64.1.1 لمشترك للإنترنت وأيضًا 100.64.1.2 للإنترنت"
    ]
  }
}
```

انظر أيضًا:

- إنشاء مشترك - توفير المشترك
- تحديث المشترك - تعديل تكوين المشترك
- ثابت - سير العمل من البداية إلى النهاية IP مثال كامل لتوفير عنوان

إدارة التجوال

تتحكم ملفات التجوال في ما إذا كان يمكن للمشتركين الوصول إلى خدمات البيانات و IMS على الشبكات التي تمت زيارتها. يتم تعيين الملفات إلى المشتركين وتتكون من قواعد تتطابق مع MCC/MNC.

قائمة ملفات التجوال

نقطة النهاية: `GET /api/roaming/profile`

إنشاء ملف تجوال

نقطة النهاية: `POST /api/roaming/profile`

جسم الطلب:

```
{
  "roaming_profile": {
    "name": "فقط شركات النقل الأمريكية",
    "data_action_if_no_rules_match": "deny",
    "ims_action_if_no_rules_match": "deny",
    "roaming_rules": []
  }
}
```

قيم الإجراء:

- `"allow"` - السماح
- `"deny"` - الرفض

الإجراءات الافتراضية:

- `data_action_if_no_rules_match` - الإجراء عند عدم تطابق أي قاعدة تجوال
- `ims_action_if_no_rules_match` - الإجراء الافتراضي الخاص بـ IMS

قائمة قواعد التجوال

نقطة النهاية: `GET /api/roaming/rule`

إنشاء قاعدة تجوال

نقطة النهاية: `POST /api/roaming/rule`

جسم الطلب:

```
{
  "roaming_rule": {
    "name": "السماح لـ AT&T",
    "mcc": "310",
    "mnc": "410",
    "data_action": "allow",
    "ims_action": "allow"
  }
}
```

الحقول:

- `mcc` - رمز الدولة المحمول (3 أرقام)
- `mnc` - رمز الشبكة المحمولة (2-3 أرقام)
- `data_action` - `"allow"` أو `"deny"` خدمات البيانات
- `ims_action` - `"allow"` أو `"deny"` خدمات IMS/الصوت

انظر أيضًا:

- وثائق التجوال - تكوينات مفصلة وأمثلة
- تدفقات البروتوكول Diameter - كيفية عمل التحكم في التجوال في تدفقات

إدارة EIR

تعمل OmniHSS كمسجل هوية المعدات (EIR) عبر واجهة S13 Diameter. قواعد EIR هي للمشترك. يتم تقييم القواعد IMSI ثم IMEI، ثم IMEISV لجهاز، تعبيرات منتظمة يتم مطابقتها مع تصاعدي ويفوز أول تطابق `precedence` في كل خطوة بترتيب.

انظر وثائق EIR للتحقق من هوية المعدات بالتفصيل، وتدفقات واجهة S13، والتحقق من IMEI، وأولوية القاعدة.

قائمة قواعد EIR

استرجاع جميع قواعد EIR.

نقطة النهاية: `GET /api/eir/rule`

لرؤية ترتيب التقييم. `precedence` قم بالفرز على. `id` تُرجع القائمة بترتيب

الحصول على قاعدة EIR

استرجاع قاعدة EIR واحدة.

نقطة النهاية: `GET /api/eir/rule/:id`

إنشاء قاعدة EIR

إضافة قاعدة ووضعها في ترتيب التقييم.

نقطة النهاية: `POST /api/eir/rule`

جسم الطلب:

```
{
  "action": "blacklist",
  "regex": "35979139461640",
  "precedence": 1
}
```

الحقول المطلوبة:

- `action` - `"whitelist"` (السماح)، `"blacklist"` (الرفض) أو `"greylist"` (السماح ولكن تتبع)
- `regex` - تعبير منتظم يتم اختباره ضد IMEISV، ثم IMEI، ثم IMSI. يجب أن يتم تجميعه

الحقول الاختيارية:

- `precedence` - عدد صحيح من 1 إلى 65535. يتم تقييم القيم الأقل أولاً. اتركه فارغًا لإلحاق القاعدة بعد أعلى أولوية حالية. إدخال قيمة يدرج القاعدة في ذلك الموضع: كل قاعدة موجودة لها أولوية متساوية أو أعلى تتحرك لأسفل بمقدار واحد، سواء كانت القيمة مستخدمة بالفعل أم لا

استجابة النجاح (201 تم الإنشاء):

```
{
  "status": "success",
  "response": {
    "id": "0362b7ab-9bd6-4d8a-8b1a-2f4c6e8d0a1c",
    "action": "blacklist",
    "regex": "35979139461640",
    "precedence": 1
  }
}
```

الأولوية في الاستجابة هي الموضع الذي تم إعطاؤه للقاعدة. تعود حالات الفشل في التحقق (إجراء غير معروف، تعبير منتظم فارغ أو غير قابل للتجميع، أولوية خارج 1 إلى 65535) في HTTP 422 تنسيق الخطأ القياسي.

تحديث قاعدة EIR

تغيير إجراء القاعدة أو نمطها أو موضعها.

نقطة النهاية: `PATCH /api/eir/rule/:id` أو `PUT /api/eir/rule/:id`

تطبق كلا الطريقتين فقط الحقول الموجودة في الجسم؛ تبقى الحقول المحذوفة بقيمها الحالية. يؤدي `PUT` إلى معرف غير موجود إلى إنشاء القاعدة بذلك المعرف (HTTP 200)، موضوعة بنفس قواعد الأسبقية مثل `POST`.

تغيير `precedence` ينقل القاعدة إلى ذلك الموضع ويغير فقط القواعد بين مواضعها القديمة والجديدة. ترك `precedence` فارغًا، أو إرسال قيمته الحالية، يبقي ترتيبها دون تغيير. لا ترسل `null`: فإنه يزيل أولوية القاعدة وتُقيم القاعدة بعد كل قاعدة مرقمة.

حذف قاعدة EIR

إزالة قاعدة.

نقطة النهاية: `DELETE /api/eir/rule/:id`

الاستجابة: HTTP 200 مع `"response": ""`.

حذف قاعدة يترك فجوة في ترقيم الأسبقية. تحتفظ القواعد المتبقية بترتيبها النسبي.

حالات الاستخدام:

- حظر الأجهزة المسروقة (معينة IMEI قائمة سوداء لمعرفات)
- تقييد أنواع الأجهزة (TAC قائمة سوداء حسب نمط)
- السماح فقط للأجهزة المعتمدة (قائمة بيضاء للنمط، مع تغيير `unknown_equipment_behaviour` من افتراضه "قائمة بيضاء" إلى "قائمة سوداء" أو "رفض المعدات غير المعروفة"؛ انظر سلوك المعدات غير المعروفة)
- تجاوز قاعدة واسعة لجهاز واحد عن طريق إعطاء القاعدة المحددة أولوية أقل

انظر أيضًا:

- S13 منطق المطابقة، أولوية القاعدة وتدفقات - وثائق EIR
- EIR وتدفق التحقق من S13 - واجهة تدفقات البروتوكول
- OmniHSS EIR - وظيفة نظرة عامة على الهندسة

وثائق إضافية

لمزيد من المعلومات، راجع الوثائق التالية:

- API - نقاط نهاية التحقق من صحة **الحالة والصحة**
- **معالجة الأخطاء** - الأخطاء الشائعة واستكشاف الأخطاء وإصلاحها
- **أمثلة استخدام API** - سير عمل توفير كامل

← العودة إلى دليل العمليات | التالي: لوحة التحكم →

حالة وصحة واجهة برمجة التطبيقات

← العودة إلى مرجع واجهة برمجة التطبيقات

حالة النظام

تحقق مما إذا كانت واجهة برمجة التطبيقات تستجيب.

نقطة النهاية: `GET /api/status`

طلب مثال:

```
curl -k https://hss.example.com:8443/api/status
```

استجابة مثال:

```
{
  "status": "ok"
}
```

حالة الاستخدام: فحص الصحة لموازني الحمل وأنظمة المراقبة.

← العودة إلى مرجع واجهة برمجة التطبيقات

نظرة عامة على معمارية OmniHSS

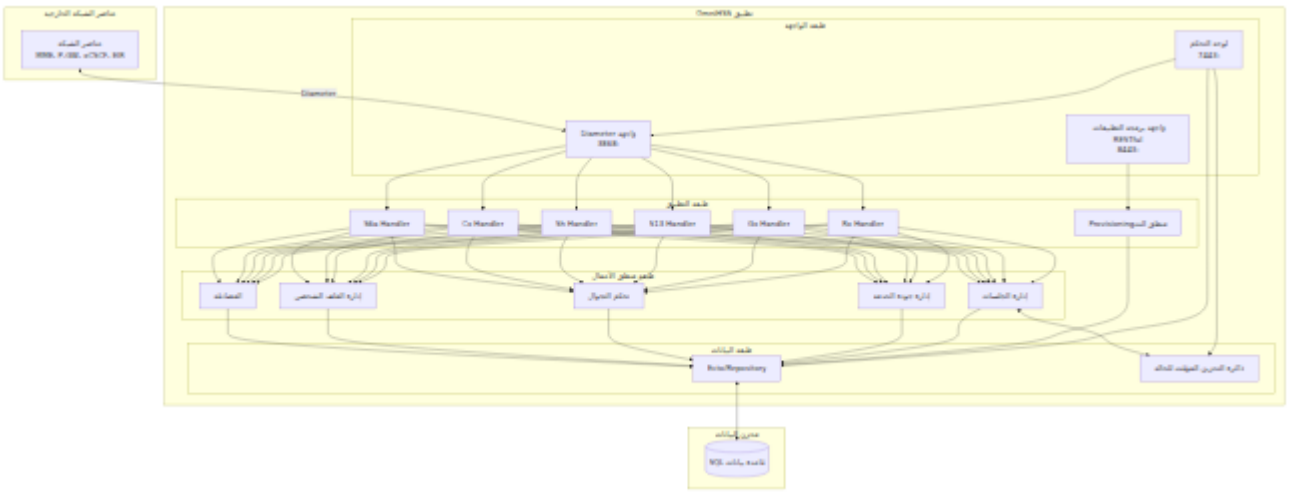
← العودة إلى دليل العمليات

جدول المحتويات

- نظرة عامة على النظام
- معمارية المكونات
- مكدس Diameter
- طبقة التطبيق
- طبقة البيانات
- الواجهات الخارجية
- معمارية النشر

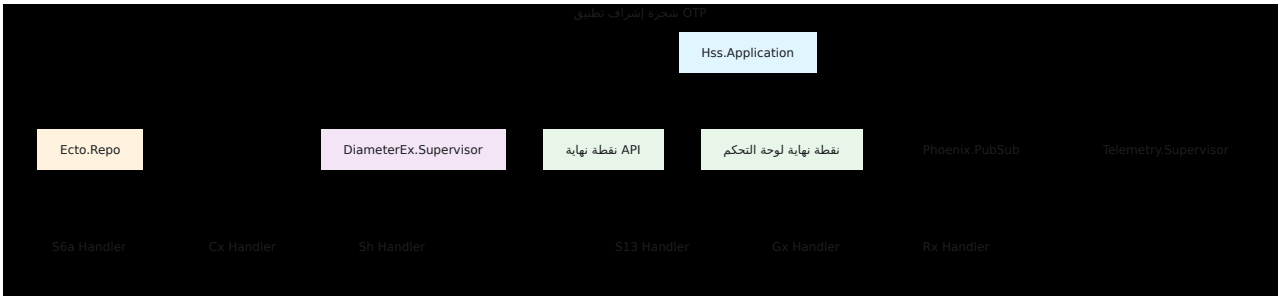
نظرة عامة على النظام

تم بناء OmniHSS على منصة Elixir وErlang/OTP، مما يوفر نظامًا عالي التزامن ومقاومًا للأخطاء مصممًا لأحمال عمل الاتصالات. تتبع المعمارية نهجًا طبقيًا مع فصل واضح بين الاهتمامات.



معمارية المكونات

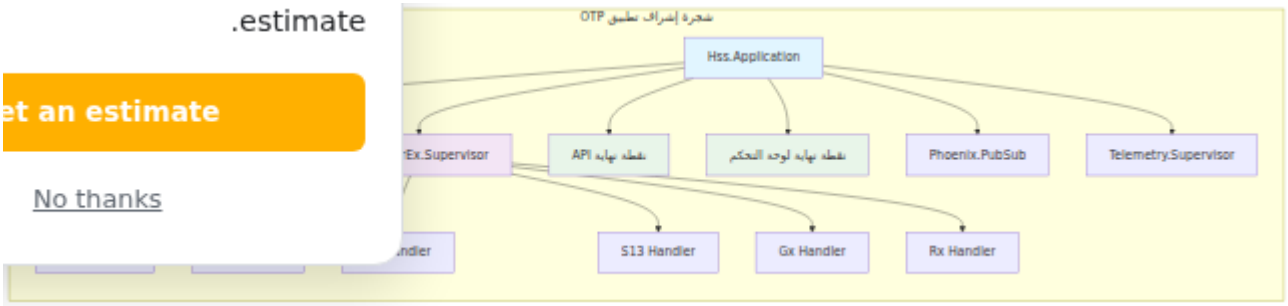
المكونات الأساسية



معالجات تطبيق Diameter

يتم تنفيذ كل تطبيق Diameter (S6a، Cx، Sh، S13، Gx، Rx) كوحدة معالجة DiameterEx التي:

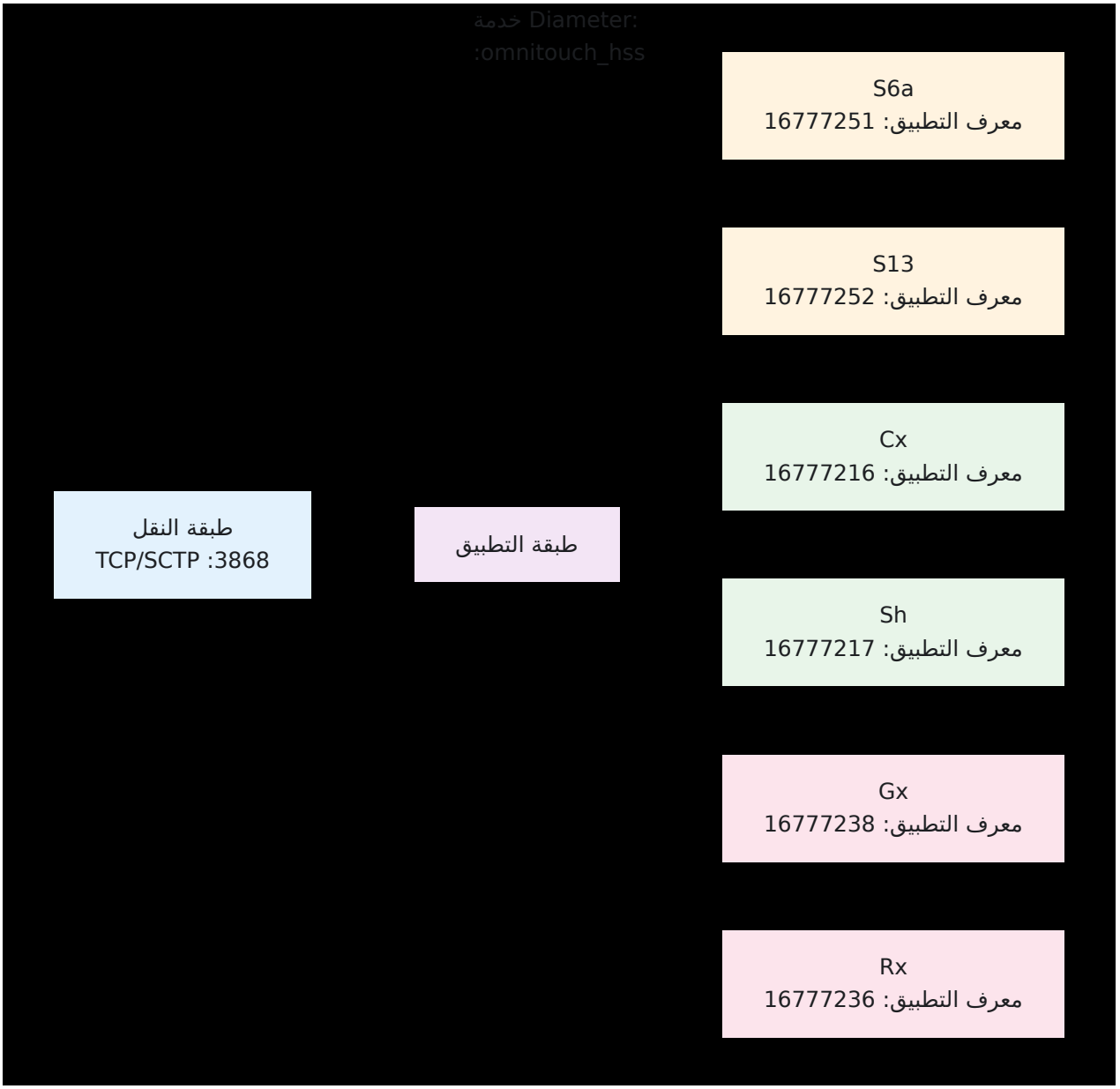
1. **تسجل مع DiameterEx** - تشترك في معرفات تطبيق Diameter محددة
2. **تتحقق من صحة الطلبات** - تستخرج AVPs، تتحقق من حالة المشترك
3. **تعالج منطق الأعمال** - تستدعي وحدات منطق الأعمال المن��سبة
4. **تبني الردود** - تبني رسائل الإجابة Diameter مع AVPs
5. **تعالج الأخطاء** - تعيد رموز نتائج Diameter المناسبة



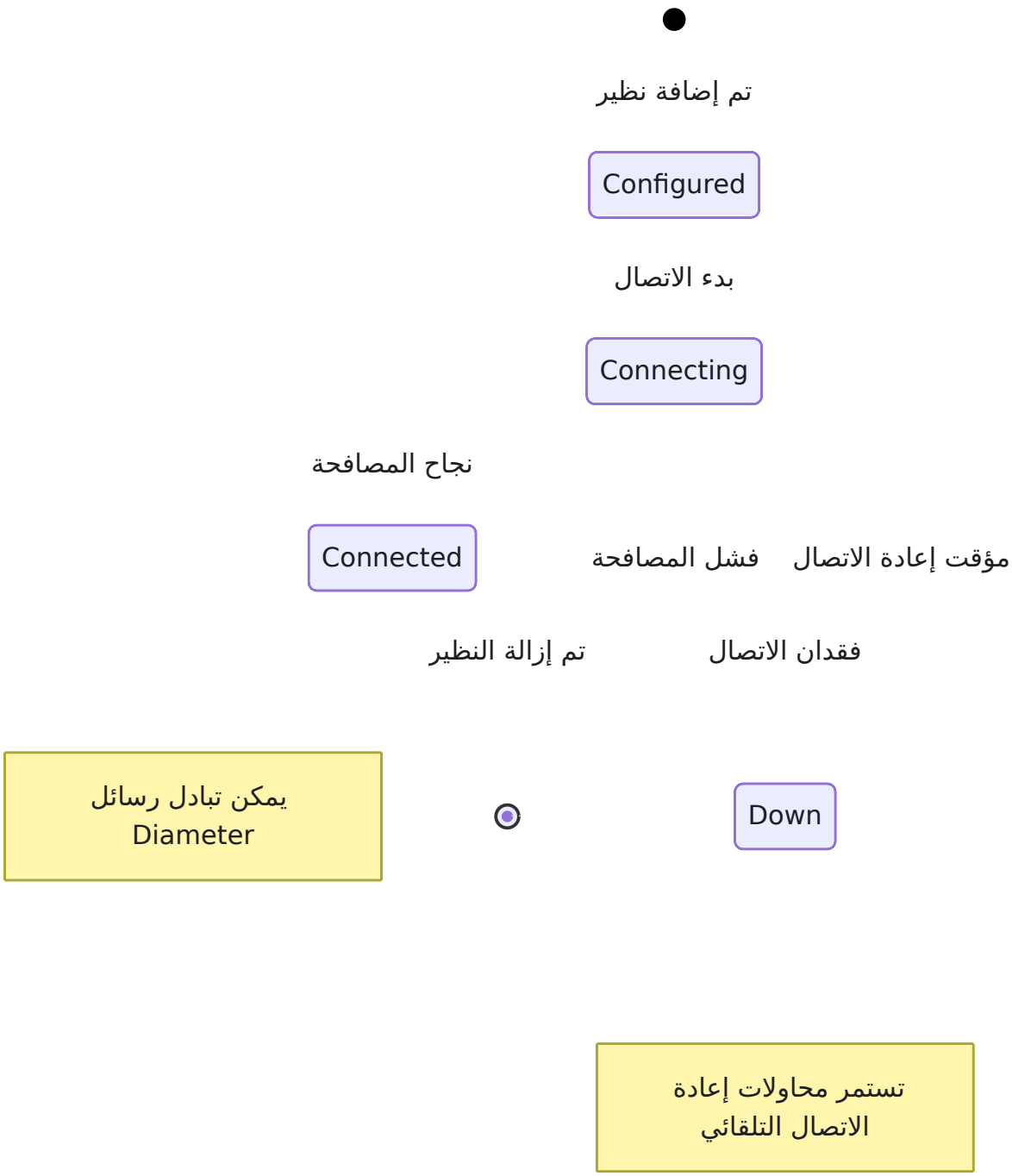
مكدس Diameter

تكوين خدمة Diameter

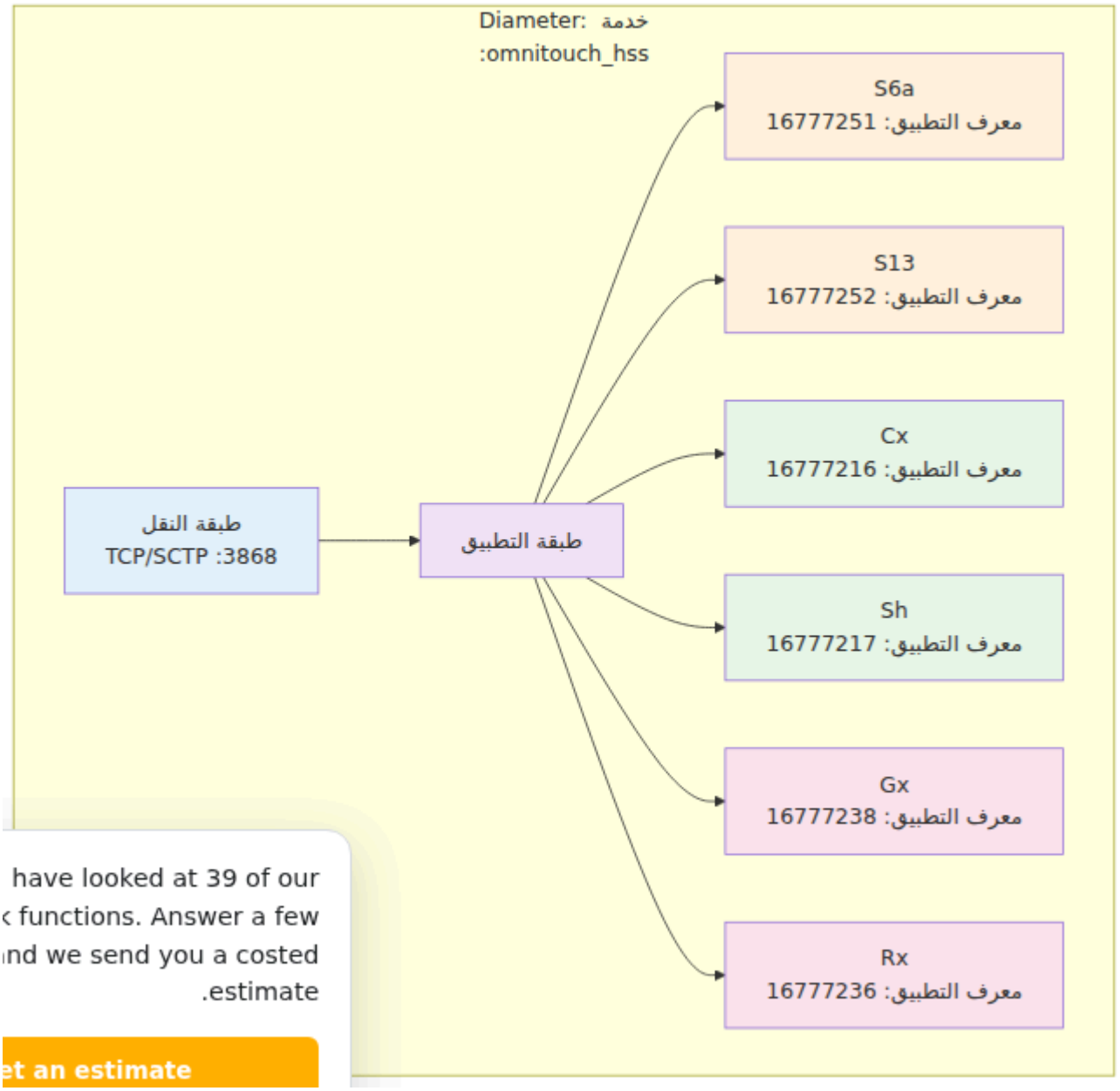
يقوم OmniHSS بتكوين خدمة Diameter واحدة مع تطبيقات متعددة مدعومة:


خدمة Diameter:
:omnitouch_hss
S6a
معرف التطبيق: 16777251
S13
معرف التطبيق: 16777252
Cx
معرف التطبيق: 16777216
Sh
معرف التطبيق: 16777217
Gx
معرف التطبيق: 16777238
Rx
معرف التطبيق: 16777236
طبقة التطبيق
طبقة النقل
TCP/SCTP :3868

إدارة اتصال الأقران



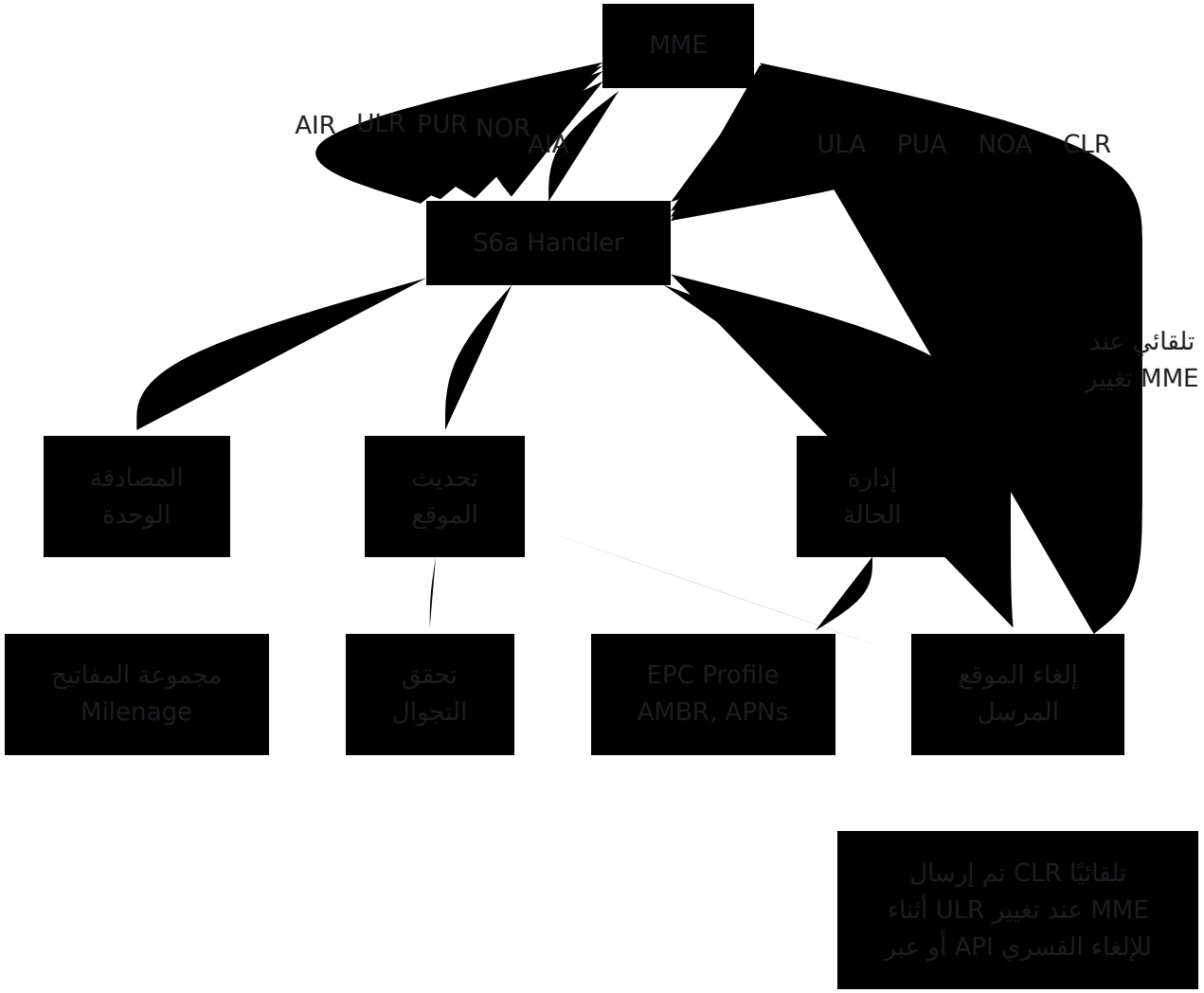
تدفق رسالة Diameter



طبقة التطبيق

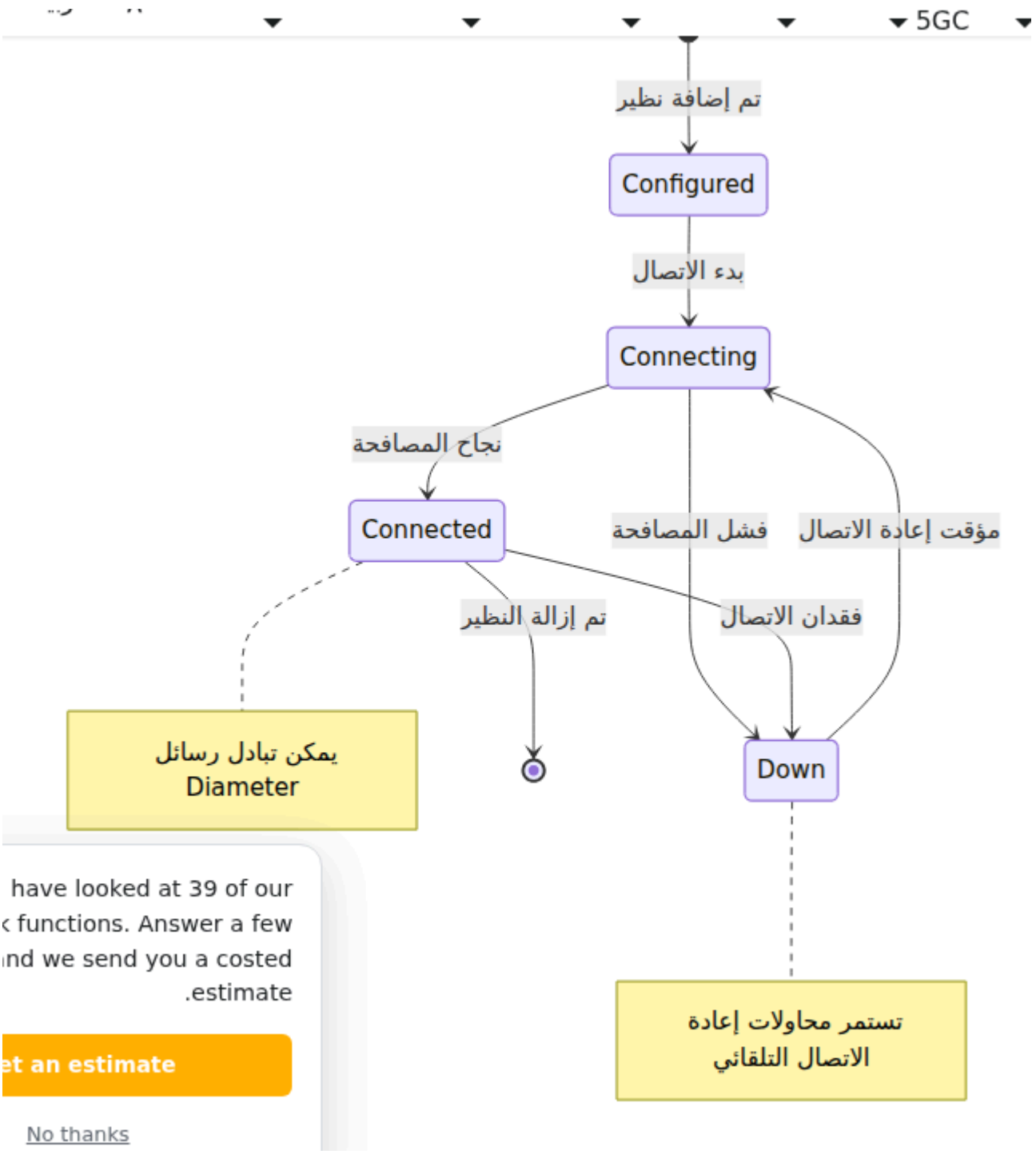
واجهة S6a (LTE/EPC)

تتعامل مع المصادقة وإدارة التنقل لشبكات LTE.



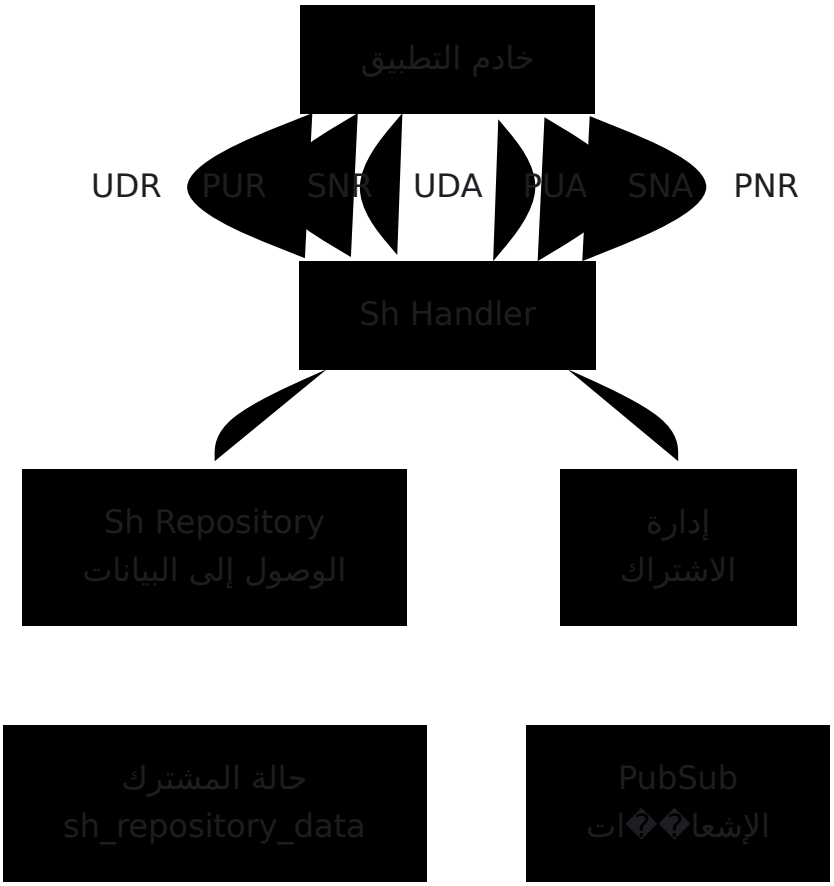
واجهة Cx (IMS)

تتعامل مع تسجيل IMS والمصادقة.



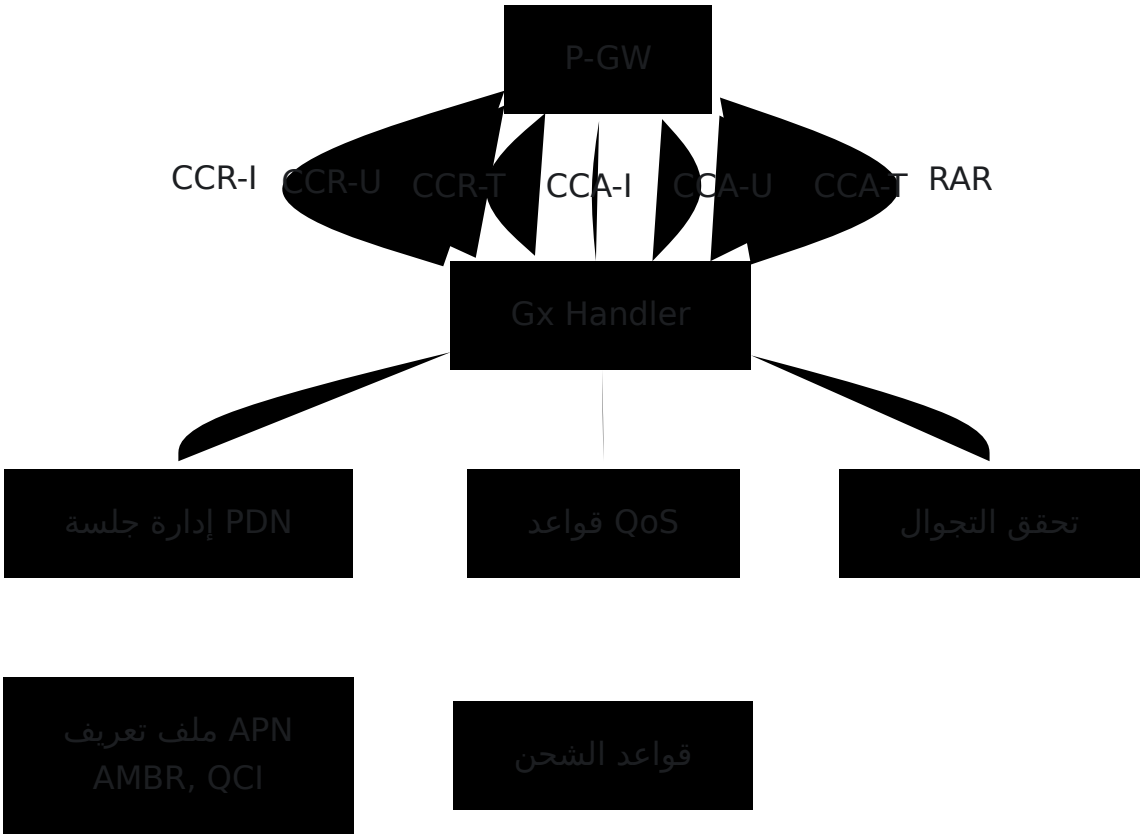
واجهة Sh (بيانات ملف تعريف IMS)

توفر خوادم تطبيق IMS الوصول إلى بيانات ملف تعريف المشترك.



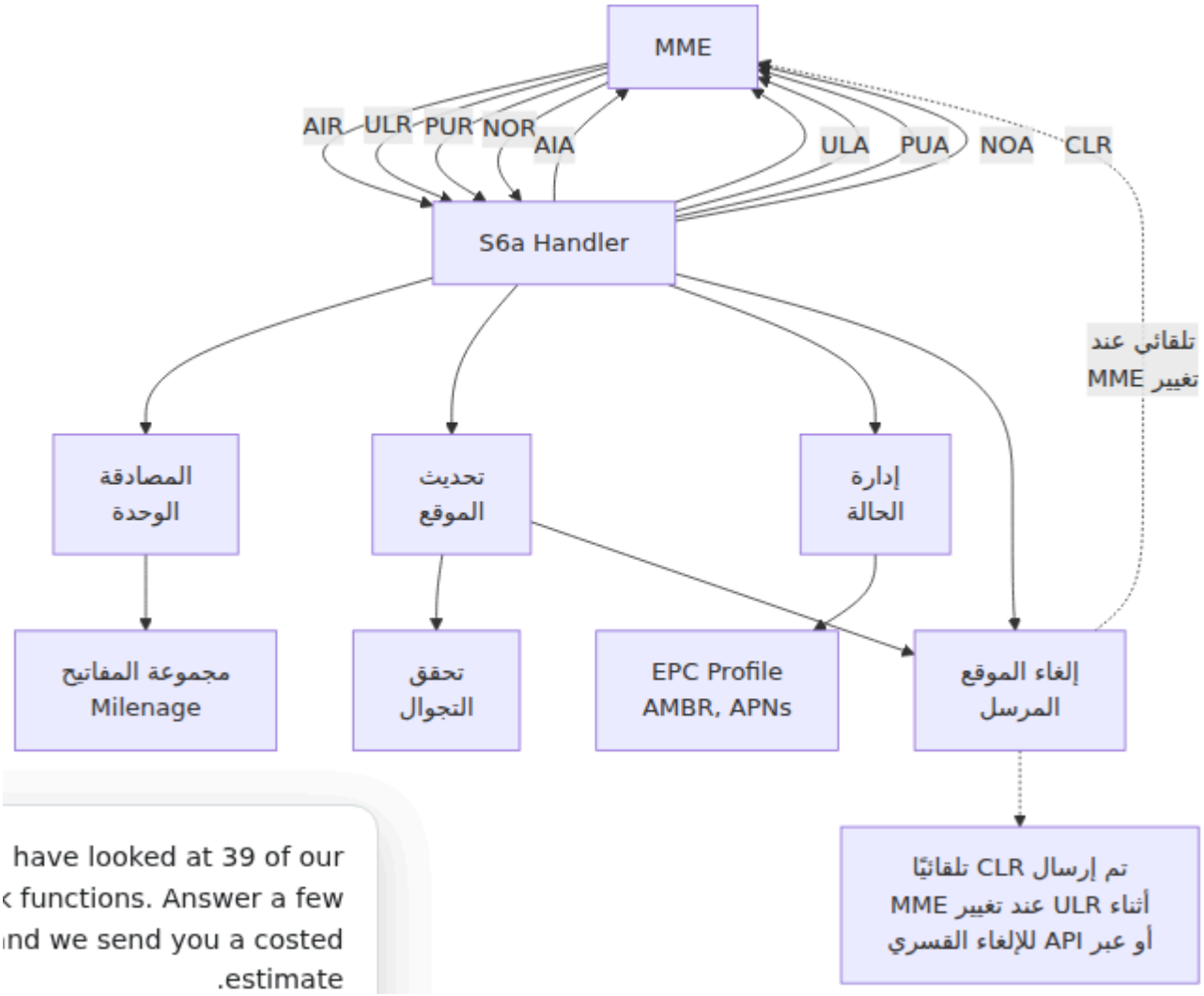
واجهة Gx (تحكم السياسة)

للحصول على PCRF تدير التحكم في السياسة والشحن لجلسات البيانات. **انظر وثائق التفاصيل.**



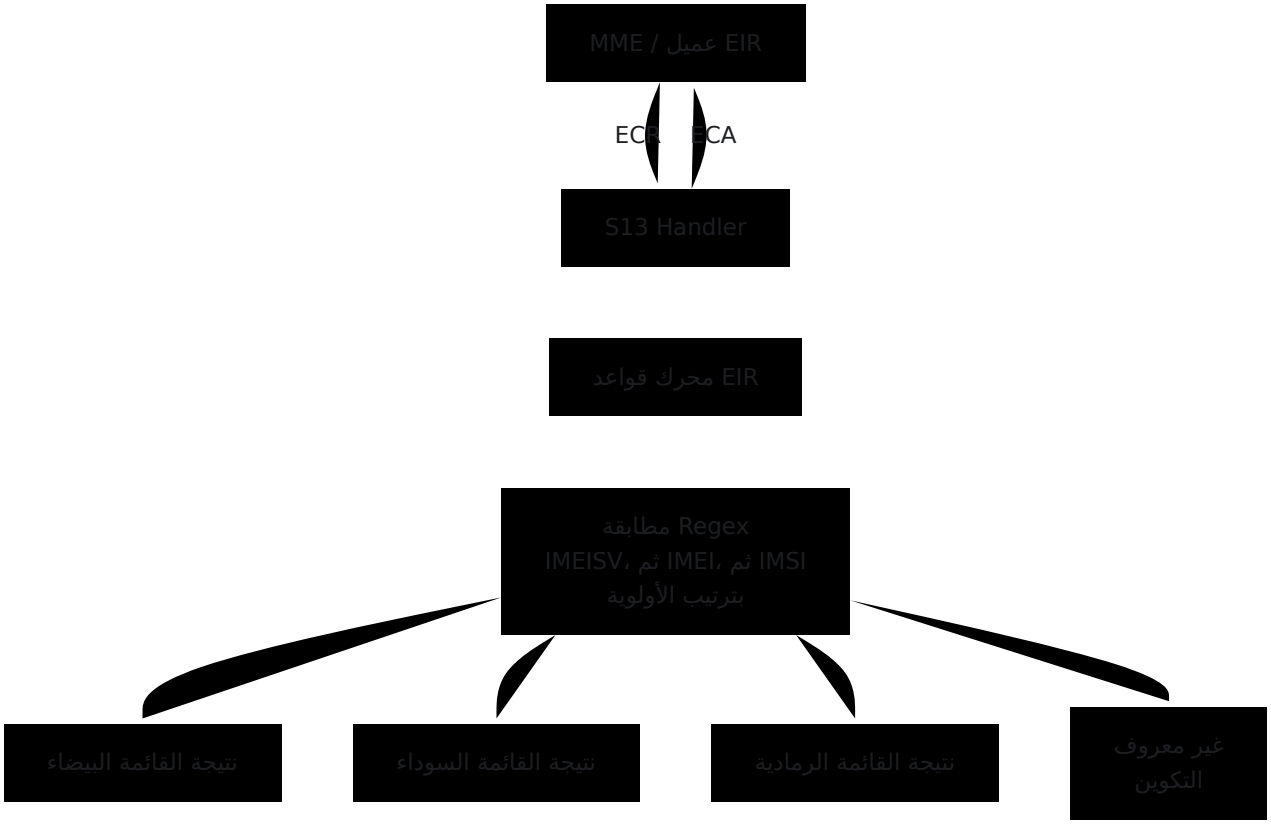
واجهة Rx (وسائط IMS)

تتحكم في سياسة وسائط IMS لـ VoLTE. وحوامل مخصصة لـ **انظر وثائق PCRF للحصول على التفاصيل.**



واجهة S13 (EIR)

يعمل OmniHSS كـ EIR. يتحقق من IMEISV وIMEI للجهاز، وخياريًا IMSI المشترك عندما يحمل اسم المستخدم، وفقًا لقواعد هوية المعدات التي يتم تقييمها بترتيب تصاعدي. **انظر** ECR AVP **وثائق EIR للحصول على التفاصيل.**



طبقة البيانات

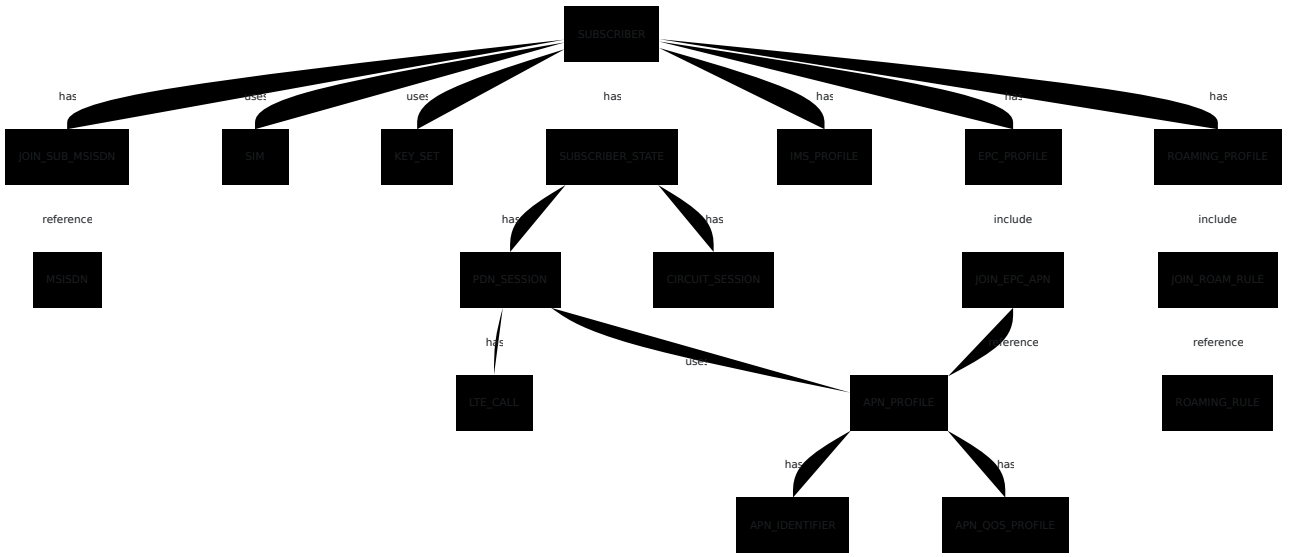
قاعدة بيانات الخلفية

يستخدم OmniHSS **PostgreSQL** كقاعدة بيانات خلفية و **Ecto** كطبقة تجريد قاعدة البيانات. تستخدم جميع الجداول مفاتيح UUID الأساسية للتعريف الفريد عالميًا عبر المواقع.

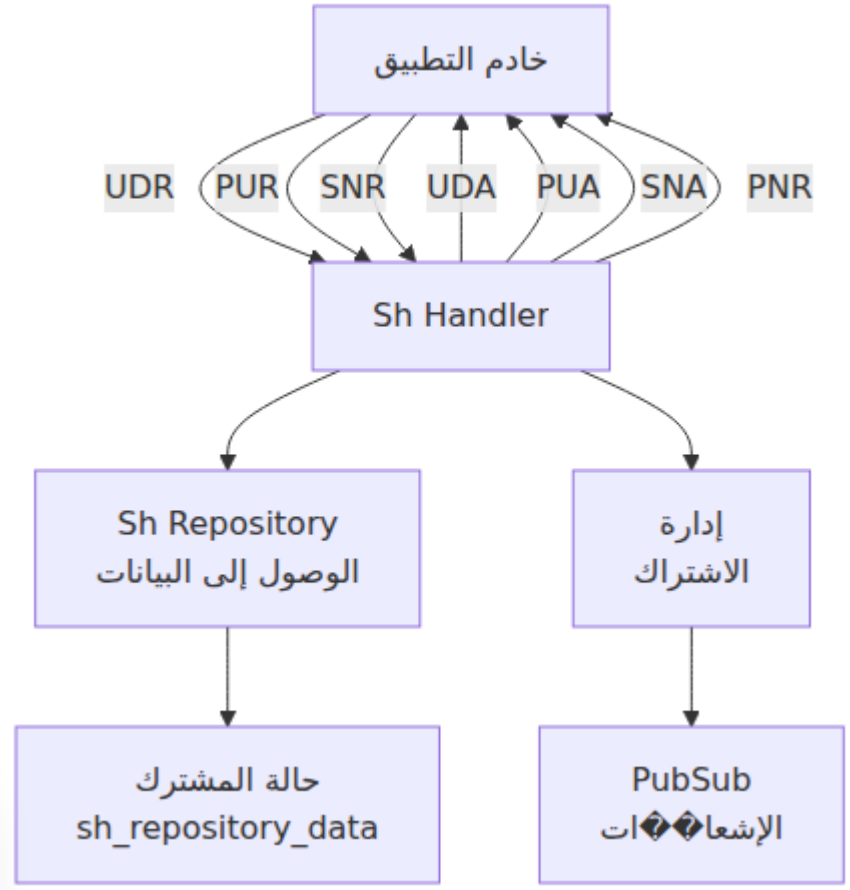
النسخ المت��اثل المنط��ي ثنائي الاتجاه لـ OmniHSS للنشر عبر مواقع متعددة، يستخدم PostgreSQL. تعمل كل موقع كقاعدة بيانات رئيسية مستقلة للقراءة/الكتابة مع نسخ متماثل غير متزامن يعتمد على WAL بين المواقع.

انظر نسخ قاعدة البيانات لتكوين النسخ المتماثل عبر المواقع والعمليات.

نظرة عامة على مخطط قاعدة البيانات

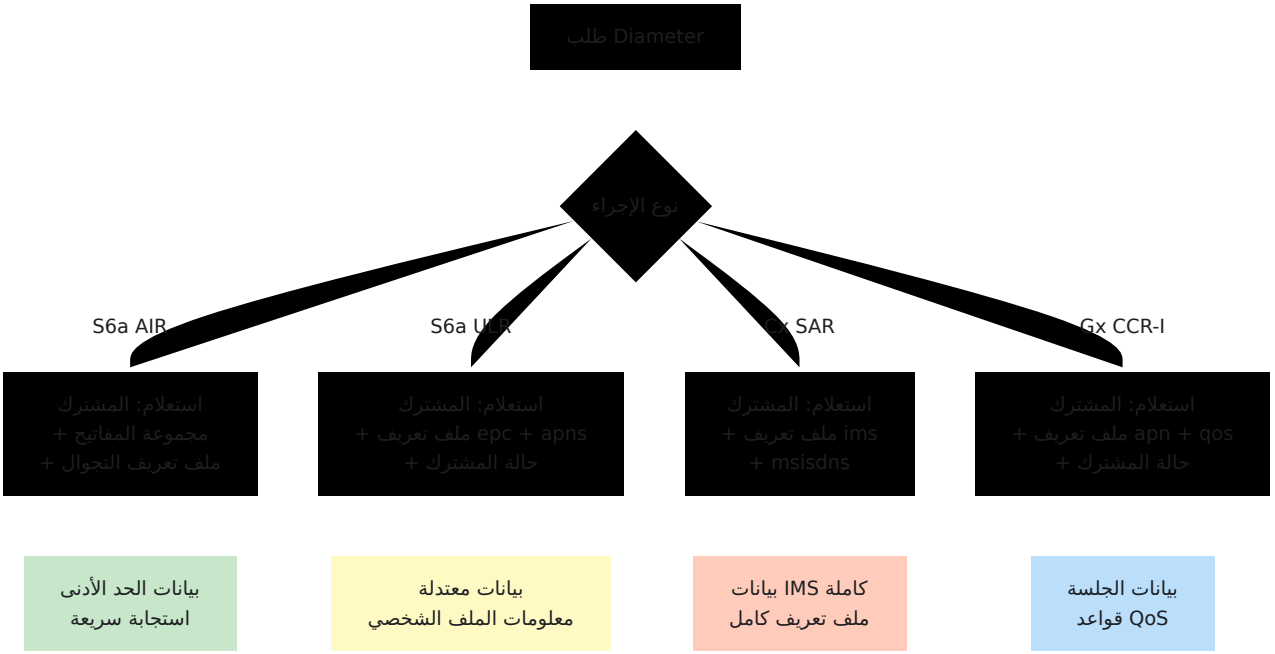


نمط مستودع Ecto



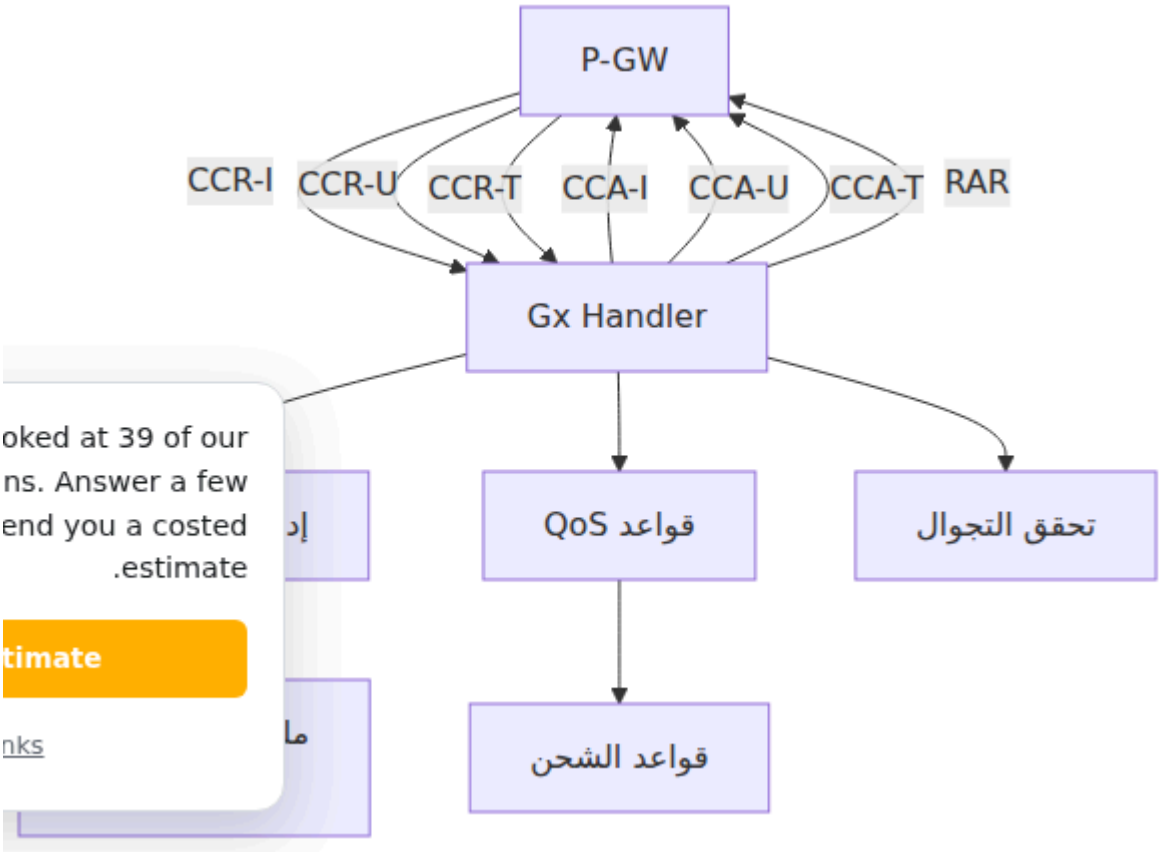
استراتيجية الاستعلام المحسّنة

استعلامات محسّنة تقوم بتحميل فقط الجمعيات الضرورية Diameter تستخدم كل إجراء:

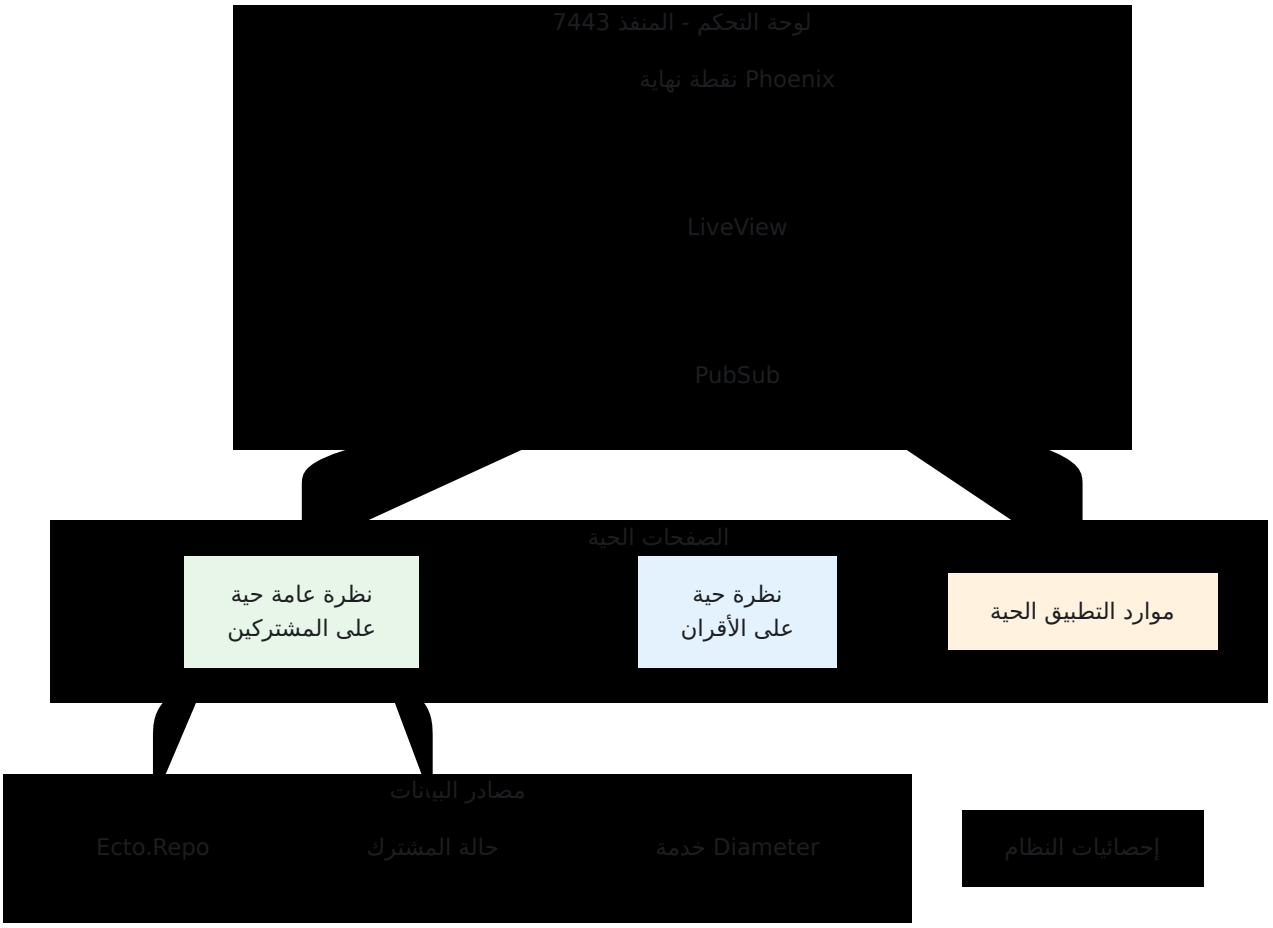


الواجهات الخارجية

معمارية API

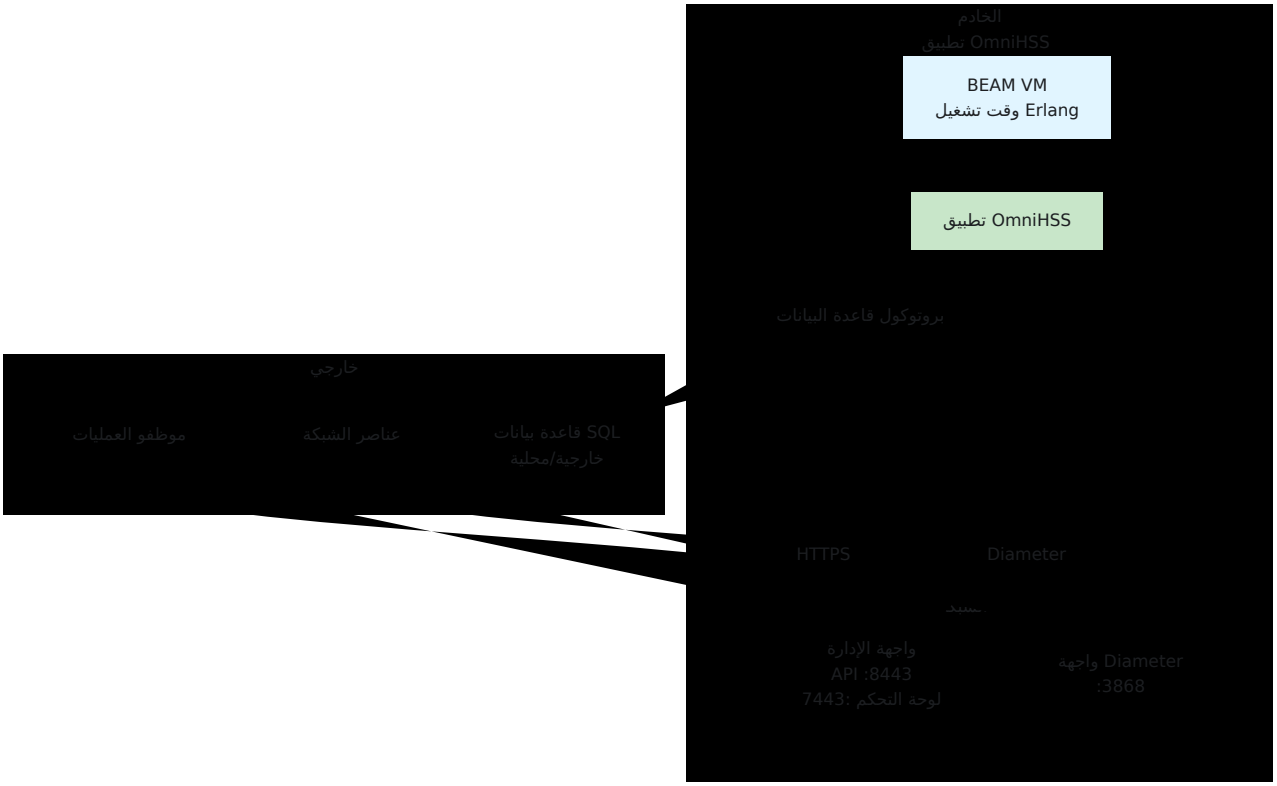


معمارية لوحة التحكم



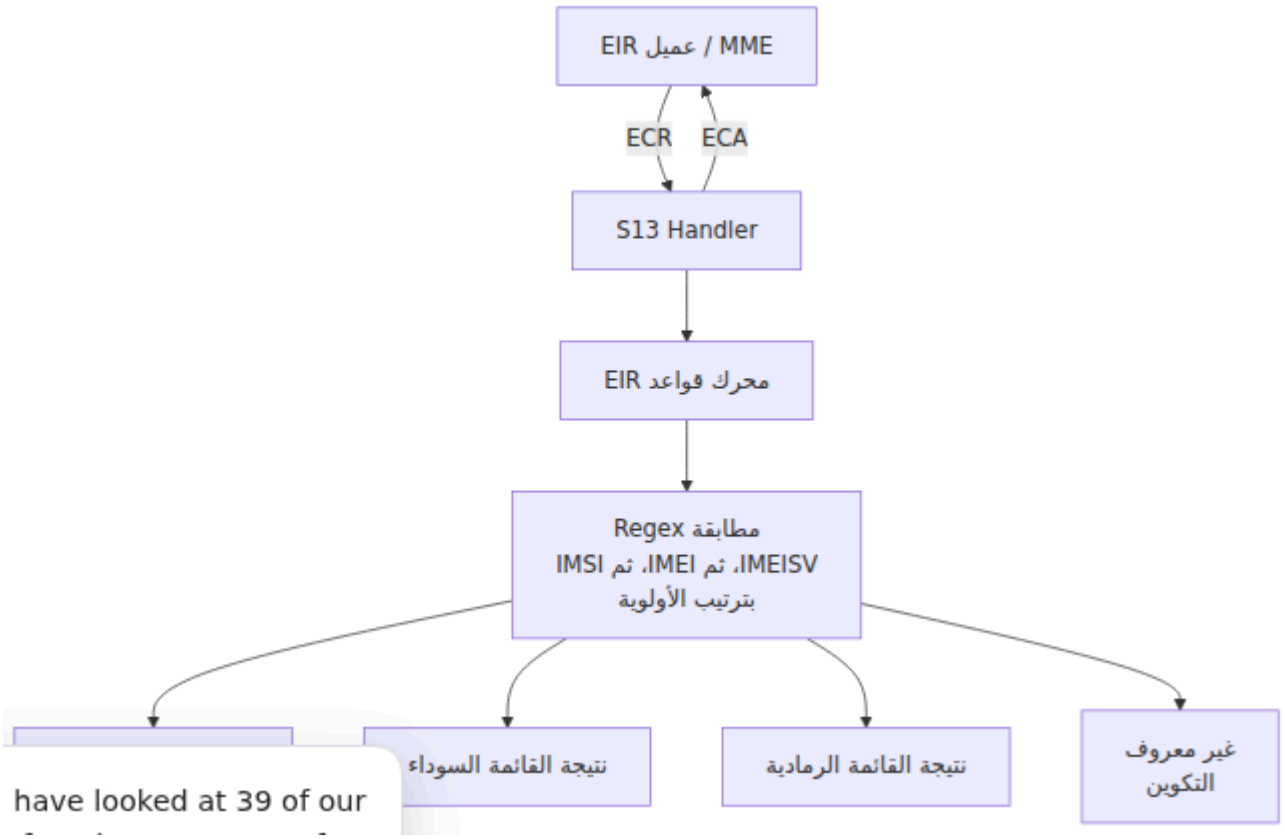
معمارية النشر

نشر عقدة واحدة



نشر HA (نسخ منطقي) عبر مواقع متعددة

النسخ المتماثل المنطقي ثنائي OmniHSS للنشر عالي التوفر عبر المواقع الجغرافية، يستخدم الاتجاه لـ PostgreSQL. تحتوي كل موقع على قاعدة بيانات مستقلة للقراءة/الكتابة.



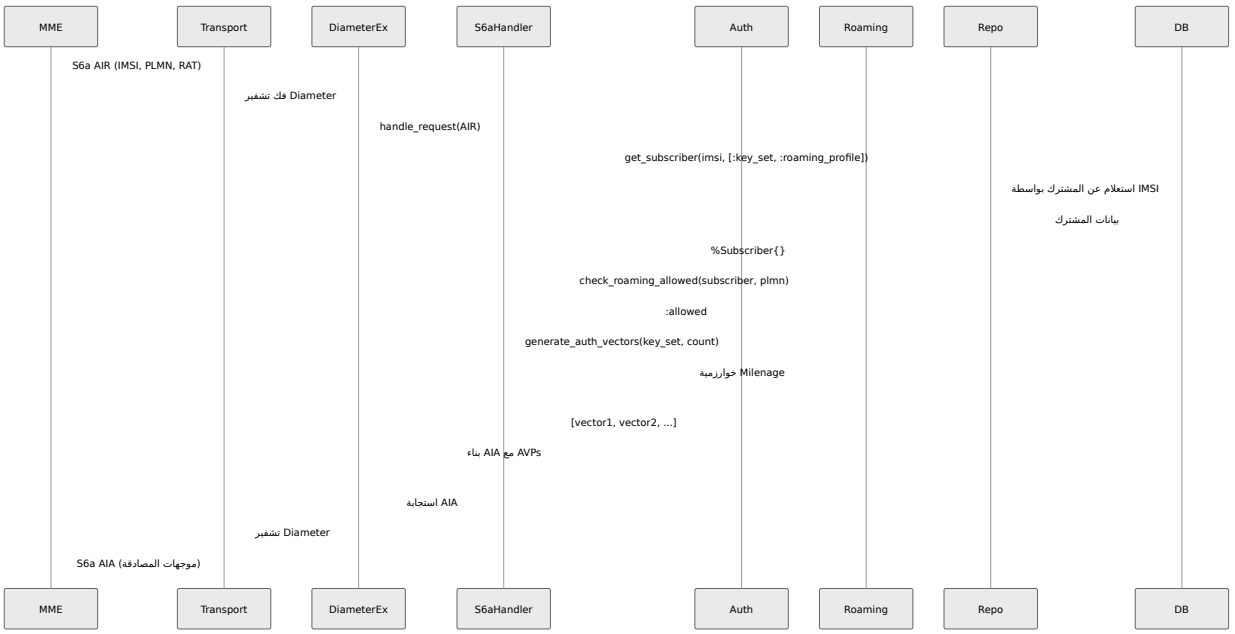
الخصائص الرئيسية:

- **كلا الموقعين قراءة/كتابة**: الكتابات المحلية فورية، ولا يتم حظرها بواسطة الموقع البعيد
- **نسخ غير متزامن**: تتدفق التغييرات عبر WAL. النسخ المتماثل لا يضيف أي عقوبة تأخير للكتابة
- **تحمل التقسيم**: يستمر كلا الموقعين في العمل إذا تعطل الرابط بين المواقع. يتم تخزين WAL محليًا ويتابع عند الاستعادة
- **لا حاجة إلى نصاب**: لا يوجد حد أدنى مطلوب لعدد العقد. يعمل بنفس الطريقة مع موقع واحد أو عدة مواقع
- **مفاتيح UUID الأساسية**: معرفات فريدة عالميًا تقضي على النزاعات بين المواقع

انظر نسخ قاعدة البيانات للحصول على تفاصيل التكوين والعمليات.

مثال على تدفق العملية: المصادقة

يوضح هذا المثال التدفق الكامل لطلب المصادقة:



المبادئ المعمارية الرئيسية

1. تحمل الأخطاء

- تشغيل العمليات الفاشلة تلقائيًا Erlang/OTP تعيد أشجار إشراف
- المعزولة الفشل المتسلسل Diameter تمنع معالجات
- تجمع اتصالات قاعدة ��لبيانات مع إعادة الاتصال التلقائي

2. التزامن

- في عمليته الخاصة Diameter يتم التعامل مع كل طلب
- لا يوجد حالة مشتركة بين معالجات الطلبات
- تجمع اتصالات قاعدة البيانات لاستعلامات متوازية

3. الوحدوية

- في وحدة منفصلة Diameter كل تطبيق
- فصل واضح بين الواجهة ومنطق الأعمال وطبقات البيانات
- خوارزميات مصادقة قابلة للتوصيل

4. الأداء

- استعلامات قاعدة بيانات محسّنة مع تحميل انتقائي
- نقل بيانات الحد الأدنى لكل نوع إجراء
- تجمع اتصالات وإبقاء الاتصال

5. القابلية للملاحظة

- مراقبة في الوقت الحقيقي عبر لوحة التحكم
- تسجيل منظم في جميع أنحاء التطبيق
- تتبع حالة نظير Diameter
- تتبع حالة المشترك مع الطوابع الزمنية

← التالي: التكوين | العودة إلى دليل العمليات →

دليل تكوين OmniHSS

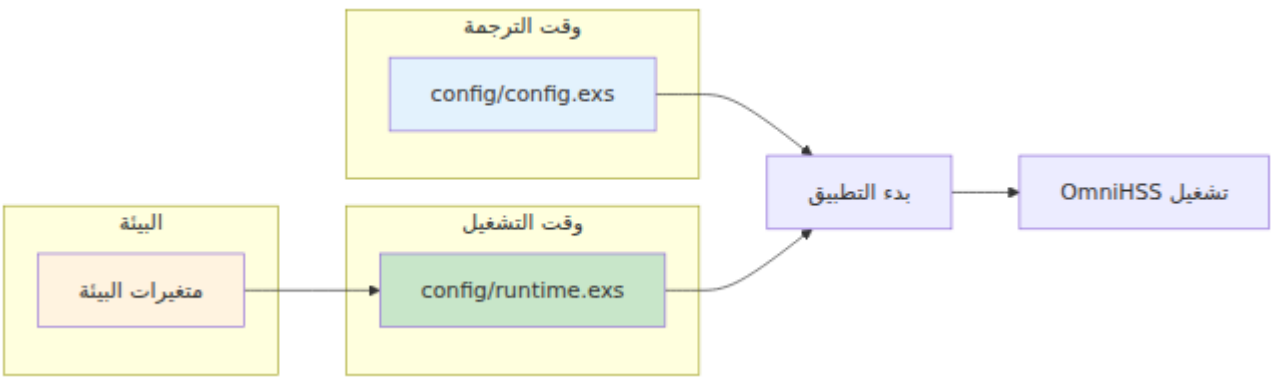
← العودة إلى دليل العمليات

جدول المحتويات

- نظرة عامة على ملف التكوين
- تكوين عميل الترخيص
- تكوين وقت التشغيل
- تكوين قاعدة البيانات
- تكوين Diameter
- تكوين الشبكة
  - تكوين PLMN المنزلي
  - تكوين نواة HSS
- تكوين IMS
- تكوين EIR
- تكوين واجهة برمجة التطبيقات ولوحة التحكم
- سير عمل التكوين

نظرة عامة على ملف التكوين

يستخدم OmniHSS ملفين رئيسيين للتكوين:



config/config.exs (وقت الترجمة)

يحتوي على تكوين ثابت لا يتغير بين البيئات:

- تكوين صفحة لوحة التحكم
- تكوين نقطة نهاية واجهة برمجة التطبيقات
- إعدادات القياس

config/runtime.exs (وقت التشغيل)

يحتوي على تكوين محدد للبيئة يتغير حسب النشر:

- معلمات اتصال قاعدة البيانات
- تكوين نظير Diameter
- إعدادات PLMN المنزلي
- اختيار S-CSCF IMS
- ربط واجهات الشبكة

تكوين عميل الترخيص

يحقق عميل الترخيص من ترخيص HSS مع خادم ترخيص بعيد:

```
# config/runtime.exs

config :license_client,
  # نقاط نهاية واجهة برمجة التطبيقات لخادم الترخيص (قائمة للتبديل)
  license_server_api_urls:
["https://license.example.com:8443/api"],

  # اسم المنظمة المرخصة
  licensee: "اسم من��متك",

  # معرف المنتج
  product_name: "omnihss"
```

معلمات تكوين الترخيص:

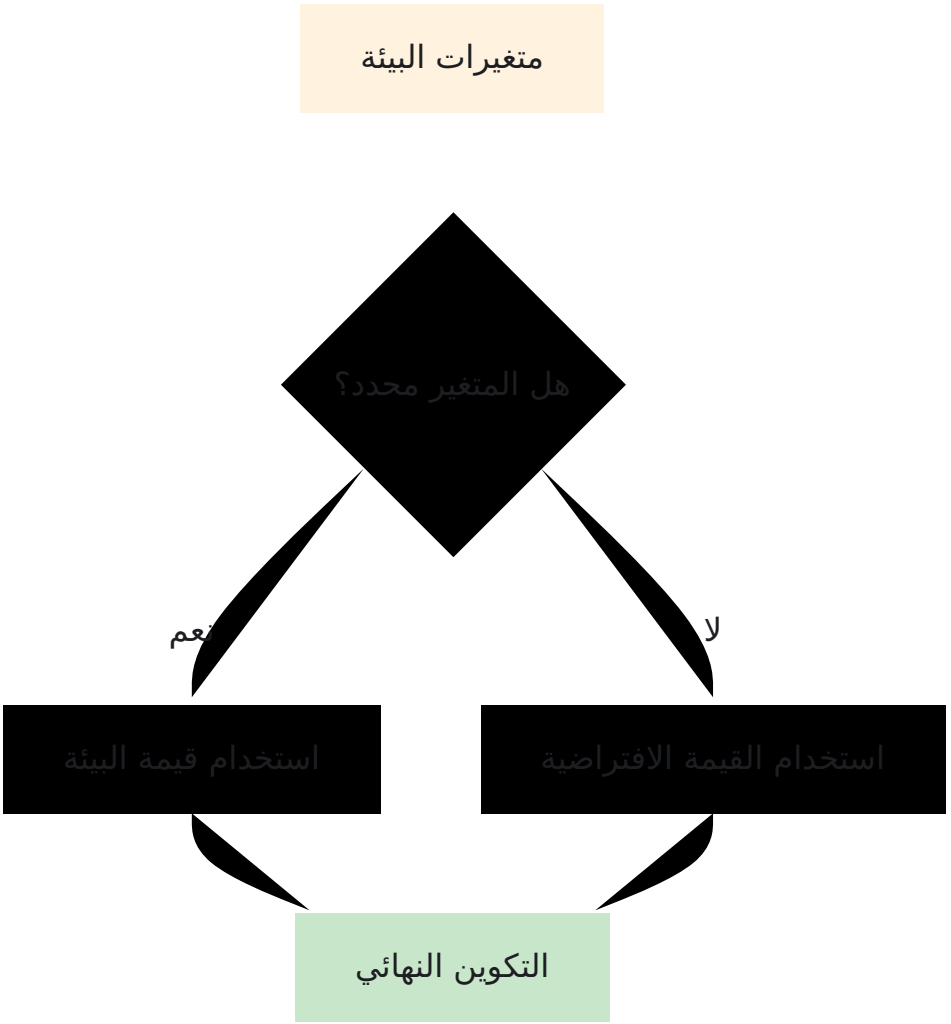
المعلمة	الوصف	مطلوب	مثال
`license_server_api_urls`	قائمة بعناوين URL لخوادم الترخيص	نعم	`["https://10.0.0.1:8443/`
`licensee`	اسم المنظمة على الترخيص	نعم	`"ACME Telecom"`
`product_name`	معرف المنتج للترخيص	نعم	`"omnihss"`

ملاحظات مهمة:

- يجب أن يكون خادم الترخيص قابلاً للوصول من HSS
- استخدم HTTPS للتحقق الآمن من الترخيص
- توفر عناوين URL المتعددة القدرة على التبديل
- يحدث التحقق من الترخيص عند بدء التشغيل وبشكل دوري

تكوين وقت التشغيل

أولوية التكوين



نمط متغير البيئة

هذا النمط للتكوين OmniHSS يتبع:

- أسماء متغيرات البيئة تكون بأحرف كبيرة مع شرطات سفلية
- يتم توفير القيم الافتراضية في runtime.exs
- يجب استخدام بيانات اعتماد قاعدة البيانات في متغيرات البيئة في الإنتاج

تكوين قاعدة البيانات

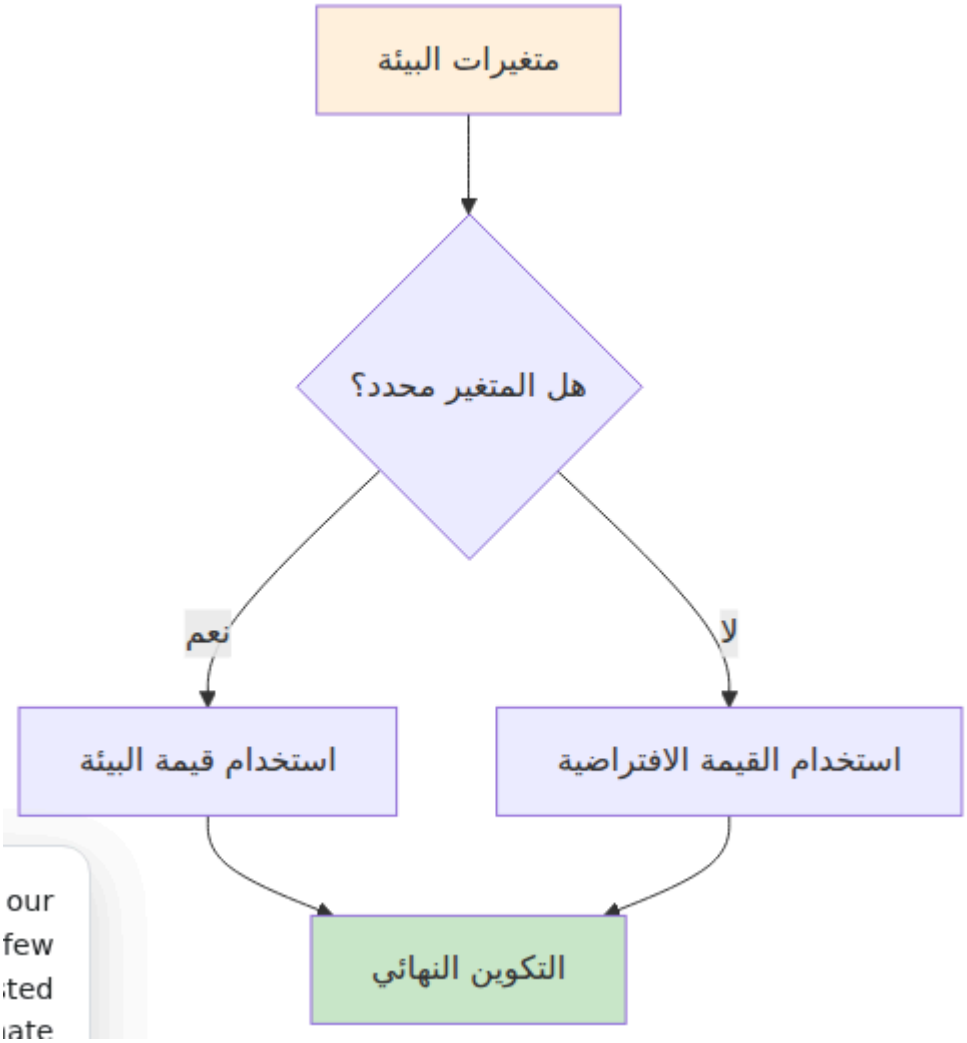
تكوين قاعدة البيانات الأساسي

```
# config/runtime.exs

config :hss, Hss.Repo,
  # معلمات اتصال قاعدة البيانات
  username: System.get_env("DATABASE_USERNAME", "root"),
  password: System.get_env("DATABASE_PASSWORD", "password"),
  hostname: System.get_env("DATABASE_HOSTNAME", "localhost"),
  database: System.get_env("DATABASE_NAME", "omnihss"),

  # إعدادات تجمع الاتصال
  pool_size:
String.to_integer(System.get_env("DATABASE_POOL_SIZE", "20")),

  # مهلات (بالملي ثانية)
  timeout: 15_000,
  connect_timeout: 15_000,

  # خيارات إضافية
  show_sensitive_data_on_connection_error: false
```

معلمات تكوين قاعدة البيانات

المعلمة	الوصف	القيمة الافتراضية	التوصية
`username`	اسم مستخدم قاعدة بيانات SQL	`"root"`	استخدم مستخدم مخصص في الإنتاج
`password`	كلمة مرور قاعدة بيانات SQL	`"password"`	استخدم كلمة مرور قوية، خزّن في متغير بيئة
`hostname`	اسم مضيف خادم قاعدة بيانات SQL	`"localhost"`	استخدم IP أو FQDN في الإنتاج
`database`	اسم قاعدة البيانات	`"omnihss"`	احتفظ بالقيمة الافتراضية ما لم يكن هناك عدة مثيلات
`pool_size`	حجم تجمع الاتصال	`20`	اضبط حسب الحمل (10-50 نموذجي)

ضبط حجم التجمع



إرشادات:

- ابدأ بـ 20 اتصال
- راقب أخطاء "مهلة تجمع الاتصال"
- زد بمقدار 10 إذا حدثت مهلات تحت الحمل ��لطبيعي
- يستخدم كل اتصال حوالي 4 ميغابايت من الذاكرة
- يمكن أن تؤدي الاتصالات الزائدة إلى تدهور أداء قاعدة بيانات SQL

مثال: تكوين قاعدة البيانات للإنتاج

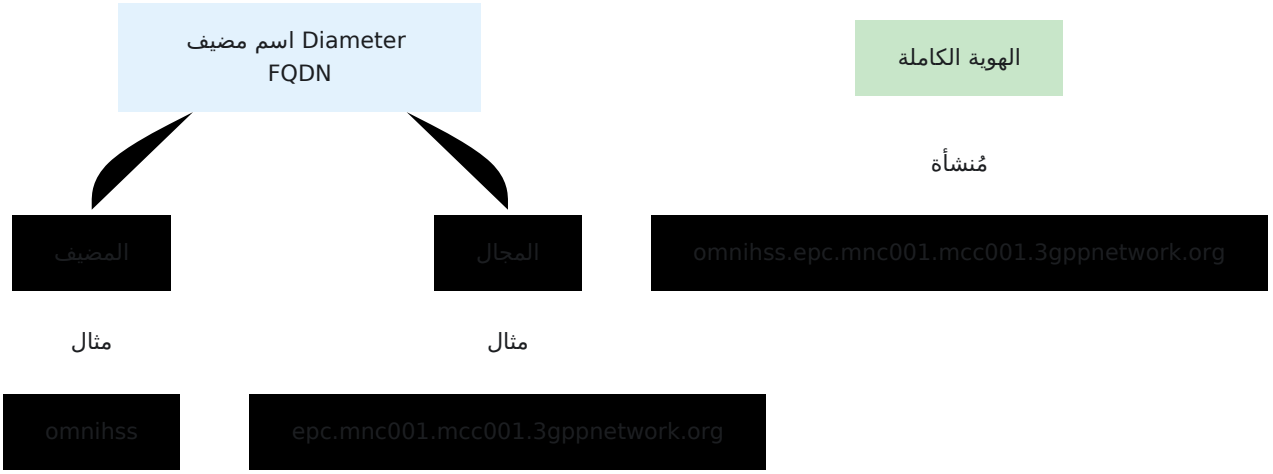
```
# config/runtime.exs - مثال الإنتاج

config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),      # مطلوب
في الإنتاج
  password: System.fetch_env!("DATABASE_PASSWORD"),      # مطلوب
في الإنتاج
  hostname: System.get_env("DATABASE_HOSTNAME",
"db.internal.example.com"),
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT",
"5432")),
  pool_size:
String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/postgres-ca.pem",
    verify: :verify_peer
  ]
```

تكوين Diameter

تكوين خدمة Diameter

```
# config/runtime.exs

diameter_config = %{
  service_name: :omnitouch_hss,

  # ربط الشبكة
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port:
String.to_integer(System.get_env("DIAMETER_LISTEN_PORT", "3868")),

  # هوية Diameter
  host: System.get_env("DIAMETER_HOST", "omnihss"),
  realm: System.get_env("DIAMETER_REALM",
"epc.mnc001.mcc001.3gppnetwork.org"),

  # تحديد المنتج
  product_name: "OmniHSS",
  vendor_id: 10415,  # 3GPP
  supported_vendor_ids: [5535, 10415],

  # إعدادات البروتوكول
  request_timeout: 5000,

  # تكوين النظير
  peers: [
    # أضف تكوينات النظير هنا
  ]
}

config :hss, :diameter, diameter_config
```

تكوين هوية Diameter



إرشادات:

- **المضيف:** اسم المضيف القصير لـ HSS (مثل "omnihss"، "hss01")
- **المجال:** مجال Diameter الذي يتطابق مع PLMN الخاص بك (مثل "epc.mnc001.mcc001.3gppnetwork.org")
- **الهوية الكاملة:** تُنشأ كـ `{host}.{realm}`

إضافة نظائر Diameter

تكوين نظير ثابت (وضع الاتصال)

```
# config/runtime.exs

peers: [
  # مثال نظير MME
  %{
    host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.100",
    port: 3868,
    transport: :sctp,  # أو :tcp
    applications: [:s6a]
  },

  # مثال نظير P-GW
  %{
    host: "pgw01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.101",
    port: 3868,
    transport: :sctp,
    applications: [:gx]
  },

  # مثال نظير I-CSCF
  %{
    host: "icscf01.ims.mnc001.mcc001.3gppnetwork.org",
    realm: "ims.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.102",
    port: 3868,
    transport: :tcp,
    applications: [:cx]
  }
]
```

وضع الاستماع فقط

لبيئات حيث يقوم النظير ببدء الاتصالات إلى HSS:

```
# config/runtime.exs

diameter_config = %{
  # ... تكوين آخر ...
  peers: []  # فارغ - قبول الاتصالات الواردة فقط
}
```

أوضاع اتصال نظير Diameter



اختيار بروتوكول النقل

التوصية	العيوب	المزايا	النقل
مفضل لـ Diameter	يتطلب دعم النواة، تكوين جدار الحماية	تعدد التدفقات، اكتشاف أفضل للأخطاء	**SCTP**
استخدم إذا لم يكن SCTP متاحًا	تدفق واحد، اكتشاف أبطأ للأخطاء	دعم عالمي، قواعد جدار حماية أبسط	**TCP**

تكوين الشبكة

تكوين PLMN المنزلي

يحدد PLMN مشغل الشبكة الخاص بك المنزلي:

```
# config/runtime.exs

config :hss, :home_plmn, %{
  mcc: System.get_env("HOME_PLMN_MCC", "001"),  # رمز الدولة
المحمول
  mnc: System.get_env("HOME_PLMN_MNC", "001")   # رمز الشبكة
المحمولة
}
```

تكوين نواة HSS

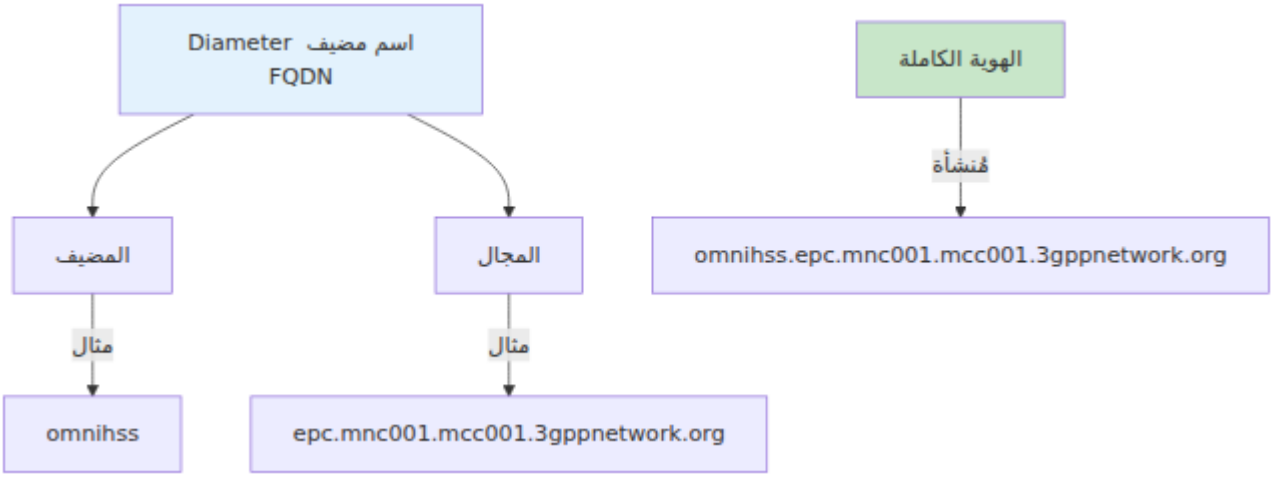
تتحكم هذه الإعدادات في سلوك HSS وميزاته:

```
# config/runtime.exs

config :hss,
  # مستودعات Ecto لعمليات قاعدة البيانات
  ecto_repos: [Hss.Repo],

  # CLR (طلب إلغاء الموقع) عند تغيير MME
  send_clr_on_mme_change: true,

  # إيقاف خدمة Diameter أثناء انقطاع قاعدة البيانات
  stop_diameter_on_database_failure: true,

  # تكوين تطبيق الترخيص
  license_enforced: true,
  license_module: LicenseClient
```

معلمات نواة HSS:

المعلمة	الوصف	القيمة الافتراضية	توصية
`ecto_repos`	قائمة بمستودعات Ecto المستخدمة من قبل التطبيق	`[Hss.Repo]`	مطلوب لعمليات قاعدة البيانات
`send_clr_on_mme_change`	إرسال طلب إلغاء الموقع عند تغيير MME للمشترك	`true`	احتفظ به مفعلًا لضمان التنقل الصحيح
`stop_diameter_on_database_failure`	تعطيل خدمة Diameter إذا أصبحت قاعدة البيانات غير متاحة	`true`	فعّل للحفاظ على اتساق البيانات
`license_enforced`	تفعيل تطبيق الترخيص	`true`	مطلوب للإنتاج
`license_module`	الوحدة التي تتعامل مع فحوصات الترخيص	`LicenseClient`	لا تغير

تنسيق رمز PLMN



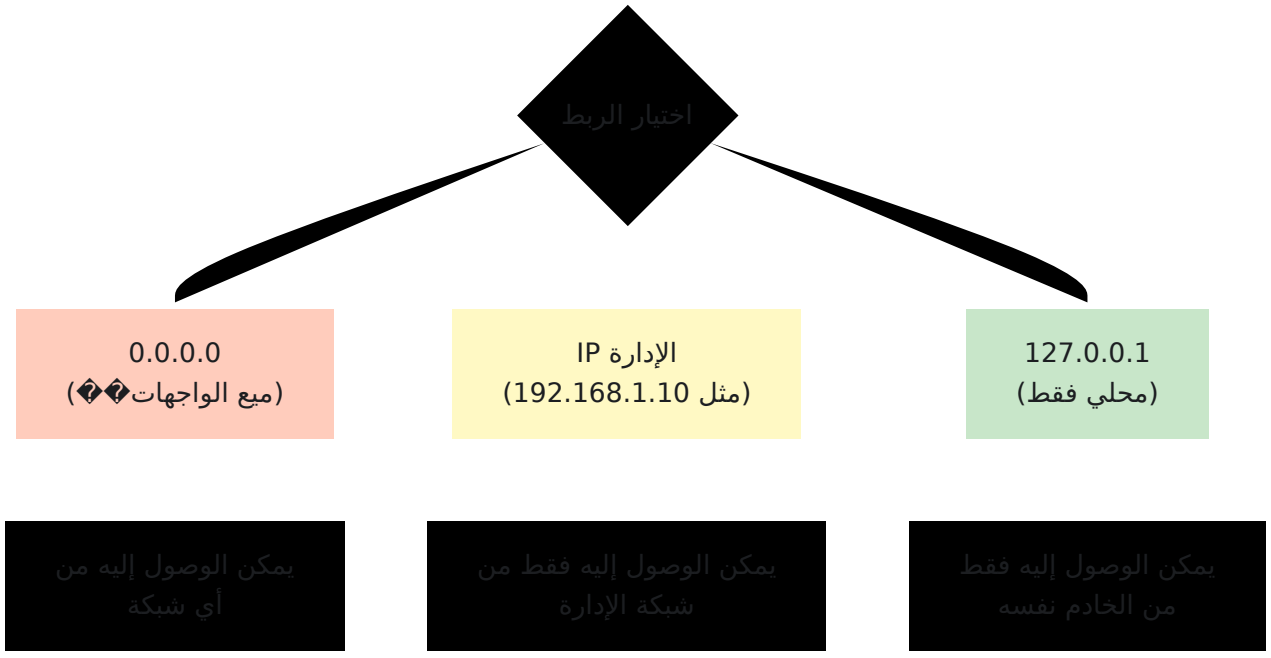
أمثلة:

- AT&T (الولايات المتحدة): MCC=310, MNC=410
- Verizon (الولايات المتحدة): MCC=311, MNC=480
- Vodafone (المملكة المتحدة): MCC=234, MNC=15
- شبكة اختبار: MCC=001, MNC=01

ربط واجهة الشبكة

```
# config/runtime.exs

# واجهة Diameter
listen_ip: System.get_env("DIAMETER_LISTEN_IP", "0.0.0.0"),  # جميع الواجهات
# أو واجهة محددة:
# listen_ip: "10.7.25.186",

# واجهة API
config :hss, HssWeb.Api.Endpoint,
  http: [
    ip: {0, 0, 0, 0},  # جميع الواجهات
    port: 8443
  ]

# واجهة لوحة التحكم
config :hss, HssWeb.ControlPanel.Endpoint,
  http: [
    ip: {0, 0, 0, 0},  # جميع الواجهات
    port: 7443
  ]
```

خيارات ربط الواجهة:



تكوين IMS

تكوين اختيار S-CSCF

يختار HSS S-CSCF فقط في أول تسجيل، عندما لا يكون هناك S-CSCF مسجل للمشترك. بعد ذلك، يعيد HSS الاسم المخزن ولا يعيد الاختيار. هذا يحافظ على نفس S-CSCF، بحيث تتقارب الدورة IMS-AKA على كل تسجيل في دورة تحدي (تخزين اسم S-CSCF انظر حالة تعيين).

الاسم المخزن هو دائمًا عقدة S-CSCF حقيقية. يتعلم HSS ذلك من SAR، لأن SAR هو أول رسالة SAR نهائي تعيد تلك العقدة. LIR وكل UAR بالعقدة التي أخذت التسجيل. كل إعادة تسجيل تخبر HSS يخزن اشتراك IMS المشترك عقدة واحدة من هذا القبيل لجميع أعضائ��. انظر S-CSCF واحد لكل اشتراك.

```
# config/runtime.exs

config :hss, :ims, %{
  scscf: %{
    # طريقة اختيار أول تسجيل: :pool_uri أو :random_peer
    selection_method: :pool_uri,

    # اسم مجموعة S-CSCF المنطقية لـ :pool_uri. لا يوجد منفذ، لذا
يقوم I-CSCF بعمل
    # بحث SRV (_sip._tcp/_udp.<name>) يعيد . عبر المجموعة. هذا HSS
    # الاسم في أول تسجيل فقط. لا يخزنه أبدًا كـ S-CSCF خادم.
    pool_uri: "sip:scscf.ims.mnc001.mcc001.3gppnetwork.org",

    # المدة التي يمكن أن تبقى فيها تحديات IMS-AKA معلقة قبل أن
يتوقف HSS عن
    # إعادة S-CSCF المتحدي في UAR.
    auth_pending_ttl_seconds: 30,

    # عقد S-CSCF لـ :random_peer (للنشر S-CSCF أيضًا مخزون)
    peers: [
      %{
        host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060"
      },
      %{
        host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060"
      }
    ]
  }
}
```

المعلمات:

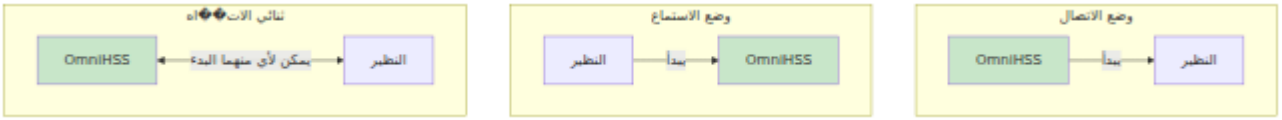
المعلمة	النوع	مطلوب	القيمة الافتراضية	ف
`selection_method`	Atom	نعم	`:pool_uri`	ة اختيار S-CSC ستخدم `:pool` `:rand` ي اختيار S-CSC
`pool_uri`	String	نعم لـ `:pool_uri`	-	جموعة CSCF في أول لا تحدد ذا يقوم CSCF ر SRV مل عبر وعة. لا H يخزن أبدًا كـ CSCF . إذا لم م تعيين `pool_` يسجل ود إلى ندة من `peers`
`auth_pending_ttl_seconds`	Integer	لا	30	ي يحترم فيها HS CSCF عد هذه يتجاهل م HSS

ف	القيمة الافتراضية	مطلوب	النوع	المعلمة
ستخدم مسجل . انظر ة تعيين CSCF.				
ة بعقد CSCF. علمات بر أدناه	-	نعم لـ `:random_peer`	قائمة	`peers`

معلمات النظير:

الوصف	القيمة الافتراضية	مطلوب	النوع	المعلمة
URI SIP لـ S-CSCF، مع FQDN قادرًا I-CSCF والمنفذ. يجب أن يكون على حله.	-	نعم	String	`host`

طرق اختيار S-CSCF



طرق الاختيار:

الطريقة	الوصف	حالة الاستخدام
`:pool_uri`	يعيد `pool_uri` بحله I-CSCF الوحيد. يقوم ويوزع الحمل عبر DNS SRV عبر الحمل ويتخطى DNS المجموعة. يتوزع عقدة ميتة في أول تسجيل.	توزيع الحمل بالإضافة إلى التبديل في أول تسجيل. التوصية الافتراضية.
`:random_peer`	يعيد عقدة واحدة من `peers`، مختارة عبر IMSI تجزئة) بشكل محدد لكل مشترك يرتبط نفس .(قائمة النظائر المرتبة المشترك دائمًا بنفس العق��ة.	ثابت لكل S-CSCF مشترك، بدون اعتماد على سجلات SRV.

الاسم `:random_peer` تاريخي. الاختيار محدد لكل مشترك، وليس عشوائيًا. يتطلب وجود خريطة S-CSCF. ثابتة، بحيث تعيد كل تسجيل في دورة تحدي واحدة نفس

إذا كانت `selection_method` تحتوي على قيمة غير معروفة، يسجل HSS تحذيرًا ويعود إلى سلوك `:random_peer`. دائمًا ما يجيب HSS على UAR.

في كل حالة UAA **ينطبق الاختيار على أول تسجيل فقط.** يوضح الجدول أدناه ما تعيده.

رمز نتيجة UAA	اسم خادم UAA	حالة المشترك
2001 (أول تسجيل)	اختيار جديد: `pool_uri`، أو عقدة من `peers`	لا يوجد مسجل S-CSCF
2002 (تسجيل لاحق)	عقدة S-CSCF المتحدية	نشط IMS-AKA تحدي
2002 (تسجيل لاحق)	عقدة S-CSCF الخادمة	مسجل، أو غير مسجل مع الاحتفاظ بالاسم
2001 أو 2002	عقدة S-CSCF المثبتة للاشتراك	مشترك IMS عضو في اشتراك يخدمه عضو آخر بالفعل

تكوين مجال IMS

عادةً ما يس��خدم IMS مجالًا منفصلًا عن EPC:

```
# مجال EPC
"epc.mnc001.mcc001.3gppnetwork.org"

# مجال IMS
"ims.mnc001.mcc001.3gppnetwork.org"
```

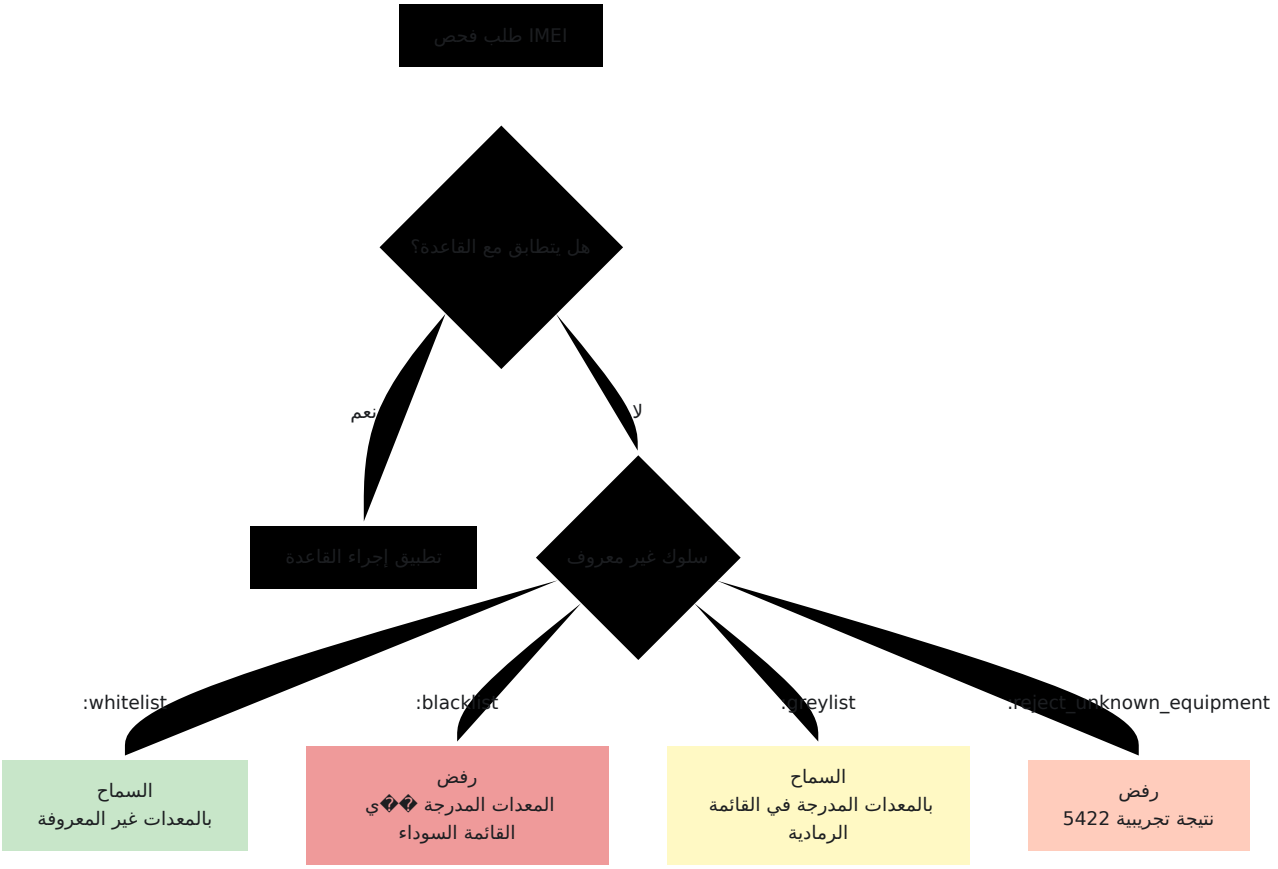
تكوين EIR

انظر وثائق EIR للحصول على تفاصيل كاملة حول فحص هوية المعدات.

إعدادات سجل هوية المعدات

```
# config/runtime.exs

config :hss, :eir, %{
  # السلوك للمعدات غير المعروفة (لا توجد قاعدة مطابقة)
  unknown_equipment_behaviour: :whitelist
  # الخيارات:
  #   :whitelist - السماح بالمعدات غير المعروفة
  #   :blacklist - حظر المعدات غير المعروفة
  #   :greylist - تتبع ولكن السماح بالمعدات غير المعروفة
  #   :reject_unknown_equipment - الرفض مع رمز نتيجة محدد
}
```

سلوك المعدات غير المعروفة



خيارات السلوك:

الخيار	النتيجة	حالة الاستخدام
`:whitelist`	السماح بجميع IMEI غير المعروفة	شبكة مفتوحة، اختبار
`:blacklist`	حظر جميع IMEI غير المعروفة	أمان معتدل
`:greylist`	السماح IMEI غير المعروفة ولكن تتبع	وضع المراقبة
`:reject_unknown_equipment`	الرفض مع رمز محدد	أمان عالي

التوصية: ابدأ بـ `:whitelist` أثناء الاختبار، انتقل إلى `:greylist` لمراقبة الإنتاج، ثم `:blacklist` للأمان الصارم.

تكوين واجهة برمجة التطبيقات ولوحة التحكم

تكوين نقطة نهاية واجهة برمجة التطبيقات

```
# config/config.exs

config :hss, HssWeb.Api.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(json)],
  pubsub_server: Hss.PubSub,

  # تكوين HTTPS
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: "priv/cert/omnitouch.crt",
    keyfile: "priv/cert/omnitouch.pem"
  ]
```

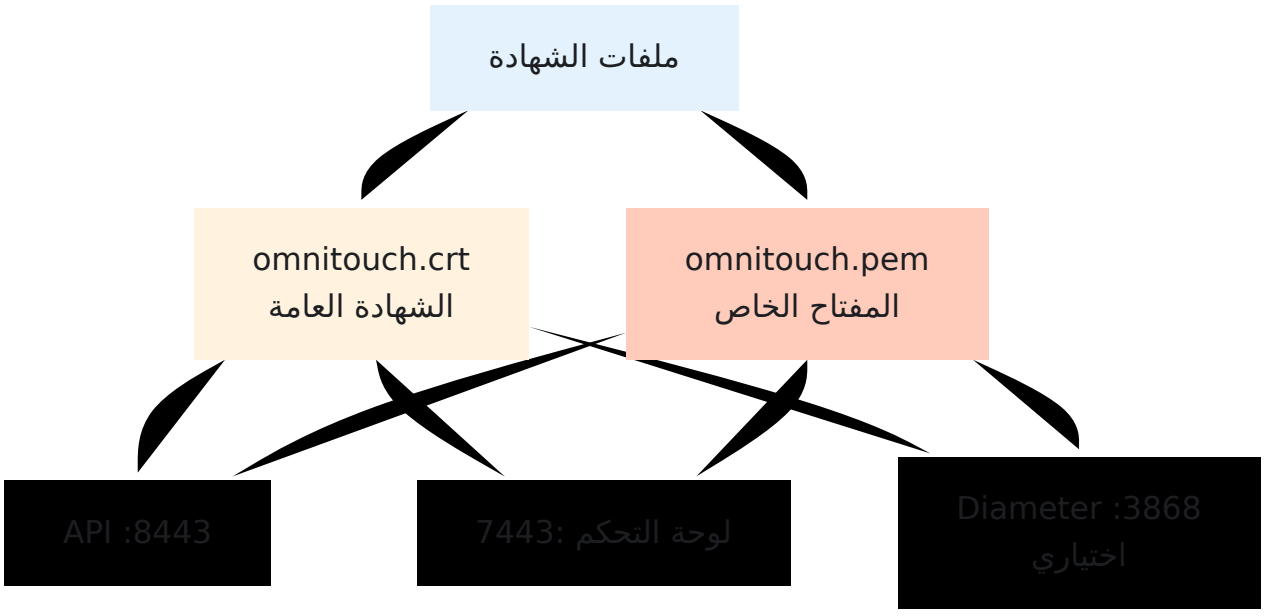
التحكم في الوصول إلى واجهة برمجة التطبيقات

مفاتيح واجهة برمجة التطبيقات في `runtime.exs` تحدد كتلة `config :api_ex, :auth` والأدوار. للحصول على جميع المعلمات، انظر التحكم في الوصول إلى واجهة برمجة التطبيقات (RBAC).

تكوين لوحة التحكم

```
# config/config.exs

config :hss, HssWeb.ControlPanel.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(html json)],
  pubsub_server: Hss.PubSub,
  live_view: [signing_salt: "some-secret"],

  # تكوين HTTPS
  https: [
    port: 7443,
    cipher_suite: :strong,
    certfile: "priv/cert/omnitouch.crt",
    keyfile: "priv/cert/omnitouch.pem"
  ]
```

تكوين شهادة TLS



متطلبات الشهادة:

- شهادة X.509 صالحة
- مفتاح خاص مطابق
- تضمين الشهادات الوسيطة إذا لزم الأمر

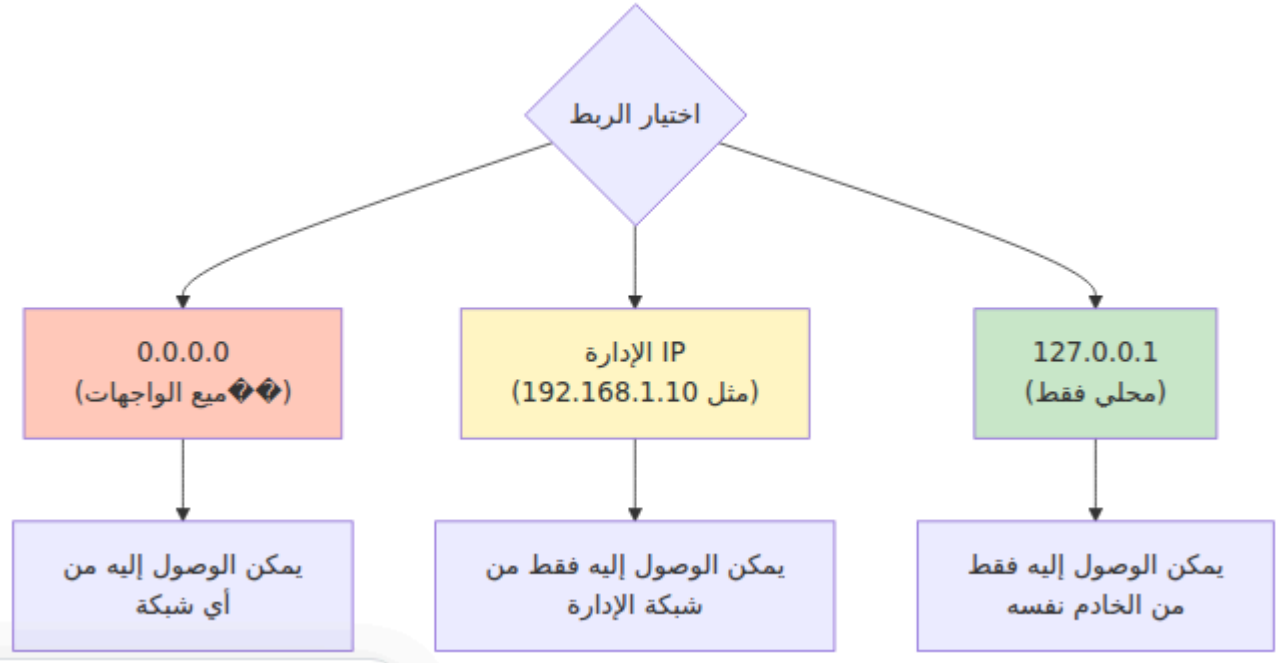
- مع اسم المضيف SAN أو CN يجب أن يتطابق

لإنتاج:

```
https: [
  port: 8443,
  cipher_suite: :strong,
  certfile: System.get_env("TLS_CERT_FILE",
"/etc/ssl/certs/omnihss.crt"),
  keyfile: System.get_env("TLS_KEY_FILE",
"/etc/ssl/private/omnihss.key"),
  cacertfile: System.get_env("TLS_CA_FILE", "/etc/ssl/certs/ca-
bundle.crt")
]
```

سير عمل التكوين

تكوين نشر أولي



قائمة التحقق من التكوين

التكوين الأساسي

- [ ] اتصال قاعدة البيانات (اسم المضيف، بيانات الاعتماد)
- [ ] PLMN المنزلية (MCC، MNC)
- [ ] مضيف Diameter والمجال
- [ ] عنوان IP ورقم المنفذ للاستماع Diameter
- [ ] شهادات TLS لـ API ولوحة التحكم
- [ ] تكوين عميل الترخيص (عناوين URL للخادم، المرخص له، اسم المنتج)
- [ ] إعدادات نواة HSS (send_clr_on_mme_change، stop_diameter_on_database_failure)

تكامل عنصر الشبكة

- [ ] تم تكوين نظراء Diameter (إذا كنت تستخدم وضع الاتصال)
- [ ] قواعد جدار الحماية تسمح بحركة مرور Diameter (المنفذ 3868)
- [ ] قواعد جدار ا��حماية تسمح بحركة مرور HTTPS (المنافذ 7443، 8443)
- [ ] حل DNS لهويات Diameter

تكوين IMS (إذا كنت تستخدم ميزات IMS)

- [ ] تم تكوين قائمة نظراء S-CSCF
- [ ] تم اختيار طريقة اختيار S-CSCF
- [ ] تم تكوين مجال IMS

التكوين الاختياري

- [ ] تم تكوين سلوك EIR
- [ ] تم ضبط حجم مجموعة قاعدة البيانات
- [ ] تم تقييد ربط واجهة الشبكة

التحقق من التكوين

بعد تعديل التكوين:

1. **تحقق من الصياغة:**

```
تحقق من السجلات بحثًا عن أخطاء تحميل التكوين
```

2. **الوصول إلى لوحة التحكم:**

```
الوصول إلى https://[hostname]:7443
تحقق من تحميل صفحة النظرة العامة
```

3. **الوصول إلى API:**

```
curl -k https://[hostname]:8443/api/status
```

4. **حالة Diameter:**

```
تحقق من صفحة Diameter في لوحة التحكم
تحقق من اتصالات النظراء
```

5. **الاتصال بقاعدة البيانات:**

```
تحق من لوحة التحكم لبيانات المشتركين
أو الاتصال مباشرة بقاعدة بيانات SQL
```

مثال كامل لتكوين وقت التشغيل

```
# config/runtime.exs - مثال كامل للإنتاج

import Config

#
==============================================================================
# تكوين قاعدة البيانات
#
==============================================================================
config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),
  password: System.fetch_env!("DATABASE_PASSWORD"),
  hostname: System.get_env("DATABASE_HOSTNAME", "db.omnihss.internal'
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT", "5432")),
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", '
  timeout: 15_000,
  connect_timeout: 15_000,
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/postgres-ca.pem",
    verify: :verify_peer
  ]

#
==============================================================================
# تكوين عميل الترخيص
#
==============================================================================
config :license_client,
  license_server_api_urls: [System.get_env("LICENSE_SERVER_URL",
"https://license.example.com:8443/api")],
  licensee: System.get_env("LICENSE_ORGANIZATION", "Your Organizatior
  product_name: "omnihss"

#
==============================================================================
# تكوين PLMN ونواة HSS المنزلية
#
==============================================================================
```

```
config :hss,
  ecto_repos: [Hss.Repo],
  home_plmn: %{
    mcc: System.get_env("HOME_PLMN_MCC", "001"),
    mnc: System.get_env("HOME_PLMN_MNC", "001")
  },
  send_clr_on_mme_change: true,
  stop_diameter_on_database_failure: true,
  license_enforced: true,
  license_module: LicenseClient

#
============================================================================
# تکوین Diameter
#
============================================================================
diameter_config = %{
  service_name: :omnitouch_hss,
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port: String.to_integer(System.get_env("DIAMETER_LISTEN_PORT
"3868")),
  host: System.get_env("DIAMETER_HOST", "omnihss01"),
  realm: System.get_env("DIAMETER_REALM",
"epc.mnc001.mcc001.3gppnetwork.org"),
  product_name: "OmniHSS",
  vendor_id: 10415,
  supported_vendor_ids: [5535, 10415],
  request_timeout: 5000,
  peers: [
    %{
      host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.7.25.100",
      port: 3868,
      transport: :sctp,
      applications: [:s6a]
    }
  ]
}

config :hss, :diameter, diameter_config

#
============================================================================
```

```
# تكوين IMS
#
============================================================================
config :hss, :ims, %{
  scscf: %{
    selection_method: :random_peer,
    peers: [
      %{host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060"},
      %{host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060"}
    ]
  }
}

#
============================================================================
# تكوين EIR
#
============================================================================
config :hss, :eir, %{
  unknown_equipment_behaviour: :whitelist
}

#
============================================================================
# تكوين نقطة نهاية API
#
============================================================================
config :hss, HssWeb.Api.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8443],
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss
    keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss
  ],
  url: [host: System.get_env("API_HOST", "api.omnihss.internal"), por
8443]

#
============================================================================
# تكوين نقطة نهاية لوحة التحكم
#
============================================================================
config :hss, HssWeb.ControlPanel.Endpoint,
```

```
    http: [ip: {0, 0, 0, 0}, port: 7443],
    https: [
      port: 7443,
      cipher_suite: :strong,
      certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss
      keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss
    ],
    url: [host: System.get_env("CP_HOST", "hss.omnihss.internal"), port
```

← التالي: علاقات الكيانات | العودة إلى دليل العمليات →

دليل لوحة التحكم OmniHSS

← العودة إلى دليل العمليات

جدول المحتويات

- نظرة عامة على لوحة التحكم
- الوصول إلى لوحة التحكم
- صفحة النظرة العامة
- صفحة القطر
- صفحة التطبيق
- صفحة التكوين
- التنقل والواجهة

نظرة عامة على لوحة التحكم

تعد لوحة التحكم OmniHSS واجهة مراقبة قائمة على الويب توفر رؤية في الوقت الفعلي لحالة النظام، ونشاط المشتركين، والاتصال بالقطر. تم بناؤها باستخدام Phoenix LiveView، وتقوم بالتحديث تلقائيًا دون الحاج�� إلى تحديث الصفحة.

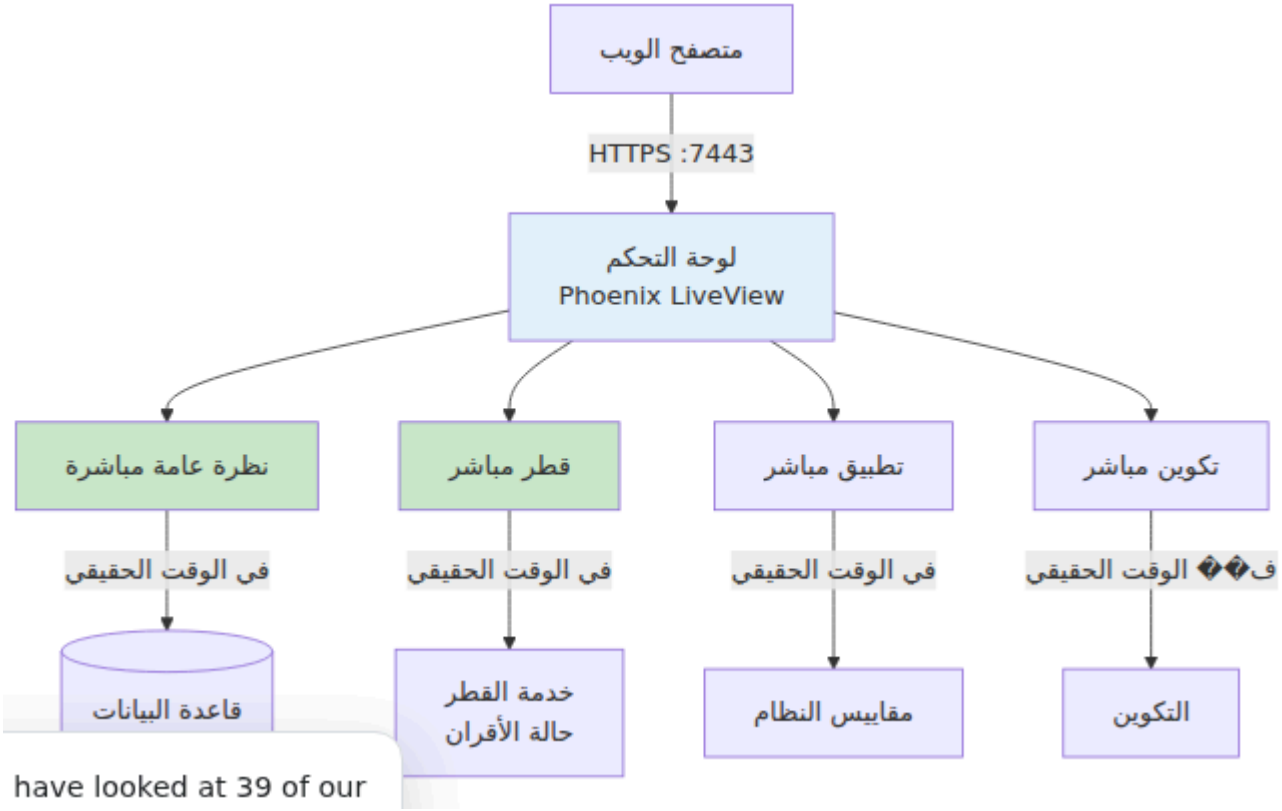
الميزات الرئيسية

- **تحديثات في الوقت الحقيقي** - يتم التحديث التلقائي كل ثانية
- **مراقبة المشتركين** - عرض المشتركين النشطين وحالتهم الحالية
- **حالة القطر** - مراقبة اتصالات الأقران في الوقت الحقيقي
- **موارد النظام** - تتبع أداء التطبيق
- **عارض التكوين** - فحص تكوين وقت التشغيل

معلومات الوصول

```
URL: https://[hostname]:7443
Protocol: HTTPS Only
Port: 7443 (configurable)
Certificate: Configured in config/config.exs
```

هيكل لوحة التحكم



الوصول إلى لوحة التحكم

الوصول الأولي

1. افتح متصفح الويب
2. انتقل إلى `https://[hostname]:7443`
3. قبول شهادة TLS (إذا كانت موقعة ذاتيًا)
4. سيتم تقديمك بصفحة النظرة العامة بشكل افتراضي

تحذيرات شهادة TLS

إذا كنت تستخدم شهادات موقعة ذاتيًا، ستظهر المتصفحات تحذيرات أمان. هذا متوقع في النشر الداخلي.

لإنتاج: استخدم الشهادات الموقعة من قبل هيئة إصدار الشهادات الموثوقة.

متطلبات الشبكة

- يجب أن يكون **المنفذ 7443** قابلاً للوصول من شبكة الإدارة الخاصة بك
- **HTTPS** إلزامي - لا يتم دعم HTTP
- يجب أن تسمح **قواعد جدار الحماية** بحركة المرور إلى المنفذ 7443

توافق المتصفح

تستخدم لوحة التحكم تقنيات الويب الحديثة (LiveView، WebSockets):

- Chrome/Chromium (موصى به)
- Firefox
- Safari
- Edge

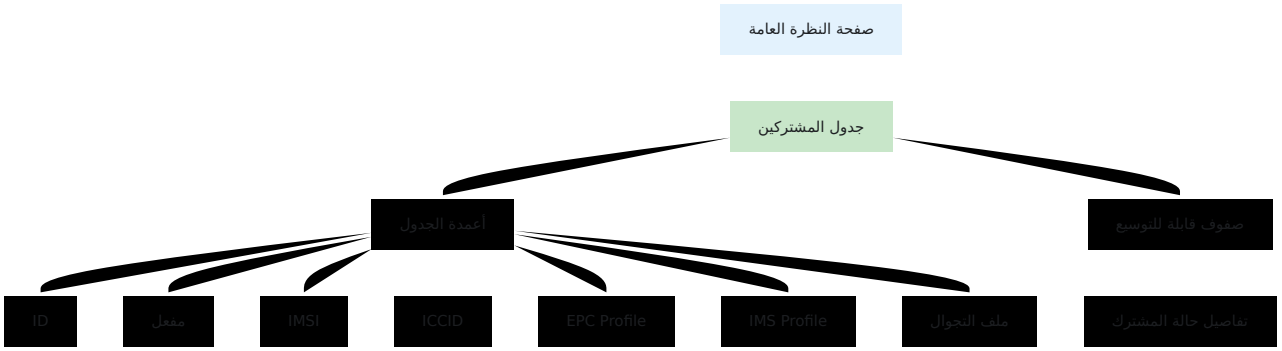
ملاح��ة: Internet Explorer ��ير مدعوم.

صفحة النظرة العامة

URL: `https://[hostname]:7443/overview`

تعرض صفحة النظرة العامة جميع المشتركين ومعلومات حالتهم في الوقت الحقيقي.

تخطيط الصفحة



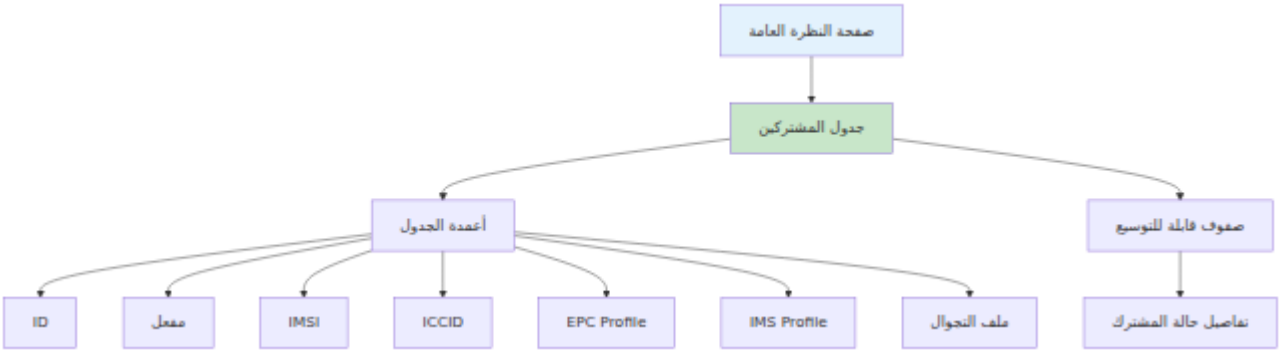
أعمدة الجدول

العمود	الوصف	القيم
ID	معرف قاعدة بيانات المشترك	سلسلة (UUID)
مفعل	حالة الخدمة	✓ (مفعل) / ✗ (معطل)
IMSI	هوية المشترك الدولية المتنقلة	رقم 14-15
ICCID	معرف بطاقة SIM	رقم أو 19-20 "N/A"
ملف EPC	اسم ملف خدمة البيانات	اسم الملف أو المعرف
ملف IMS	اسم ملف خدمة الصوت	اسم الملف، المعرف، أو "N/A"
ملف التجوال	اسم سياسة التجوال	اسم الملف، المعرف، أو "N/A"

تفاصيل الصف القابل للتوسيع

انقر على أي صف للتوسيع وعرض حالة المشترك بالتفصيل:

معلومات الموقع



الحقول:

- **MCC** - رمز الدولة المتنقلة (3 أرقام)
- **MNC** - رمز الشبكة المتنقلة (2-3 أرقام)
- **TAC** - رمز منطقة التتبع
- **معرف الخلية** - معرف الخلية الخدمية
- **معرف eNodeB** - معرف محطة القاعدة
- **ECI** - معرف خلية E-UTRAN

معلومات الشبكة

الحقول:

- MME الخدمي الحالي - **تم رؤيته** **آخر MME** اسم مضيف
- MME **آخر مجال تم رؤيته** - مجال القطر لـ
- **نوع RAT** - تقنية الوصول اللاسلكي (مثل "E-UTRAN" لـ LTE)
- **آخر رؤية في** - الطابع الزمني لآخر رسالة قطر

معلومات IMS

الحقول:

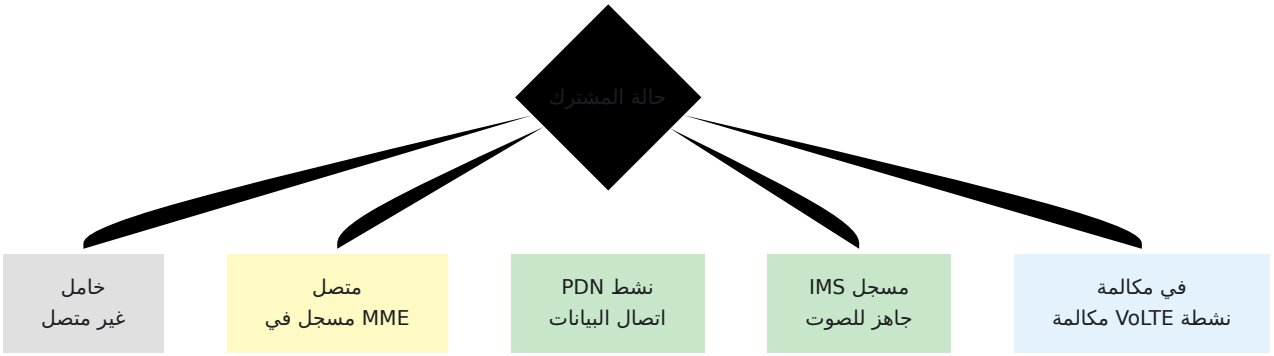
- **S-CSCF المعين** - URI SIP لـ S-CSCF المعين حاليًا
- **الهوية العامة IMS** - URI SIP (مثل sip:+14155551234@ims.example.com)
- HSS اتصل بـ P-CSCF - **تم رؤيته** **آخر P-CSCF** آخر
- HSS اتصل بـ I-CSCF - **تم رؤيته** **آخر I-CSCF** آخر

معلومات الجلسة

الحقول:

- **جلسات PDN** - عدد الاتصالات النشطة للبيانات
- **المكالمات النشطة** VoLTE - عدد المكالمات النشطة

مؤشرات الحالة



كيفية تحديد الحالة:

- **خامل:** لا توجد معلومات موقع، لا يوجد MME
- **متصل:** آخر MME متاحة معلومات الموقع، تم رؤيته موجود
- **نشط:** عدد جلسات PDN > 0 **PDN**
- **مسجل IMS:** S-CSCF المعين موجود
- **في مكالمة:** عدد المكالمات النشطة > 0

التحديث التلقائي

تقوم صفحة النظرة العامة بالتحديث تلقائيًا **كل 1 ثانية** لعرض التحديثات في الوقت الحقيقي.

مؤشرات بصرية:

- تظهر البيانات الجديدة دون إعادة تحميل الصفحة
- يتم تحديث الطوابع الزمنية في الوقت الحقيقي
- لا حاجة للتحديث اليدوي

حالات الاستخدام

1. **مراقبة المشتركين النشطين**
    - رؤية أي المشتركين متصلين حاليًا
    - التحقق من الشبكة الخدمية الحالية (للتجوال)

- التحقق من حالة تسجيل IMS

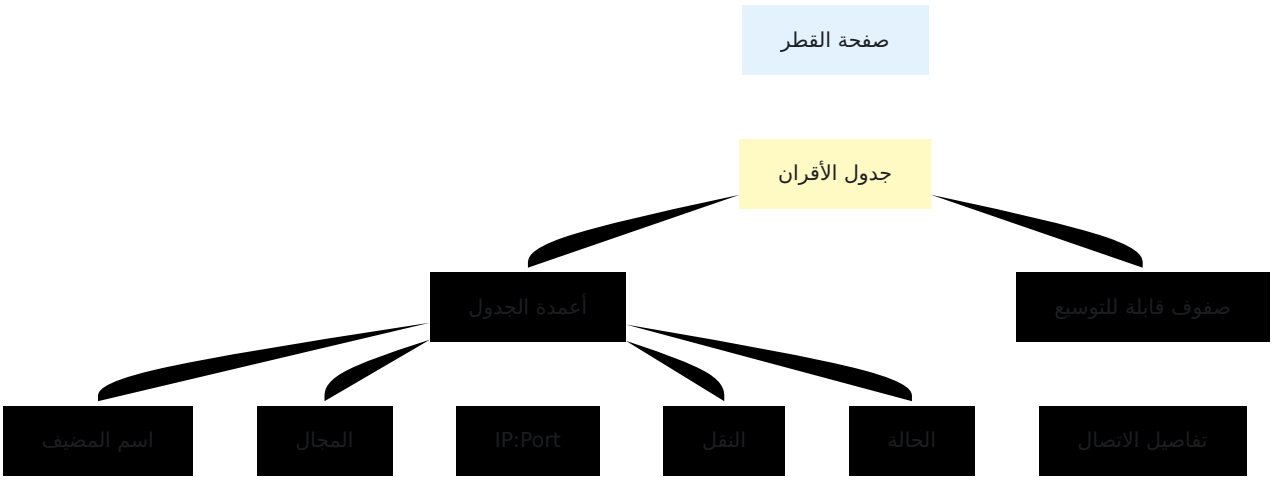
2. **استكشاف الأخطاء**
   - التحقق مما إذا كان المشترك مفعلًا
   - التحقق من الطابع الزمني الأخير (هل المشترك يستجيب؟)
   - تأكيد تعيينات الملفات
   - عرض معلومات الموقع الحالية
3. **مراقبة السعة**
   - عد إجمالي المشتركين المتصلين
   - مراقبة عدد جلسات PDN
   - تتبع المكالمات النشطة VoLTE

صفحة القطر

URL: `https://[hostname]:7443/diameter`

تعرض صفحة القطر الحالة في الوقت الحقيقي لجميع اتصالات الأقران في القطر.

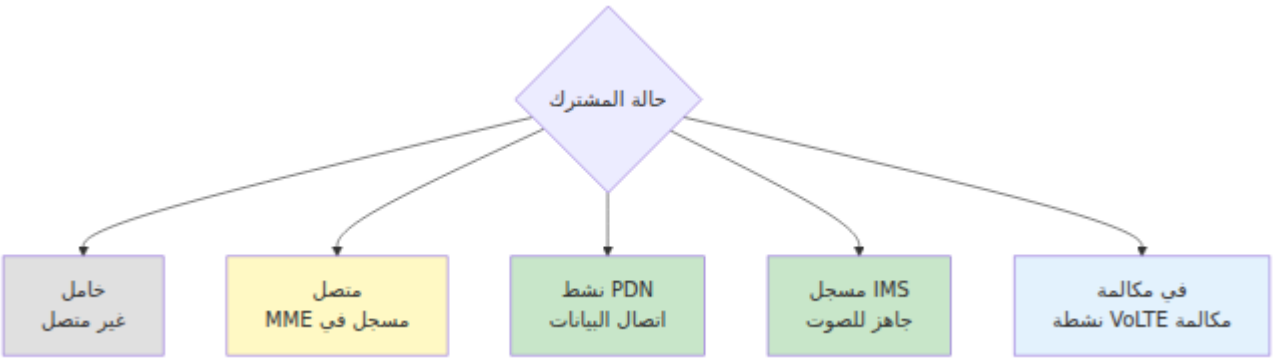
تخطيط الصفحة



أعمدة الجدول

العمود	الوصف	القيم
اسم المضيف	اسم مضيف القطر	FQDN
المجال	مجال القطر	اسم النطاق
IP:Port	عنوان الشبكة	عنوان IP والمنفذ
النقل	بروتوكول النقل	SCTP أو TCP
الحالة	حالة الاتصال	متصل / مفصول

حالة الاتصال



تفاصيل الصف القابل للتوسيع

انقر على أي قرين لعرض معلومات إضافية:

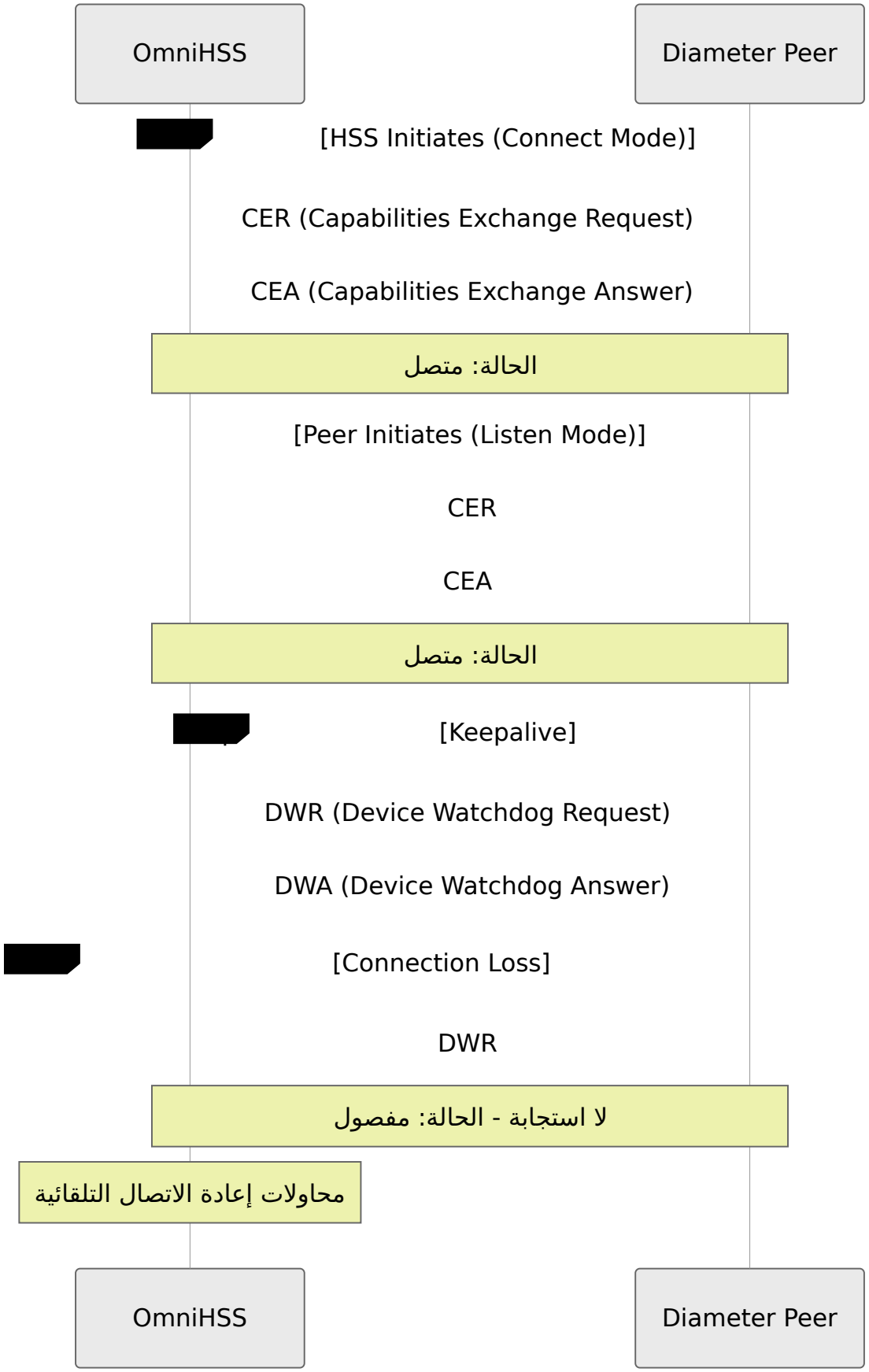
معلومات الاتصال:

- **نوع الاتصال** - تم الشروع به من قبل أو القرين HSS
- **اسم المنتج** - تعريف المنتج للقرين
- **معرفات التطبيقات** - التطبيقات المدعومة في القطر

أمثلة على معرفات التطبيقات:

- 16777251 - S6a (MME)
- 16777238 - Gx (P-GW)
- 16777216 - Cx (I-CSCF، S-CSCF)
- 16777217 - Sh (خادم التطبيق)
- 16777236 - Rx (P-CSCF)
- 16777252 - S13 (عميل EIR، إذا كان خارجيًا)

تدفق اتصال القرين



التحديث التلقائي

تقوم صفحة القطر بالتحديث تلقائيًا **كل 1 ثانية**.

حالات الاستخدام

1. **التحقق من الاتصال**
    - تأكد من أن جميع الأقران المتوقعين متصلين
    - تحديد الأقران المفصولة على الفور
    - مراقبة الاتصالات المتقلبة
2. **استكشاف الأخطاء**
    - تحقق مما إذا كان القرين قابلًا للوصول
    - تحقق من بروتوكول النقل (SCTP مقابل TCP)
    - تأكد من أن معرفات التطبيقات تتطابق مع التوقعات
    - تحديد أي جانب بدأ الاتصال
3. **تخطيط السعة**
    - عد إجمالي الأقران المتصلة
    - مراقبة استقرار الاتصال
    - التخطيط لسعة إضافية للقرين

المشكلات الشائعة

ال��رين يظهر مفصولًا

الأسباب المحتملة:

1. مشكلة في الاتصال بالشبكة
2. القرين متوقف أو يعيد التشغيل
3. جدار الحماية يحظر حركة المرور
4. عدم تطابق تكوين القطر
5. مشكلة في الشهادة (إذا كنت تستخدم TLS)

خطوات استكشاف الأخطاء:

1. تحقق من الاتصال بالشبكة: `ping [peer-ip]`
2. تحقق من أن المنفذ قابل للوصول: `telnet [peer-ip] 3868`
3. تحقق من قواعد جدار الحماية
4. مراجعة سجلات HSS للرسائل الخطأ
5. تحقق من أن تكوين القطر للقرين يتطابق مع HSS

القرين يتصل ويفصل بشكل متكرر

الأسباب المحتملة:

1. عدم استقرار الشبكة
2. عدم تطابق مهلة keepalive
3. مشكلات موارد القرين
4. عدم تطابق تطبيق القطر

خطوات استكشاف الأخطاء:

1. تحقق من استقرار الشبكة
2. مراجعة مؤقتات keepalive على كلا الجانبين
3. تحقق من موارد نظام القرين
4. تحقق من أن معرفات التطبيقات تتطابق على كلا الجانبين

صفحة التطبيق

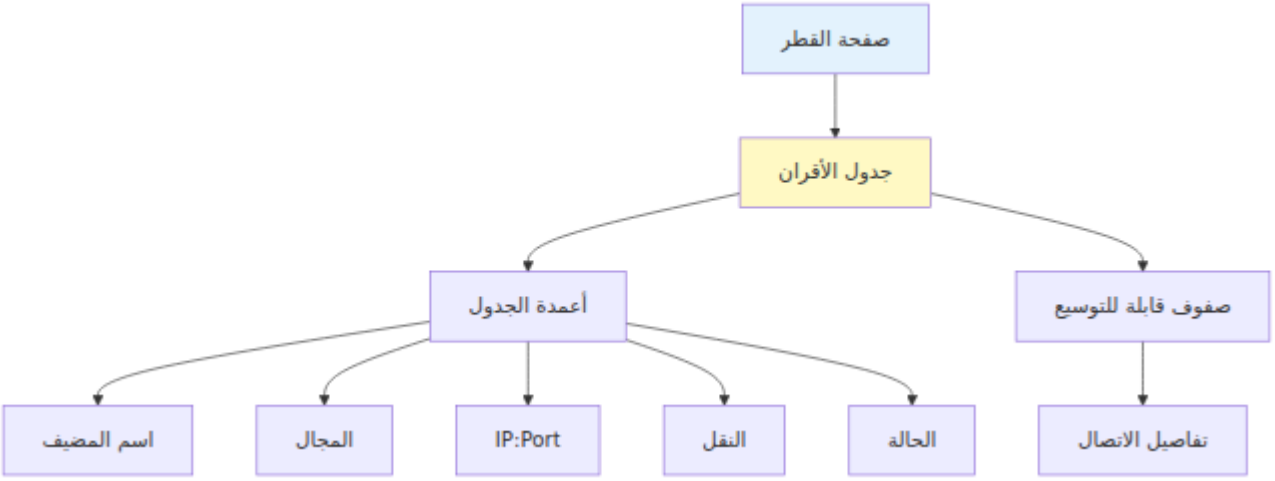
URL: `https://[hostname]:7443/application`

توفر صفحة التطبيق معلومات مراقبة على مستوى النظام واستخدام الموارد.

الميزات

- **معلومات العملية** - عدد عمليات VM Erlang والذاكرة
- **ذاكرة النظام** - الذاكرة الإجمالية والمستخدمة
- **مدة تشغيل التطبيق** - المدة التي تم فيها تشغيل OmniHSS
- **إصدار VM Erlang** - معلومات إصدار وقت التشغيل

المقاييس الرئيسية



حالات الاستخدام

1. **مراقبة الصحة**
    - تحقق من أن التطبيق يعمل
    - تحقق من تسرب الذاكرة (زيادة الذاكرة بمرور الوقت)
    - مراقبة نم�� عدد العمليات
2. **تخطيط السعة**
    - تتبع اتجاهات استخدام الذاكرة
    - التخطيط للتوسع بناءً على عدد العمليات
    - تحقق من موارد النظام الكافية
3. **استكشاف الأخطاء**
    - تحديد استنفاد الموارد
    - تحقق مما إذا كان يجب إعادة التشغيل
    - تحقق من إصدار VM Erlang

صفحة التكوين

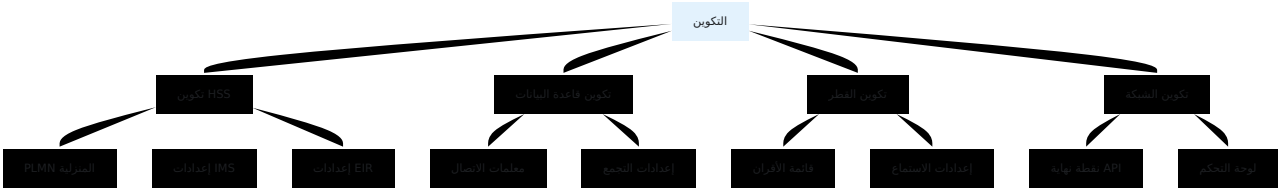
URL: `https://[hostname]:7443/configuration`

تعرض صفحة التكوين التكوين الحالي لوقت التشغيل لـ OmniHSS.

الميزات

- **عرض التكوين** - فحص جميع معلمات التكوين
- **البحث عن التكوين** - العثور على إعدادات محددة
- **المتغيرات البيئية** - رؤية القيم المحلولة

فئات التكوين



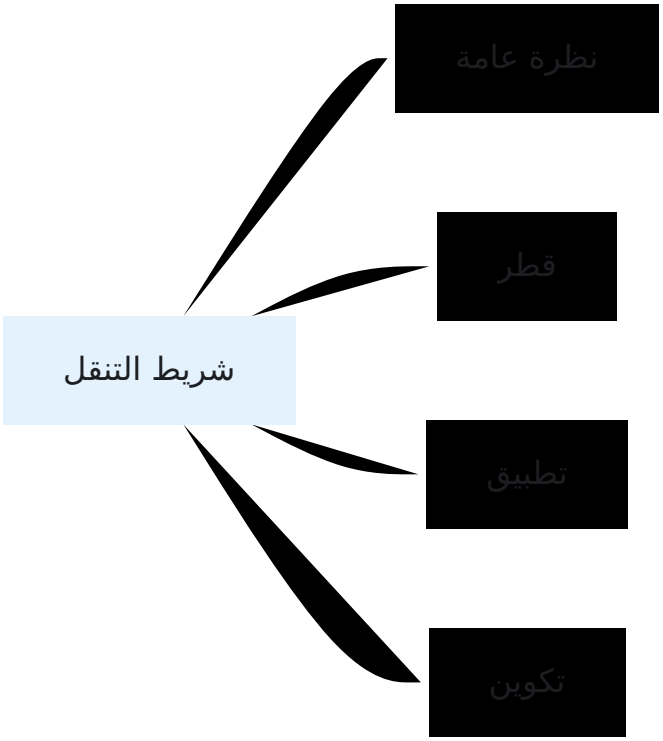
حالات الاستخدام

1. **التحقق من التكوين**
    - تحقق من تطبيق إعدادات runtime.exs
    - تأكيد معلمات اتصال قاعدة البيانات
    - تحقق من تكوين قرين القطر
2. **استكشاف الأخطاء**
    - تحديد عدم التطابق في التكوين
    - تحقق من تعيين المتغيرات البيئية بشكل صحيح
    - مقارنة التكوين المتوقع مقابل الفعلي
3. **التوثيق**
    - تصدير التكوين الحالي للتوثيق
    - مشاركة التكوين مع فريق الدعم

ملاحظة أمنية: قد تعرض صفحة التكوين معلومات حساسة (كلمات مرور قاعدة البيانات، المفاتيح). قيد الوصول بشكل مناسب.

التنقل والواجهة

شريط التنقل العلوي



التنقل مرئي دائمًا في أعلى الصفحة للوصول السريع.

اختصارات لوحة المفاتيح

لا تنفذ لوحة التحكم اختصارات لوحة مفاتيح مخصصة. تعمل اختصارات المتصفح القياسية:

- **Ctrl+R / F5** - تحديث الصفحة يدويًا (على الرغم من أن التحديث التلقائي يجعل هذا غير ضروري)
- **Ctrl+F** - البحث في الصفحة
- **Ctrl+T** - فتح علامة تبويب جديدة (لصفحات متعددة)

مراقبة متعددة العلامات

يمكنك فتح صفحات لوحة التحكم متعددة في علامات تبويب متصفح منفصلة للمراقبة المتزامنة:

إعداد المثال:

- علامة التبويب 1: صفحة النظرة العامة (مراقبة المشتركين)

- علامة التبويب 2: صفحة القطر (مراقبة الاتصال)
- علامة التبويب 3: صفحة التطبيق (مراقبة الموارد)

ستقوم جميع علامات التبويب بالتحديث التلقائي بشكل مستقل.

التصميم المتجاوب

تم تحسين لوحة التحكم لمتصفحات سطح المكتب. يتم دعم متصفحات الهواتف المحمولة ولكن قد تتطلب تمريرًا أفقيًا للجدول.

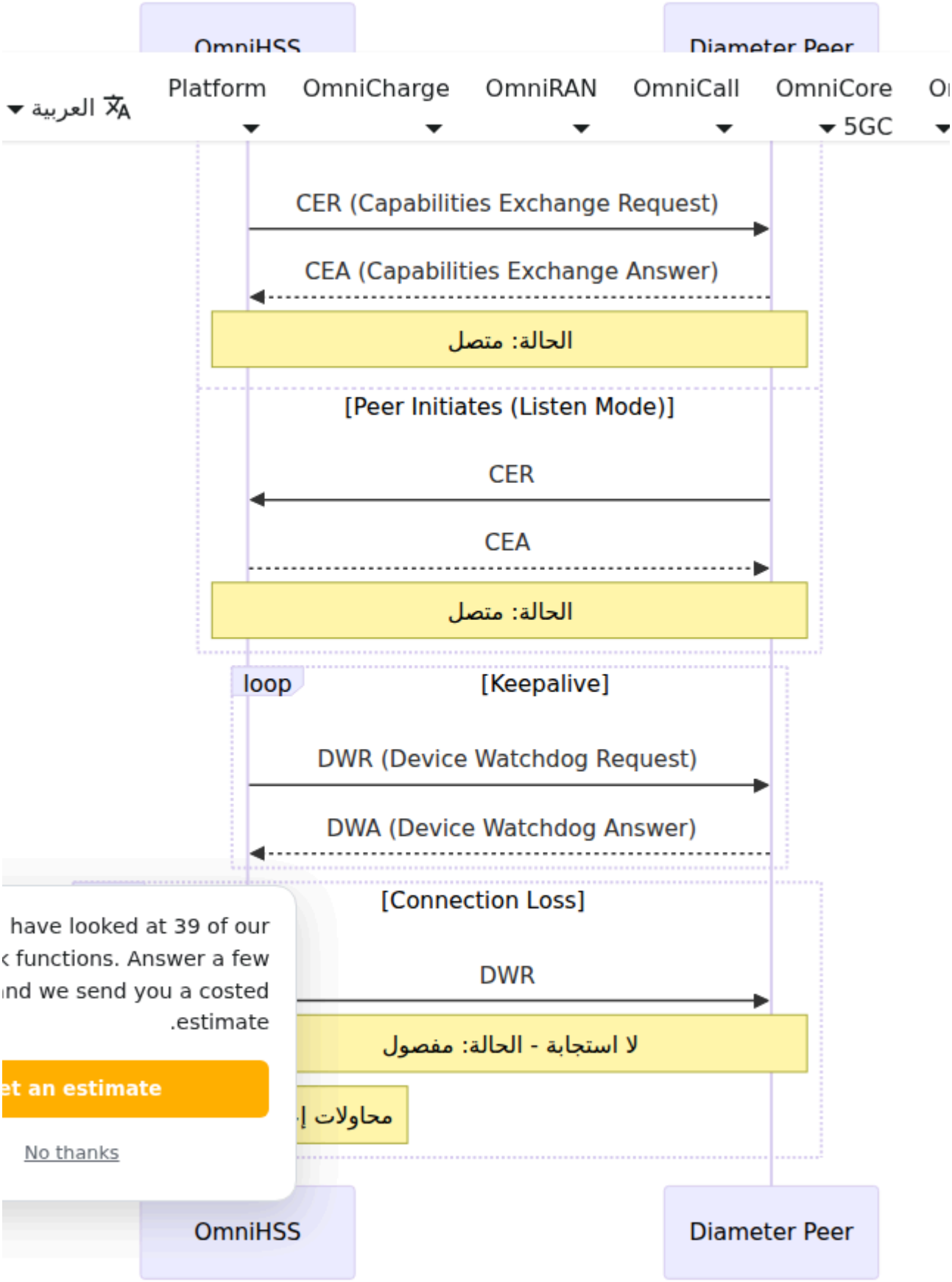
الدقة الموصى بها: 1920x1080 أو أعلى لعرض مريح.

أفضل ممارسات المراقبة

العمليات اليومية

1. **بداية الوردية**
    - افتح صفحة نظرة عامة لوحة التحكم
    - تحقق من أن العدد المتوقع من المشتركين متصلين
    - تحقق من صفحة القطر - جميع الأقران متصلون
2. **أثناء الوردية**
    - احتفظ بصفحة النظرة العامة مفتوحة للمراقبة في الوقت الحقيقي
    - راقب أي تغييرات غير عادية في الحالة
    - راقب الأقران المفصولة في صفحة القطر
3. **نهاية الوردية**
    - تحقق من استقرار النظام
    - تحقق من صفحة التطبيق لاتجاهات استخدام الموارد
    - وثق أي شذوذ

سير عمل استكشاف الأخطاء



عتبات التنبيه

حدد عتبات المراقبة للتنبيه الاستباقي:

المقياس	تحذير	حرجة
الأقران المفصولة في القطر	1 قرين	2+ أقران أو قرين حرج
استخدام الذاكرة	> 80%	> 90%
فشل مصادقة المشتركين	> 5%	> 10%
عدد العمليات	> 80% من الحد	> 95% من الحد

← التالي: المقاييس والمراقبة | العودة إلى دليل العمليات →

تكرار قاعدة البيانات

← العودة إلى دليل العمليات

جدول المحتويات

- نظرة عامة
- كيف يعمل
- هندسة النشر
- مرجع التكوين
- إدارة الأقران
- المراقبة
- استكشاف الأخطاء وإصلاحها

نظرة عامة

تستخدم OmniHSS **PostgreSQL** للنشر عالي التوافر عبر **تكرار منطقي ثنائي الاتجاه** مع مواقع متعددة. يعمل كل موقع كقاعدة بيانات رئيسية مستقلة للقراءة والكتابة. لا يوجد ماستر واحد أو نسخ للقراءة فقط.

الخصائص الرئيسية

- **كلا الموقعين قراءة/كتابة**: تحتوي كل موقع على قاعدة بيانات رئيسية كاملة. الكتابات المحلية فورية بغض النظر عن جودة الرابط بين ا��مواقع
- **تكرار غير متزامن**: تتكرر التغييرات عبر سجل الكتابة المتقدم (WAL) في PostgreSQL. لا يتم حظر أي كتابة في انتظار اعتراف موقع بعيد
- **تحمل التقسيم**: إذا تعطل الرابط بين المواقع، تستمر كلا الموقعين في العمل بشكل محليًا وتعيد التشغيل تلقائيًا عند استعادة الرابط WAL مستقل. تتجمع مقاطع
- **لا حاجة إلى نصاب**: على عكس نهج الكلاستر المتزامن، لا يوجد مفهوم للنصاب. يعمل النشر لموقع واحد بشكل مطابق للنشر عبر مواقع متعددة

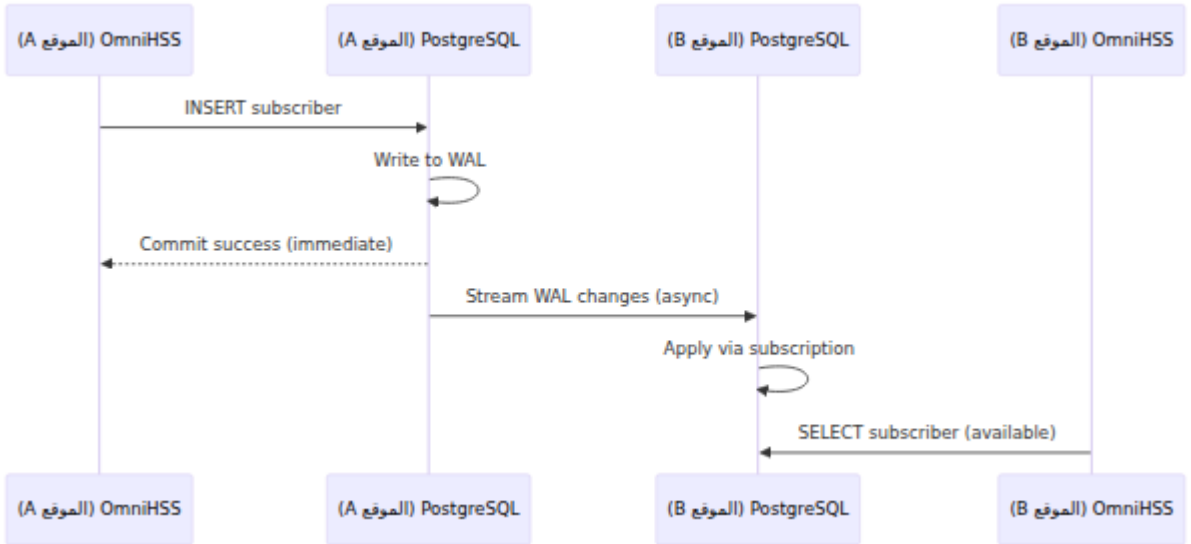
- **مفاتيح أساسية UUID**: تستخدم جميع السجلات مفاتيح أساسية UUIDv4، مما يقضي على تصادمات المعرفات بين المواقع دون تنسيق

كيف يختلف هذا عن التكرار المتزامن

	متزامن	تكرار منطقي غير متزامن
زمن الكتابة	محجوز من أبطأ عقدة	محلي فقط: أقل من مللي ثانية
فشل الرابط	يصبح الموقع الأقلية للقراءة فقط	تستمر كلا الموقعين في القراءة/الكتابة
الحاجة إلى نصاب	نعم (أغلبية العقد)	لا
اتساق البيانات	قوي (جميع العقد متطابقة)	نهائي (تأخير تكرار قصير)
مناسب لروابط الأقمار الصناعية	لا (الزمن يقتل أداء الكتابة)	نعم (تتجمع WAL وتلحق بالركب)

كيف يعمل

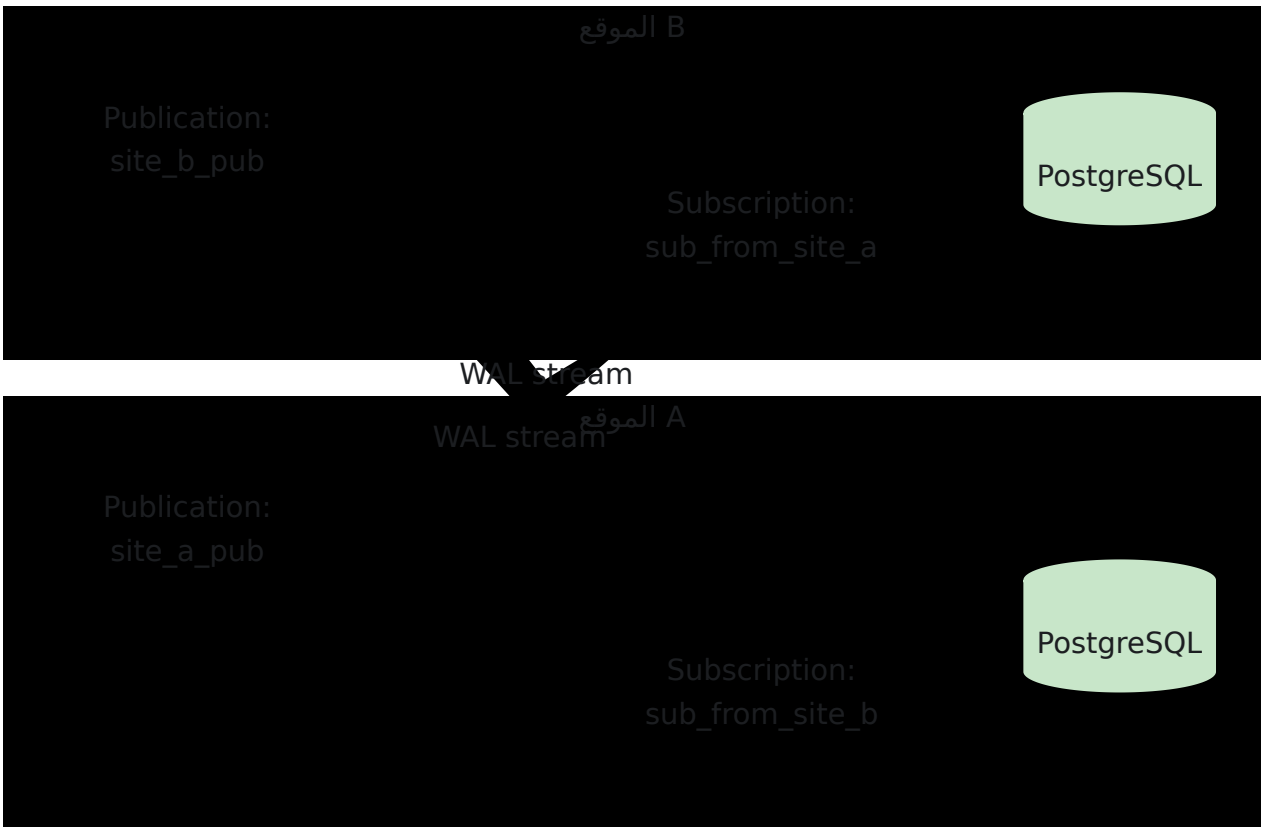
تدفق التكرار المنطقي



نموذج النشر / الاشتراك

كل موقع لديه:

- **نشر** يبث جميع تغييرات الجداول (باستثناء `schema_migrations`)
- **اشتراك** في نشر كل موقع نظير



أثناء انقطاع الرابط WAL تجميع

عندما يكون الرابط بين المواقع غير متاح:

1. تستمر الكتابات المحلية دون انقطاع
2. على جانب النشر WAL تتجمع مقاطع
3. تتعقب فتحة التكرار المكان الذي توقف فيه كل مشترك
4. عند استعادة الرابط، تعيد المقاطع المتراكمة التشغيل من آخر موقع معترف به
5. تتقارب كلا الموقعين إلى حالة متطابقة

لمنع النمو غير `max_slot_wal_keep_size` محدودة بواسطة WAL تكون مدة الاحتفاظ بـ المحدود للقرص أثناء الانقطاعات الطويلة.

منع التصادم

الأساسية المصدر الرئيسي للتصادمات في التكرار الثنائي الاتجاه. نظرًا لأن كل UUID تزيل مفاتيح موقع يولد معرفات فريدة عالم��ا بشكل مستقل، فإن عمليات INSERT لا تتصادم أبدًا.

حلقات التكرار. التغييرات التي وصلت عبر التكرار لا يتم `origin = none` تمنع خيار الاشتراك إعادة نشرها إلى مشتركين آخرين.

من النشر لأن كلا الموقعين يقومان بتشغيل ترحيلات `schema_migrations` يتم استبعاد جدول متطابقة بشكل مستقل.

آخر كتابة تفوز للحالة الديناميكية

تتم تحديث جداول الحالة الديناميكية (`subscriber_state`, `pdn_session`, `lte_call`) يحدث جلسة CCR الخادم، كل MME يحدث ULR. كل Diameter بشكل متكرر بواسطة إشارات PGW، وكل AAR يحدث المكالمة النشطة.

في نشر متعدد المواقع، يتم خدمة مشترك من موقع واحد في كل مرة. عندما ينتقل المشترك بين المواقع، قد تحتوي كلا الموقعين على تحديثات لنفس صف `subscriber_state` من أوقات مختلفة. بدون حل التصادم، سيحدد ترتيب التكرار أي قيمة تبقى. قد يؤدي ذلك إلى الكتابة فوق الحالي بقيمة قديمة MME.

تستخدم OmniHSS **محفزات آخر كتابة تفوز (LWW)** على جداول الحالة الديناميكية:

```
CREATE TRIGGER lww_subscriber_state_trigger
  BEFORE UPDATE ON subscriber_state
  FOR EACH ROW
  EXECUTE FUNCTION lww_subscriber_state();
```

للتحديث المكرر الوارد مع الصف الموجود. إذا كان `updated_at` يقارن المحفز الطابع الزمني الصف الموجود أحدث، يتم كتم التحديث بصمت. يضمن هذا:

- عندما ينتقل مشترك من الموقع A إلى الموقع B، فإن التحديث الأحدث من الموقع B يفوز دائمًا
- يتم تجاهل التحديثات القديمة من الموقع A (من قبل انتقال المشترك)
- تتقارب كلا الموقعين إلى نفس القيمة: أحدث كتابة

الجداول التي تحتوي على محفزات LWW:

الجدول	تم تحديثه بواسطة	التكرار
`subscriber_state`	ULR, SAR, AIR, PUR, ECR, CCR	كل تحديث للاتصال/الموقع
`pdn_session`	CCR-I, CCR-T	كل إنشاء/حذف جلسة PDN
`lte_call`	AAR, STR	كل إعداد/إلغاء إعداد مكالمة VoLTE
`ims_subscription`	UAR, SAR (S-CSCF المشتر��)	كل تسجيل لعضو مجمع

يقوم LWW. إلى (APNs، المشتركون، الملفات الشخصية، المفاتيح) لا تحتاج بيانات التزويد الثابتة واجهة برمجة التطبيقات الخاصة بالتزويد بتحديث هذه السجلات فقط، عادةً من طبقة إدارة واحدة.

اتفاقية التسمية (مطلوبة للجداول الجديدة)

يجب أن تُسمى `foo`، والمحفزات هي **عقد**، وليست خيارًا حرًا. بالنسبة لجدول LWW أسماء دالة الدالة `lww_foo()` ويجب أن يُسمى المحفز `lww_foo_trigger`.

بقائمة خاصة بهذه الجداول. يكتشف كل `omnihss` الخاص بـ OmniCore Ansible لا يحتفظ دور `ENABLE REPLICA` ويضمن أن يكون كل منها في وضع `lww_<table>_trigger` محفز يتطابق اسمه مع عبر الشبكة. المحفز الذي يحمل أي اسم آخر يكون غير مرئي لتلك المصالحة، لذا لن يتم فرض حل التصادم عبر المواقع بشكل صامت على ذلك الجدول.

الحية على أكثر Diameter جدول مكتوب من حركة مرور) عند إضافة جدول حالة ديناميكية جديد اتبع هذه الخطوات، (من موقع في وقت واحد:

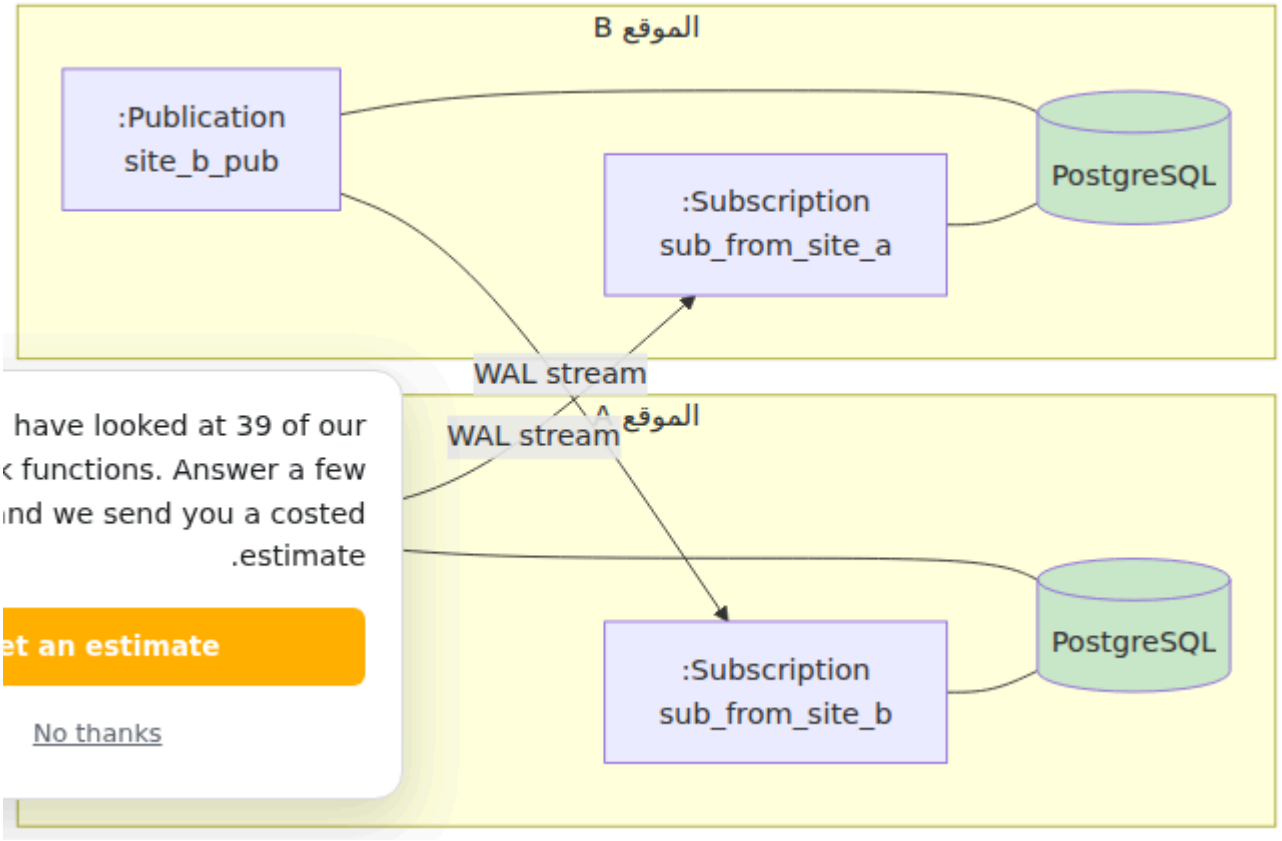
1. أعط الجدول عمود `updated_at` (تضيف ماكرو Ecto `timestamps()` ذلك).
2. في نفس الترحيل، أنشئ `lww_<table>()` و `lww_<table>_trigger` بهذه الأسماء بالضبط.
3. في نفس الترحيل، قم بتشغيل `ALTER TABLE <table> ENABLE REPLICA TRIGGER lww_<table>_trigger`، بحيث يتم تشغيل المحفز أثناء تطبيق التكرار، وليس على الكتابات المحلية.

هو المثال المرجعي: يقوم ترحيله بإنشاء `ims_subscription` جدول `lww_ims_subscription()` و `lww_ims_subscription_trigger`، ثم يمكّن المحفز في

وضع النسخ. اتبع نفس الشكل، ولا تعيد تسمية الدالة أو المحفز.

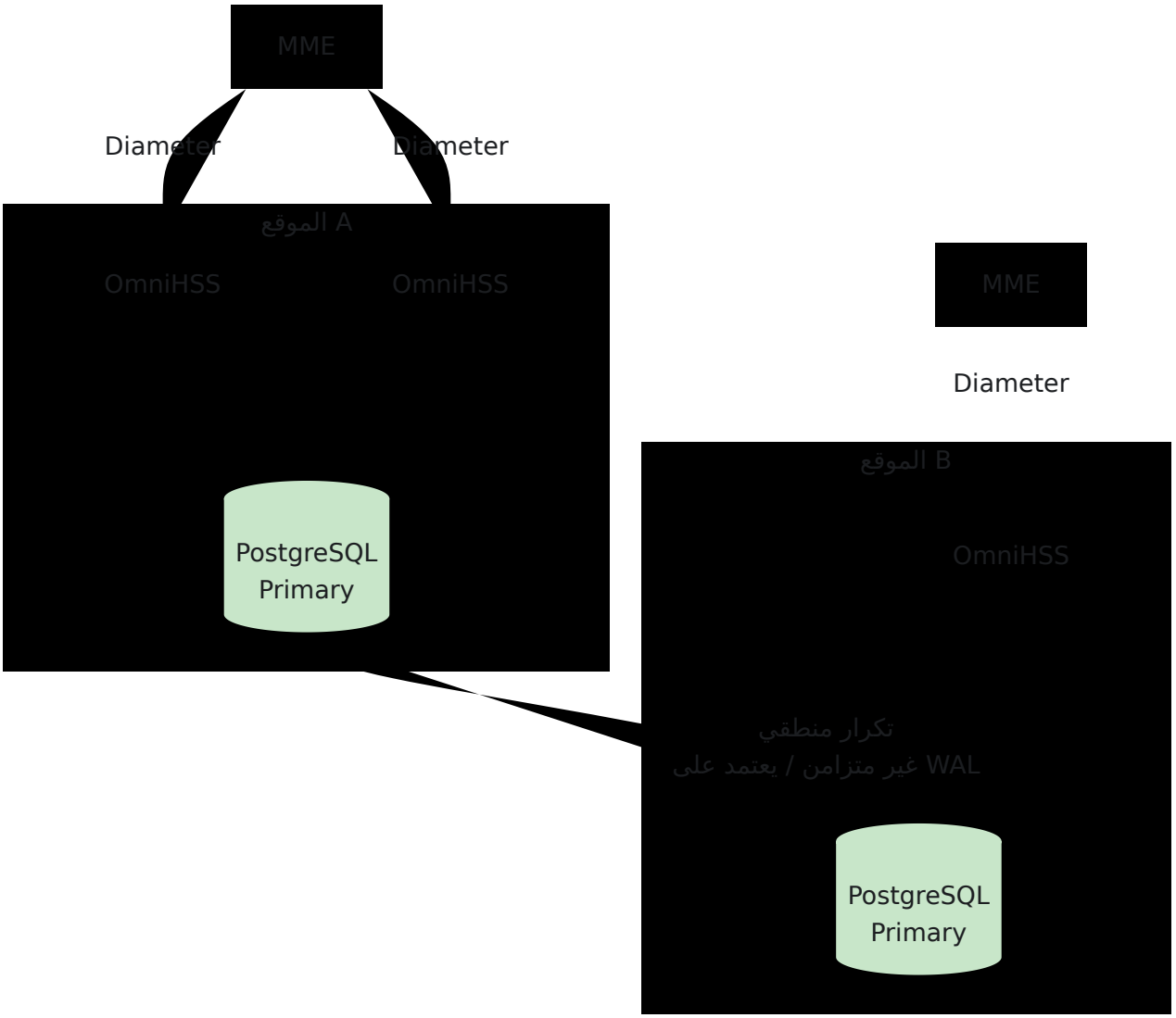
هندسة النشر

موقع واحد (بدون تكرار)



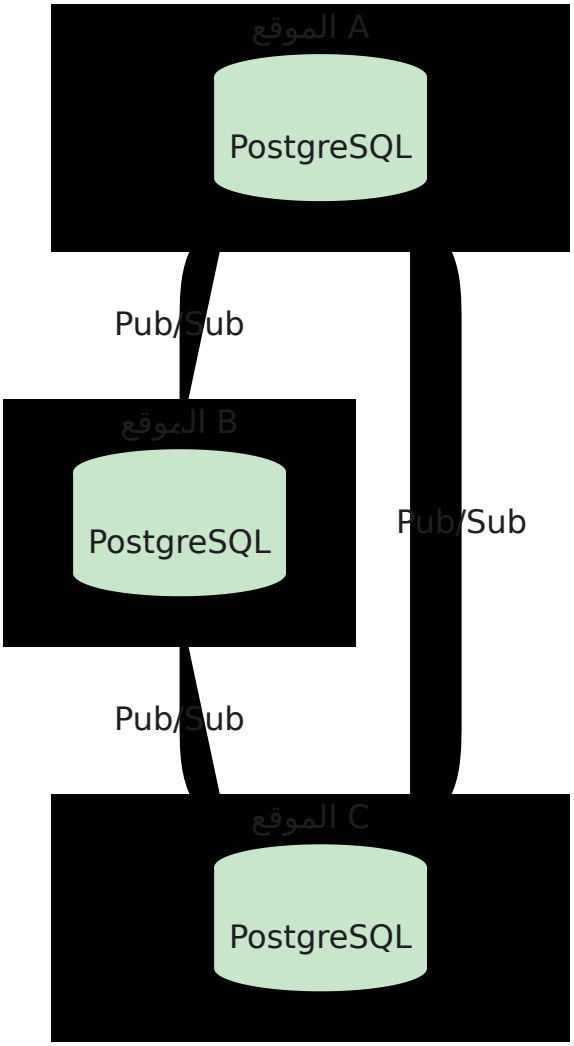
واحدة. يمكن استخدام تكرار PostgreSQL قاعدة بيانات HSS تشارك عدة مثيلات من تطبيق القياسي للتكرار المحلي لقاعدة البيانات إذا لزم الأمر PostgreSQL.

نشر موقعين



كلا الموقعين هما رئيسيان كاملان. يتم تكرار تزويد المشترك في أي من الموقعين إلى الآخر. يتصل كل MME بـ HSS المحلي له. لا يوجد اعتماد على Diameter عبر المواقع.

نشر متعدد المواقع



لإضافة Ansible. يشترك كل موقع في نشر كل موقع آخر. يتم اكتشاف الأقران تلقائيًا من جرد موقع، أضفه إلى مجموعة جرد `hss` وقم بتشغيل playbook.

متطلبات الشبكة

الغرض	البروتوكول	المنفذ
اتصالات عميل PostgreSQL والتكرار	TCP	5432

مرجع التكوين

متغيرات Ansible

يتم تكوين التكرار لكل مجموعة HSS في جردك:

```yaml
hss:
  hosts:
    site-a-hss01:
      ansible_host: 10.80.12.140
    site-a-hss02:
      ansible_host: 10.80.12.141
  vars:
    omnihss:
      database_type: postgres
      database_host: localhost
      database_port: 5432
      database_name: omnihss
      database_username: omnihss
      database_password: "secure_password"
      replication:
        enabled: true
```

معلمات Ansible

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`database_type`	سلسلة	لا	`postgres`	قاعدة البيانات الخلفية. يجب أن تكون `postgres` للتكرار.
`database_host`	سلسلة	لا	`localhost`	مضيف PostgreSQL. استخدم `localhost` عندما يعمل Postgres على نفس المضيف مثل OmniHSS.
`database_port`	عدد صحيح	لا	`5432`	منفذ PostgreSQL.
`database_name`	سلسلة	لا	`omnihss`	اسم قاعدة البيانات.
`database_username`	سلسلة	نعم	-	مستخدم PostgreSQL. يجب أن يمتلك امتيازات `CREATEDB` و `REPLICATION`.
`database_password`	سلسلة	نعم	-	كلمة مرور PostgreSQL.
`replication.enabled`	منطقي	لا	`false`	تمكين التكرار المنطقي الثنائي الاتجاه. عندما تكون `true`، يقوم دور Ansible بتكوين النشر، والاشتراكات،

الوصف	الافتراضي	مطلوب	النوع	المعلمة
وإدخالات `pg_hba.conf` تلقائيًا.				

اكتشاف الأقران

يتم اكتشاف الأقران تلقائيًا من مصدرين:

1. مجموعة Ansible `hss` **مجموعة الجرد المحلية**: جميع المضيفين الآخرين في مجموعة
2. **المواقع البعيدة**: الإدخالات في `connected_sites.hss` من `prod_master_peers.yml`

لا يتطلب الأمر تكوين قرين لكل مضيف. يكفي إضافة مضيف إلى مجموعة `hss` أو إلى `connected_sites.hss` وتشغيل playbook.

أقران المواقع البعيدة (prod_master_peers.yml)

للتكرار بين المواقع عبر المواقع الجغرافية:

```
# group_vars/prod_master_peers.yml
connected_sites:
  hss:
    - remote-site-hss01: 10.80.20.140
    - remote-site-hss02: 10.80.20.141
```

تكوين PostgreSQL

يقوم دور Ansible بتكوين المعلمات التالية في PostgreSQL تلقائيًا عند تمكين التكرار:

المعلمة	القيمة	الغرض
`wal_level`	`logical`	مطلوب للتكرار المنطقي. يتضمن بيانات الصف الكامل في WAL.
`max_wal_senders`	`10`	الحد الأقصى لعمليات إرسال WAL المتزامنة (واحدة لكل مشترك).
`max_replication_slots`	`10`	الحد الأقصى لفتحات التكرار. يستخدم كل نظير فتحة واحدة.
`listen_addresses`	`*`	قبول الاتصالات من مواقع الأقران.

يضيف الدور أيضًا إدخالات `pg_hba.conf` للأقران IP للسماح باتصالات التكرار من كل عنوان المكتشفة.

إدارة الأقران

إضافة موقع جديد

1. أضف المضيفين الجدد إلى مجموعة جرد `hss`، أو أضف إلى `connected_sites.hss` في `prod_master_peers.yml`
2. قم بتشغيل playbook الخاص بـ OmniHSS

سوف يقوم الدور بـ:

- تثبيت OmniHSS وPostgreSQL على المضيف الجديد
- تشغيل ترحيلات قاعدة البيانات
- إنشاء نشر للموقع الجديد
- إنشاء اشتراكات لجميع الأقران الموجودين
- تحديث `pg_hba.conf` على جميع الأقران الموجودين للسماح بالموقع الجديد
- إنشاء اشتراكات من الأقران الموجودة إلى الموقع الجديد

إزالة موقع

```
ansible-playbook -i hosts site.yml --tags hss-remove-peer \
  -e "peer_name=site_b confirm_remove=yes"
```

المتابعة playbook مطلوبة كإجراء احترازي. بدونها، يرفض `confirm_remove=yes` المعلمة ويعرض ما سيحدث.

إزالة قرين:

- يسقط الاشتراك (يتوقف عن التكرار الوارد من ذلك القرين)
- يزيل عنوان IP للقرين من `pg_hba.conf`
- تبقى البيانات التي تم تكرارها بالفعل من القرين في قاعدة البيانات المحلية
- يجب إزالة اشتراك موقع القرين في هذا الموقع بشكل منفصل على القرين

إضافة قرين بشكل عشوائي

في الحالات التي تحتاج فيها إلى إضافة قرين خارج تدفق playbook القياسي:

```
ansible-playbook -i hosts site.yml --tags hss-add-peer \
  -e "peer_name=site_b peer_host=10.80.20.140"
```

المراقبة

مقاييس Prometheus

تشغل خدمة **postgres_exporter** على كل مضيف HSS، مما يكشف على المنفذ `9187` مقاييس PostgreSQL لـ Prometheus.

مقاييس التكرار

المقياس	النوع	الوصف
`pg_replication_slots_active`	Gauge	إذا كانت `1` فتحة التكرار نشطة (متصلة بالقرين)، `0` إذا كانت غير نشطة
`pg_replication_slots_pg_wal_lsn_diff`	Gauge	تأخير التكرار بالبايت. المسافة بين موضع WAL الحالي وآخر موضع مؤكد للقرين
`pg_stat_replication_pg_current_wal_lsn_bytes`	Gauge	موضع WAL الحالي على هذه العقدة

استعلامات Prometheus النموذجية

```
# فتحة التكرار نشطة (1 = متصلة، 0 = غير متصلة)
pg_replication_slots_active{slot_name=~"sub_from_.*"}

# تأخير التكرار بالميغابايت
pg_replication_slots_pg_wal_lsn_diff / 1048576

# تنبيه: فتحة التكرار غير نشطة لأكثر من 60 ثانية
pg_replication_slots_active == 0
```

التنبيهات الموصى بها

التنبيه	الشرط	الشدة	الوصف
فتحة التكرار غير نشطة	`pg_replication_slots_active == 0` لمدة 60 ثانية	حرجة	القرين غير متصل. تتجمع WAL.
تأخير WAL مفرط	`pg_replication_slots_pg_wal_lsn_diff > 104857600` لمدة 5 دقائق	تحذير	يتجاوز تأخير التكرار 100 ميغابايت. قد يكون القرين بطيئًا أو الرابط متدهورًا.
فتحة WAL مفقودة	حالة WAL هي `lost`	حرجة	تم إبطال الفتحة. يحتاج القرين إلى إعادة تزويد كاملة.

Ansible تحقق

يتحقق playbook الخاص بـ OmniHSS. يؤكد من صحة التكرار في نهاية كل تشغيل:

1. أن جميع عمال الاشتراك على قيد الحياة
2. أن جميع فتحات التكرار نشطة
3. أن تأخير WAL (ضمن العتبة الافتراضي 100 ميغابايت)
4. أن حالة فتحة WAL هي `reserved` أو `extended` (وليس `lost`)

إذا فشلت أي تأكيد، يفشل playbook مع رسالة خطأ واضحة تحدد المشكلة.

التحقق اليدوي

```
# تحقق من أن عمال الاشتراك على قيد الحياة
sudo -u postgres psql -d omnihss -c \
  "SELECT subname, pid IS NOT NULL as worker_alive FROM
pg_stat_subscription;"

# تحقق من فتحات التكرار والتأخير
sudo -u postgres psql -d omnihss -c \
  "SELECT slot_name, active,
    pg_wal_lsn_diff(pg_current_wal_lsn(), confirmed_flush_lsn) as
lag_bytes,
    wal_status
  FROM pg_replication_slots WHERE slot_type = 'logical';"

# قارن عدد المشتركين بين المواقع
sudo -u postgres psql -d omnihss -c "SELECT count(*) FROM
subscriber;"
```

استكشاف الأخطاء وإصلاحها

عامل الاشتراك ميت

الأعراض: تظهر `pg_stat_subscription` أن `pid IS NULL` لاشتراك. يفشل تحقق Ansible مع "عمال ميتين."

الأسباب الشائعة:

- عدم تطابق DDL) الجدول موجود على الناشر ولكن ليس على المشترك)
- تصادم مفتاح مكرر من سجل تم إدخاله يدويًا
- القرين غير قابل للوصول لفترة طويلة مما تسبب في إبطال فتحة WAL

الحل:

1. تحقق من سجلات PostgreSQL للخطأ المحدد:

```
journalctl -u postgresql | grep "logical replication" |
tail -20
```

2. قم بتطبيق الترحيل المفقود على هذا الموقع، ثم سيعيد DDL: إذا كان هناك عدم تطابق العامل التشغيل تلقائيًا
3. إذا كان هناك مفتاح مكرر: قم بحل التصادم يدويًا، ثم أعد تمكين الاشتراك:

```
ALTER SUBSCRIPTION sub_from_<peer> ENABLE;
```

فتحة التكرار غير نشطة

الأعراض: تظهر `pg_replication_slots` أن `active = false`. يتم إطلاق تنبيه Prometheus.

الأسباب الشائعة:

- مشكلة في الاتصال الشبكي بين المواقع
- توقف PostgreSQL على موقع القرين
- جدار ناري يحظر المنفذ 5432 من عنوان IP للقرين

الحل:

1. تحقق من الاتصال الشبكي بالقرين:

```
pg_isready -h <peer_ip> -U <db_user> -d omnihss
```

2. تحقق من أن PostgreSQL يعمل في موقع القرين
3. تحقق من أن قواعد جدار الحماية تسمح بالمنفذ 5432 من عنوان IP لهذا الموقع

سيعيد عامل الاشتراك الاتصال تلقائيًا عندما يصبح القرين قابلًا للوصول.

فتحة WAL مفقودة

الأعراض: تظهر `pg_replication_slots` أن `wal_status = 'lost'`. يفشل تحقق Ansible مع "فتحة WAL حرجة."

السبب: تم فصل القرين لفترة طويلة لدرجة أن WAL المحتفظ به تجاوز `max_slot_wal_keep_size` وتم تنظيفه.

الحل: يحتاج القرين إلى إعادة تزويد كاملة:

1. اسقط الاشتراك المعطل في هذا الموقع:

```
DROP SUBSCRIPTION sub_from_<peer>;
```

2. اسقط الفتحة المعطلة في موقع القرين:

```
SELECT pg_drop_replication_slot('sub_from_<this_site>');
```

3. أعد تشغيل playbook الخاص بـ OmniHSS. سيعيد إنشاء الاشتراك مع `copy_data = true` لإجراء مزامنة أولية.

مفرط WAL تأخير

الأعراض: `pg_replication_slots_pg_wal_lsn_diff` كبير وينمو. يتم إطلاق تنبيه Prometheus.

الأسباب الشائعة:

- رابط بين المواقع عالي الزمن أو مزدحم
- موقع القرين تحت حمل ثقيل (لا يمكن لعامل التطبيق مواكبة ذلك)
- كبير WAL عملية ضخمة (مثل التزويد الجماعي) تولد حجم

الحل:

1. تحقق مما إذا كان التأخير ينمو أو مستقرًا:

```
SELECT slot_name,
  pg_wal_lsn_diff(pg_current_wal_lsn(),
confirmed_flush_lsn) as lag_bytes
FROM pg_replication_slots WHERE slot_type = 'logical';
```

2. إذا كان مستقرًا: فإن القرين يطبق التغييرات ولكنه متأخر. سيلحق بالركب.
3. إذا كان ينمو: تحقق من رابط الشبكة أو حمل موقع القرين.
4. بالنسبة للعمليات الضخمة: التأخير أثناء العملية متوقع وسيتحل بعد اكتمال العملية.

تنسيق ترحيل المخطط

مهم: لا تتكرر تغييرات مخطط قاعدة البيانات (الترحيلات) عبر التكرار المنطقي. عند نشر إصدار جديد من OmniHSS يتضمن تغييرات في المخطط:

1. قم بتطبيق الترحيل على **جميع المواقع** قبل نشر كود التطبيق الذي يعتمد على أعمدة/جداول جديدة
2. مع ذلك تلقائيًا. يقوم بتشغيل الترحيلات على كل Ansible الخاص بـ playbook يتعامل مضيف
3. إذا كنت تنشر يدويًا، قم بتشغيل الترحيلات على جميع المواقع أولاً:

```
/opt/omnihss/bin/hss rpc "Hss.Command.Database.migrate()"
```

علاقات كيان OmniHSS

← العودة إلى دليل العمليات

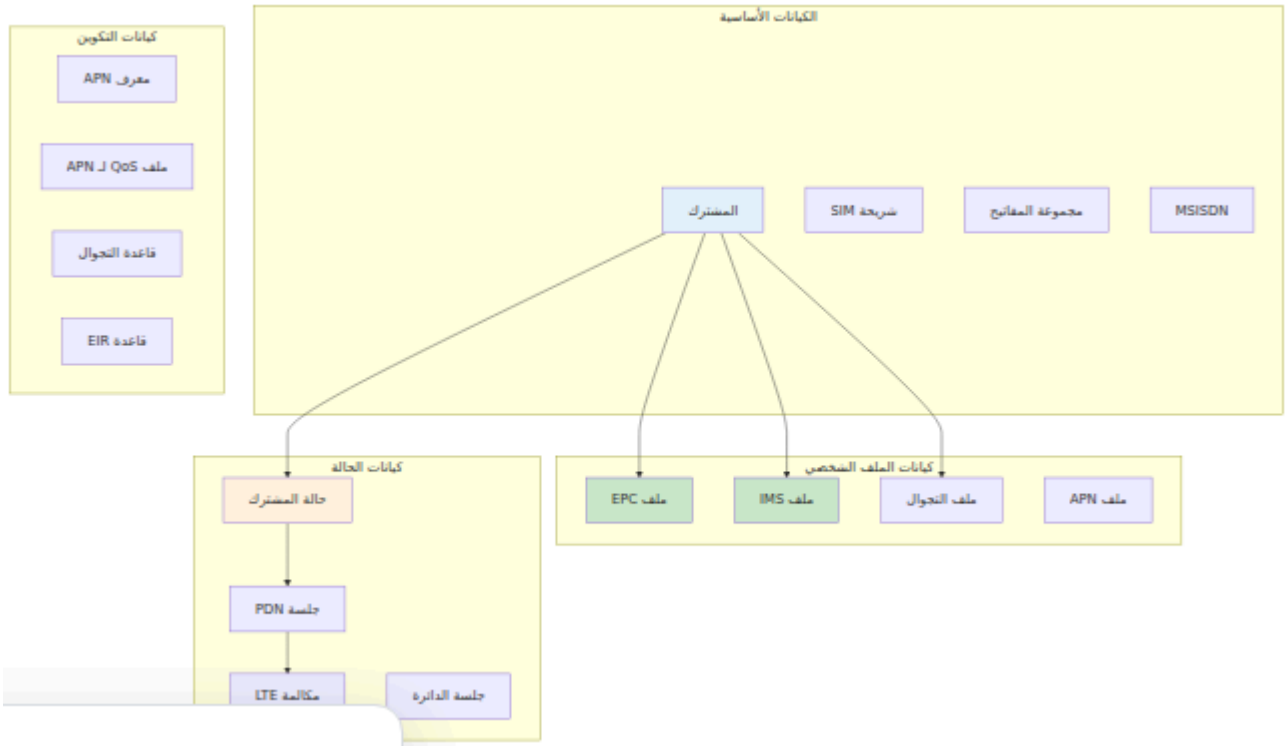
جدول المحتويات

- نظرة عامة على الكيانات
- الكيانات الأساسية
- كيانات الملف الشخصي
- كيانات الحالة
- مخططات علاقات الكيان
- دورة حياة الكيان
- أنماط تدفق البيانات

نظرة عامة على الكيانات

تنظم OmniHSS بيانات المشتركين في كيانات منطقية ذات علاقات واضحة. فهم هذه الكيانات أمر ضروري للمهام التشغيلية مثل التزويد، واستكشاف الأخطاء، وتخطيط السعة.

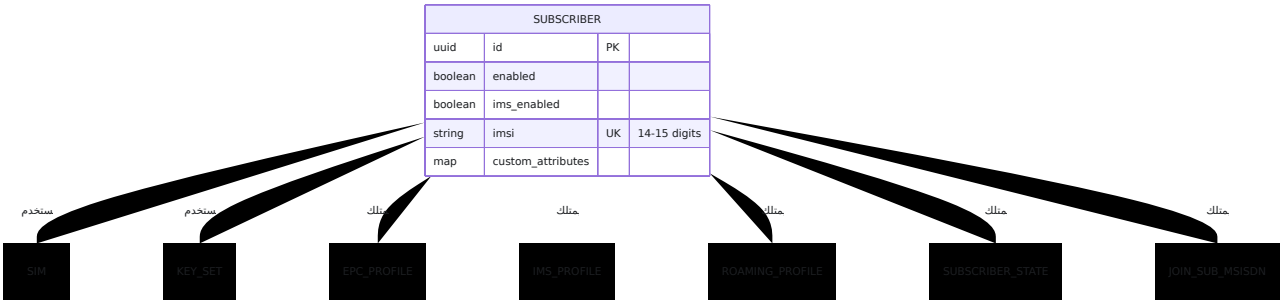
فئات الكيانات



الكيانات الأساسية

المشترك

المشترك هو الكيان المركزي الذي يمثل مستخدم الهاتف المحمول.



الحقول:

الحقل	النوع	الوصف	القيود
`id`	uuid	المفتاح الأساسي	UUID، مُولد (`gen_random_uuid()`)
`enabled`	boolean	علامة تمكين الخدمة	الافتراضي: true
`ims_enabled`	boolean	خدمات IMS مفعلة	الافتراضي: true
`imsi`	string	هوية المشترك الدولية للهاتف المحمول	رقم، فريد 14-15
`custom_attributes`	map	بيانات مفتاح-قيمة مخصصة	اختياري
`sim_id`	uuid	مفتاح خارجي إلى شريحة SIM	مطلوب للمصادقة (قد يكون فارغًا أثناء السكون)
`key_set_id`	uuid	مفتاح خارجي إلى مجموعة المفاتيح	مطلوب
`epc_profile_id`	uuid	مفتاح خارجي إلى ملف EPC	مطلوب لخدمة البيانات (قد يكون فارغًا أثناء السكون)
`ims_profile_id`	uuid	مفتاح خارجي إلى ملف IMS	مطلوب لخدمات IMS/الصوت (قد يكون فارغًا أثناء السكو��)

الحقل	النوع	الوصف	القيود
`roaming_profile_id`	uuid	مفتاح خارجي إلى ملف التجوال	اختياري؛ إذا كان فارغًا، لا يمكن للمشترك التجوال (شبكة المنزل فقط)
`subscriber_state_id`	uuid	مفتاح خارجي إلى حالة المشترك	يتم إنشاؤه تلقائيًا
`ims_subscription_id`	uuid	مفتاح خارجي إلى اشتراك IMS	اختياري

توضح عمود "القيود" أعلاه ما هو مطلوب لكل كائن **لخدمة**، وليس ما يحتاجه قاعدة البيانات لإدراج ومجموعة مفاتيح. مثل هذا المشترك هو *خامل*: IMSI صف. تقبل قاعدة البيانات مشتركًا لديه فقط إنه موجود، لكن لا تعمل أي خدمة حتى تقوم بتعيين الكائن المطابق. استخدم هذا لتزويد المشتركين مسبقًا، ثم قم بتنشيطهم لاحقًا. انظر تزويد المشترك الخامل مسبقًا.

ما يمكّن كل كائن:

يحتاج المشترك	لجعل هذا يعمل
`sim` و `key_set`	المصادقة (التوصيل، مصادقة IMS)
`epc_profile`	خدمة بيانات LTE (توصيل S6a)
واحد على الأقل MSISDN و، `ims_profile`	الصوت / IMS (تسجيل Cx)
مع قاعدة مطابقة `roaming_profile` ملف	التجوال على شبكة زائرة

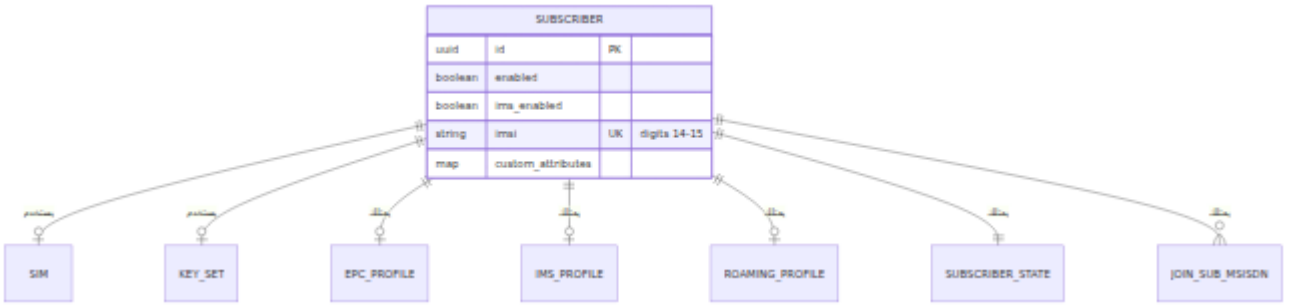
إذا كان كائن مطلوب مفقودًا عندما يظهر المشترك على الشبكة، يرفض HSS الطلب ويسجل السبب الدقيق. انظر سلوك المشترك الخامل على الشبكة.

نقاط رئيسية:

- يجب أن يحتوي كل مشترك على IMSI واحد بالضبط.
- يجب أن يكون IMSI (لا أحرف أو رموز خاصة) رقمًا من 14-15 مكونًا.
- يمكن أن يحتوي المشترك على عدة MSISDNs (أرقام هواتف).
- يتم إنشاء حالة المشترك تلقائيًا عند إنشاء المشترك.
- تتحكم علامة `enabled` في جميع الخدمات (و البياناتIMS).
- تتحكم علامة `ims_enabled` في خدمات IMS فقط.
- ومجموعة المفاتيح لإدراج مشترك. كل كائن آخر IMSI تحتاج قاعدة البيانات فقط إلى استخدام IMS مطلوب لخدمته الخاصة، كما هو مدرج أعلاه. لا يمكن لمشترك بدون ملف IMS، على الرغم من أن السجل يتم حفظه بدون واحد.
- مشترك بدون `ims_subscription_id` هو مستقل. قم بتعيين `ims_subscription_id` لتجميع عدة مشتركين (IMSIs) في اشتراك IMS واحد. انظر اشتراك واحد S-CSCFيشارك هوية عامة و هويةو المستخدم العامة IMS المشتركة.

شريحة SIM

تمثل كيان **SIM** شريحة SIM فعلية أو مدمجة.



الحقول:

الحقل	النوع	الوصف	مستوى الأمان
`iccid`	string	معرف بطاقة الدائرة المتكاملة	عام
`sim_vendor`	string	مصنع شريحة SIM	عام
`batch_name`	string	دفعة التصنيع	عام
`is_esim`	boolean	علامة شريحة SIM المدمجة	عام
`pin1`, `pin2`	string	رموز PIN	حساسة
`puk1`, `puk2`	string	رموز PUK	حساسة
`adm1` - `adm10`	string	رموز إدارية	حساسة للغاية
`kic`, `kid`	binary	مفاتيح أمان OTA	حساسة ل��غاية

نقاط رئيسية:

- يحدد شريحة SIM بشكل فريد ICCID
- يمكن تخصيص شريحة SIM واحدة لمشترك واحد في كل مرة
- رموز PIN/PUK مخصصة لقفل شريحة SIM للمستخدم النهائي
- رموز ADM مخصصة لعمليات SIM الإدارية
- KIC/KID مخصصة لتحديثات SIM OTA (عبر الهواء)

مجموعة المفاتيح

تحتوي **مجموعة المفاتيح** على مفاتيح تشفير للمصادقة.

KEY_SET			
uuid	id	PK	
binary	ki		128-bit
binary	opc		128-bit
binary	op		128-bit
binary	amf		16-bit
bigint	sqn		48-bit sequence
string	authentication_algorithm		

ستخدم من قبل



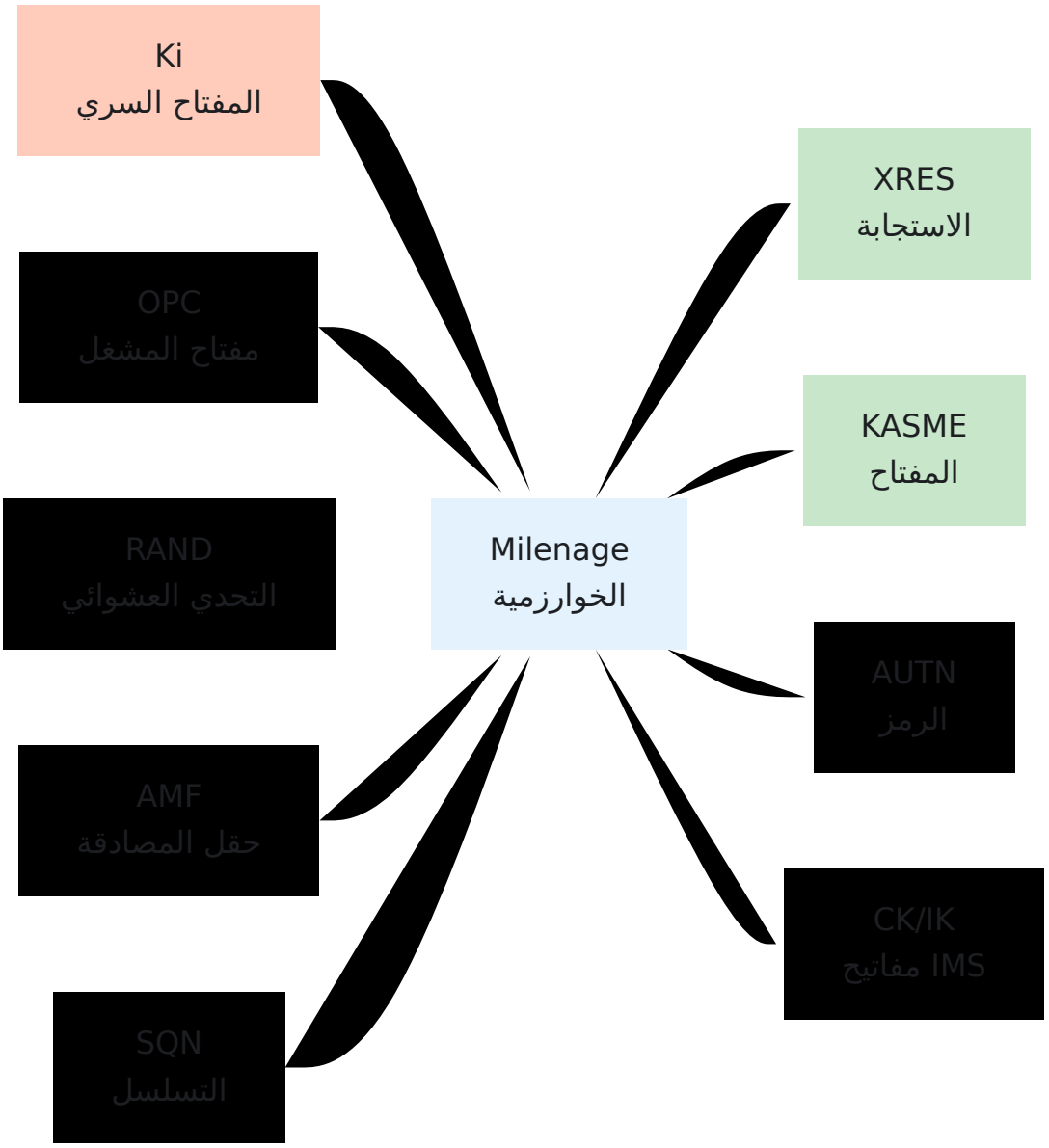
الحقول:

الحقل	النوع	الوصف	الحجم
`ki`	binary	المفتاح السري	128 بت (16 بايت)
`opc`	binary	مفتاح متغير المشغل (مشتق)	128 بت
`op`	binary	مفتاح المشغل (لإشتقاق OPC)	128 بت
`amf`	binary	حقل إدارة المصادقة	16 بت (2 بايت)
`sqn`	bigint	رقم التسلسل (مضاد لإعادة التشغيل)	48 بت
`authentication_algorithm`	string	اسم الخوارزمية	حاليًا "milenage"
`ota_counter`	bigint	عداد عملية OTA	عدد صحيح

نقاط رئيسية:

- يمكن لمشتركين متعددين مشاركة نفس مجموعة المفاتيح
- Ki هو السر الرئيسي المشترك مع شريحة SIM
- يجب توفير إما OPC أو OP (يمكن اشتقاق OPC من OP)
- يتم زيادة SQN مع كل مصادقة
- Milenage هو الخوارزمية المدعومة حاليًا فقط

خوارزمية المصادقة:

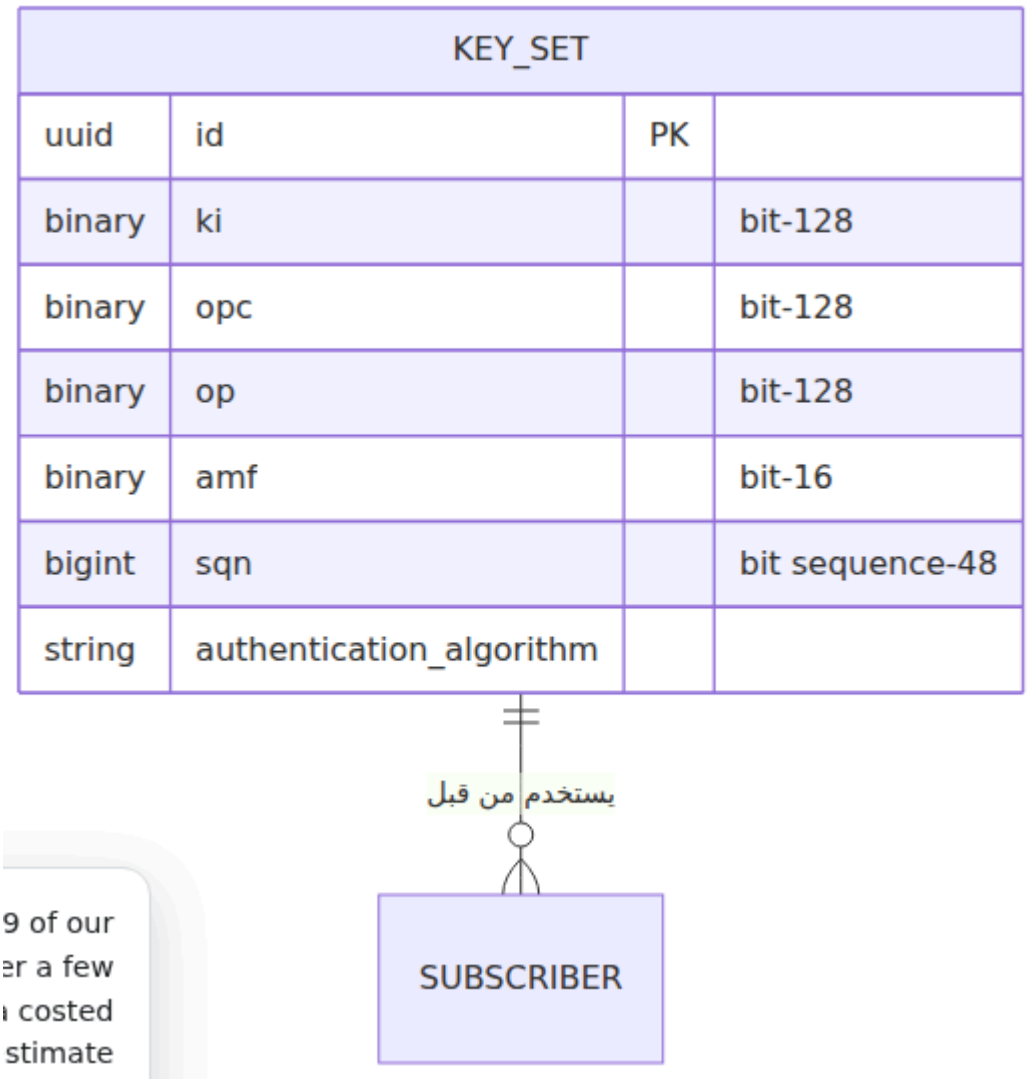


مجموعة المفاتيح، شريحة SIM، والمشترك

تعد شريحة SIM، والمشترك كائنات منفصلة. لكل كائن دورة حياة خاصة، مجموعة المفات��ح، والمشترك هو السجل الذي يربط بينهم.

- **شريحة SIM** - البطاقة الفعلية أو شريحة eSIM. تحتوي على ICCID ورموز PIN وPUK وADM. إنها مخزون.
- مفاتيح المصادقة - **مجموعة المفاتيح** (Ki، OPc، AMF، SQN). تقوم الشبكة بالمصادقة ضد هذه المفاتيح.
- الهوية الشبكية والخدمة - **المشترك** (IMSI، MSISDN، حالة التمكين، الملفات الشخصية).

يشير المشترك إلى شريحة SIM واحدة (`sim_id`) ومجموعة مفاتيح واحدة (`key_set_id`). لا تشير مجموعة المفاتيح إلى شريحة SIM، للعثور على الشريحة التي تنتمي إليها مجموعة المفاتيح. اقرأ المشترك الذي يشير إلى كلاهما.



لماذا ا��كائنات من��صلة

الكائنات منفصلة لأنها لا تتطابق واحد لواحد في كل حالة:

- **تبديل شريحة SIM.** يسقط مشترك هاتفًا ويحتاج إلى شريحة SIM جديدة. تحتفظ بالمشترك، مع MSISDN والملفات الشخصية، وبيانات IMS الخاص به. تشير إلى شريحة SIM جديدة ومجموعة مفاتيح جديدة. تستمر الخدمة.
- **شريحة SIM متعددة IMSI.** يحمل ICCID واحد عدة IMSIs. كل IMSI هو مشترك مختلف. تمتلك بعض IMSIs مجموعة مفاتيح واحدة. تشارك بعض IMSIs مجموعة مفاتيح خاصة بها. تنتمي المفاتيح إلى IMSI، وليس إلى بطاقة SIM. انظر دعم شريحة متعددة IMSI.

- بالمصادقة باستخدام SIM **التجوال المستضاف أو المدعوم.** تقوم تطبيق شريحة المنزل قبل أن يصل IMSI الزائر إلى IMSI زائر. تقوم الشبكة المضيفة بترجمة IMSI الطلب إلى HSS. تشارك IMSIs الاثنين مجموعة مفاتيح واحدة.

يمكن لمجموعة مفاتيح أن تخدم أكثر من مشترك واحد. لهذا السبب تعتبر مجموعة المفاتيح كائنًا منفصلًا، وليست حقلًا في شريحة SIM.

الارتباط عند الاستيراد

والمفاتيح في صف واحد. عند الاستيراد، تقوم بإنشاء ICCID لك SIM يوفر ملف بائع شريحة وإنشاء المشترك الذي يشير إلى كلاهما. المشترك هو SIM، مجموعة المفاتيح، وإنشاء شريحة السجل الرابط. لعملية استيراد العمل، انظر تزويد المشترك الخامل مسبقًا.

MSISDN

يمثل **MSISDN** رقم الهاتف.

MSISDN			
uuid	id	PK	
string	msisdn	UK	1-15 digits

خصصة لـ

JOIN_SUB_MSISDN		
uuid	subscriber_id	FK
uuid	msisdn_id	FK

تمي إلى



الحقول:

الحقل	النوع	الوصف	التنسيق
`msisdn`	string	رقم ISDN لمحطة المحمول	E.164 رقم، تنسيق 1-15

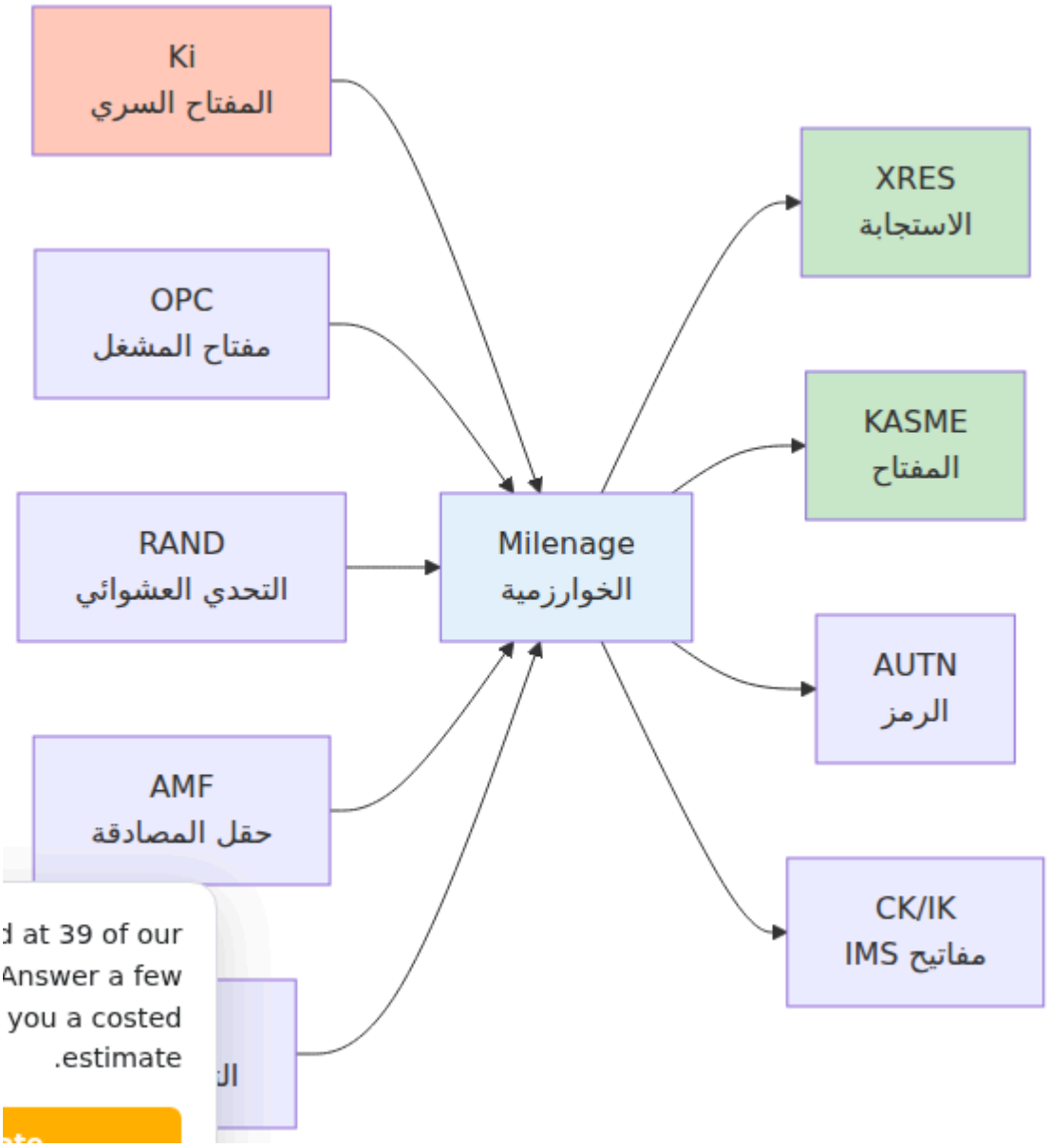
نقاط رئيسية:

- MSISDN هو رقم الهاتف بالتنسيق الدولي.
- يمكن أن يكون لمشترك واحد العديد من MSISDNs (IMSI الأرقام من العديد، واحد).
- يمكن تعيين MSISDN واحد للعديد من المشتركين (العديد من IMSIs، رقم واحد). استخدم هذا لرقم مشترك، على سبيل المثال هاتف وساعة ذكية. يتم تخزين الرقم كسجل MSISDN ويحتفظ كل مشترك بسجل انضمام له واحد.
- تعيد عملية البحث العكسي بواسطة MSISDN (على سبيل المثال API `GET /subscriber/msisdn/:msisdn`، أو بحث Diameter على الرقم (مفاتيح مشتركًا

لاختيار مشترك محدد ICCID أو IMSI واحدًا. عند مشاركة رقم، استخدم.

- التنسيق: رمز الدولة + الرقم الوطني، أرقام فقط - بدون بادئة `+` (على سبيل المثال، `14155551234` وليس `+14155551234`)
- S-CSCF عندما يرسل Diameter Cx/Rx تتم إزالة بادئة `+` تلقائيًا أثناء عمليات البحث أو P-CSCF URI SIP مع أو بدون `+`

نمط متعدد MSISDN:

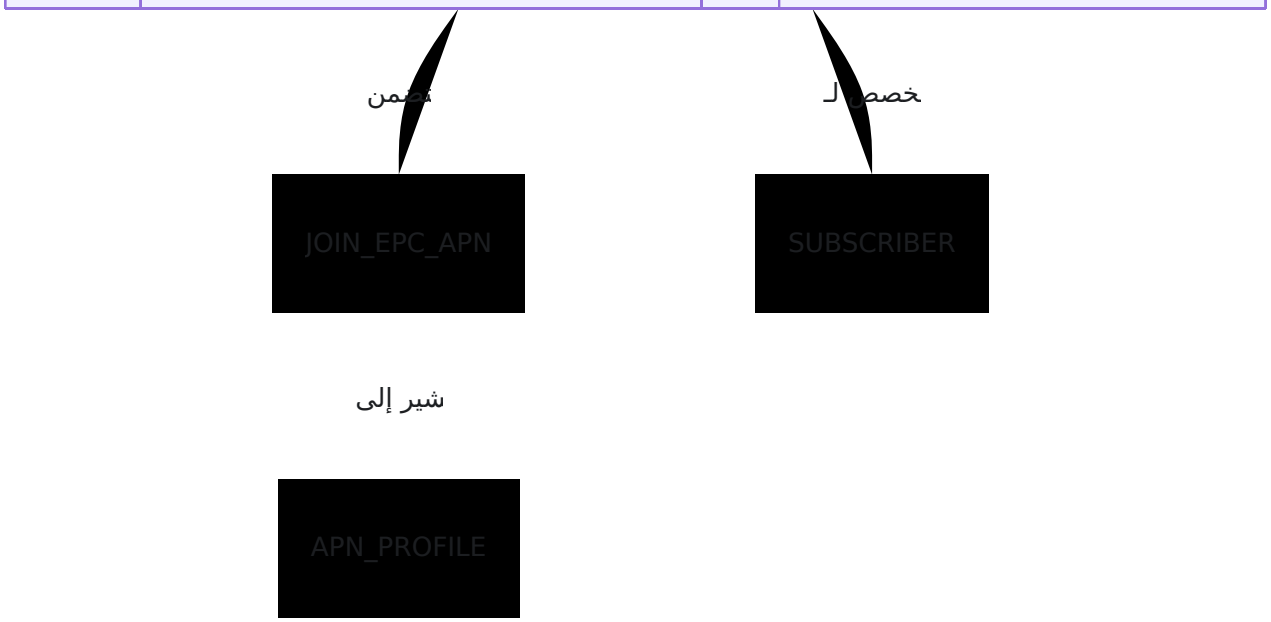


كيانات الملف الشخصي

ملف EPC

ملف يحدد **EPC** خصائص خدمة البيانات لـ LTE.

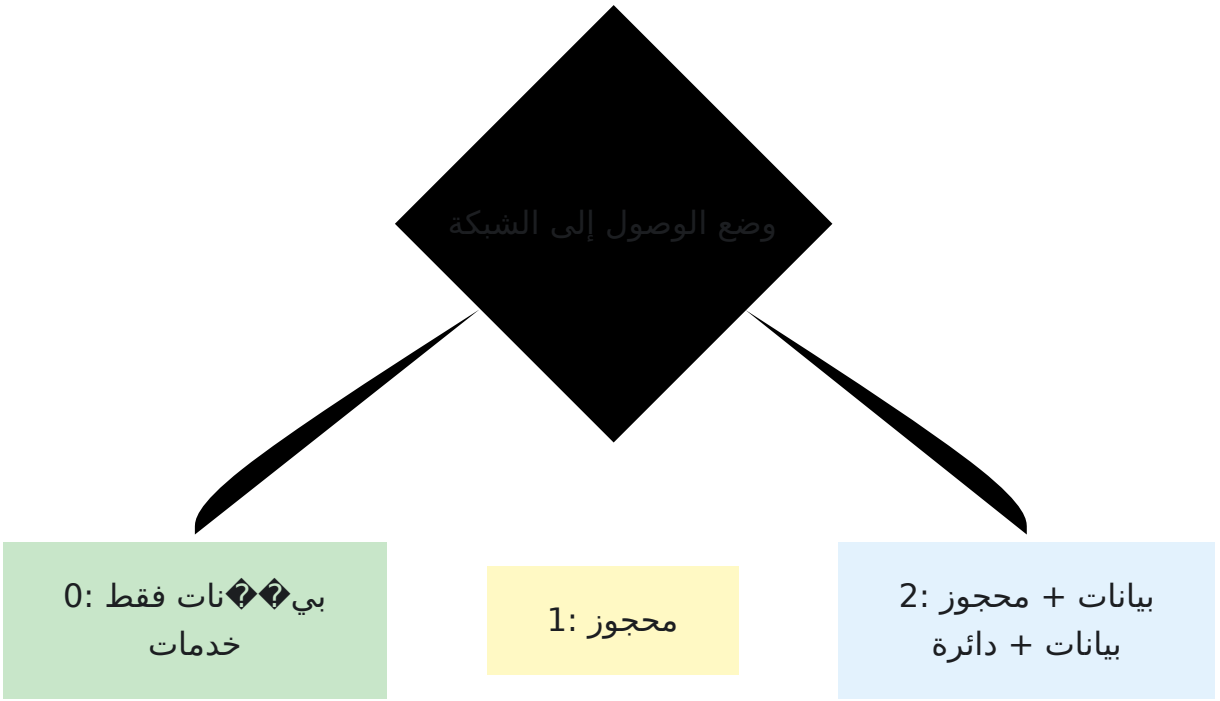
EPC_PROFILE			
uuid	id	PK	
string	name	UK	
integer	ue_ambr_dl_kbps		
integer	ue_ambr_ul_kbps		
string	network_access_mode		packet_only or packet_and_circuit
integer	tracking_area_update_interval_seconds		



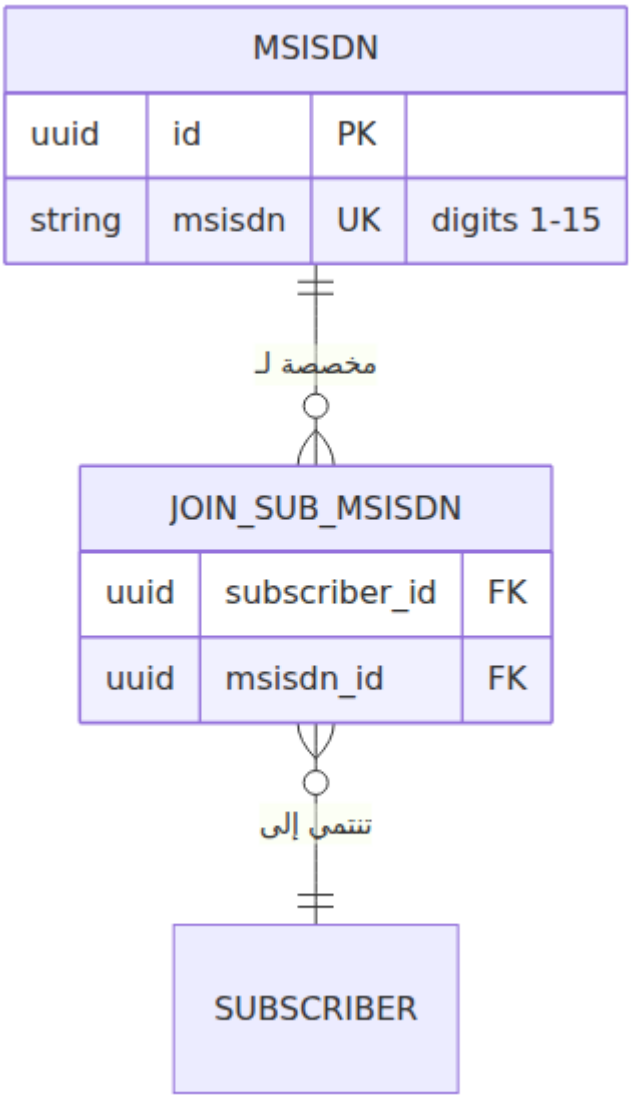
الحقول:

الحقل	النوع	الوصف	وحدات
`name`	string	اسم الملف الشخصي	نص
`ue_ambr_dl_kbps`	integer	حد عرض النطاق الترددي للتنزيل	Kbps
`ue_ambr_ul_kbps`	integer	حد عرض النطاق الترددي للرفع	Kbps
`network_access_mode`	string	قيود الوصول	"packet_onl "packet_and
`tracking_area_update_interval_seconds`	integer	فترة تحديث منطقة التتبع	ثواني

أنماط الوصول إلى الشبكة:



AMBR (معدل البت الأقصى المجمع):



ملف IMS

ملف يحدد **IMS** خصائص خدمة الصوت/الفيديو.

IMS_PROFILE		
uuid	id	PK
string	name	UK
text	ifc_template	

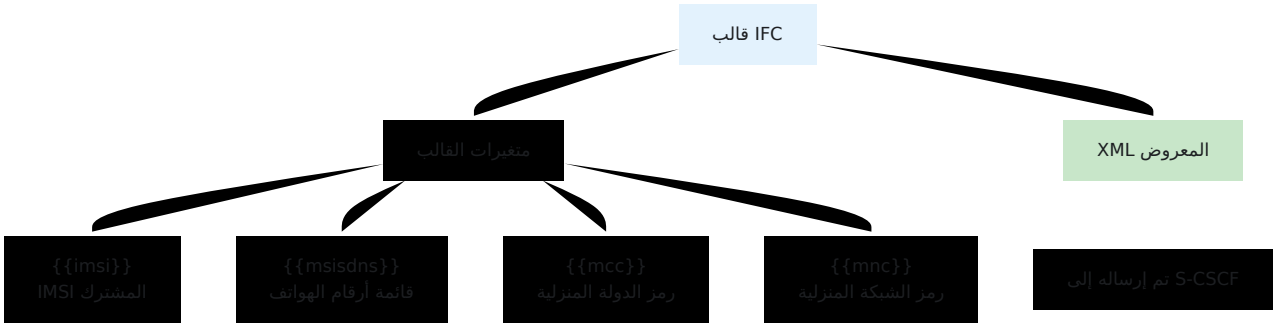
خصص لـ



الحقول:

الحقل	النوع	الوصف	التنسيق
`name`	string	اسم الملف الشخصي	نص
`ifc_template`	text	قالب معايير التصفية الأولية XML	XML مع متغيرات

متغيرات قالب IFC:



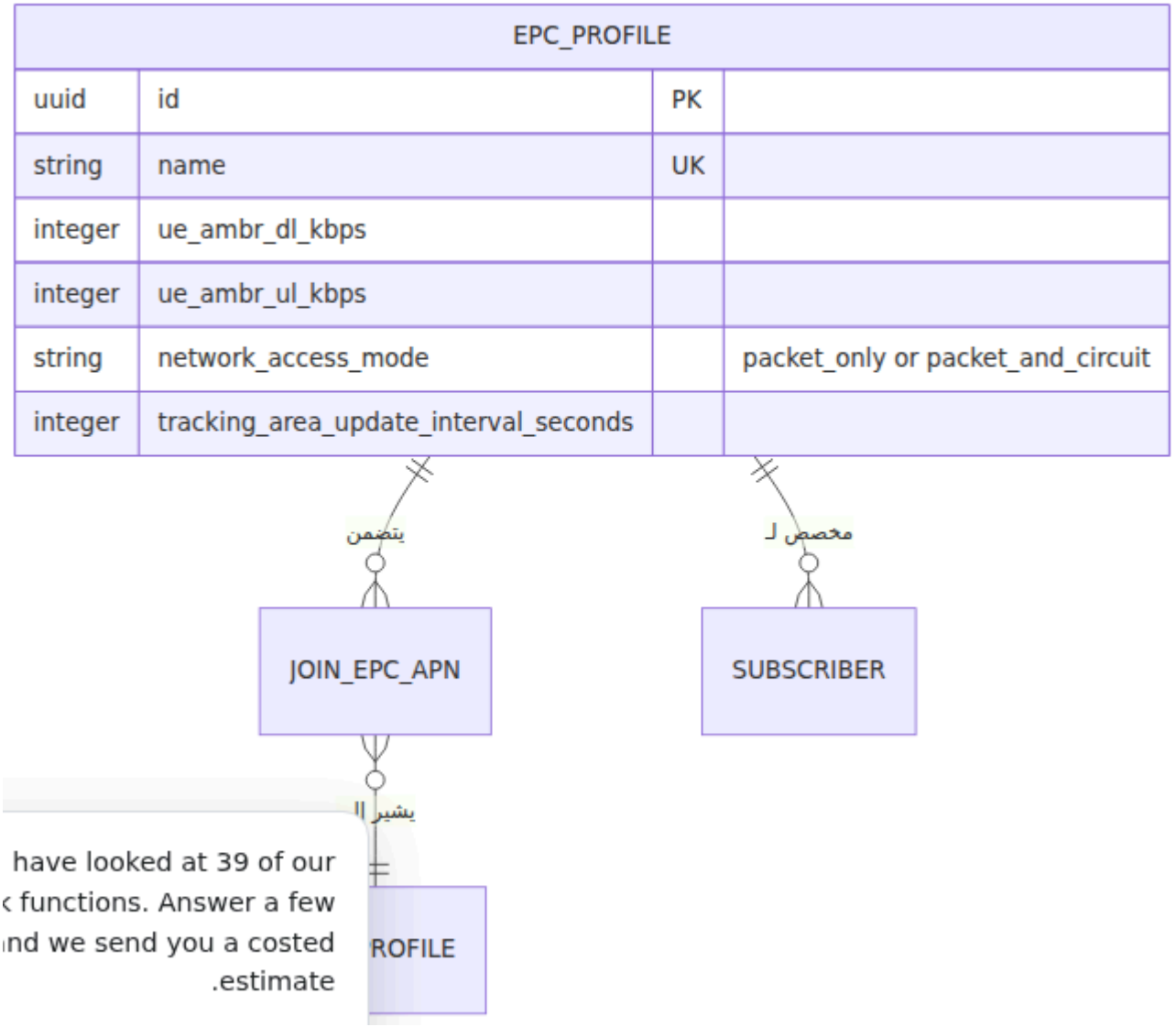
نقاط رئيسية:

- تتحكم IFC (معايير التصفية الأولية) في توجيه المكالمات في IMS
- يتم عرض القالب عند تسجيل المشترك
- يتم استبدال المتغيرات ببيانات المشترك الفعلية

- يتم إرساله إلى S-CSCF أثناء تسجيل IMS

ملف APN

ملف يحدد **APN** خصائص نقطة الوصول المحددة للبيانات.



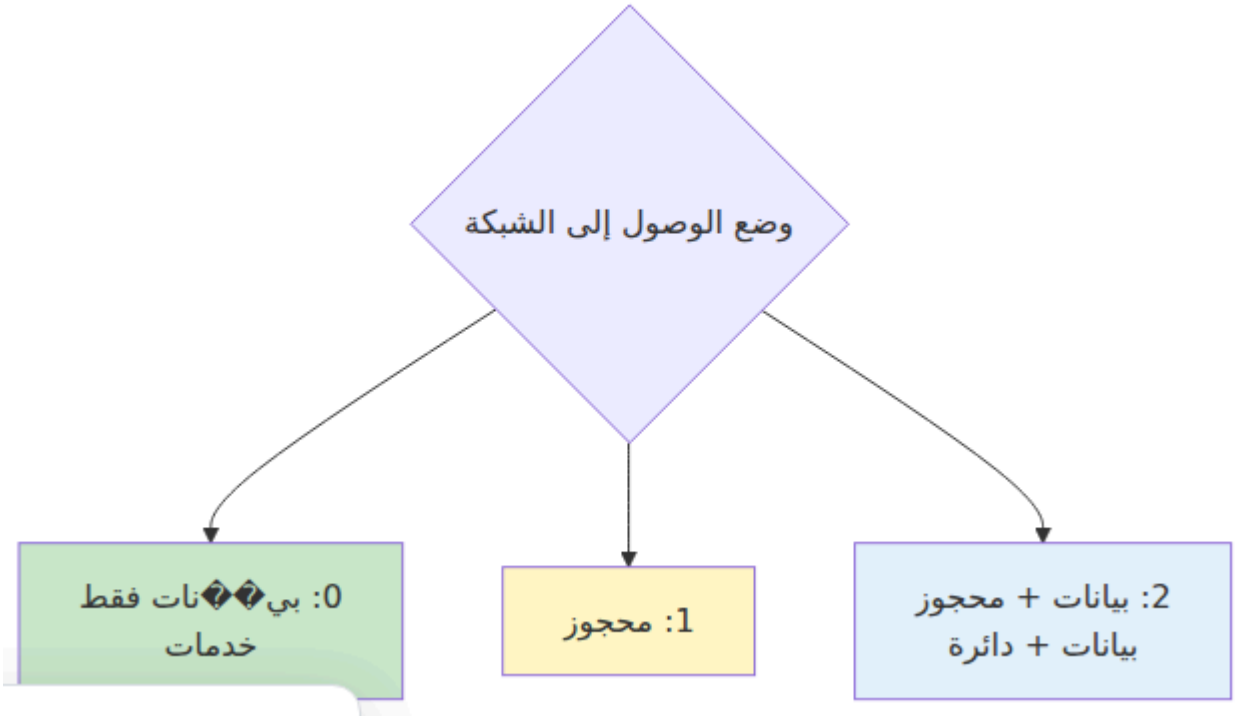
الكيانات ذات ��لصلة:

معرف APN

APN_IDENTIFIER			
uuid	id	PK	
string	apn	UK	
string	ip_version		ipv4, ipv6, ipv4v6, or ipv4_or_ipv6

الحقل	النوع	الوصف	مثال
`apn`	string	اسم APN	"الإنترنت"، "ims"، "mms"
`ip_version`	string	دعم بروتوكول IP	انظر أدناه

خيارات إصدار IP:



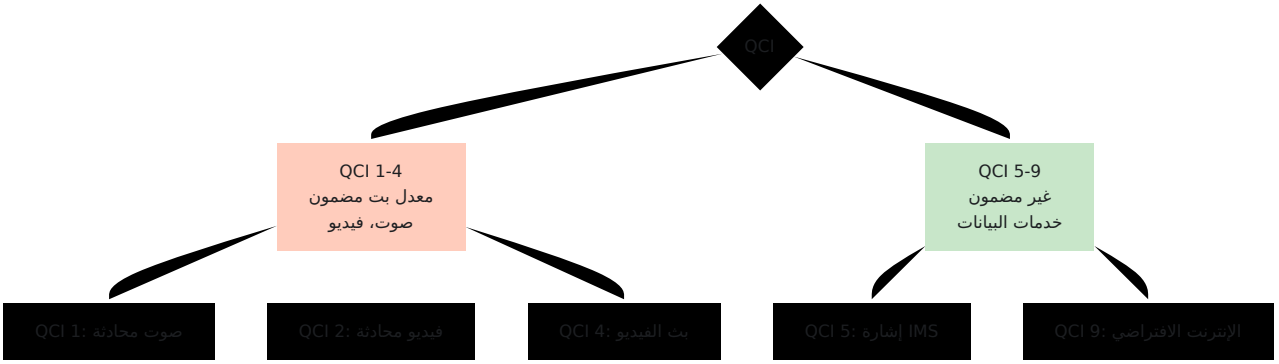
ملف QoS لـ APN

APN_QOS_PROFILE		
uuid	id	PK
string	name	UK
integer	qci	
integer	allocation_retention_priority	
integer	apn_ambr_dl_kbps	
integer	apn_ambr_ul_kbps	
boolean	pre_emption_capability	
boolean	pre_emption_vulnerability	

معلمات QoS:

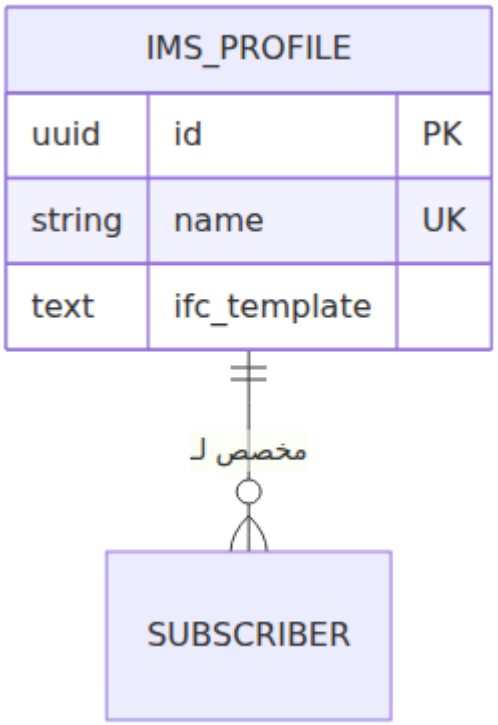
المعلمة	الوصف	النطاق	الناقل الافتراضي
`qci`	معرف فئة QoS	1-9	QCI 9 (الإنترنت)
`allocation_retention_priority`	أولوية ARP	1-15	8 (أولوية أقل)
`apn_ambr_dl_kbps`	حد تنزيل APN	0+	يختلف
`apn_ambr_ul_kbps`	حد رفع APN	0+	يختلف
`pre_emption_capability`	يمكن أن يسبق الآخرين	true/false	false
`pre_emption_vulnerability`	يمكن أن يتم تجاوزه	true/false	true

قيم QCI:



ملف التجوال

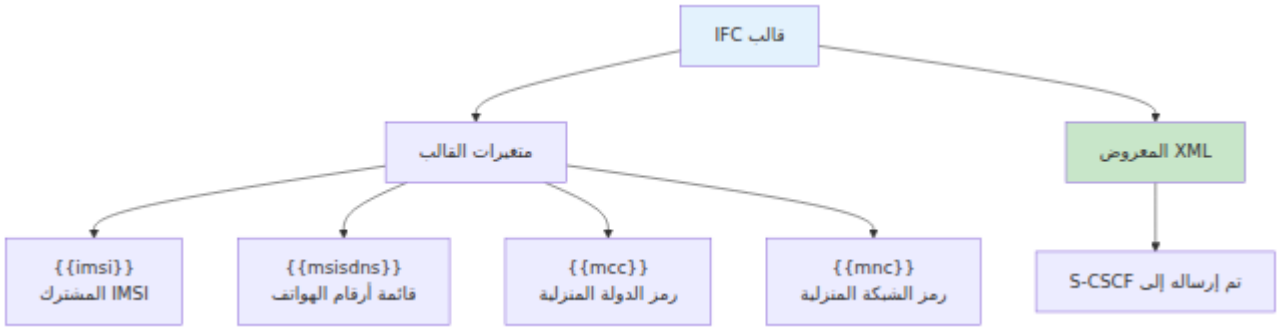
يتحكم **ملف التجوال** في الوصول عندما يزور المشترك شبكات أخرى.



قاعدة التجوال:

ROAMING_RULE			
uuid	id	PK	
string	name	UK	
string	mcc		3 digits
string	mnc		2-3 digits
string	data_action		السماح أو الرفض
string	ims_action		السماح أو الرفض

تقييم القاعدة:



قاعدة EIR

مستقلة وليست EIR قواعد EIR S13. قواعد هوية المعدات التي يتم تقييمها بواسطة وظيفة مرتبطة بمشترك أو ملف شخصي. انظر وثائق EIR.

EIR_RULE			
uuid	id	PK	
string	action		قائمة بيضاء، قائمة سوداء أو قائمة رمادية
string	regex		يتم اختباره ضد IMEISV، ثم IMEI، ثم IMSI
integer	precedence		1-65535، الأقل يتم تقييمه أولاً

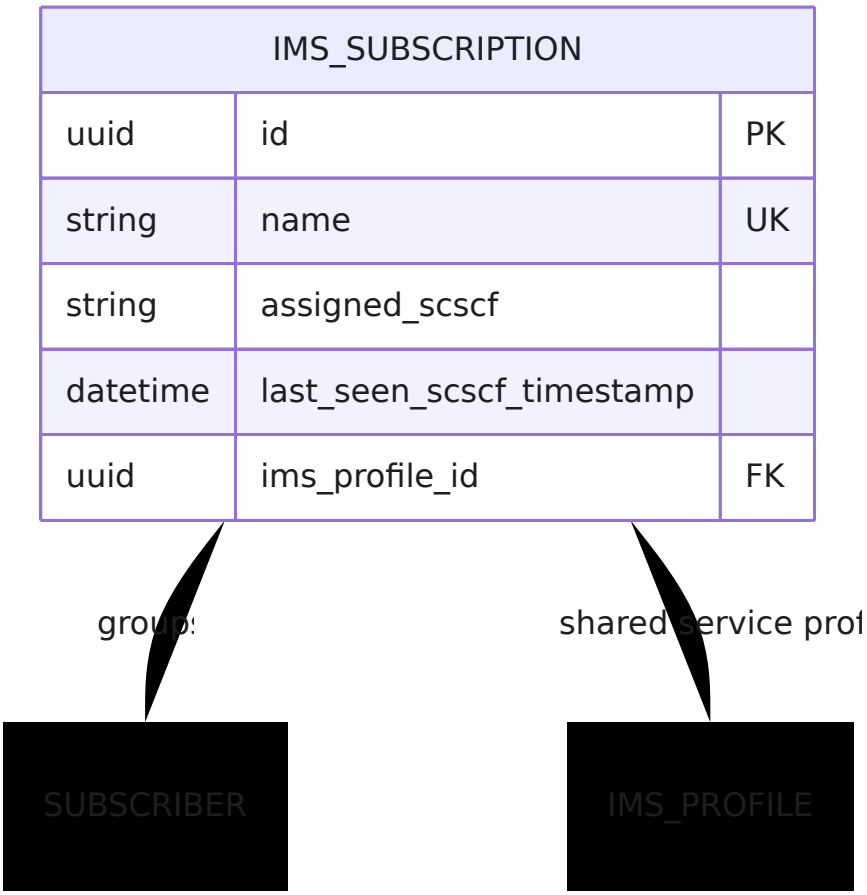
الحقل	النوع	الوصف	مثال
`action`	string	النتيجة المعادة عند تطابق القاعدة	"قائمة سوداء"
`regex`	string	تعبير منتظم يتم اختباره ضد IMEISV، ثم IMEI، ثم IMSI	"359791394616 40"
`precedence`	integer	ترتيب التقييم ضمن كل خطوة مطابقة، الأقل أولاً. احذف عند الإنشاء للإضافة؛ قدم قيمة للإدراج في ذلك الموضع وتحريك القواعد في ذلك الموضع أو بعده لأسفل بمقدار واحد	1

انظر أولوية القاعدة لسلوك الترتيب الكامل.

كيانات الحالة

اشتراك IMS

اشتراك IMS يجمع عدة مشتركين (IMPIs / IMSIs) في اشتراك IMS واحد يشارك هوية (المشتركة IMPU 3GPP TS 23.228) واحد للخدمة S-CSCF مستخدم عامة و استخدمه لخدمة. رقم واحد على عدة أجهزة، على سبيل المثال هاتف وساعة ذكية على شرائح SIM منفصلة.


IMS_SUBSCRIPTION
uuid
id
PK
string
name
UK
string
assigned_scscf
datetime
last_seen_scscf_timestamp
uuid
ims_profile_id
FK
shared service prof
SUBSCRIBER
IMS_PROFILE

الحقول:

الحقل	النوع	الوصف	القيود
`name`	string	اسم قابل للقراءة البشرية	مطلوب، فريد
`assigned_scscf`	string	S-CSCF المشتركة للخدمة للمجموعة	حالة وقت التشغيل، يتم تعيينها بواسطة HSS
`last_seen_scscf_timestamp`	datetime	متى تم كتابة S-CSCF المشتركة آخر مرة	حالة وقت التشغيل
`ims_profile_id`	uuid	ملف تعريف الخدمة المشتركة الاختياري لهويات المجموعة المشتركة	اختياري

نقاط رئيسية:

- الأعضاء يشيرون إلى المجموعة عبر `subscriber.ims_subscription_id`.
- يقوم HSS بتعيين S-CSCF واحدة عند تسجيل العضو الأول ويقوم بإلغاء تعيينها عند إلغاء تسجيل العضو الأخير. لا تقم بتعيين `assigned_scscf` بنفسك.
- عندما يتم تعيين `ims_profile_id`، يقوم IMS بعرض ملف تعريف الخاص بالمجموعة على الهويات المشتركة؛ بخلاف ذلك، يقوم كل عضو بعرض ملف تعريف IMS الخاص به.
- لا يحذف مشتركيه؛ يتم مسح IMS حذف اشتراك `ims_subscription_id` الخاص بهم.

انظر إلى الهوية العامة للمستخدم المشترك للحصول على النموذج الكامل والت provisioning.

حالة المشترك

تتبع **حالة المشترك** حالة المشترك في الوقت الحقيقي.

APN_IDENTIFIER			
uuid	id	PK	
string	apn	UK	
string	ip_version		ipv4, ipv6, ipv4v6, or ipv4_or_ipv6

الحقول الرئيسية:

معلومات الموقع:

- `last_seen_mcc`, `last_seen_mnc` - الشبكة التي تمت زيارتها
- `last_seen_tac` - رمز منطقة التتبع
- `last_seen_cell_id` - معرف الخلية
- `last_seen_enodeb_id` - معرف eNodeB
- `last_seen_eci` - معرف خلية E-UTRAN

عناصر الشبكة:

- `last_seen_mme` - MME الحالي الذي يخدم المشترك
- `last_seen_realm` - مجال Diameter لـ MME
- `last_seen_rat_type` - تقنية الوصول اللاسلكي (LTE، 5G، إلخ.)

معلومات IMS:

- `assigned_scscf` - S-CSCF الحالي الذي يخدم المشترك
- `ims_public_identity` - SIP URI (مثل، sip:+14155551234@ims.example.com)
- `sh_repository_data` - بيانات ملف IMS مخصصة

المعدات:

- `last_seen_imei` - معلومات الطرفية لـ AVP الذي تم الإبلاغ عنه آخر مرة في IMEI S13 ECR أو S6a ULR
- `last_seen_imei_software_version` - إصدا�� البرنامج المبلغ عنه مع ذلك IMEI (IMEISV = IMEI + إصدار البرنامج)؛ يتم الاحتفاظ به من التقرير السابق عندما بدون واحد IMEI يصل نفس

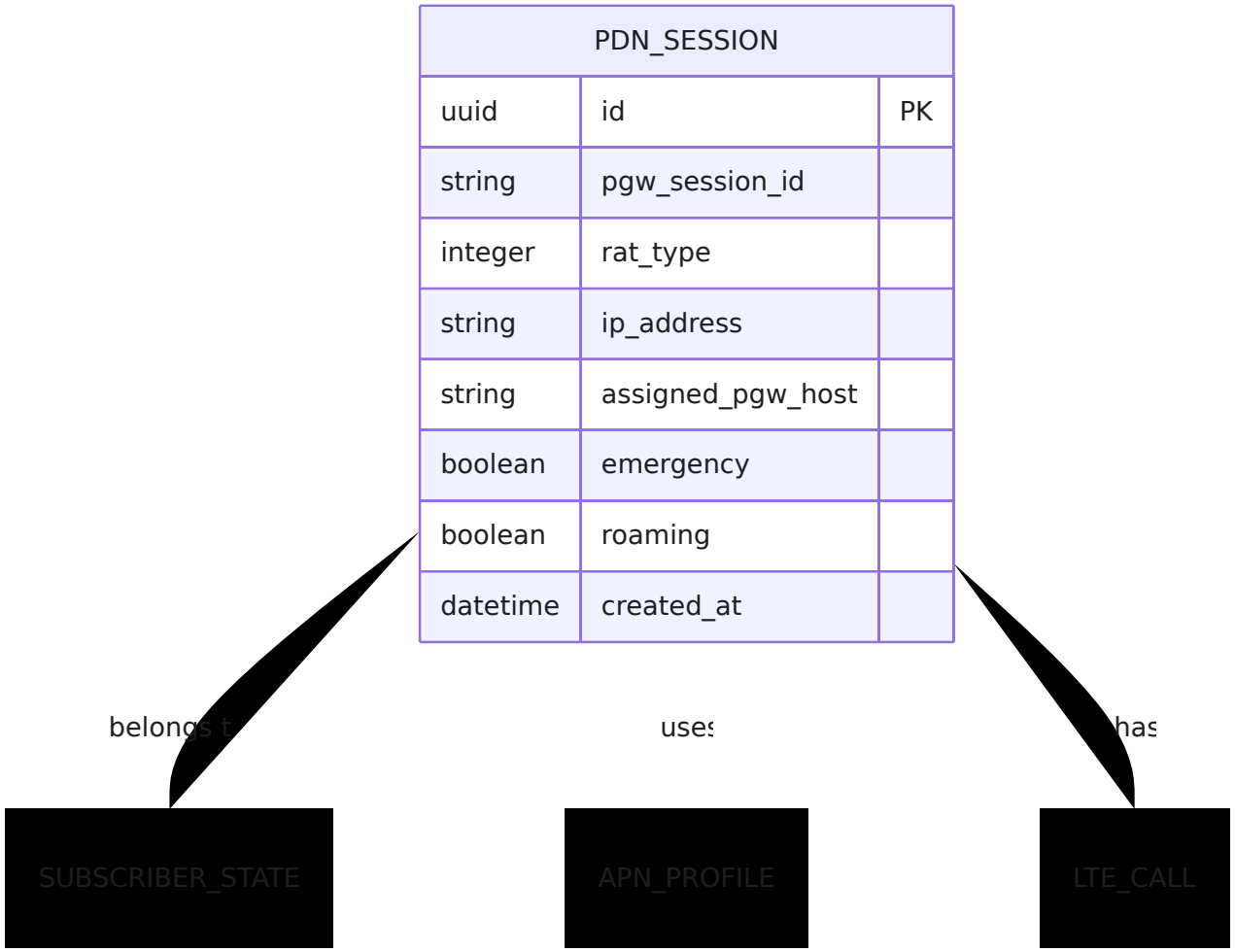
- `last_seen_imei_timestamp` - آخر مرة IMEI متى تم الإبلاغ عن

الطوابع الزمنية:

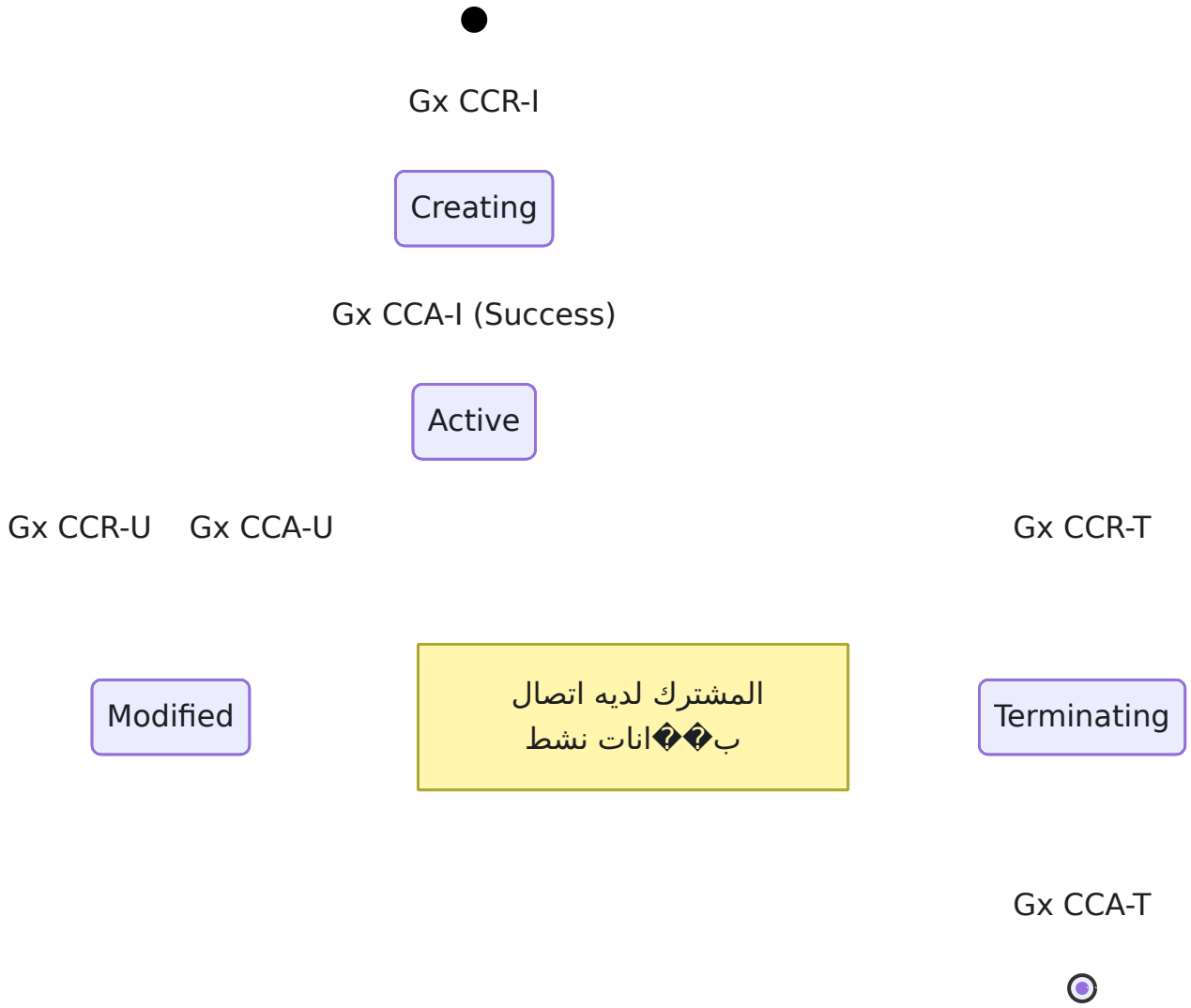
- `last_seen_at` - آخر رسالة Diameter تم استلامها
- الطوابع الزمنية لإجراءات مختلفة `last_*_at` مختلف

جلسة PDN

جلسة تمثل **PDN** اتصال البيانات النشط.



دورة حياة جلسة PDN:

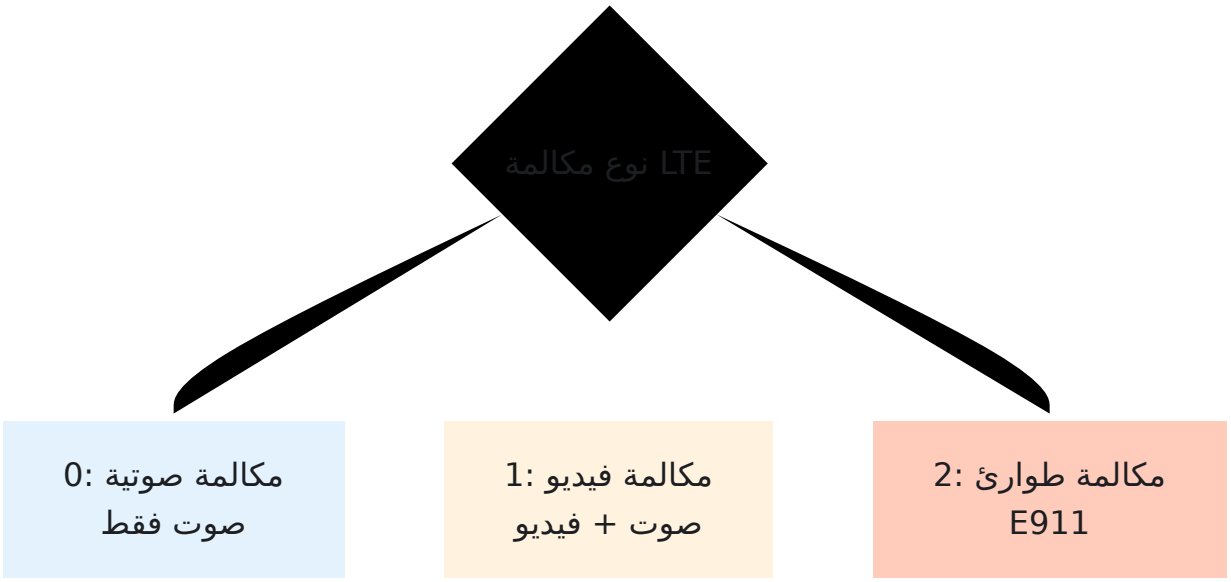


مكالمة LTE

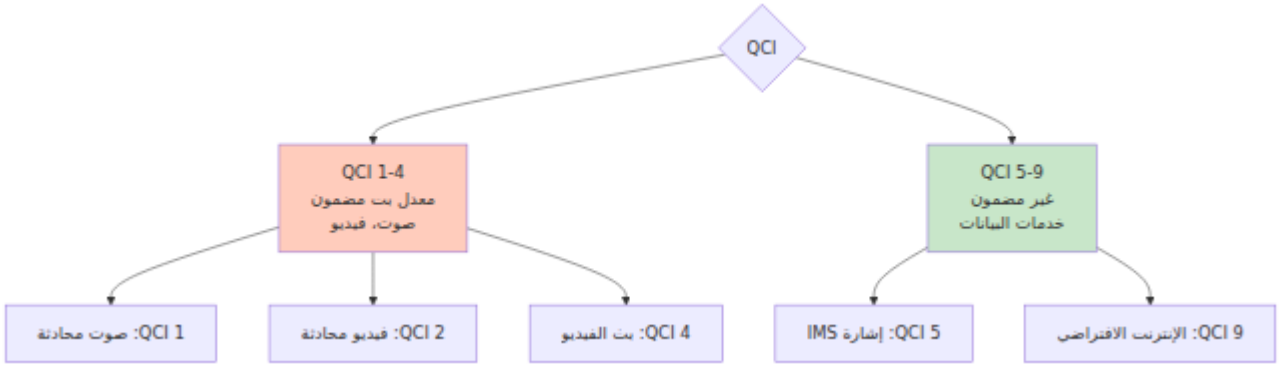
مكالمة تمثل **LTE** مكالمة صوتية/فيديو VoLTE النشطة.

APN_QOS_PROFILE		
uuid	id	PK
string	name	UK
integer	qci	
integer	allocation_retention_priority	
integer	apn_ambr_dl_kbps	
integer	apn_ambr_ul_kbps	
boolean	pre_emption_capability	
boolean	pre_emption_vulnerability	

أنواع المكالمات:

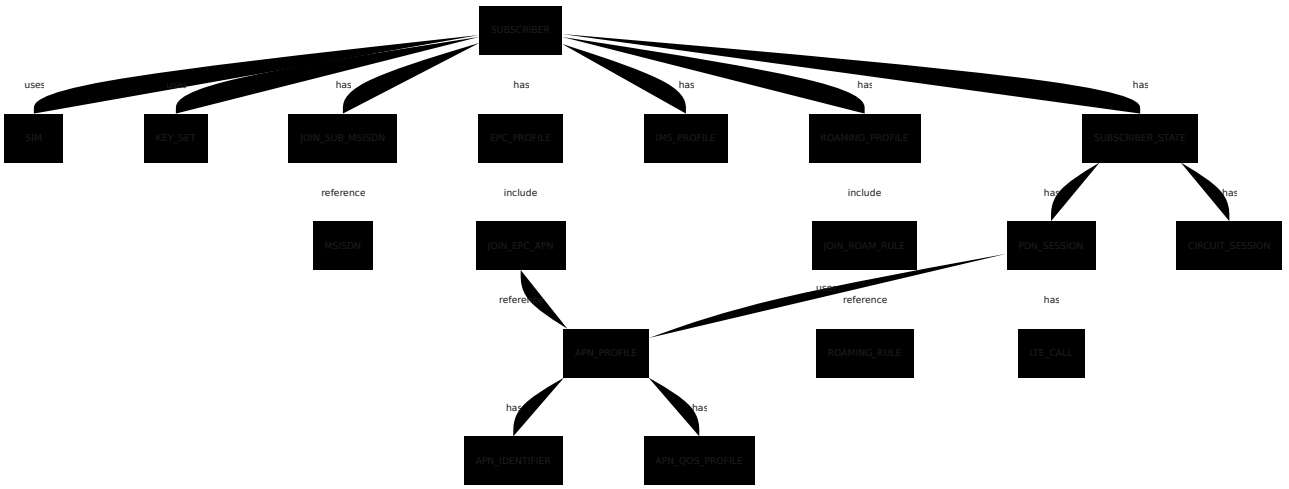


تدفق مكالمة VoLTE:



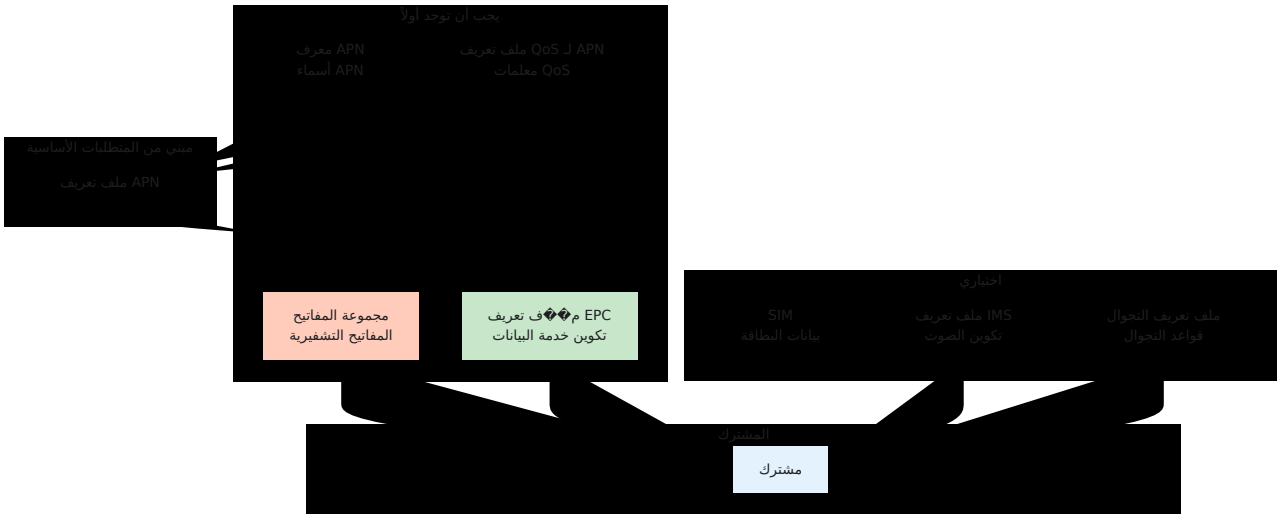
مخططات العلاقة الكيانية

العلاقات الكيانية الكاملة



علاقات التكوين

يوضح هذا المخطط ما يجب أن يوجد قبل إنشاء مشترك:

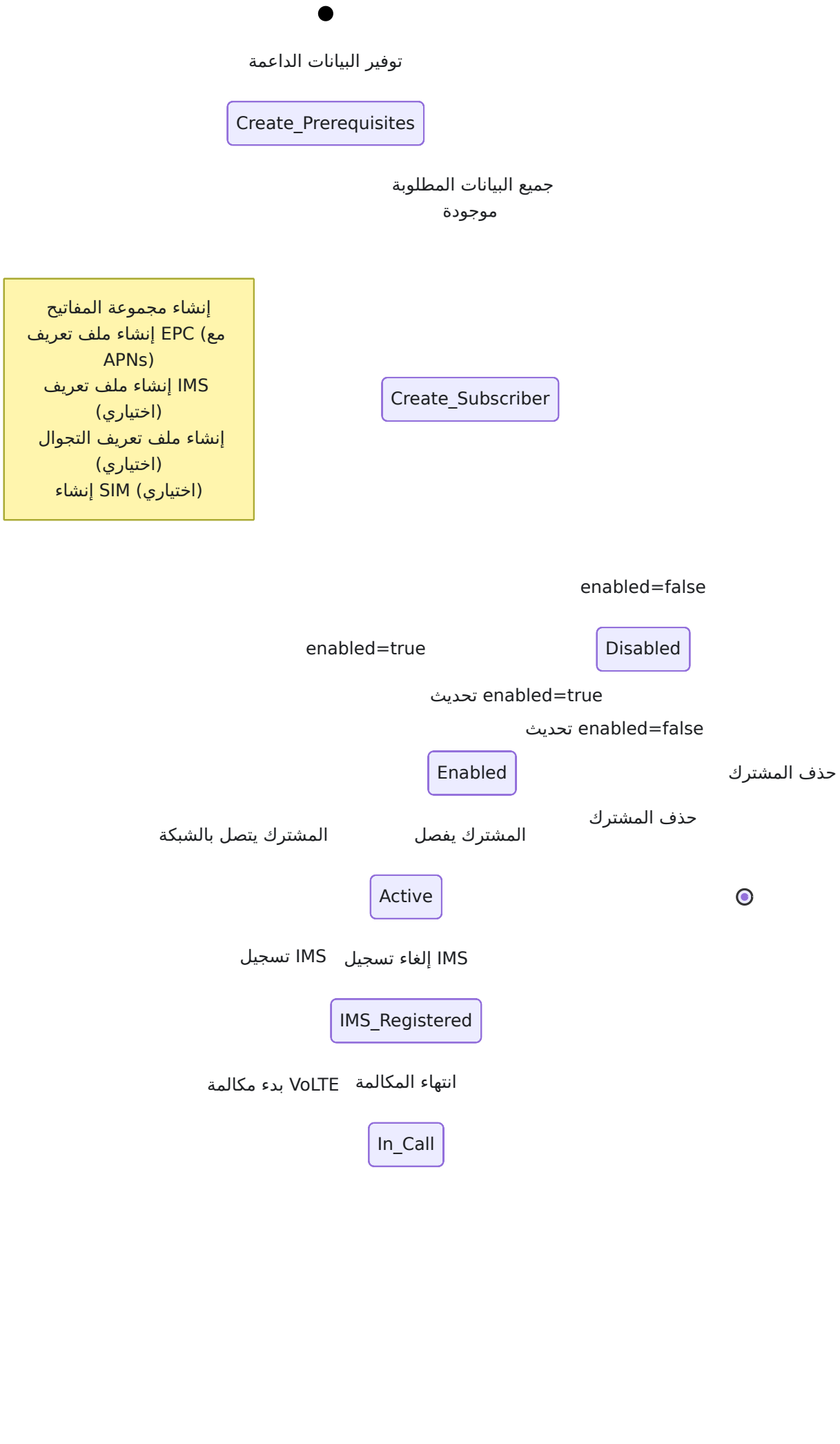


علاقات حالة الجلسة

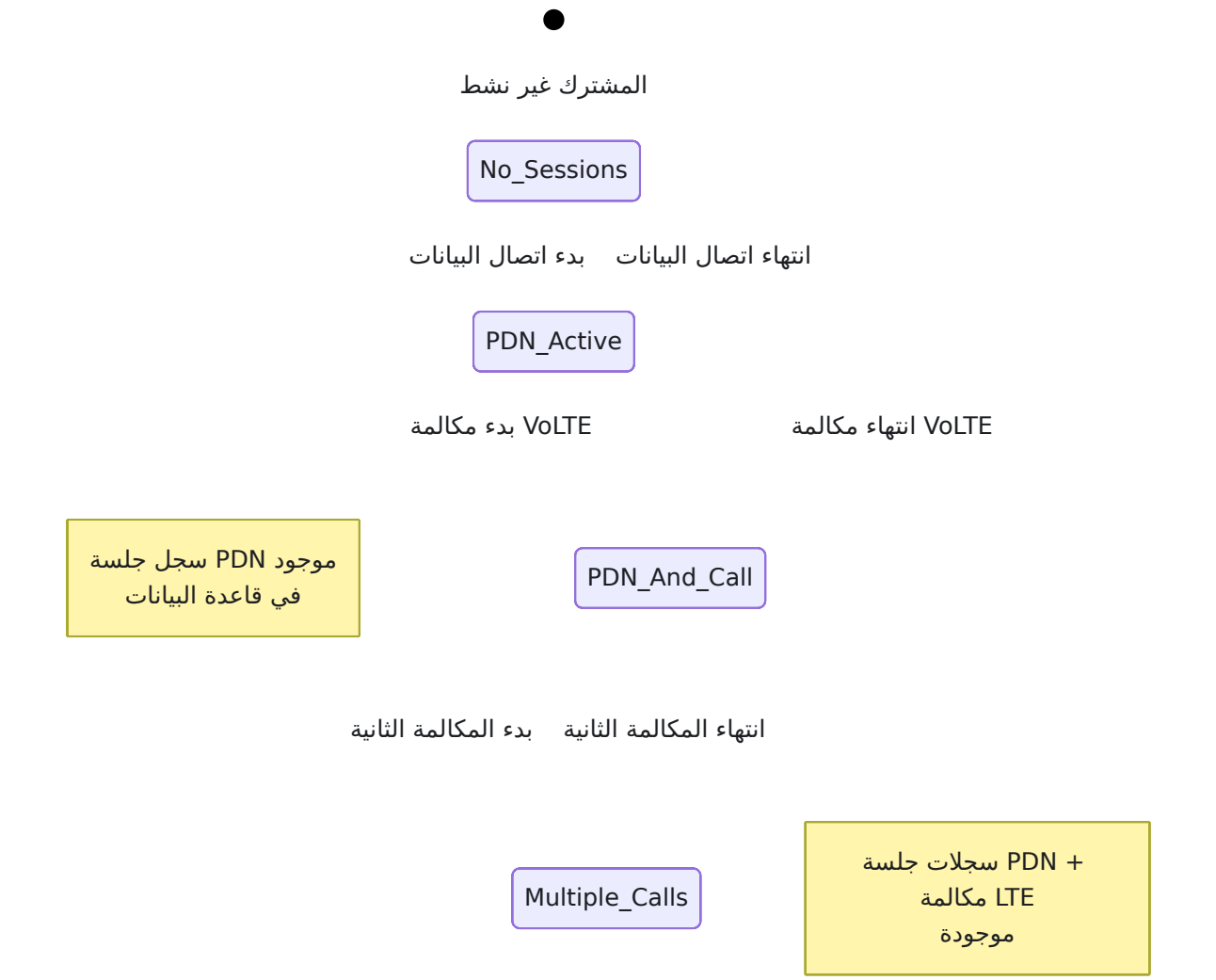
ROAMING_RULE			
uuid	id	PK	
string	name	UK	
string	mcc		digits 3
string	mnc		digits 2-3
string	data_action		السماح أو الرفض
string	ims_action		السماح أو الرفض

دورة حياة الكيان

دورة حياة تكوين المشترك


توفير البيانات الداعمة
Create_Prerequisites
جميع البيانات المطلوبة
موجودة
إنشاء مجموعة المفاتيح
إنشاء ملف تعريف EPC (مع APNs)
إنشاء ملف تعريف IMS (اختياري)
إنشاء ملف تعريف التجوال (اختياري)
إنشاء SIM (اختياري)
Create_Subscriber
enabled=false
Disabled
enabled=true
تحديث enabled=true
تحديث enabled=false
Enabled
حذف المشترك
حذف المشترك
المشترك يفصل
المشترك يتصل بالشبكة
Active
إلغاء تسجيل IMS
تسجيل IMS
IMS_Registered
انتهاء المكالمة
بدء مكالمة VoLTE
In_Call

دورة حياة الجلسة

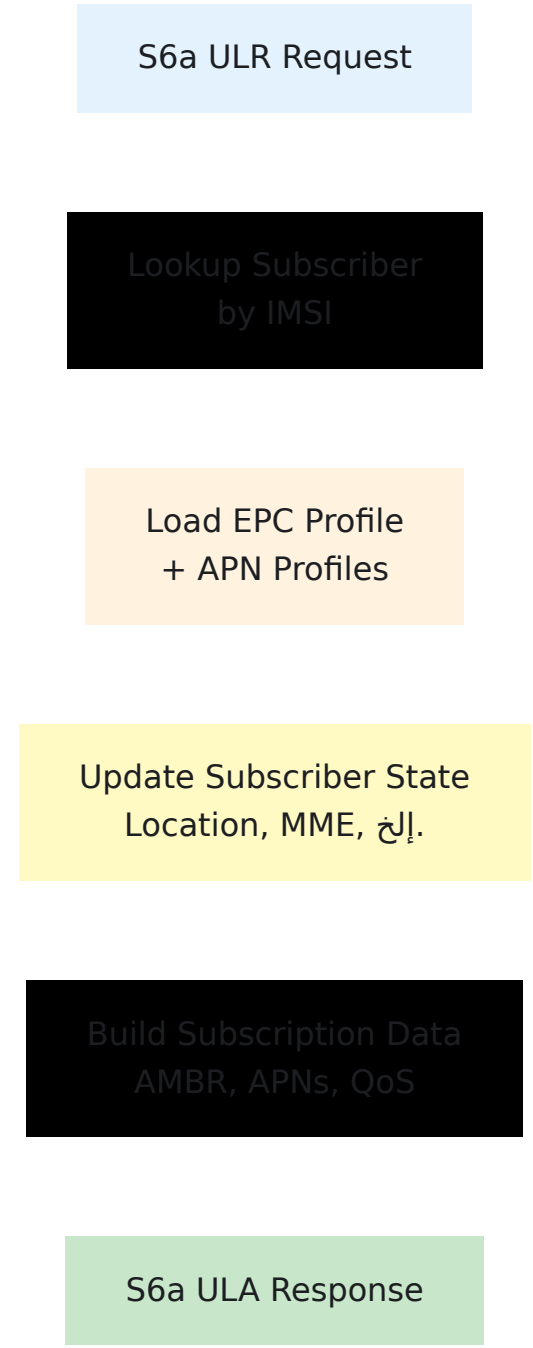


أنماط تدفق البيانات

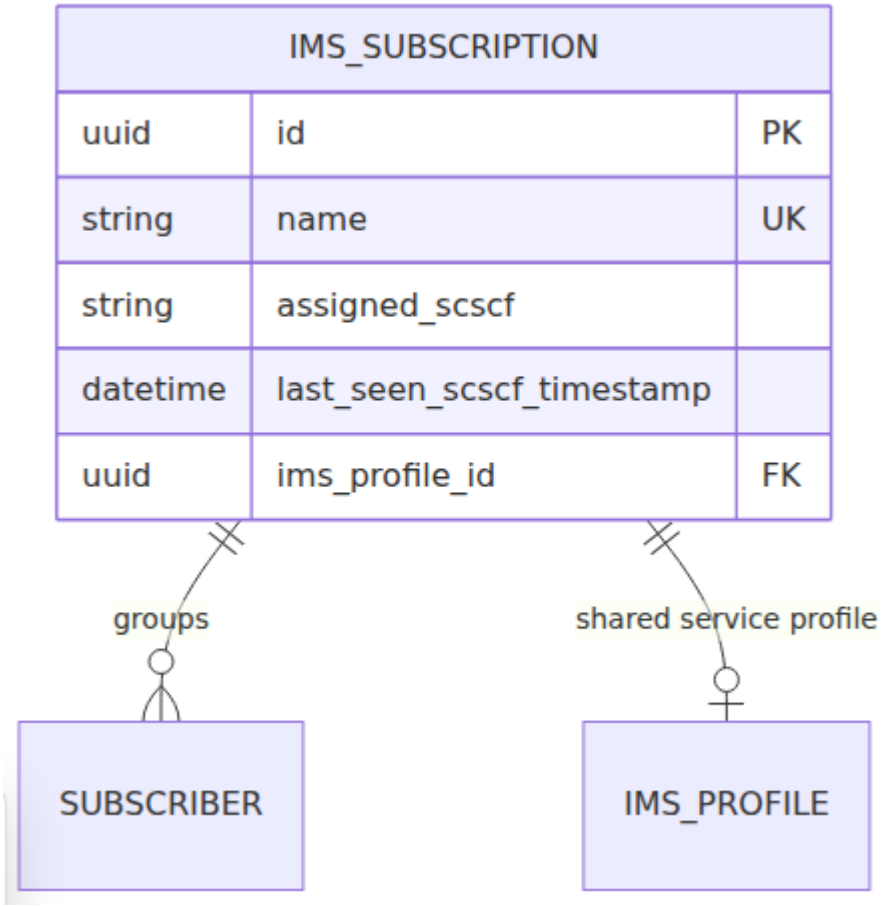
تدفق المصادقة

EIR_RULE			
uuid	id	PK	
string	action		قائمة بيضاء، قائمة سوداء أو قائمة رمادية
string	regex		يتم اختباره ضد IMEISV، ثم IMEI، ثم IMSI
integer	precedence		1-65535، الأقل يتم تقييمه أولاً

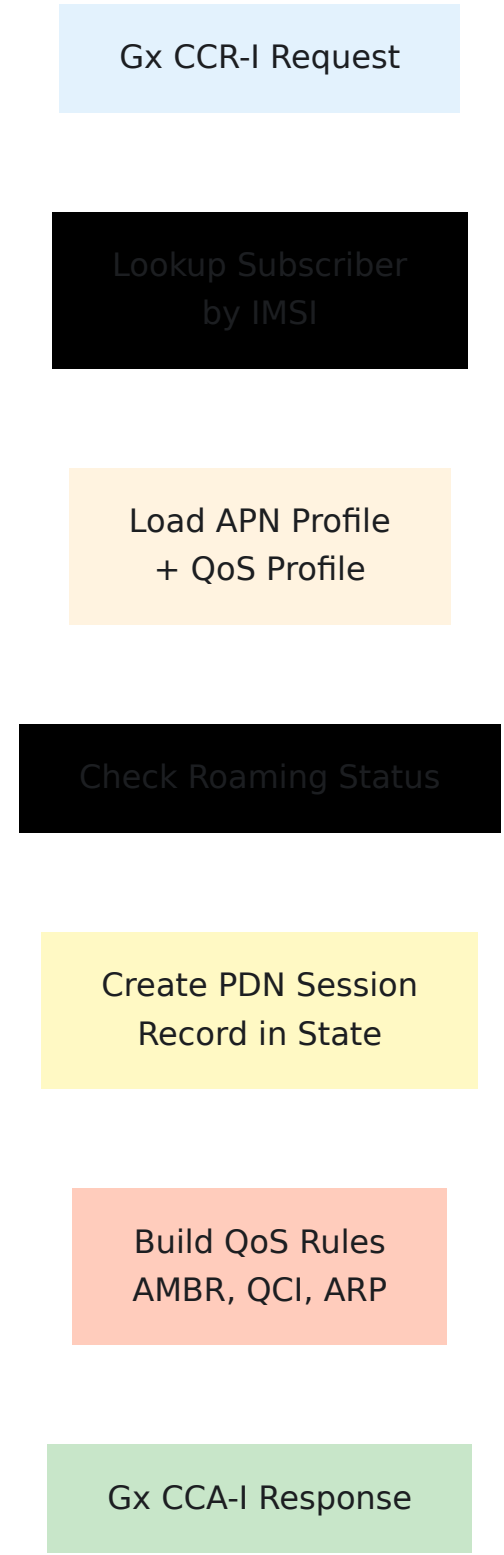
تدفق تحديث ��لموقع



تدفق تسجيل IMS



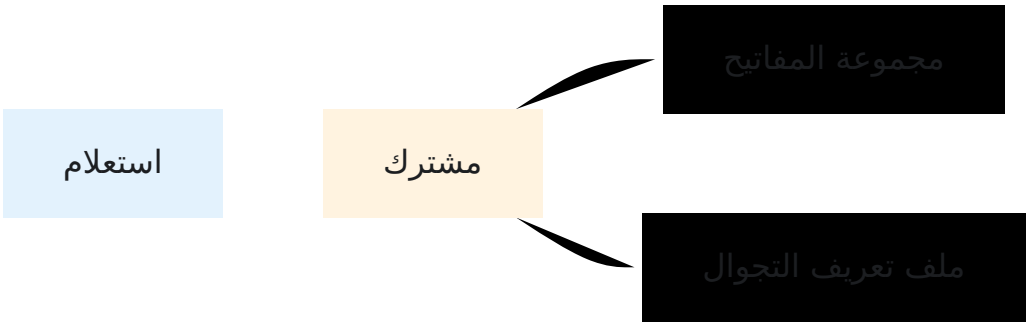
تدفق إنشاء الجلسة



أنماط تحسين الاستعلامات

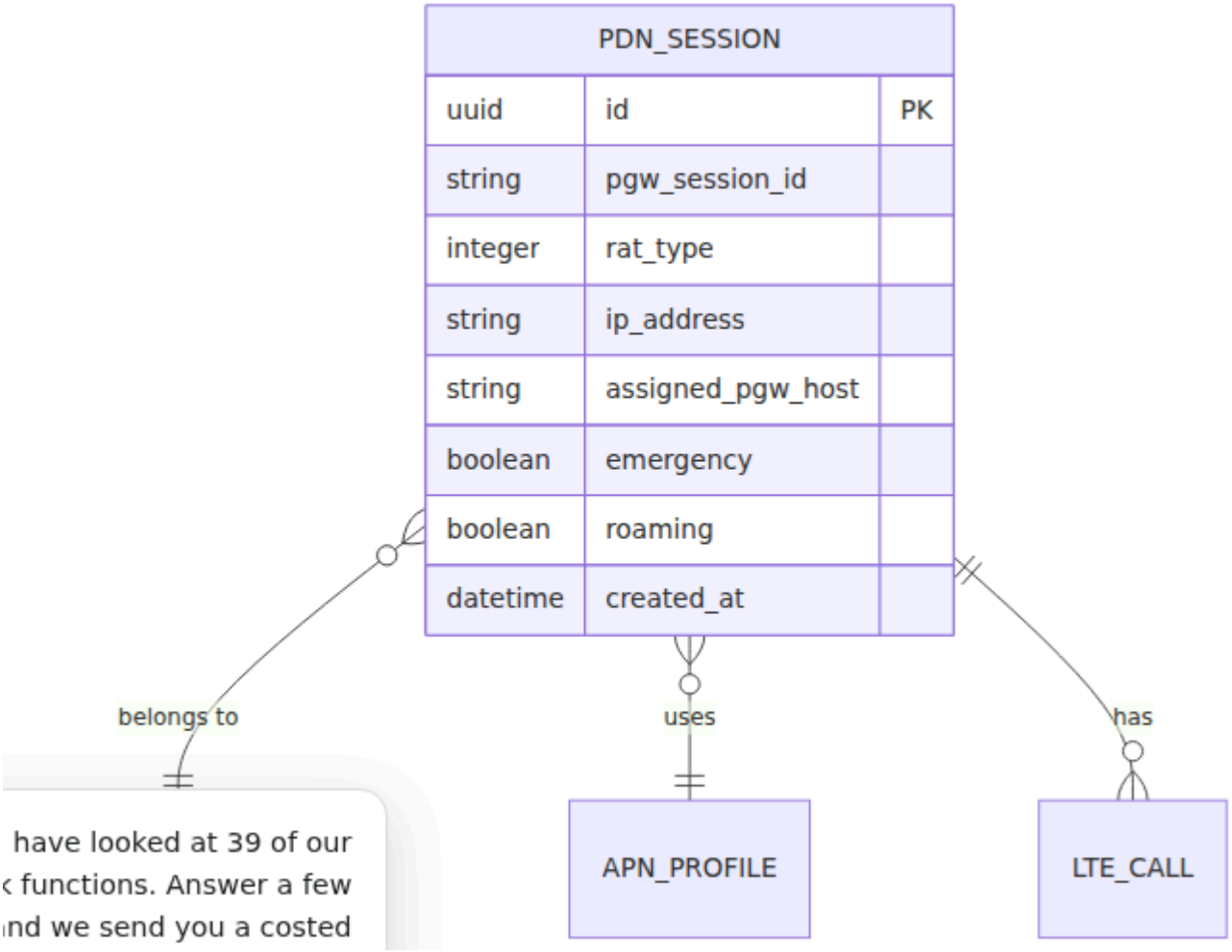
يقوم OmniHSS بتحسين استعلامات قاعدة البيانات عن طريق تحميل فقط الجمعيات اللازمة لكل عملية بشكل انتقائي:

استعلام الحد الأدنى (المصادقة)



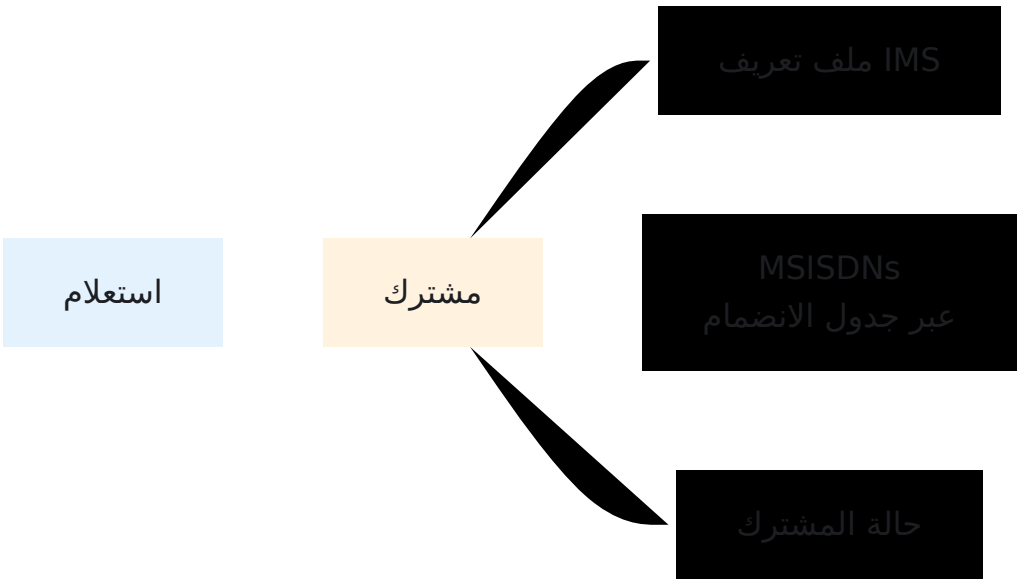
حالة الاستخدام: S6a AIR - يحتاج فقط إلى مفاتيح التشفير وقواعد التجوال

استعلام معتدل (تحديث الموقع)



حالة الاستخدام: S6a ULR - يحتاج إلى بيانات ملف تعريف EPC كاملة

استعلام كامل (تسجيل IMS)



حالة الاستخدام: Cx SAR - يحتاج إلى ملف تعريف IMS وجميع أرقام الهواتف

← التالي: مرجع | العودة إلى دليل العمليات API →

رسم بيانات استجابة القطر

← العودة إلى دليل العمليات

يوفر هذا المستند مخططات ميرميد تفصيلية توضح من أين يتم الحصول على كل حقل في استجابات بروتوكول القطر من نظام OmniHSS.

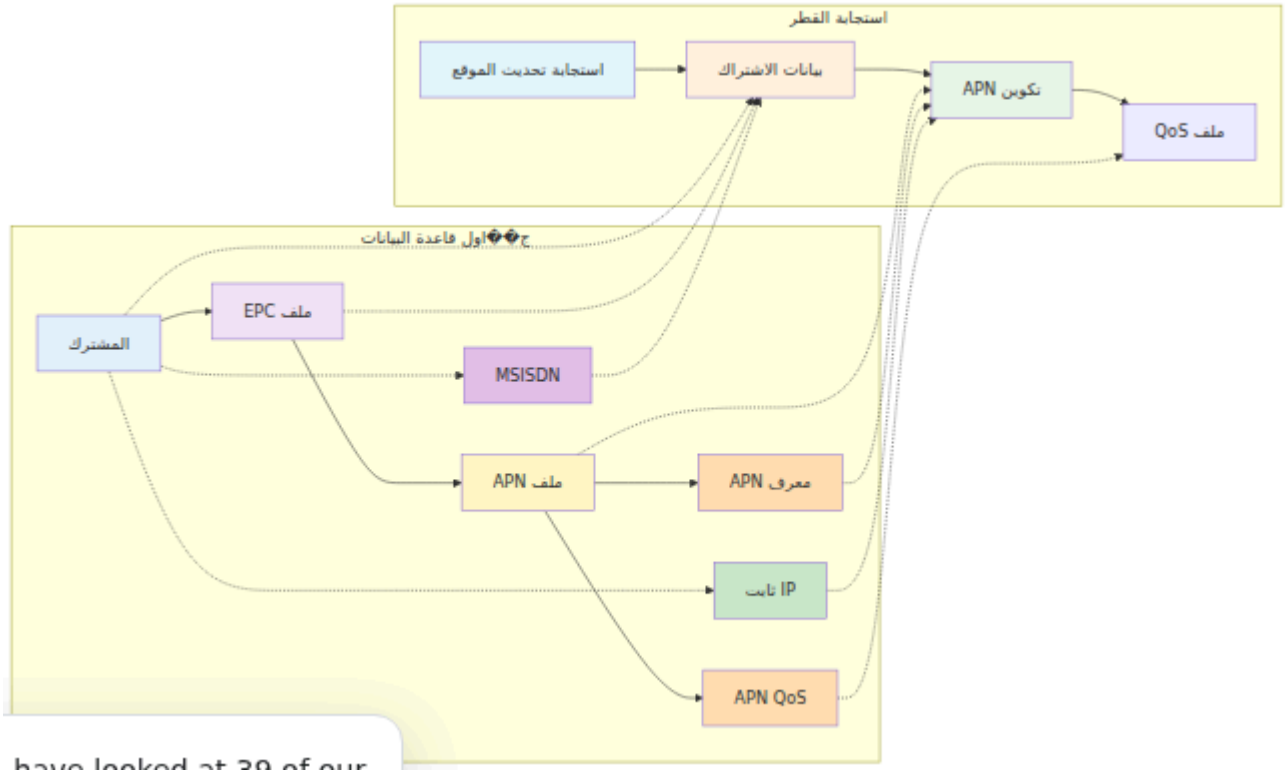
جدول المحتويات

- استجابة تحديث الموقع (S6a ULA)
- استجابة معلومات المصادقة (S6a AIA)
- استجابة تعيين الخادم (Cx SAA)
- استجابة التحكم في الائتمان (Gx CCA)
- استجابة بيانات المستخدم (Sh UDA)
- استجابة تحقق هوية ME (S13 ECA)

استجابة تحديث الموقع (S6a ULA)

يتم إرسال استجابة تحديث الموقع من HSS إلى MME خلال إجراءات الاتصال LTE. توضح هذه المخططات تدفق البيانات الكامل من جداول قاعدة البيانات إلى AVPs القطرية.

رسم مصدر البيانات



رسم الحقول بالتفصيل

مصدر قاعدة البيانات	الحقل	A
subscriber.enabled	`true/false`	Su St
msisdn.msisdn	`'14155551234'`	MS
epc_profile.ue_ambr_ul_kbps	`50000`	Ma Re Ba UL
epc_profile.ue_ambr_dl_kbps	`100000`	Ma Re Ba DL
epc_profile.network_access_mode	`'packet_only'`	Ne Ac Mo
apn_identifier.apn	`'internet'`	Se Se
apn_identifier.ip_version	`'ipv4v6'`	PD
apn_qos_profile.qci	`9`	Qo Id
apn_qos_profile.allocation_retention_priority	`8`	Pr Le

مصدر قاعدة البيانات	الحقل	A
apn_qos_profile.pre_emption_capability	`false`	Pr en Ca
apn_qos_profile.pre_emption_vulnerability	`true`	Pr en Vu
apn_qos_profile.apn_ambr_ul_kbps	`25000`	AP UL
apn_qos_profile.apn_ambr_dl_kbps	`50000`	AP DL
static_ip.ipv4_static_ip	`'100.64.1.1'`	Se Pa Ad (IP
static_ip.ipv6_static_ip	`'2606:4700::1111'`	Se Pa Ad (IP

التحويلات الرئيسية:

1. **عرض النطاق الترددي AMBR**: تخزن قاعدة البيانات بالـ kbps، ويتوقع القطر بالـ bps (مضاعفة بـ 1000)
2. **ترميز إصدار IP**: `0=IPv4, 1=IPv6, 2=IPv4v6, 3=IPv4_or_IPv6`
3. **حالة المشترك**: `enabled: true → 0 (SERVICE_GRANTED)`, `enabled: false → 1 (OPERATOR_DETERMINED_BARRING)`
4. **معرف السياق**: ترقيم تسلسلي (0، 1، 2...) لكل APN في الملف الشخصي
5. **الثابت IP**: يتم تضمينه فقط إذا تم تعيينه عبر علاقة `static_ips` العديد إلى العديد

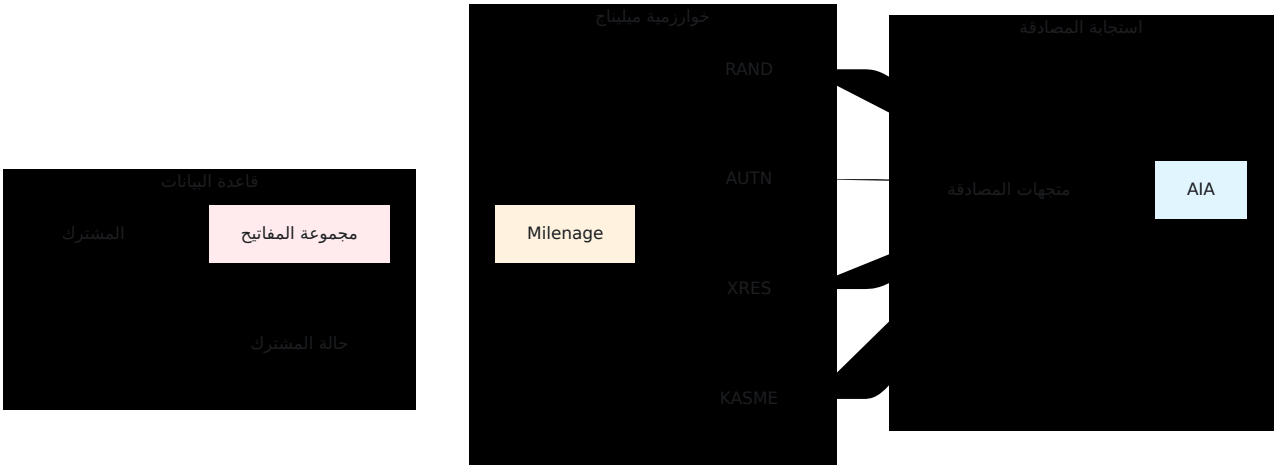
تحقق من منطق الأعمال:

- التي تمت زيارتها مع PLMN تحقق من التجوال: مطابقة `roaming_profile.roaming_rules`
- تحقق من تمكين المشترك: `subscriber.enabled == true`
- تصفية APNs: قد يتم استبعاد APNs IMS إذا كانت سياسة التجوال تمنع IMS

استجابة معلومات المصادقة (S6a AIA)

توفر استجابة معلومات المصادقة متجهات المصادقة لمشتركي LTE/EPC.

رسم مصدر البيانات



المكونات الرئيسية:

1. **المفاتيح التشفيرية** `key_set`: جميع المفاتيح مخزنة كسلاسل سداسية في جدول
2. **إدارة SQN**: يتم زيادة رقم التسلسل بعد كل توليد لمتجه المصادقة (يمنع هجمات إعادة التشغيل)
3. **خوارزمية ميليناج**: 3GPP TS 35.206 - تولد متجهات المصادقة
4. **اشتقاق KASME**: مفتاح مشتق من CK||IK باستخدام KDF وفقًا لـ TS 33.401

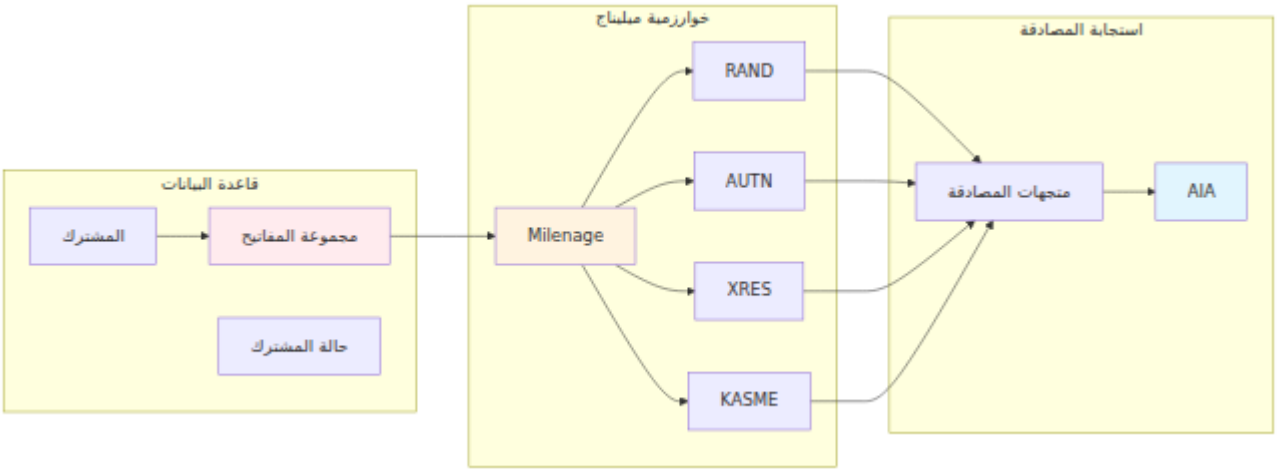
ميزات الأمان:

- يتم تخزين SQN (ليس عالميًا) لكل مشترك
- لا تترك Ki/OPc HSS (فقط القيم المشتقة تُنقل) أبدًا
- يتضمن AUTN رقم التسلسل (SQN) وAMF لمصادقة الشبكة
- توفر خوارزمية ميليناج مصادقة متبادلة بين UE والشبكة

استجابة تعيين الخادم (Cx SAA)

يتم إرسال استجابة تعيين الخادم من HSS إلى S-CSCF خلال تسجيل IMS.

رسم مصدر البيانات



الميزات الرئيسية:

1. **قالب IFC**: قالب XML مخزن في `ims_profile.ifc_template`
2. **استدال ديناميكي**: يستبدل `{{msisdn}}`، `{{imsi}}`، `{{impu}}` في وقت التشغيل
3. **تعيين S-CSCF**: يخزن S-CSCF المعين في `subscriber_state.assigned_scscf`
4. **الهوية العامة IMS**: التنسيق: `sip:+{msisdn}@{ims_domain}` أو `tel:+{msisdn}`

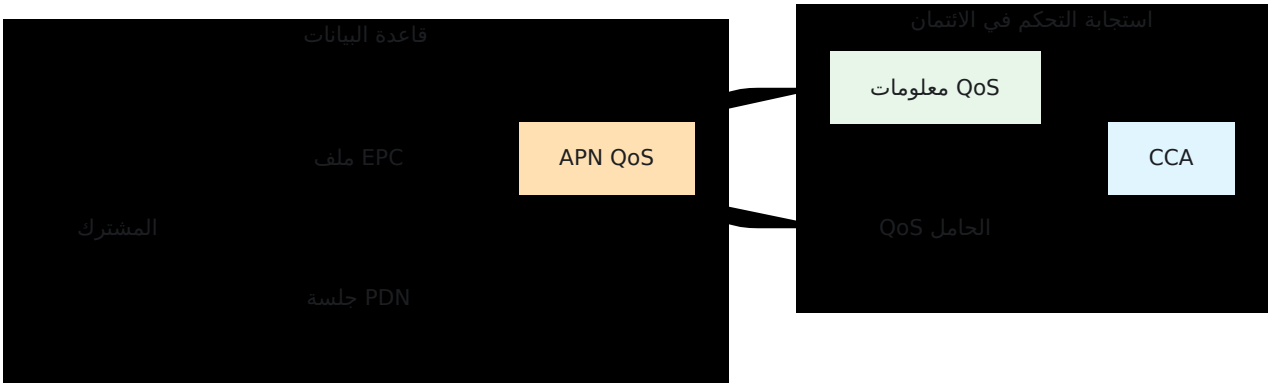
معلمات قالب IFC:

- `{{msisdn}}` - أول MSISDN من المشترك
- `{{imsi}}` - IMSI المشترك
- `{{impu}}` - هوية المستخدم العامة IMS (من subscriber_state)
- `{{impi}}` - هوية المستخدم الخاصة IMS (عادةً IMSI@realm)

استجابة التحكم في الائتمان (Gx CCA)

يتم إرسال استجابة التحكم في الائتمان من وظيفة PCRF إلى PGW خلال إنشاء الحامل.

رسم مصدر البيانات



الميزات الرئيسية:

1. **تتبع الجلسة**: ينشئ/يحدث سجل `pdn_session` لكل حامل
2. **فرض QoS**: يوفر QCI وحدود النطاق الترددي من ملف APN QoS
3. **قواعد الشحن**: يعيد قواعد الشحن الافتراضية لتكامل الفوترة
4. **نوع طلب CC**: يتعامل مع INITIAL (1)، UPDATE (2)، TERMINATION (3)

إدارة حالة الجلسة:

- `INITIAL_REQUEST`: ينشئ سجل جلسة PDN جديدة
- `UPDATE_REQUEST`: يحدث جلسة PDN الحالية
- `TERMINATION_REQUEST`: يحذف سجل جلسة PDN

استجابة بيانات المستخدم (Sh UDA)

يتم إرسال استجابة بيانات المستخدم من HSS إلى AS (خادم التطبيق) عبر واجهة Sh.

رسم مصدر البيانات



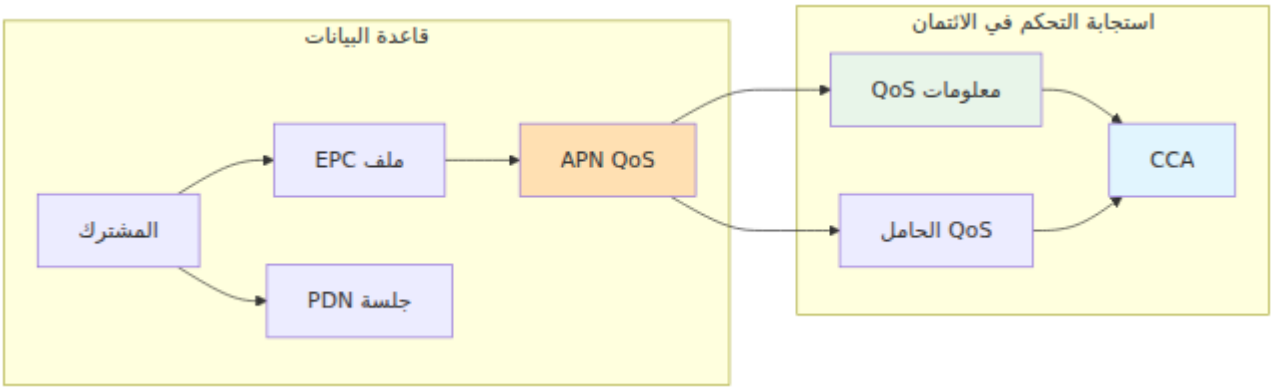
الميزات الرئيسية:

1. مخصص في XML **بيانات المستودع**: يمكن تخزين `subscriber_state.sh_repository_data`
2. **إشارة الخدمة**: تصفية البيانات حسب الخدمة المطلوبة (مثل، الحضور، الرسائل)
3. للمشترك IMS **الهويات العامة**: تعيد جميع الهويات العامة
4. **المرجع مقابل الشفافية**: تدعم كلا الوضعين المرجعي والشفاف للبيانات

استجابة تحقق هوية ME (S13 ECA)

يتم إرسال استجابة تحقق هوية ME من وظيفة EIR إلى MME للتحقق من IMEI.

سم مصدر البيانات



الميزات الرئيسية:

1. **مطابقة Regex**: القواعد هي تعبيرات منتظمة يتم اختبارها ضد IMEISV، ثم IMEI، ثم IMSI إذا كانت الطلب يحمل واحدة. ضمن كل خطوة يتم تقييم القواعد بترتيب `precedence` تصاعدي وأول مطابقة تفوز. انظر منطق مطابقة المعدات و أولوية القاعدة

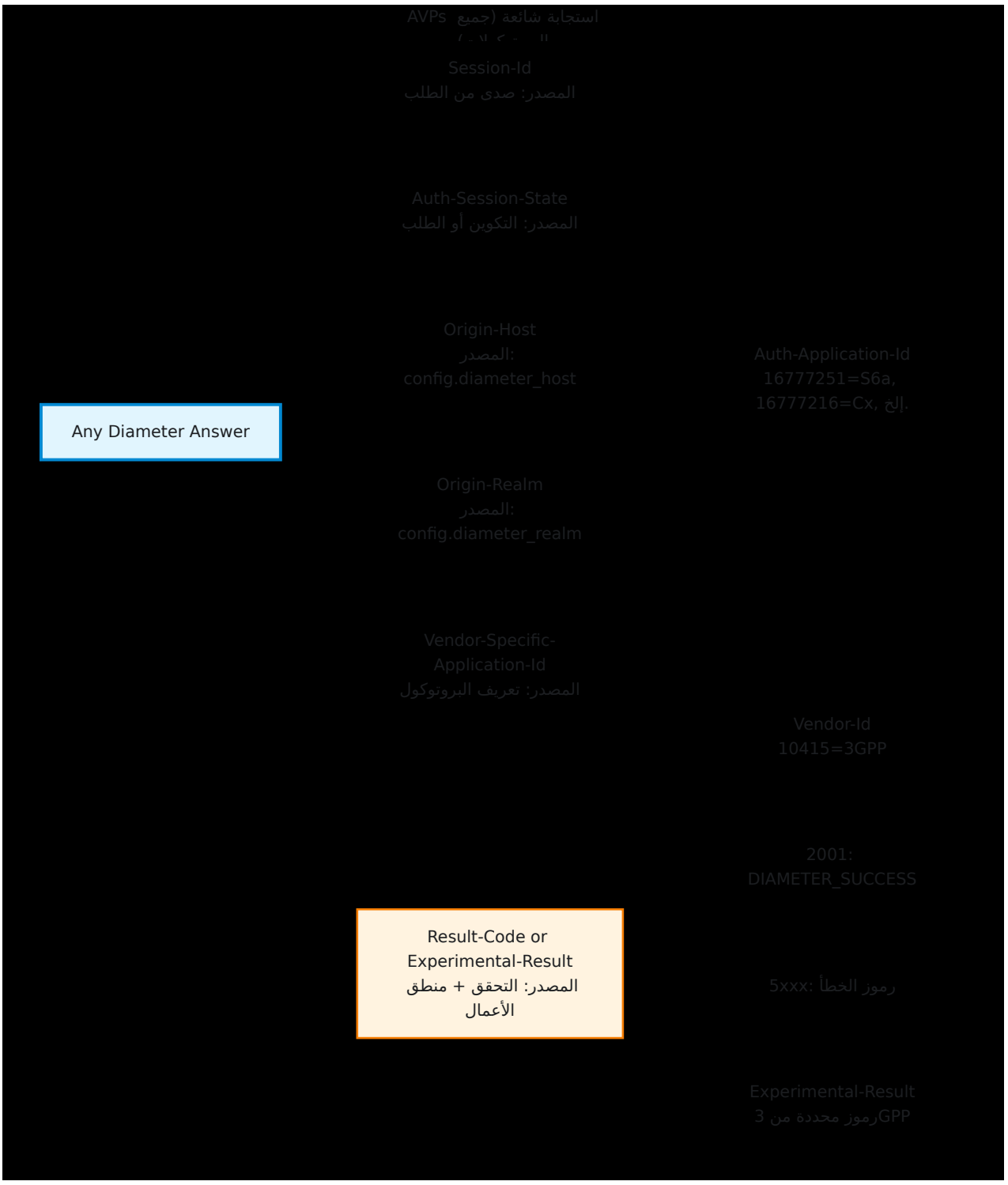
2. **قواعد قائمة على TAC**: (أول 8 أرقام) يمكن أن تطابق رمز تخصيص النوع
3. **السلوك الافتراضي**: يحدد `unknown_equipment_behaviour` قائمة بيضاء، قائمة سوداء، قائمة رمادية أو رفض (Experimental-Result 5422) لمطابقة المعدات التي لا توجد لها قاعدة. انظر تكوين EIR
4. **قيم حالة المعدات**:
   - `0` = (مسموح بها صراحة) قائمة بيضاء
   - `1` = (مسروقة/محظورة) قائمة سوداء
   - `2` = (مسموح بها ولكن مراقبة) قائمة رمادية
   - يحدد: لا مطابقة `unknown_equipment_behaviour` من المكونة واحدة رمز ECA تحمل `:reject_unknown_equipment` القيم السابقة، أو مع (DIAMETER_ERROR_EQUIPMENT_UNKNOWN) نتيجة تجريبية 5422 بدلاً من حالة المعدات

حالات الاستخدام:

- حظر الأجهزة المسروقة حسب IMEI الدقيق
- حظر نماذج الأجهزة حسب نمط TAC
- قائمة بيضاء للأجهزة المعتمدة فقط
- تتبع الأجهزة في السوق الرمادي

عناصر الاستجابة الشائعة

تشارك جميع استجابات القطر هذه AVPs الشائعة:

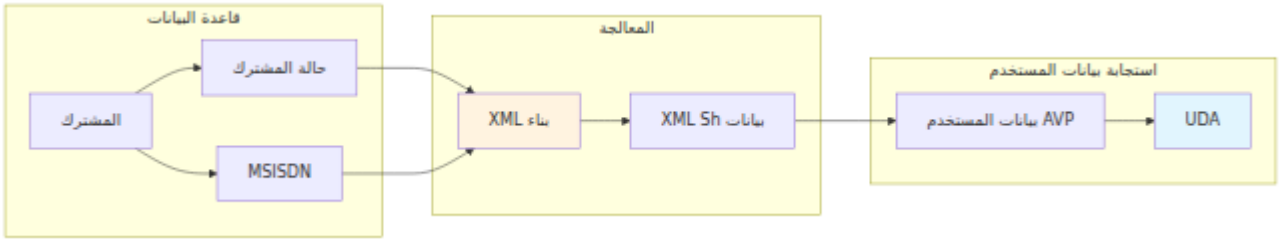


مثال على التكوين:

```
config :diameter_ex,
  diameter_host: "hss",
  diameter_realm: "example.com",
  diameter_service_name: "OmniHSS"
```

ملخص تدفق البيانات

خط معالجة الطلبات



ملاحظات التنفيذ

معالجات البروتوكول

يطبق النظام معالجات للبروتوكولات القطرية التالية:

- **S6a** - واجهة LTE/MME للمصادقة وتحديث الموقع
- **Cx** - واجهة IMS/CSCF لتسجيل IMS وتعيين الخادم
- **Sh** - واجهة IMS/AS لاسترجاع بيانات المشترك
- **Gx** - واجهة PCRF للتحكم في السياسة والفوترة
- **Rx** - واجهة IMS/AF لتفويض الوسائط
- **S13** - واجهة EIR للتحقق من IMEI
- **SWx** - واجهة WiFi/IMS 3 غير الوصول لمصادقةGPP

نماذج البيانات

يتضمن مخطط قاعدة البيانات الكيانات الأساسية التالية:

- IMSI - سجل المشترك الأساسي مع **المشترك**
- **مجموعة المفاتيح** - المفاتيح التشفيرية للمصادقة
- **ملف EPC** - تكوين خدمة LTE
- **ملف APN** - تكوين نقطة الوصول
- **ملف IMS** - تكوين خدمة IMS مع قوالب IFC
- **ملف التجوال** - قواعد وقيود التجوال

- **حالة المشترك** - تتبع الجلسة والحالة الديناميكية
- **جلسة PDN** - تتبع جلسة الحامل النشطة
- **IP الثابت** - تعيينات عنوان IP الثابت
- **قاعدة EIR** - قواعد هوية المعدات (regex ضد IMEISV، IMEI أو IMSI، يتم تقييمها بترتيب الأولوية)

← مرجع | العودة إلى دليل العمليات API → | تدفقات البروتوكول →

دليل قياس ومراقبة OmniHSS

← العودة إلى دليل العمليات

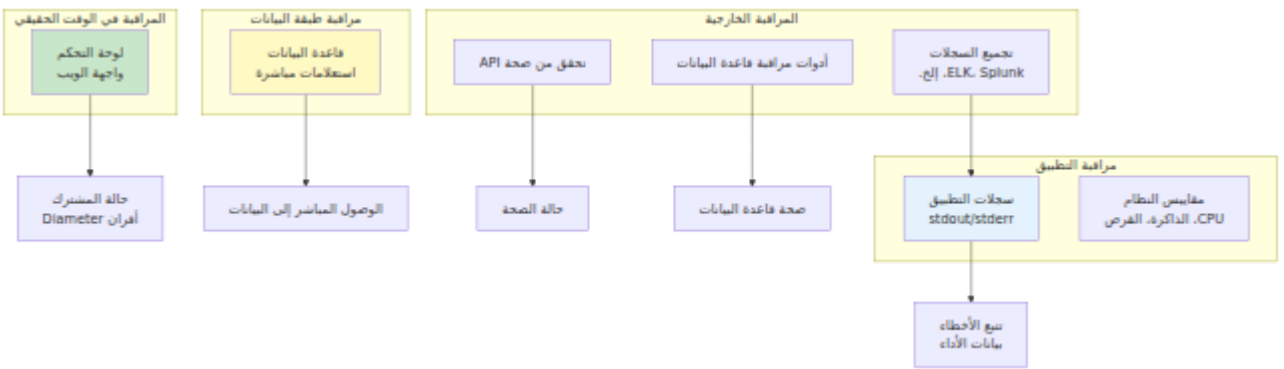
جدول المحتويات

- نظرة عامة على المراقبة
- مراقبة لوحة التحكم
- مراقبة قاعدة البيانات
- مراقبة السجلات
- تكامل المراقبة الخارجية
- مؤشرات الأداء الرئيسية
- استراتيجيات التنبيه

نظرة عامة على المراقبة

يوفر OmniHSS عدة آليات لمراقبة صحة النظام وأدائه ونشاط المشتركين. يجب على موظفي العمليات استخدام مجموعة من هذه الأدوات للحصول على رؤية كاملة.

طبقات المراقبة



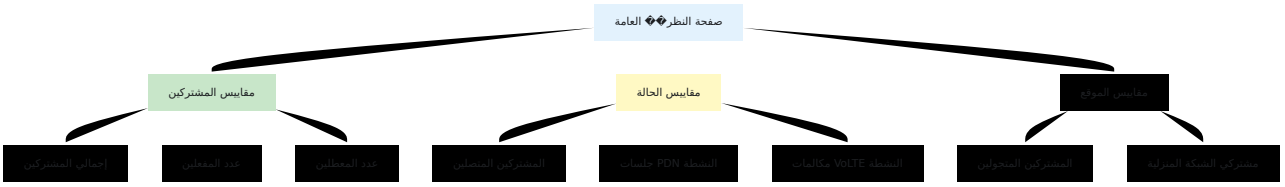
مراقبة لوحة التحكم

توفر لوحة التحكم الواجهة الرئيسية للمراقبة في الوقت الحقيقي.

مراقبة صفحة النظرة العامة

URL: `https://[hostname]:7443/overview`

المقاييس الرئيسية المتاحة



حالات المشتركين المراقبة

الحالة	المؤشر	ماذا يعني
خامل	لا توجد معلومات عن الموقع	المشترك مغلق أو خارج نطاق التغطية
متصل	موجود MME	المشترك مسجل في الشبكة
نشط PDN	عدد جلسات PDN > 0	اتصال بيانات نشط
مسجل IMS	تم تعيين S-CSCF	خدمات الصوت جاهزة
في مكالمة	عدد المكالمات النشطة > 0	مكالمة VoLTE جارية

استخراج المقاييس من النظرة العامة

لا تقوم لوحة التحكم بتصدير المقاييس مباشرة. يمكنك:

1. **عد الصفوف المرئية** للحصول على إجمالي المشتركين
2. **البحث عن علامات الاختيار الخضراء** لعد المشتركين المفعلين
3. **مراجعة التفاصيل الموسعة** للحصول على معلومات الحالة
4. **ملاحظة الطوابع الزمنية الأخيرة** للاستجابة

مراقبة صفحة Diameter

URL: `https://[hostname]:7443/diameter`

المقاييس الرئيسية



مراقبة الأقران الحرجة

حدد الأقران الحرجة وراقب حالتها:

نوع القرين	الأهمية	التأثير إذا كان معطلاً
MME	عالي	لا توجد اتصالات LTE جديدة
P-GW	عالي	لا توجد جلسات بيانات
S-CSCF	عالي	لا توجد تسجيلات IMS
P-CSCF	عالي	لا توجد مكالمات VoLTE
I-CSCF	متوسط	مشاكل توجيه IMS
AS	منخفض-متوسط	خدمة معينة غير متاحة

مراقبة صفحة التطبيق

URL: `https://[hostname]:7443/application`

المقاييس الرئيسية

المقياس	الوصف	النطاق الطبيعي	عتبة العمل
عدد العمليات	عمليات Erlang النشطة	يختلف حسب الحمل	> 90% من الحد
استخدام الذاكرة	إجمالي الذاكرة المستهلكة	< 80%	> 90%
مدة التشغيل	الوقت منذ آخر إعادة تشغيل	N/A	تتبع للاستقرار

مراقبة قاعدة البيانات

استعلامات قاعدة البيانات المباشرة

اتصل بقاعدة بيانات SQL لاستخ��اج مقاييس مفصلة:

عدد المشتركين

استعلام قاعدة البيانات لاسترجاع:

- إجمالي عدد جميع المشتركين
- عدد المشتركين المفعلين
- عدد المشتركين المفعلين لـ IMS

إحصائيات الجلسات

استعلام قاعدة البيانات لاسترجاع:

- عدد جلسات PDN النشطة
- عدد مكالمات VoLTE النشطة
- توزيع جلسات PDN حسب ملف APN

إحصائيات الموقع

استعلام قاعدة البيانات لاسترجاع:

- عدد المشتركين مجمعة حسب الشبكة التي تمت زيارتها (مزيج MCC-MNC)
- عدد المشتركين المتجولين حالياً (ليس على PLMN 001-001 المنزلية)
- توزيع المشتركين عبر الشبكات المختلفة التي تمت زيارتها

النشاط الأخير

استعلام قاعدة البيانات لاسترجاع:

- عدد المشتركين الذين تم رؤيتهم في الساعة الماضية
- توزيع المشتركين حسب MME الخادم
- تحليل الطوابع الزمنية لأحدث نشاط للمشترك

مراقبة صحة قاعدة البيانات

راقب صحة قاعدة البي��نات من خلال الاستعلام عن:

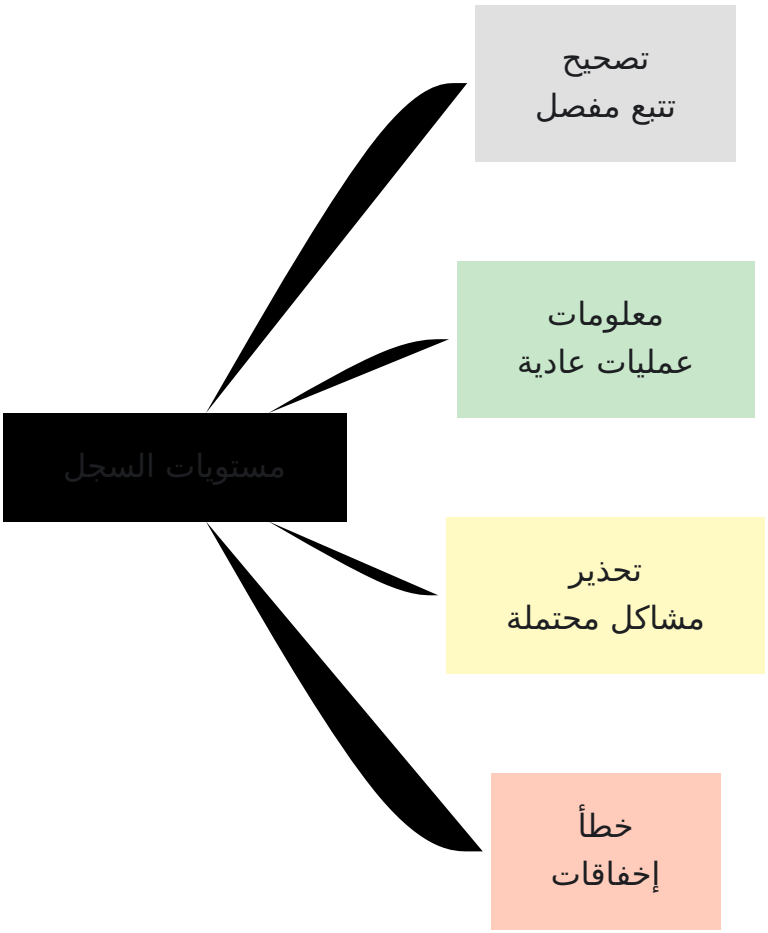
- إجمالي حجم قاعدة البيانات واتجاهات النمو
- أحجام الجداول الفردية وعدد الصفوف
- عدد الاتصالات الحالية بقاعدة البيانات
- أداء الاستعلام واستخدام الموارد

مراقبة السجلات

مخرجات السجلات

يخرج OmniHSS السجلات إلى **stdout/stderr**، والتي يجب أن يتم التقاطها بواسطة مدير العمليات الخاص بك.

مستويات السجل



أنماط السجل الرئيسية للمراقبة

أحداث أقران Diameter:

```
[info] تم الاتصال بالقرين Diameter: mme01.epc.example.com
[warn] تم فصل القرين Diameter: pgw01.epc.example.com
[error] فشل الاتصال بالقرين Diameter: انتهاء المهلة
```

أحداث ��اعدة البيانات:

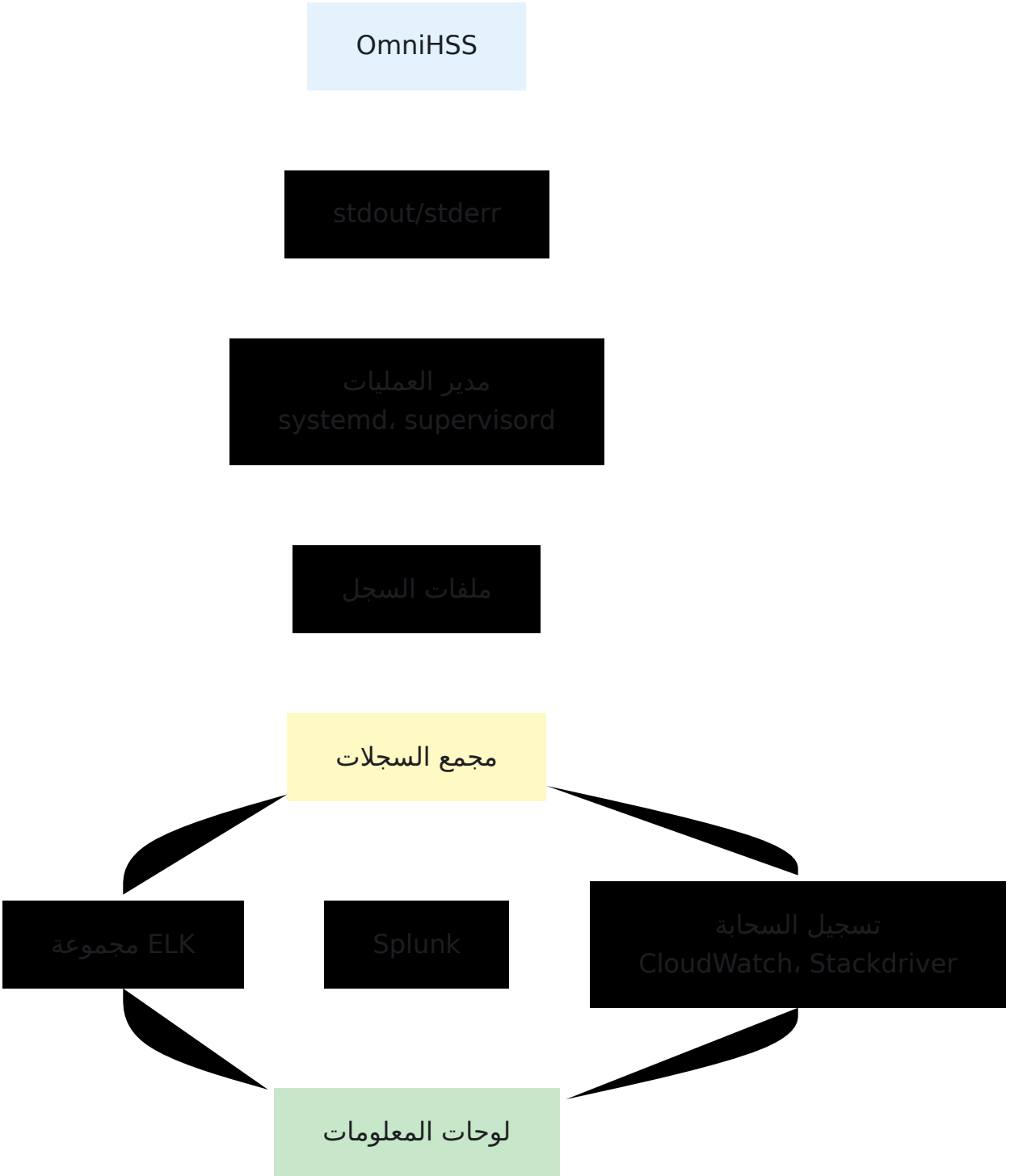
```
[info] تم إنشاء اتصال قاعدة البيانات
[error] فقدان اتصال قاعدة البيانات: انتهاء المهلة
[error] فشل استعلام قاعدة البيانات: تم الكشف عن حالة توقف
```

أحداث المصادقة:

```
[info] المصادقة ناجحة: IMSI 001001123456789
[warn] فشلت المصادقة: IMSI 001001123456789، متجه غير صالح
[error] تم رفض التجوال: IMSI 001001123456789، MCC 310 MNC 410
```

تجميع السجلات

للتنفيذات الإنتاجية، نفذ تجميع السجلات:



تكامل المراقبة الخارجية

نقطة نهاية تحقق الصحة

تحقق صحة API: `GET /api/status`

```
curl -k https://hss.example.com:8443/api/status
```

الاستجابة المتوقعة:

```
{"status": "ok"}
```

حالة HTTP: 200 OK

تكامل أدوات المراقبة

مثال Nagios/Icinga

```
#!/bin/bash
# check_omnihss.sh

API_URL="https://hss.example.com:8443/api/status"

response=$(curl -k -s -o /dev/null -w "%{http_code}" "$API_URL" --
max-time 5)

if [ "$response" = "200" ]; then
    echo "OK - OmniHSS API responding"
    exit 0
else
    echo "CRITICAL - OmniHSS API not responding (HTTP $response)"
    exit 2
fi
```

تكامل Prometheus

يعرض OmniHSS نقطة نهاية مقاييس Prometheus الأصلية. قم بجمع `http://<host>:9568/metrics`. يتم تعيين المنفذ بواسطة `prometheus_metrics_port` ويكون الافتراضي هو `9568`.

تتضمن نقطة النهاية مقاييس وقت تشغيل BEAM، ومقاييس تجمع قاعدة البيانات، وحالة أقران Cx أدناه. لكل تطبيق، وعدد Diameter وعدد رسائل Diameter،

S-CSCF عدّ التخلي عن مصادقة

المقياس: `hss_cx_auth_abandon_total` يعدّ: **الوصف**: عداد **النوع**: Cx SARs التي تنهي S-CSCF SAR دون تسجيل ناجح. هذا تحدٍ مهجور أو فاشل. يرسل IMS-AKA تحدي على تحدٍ مهجور، أو `auth_vector_timeout` عندما تنتهي مدة `AUTHENTICATION_TIMEOUT` SAR `AUTHENTICATION_FAILURE` عند استجابة سيئة. انظر حالة تعيين S-CSCF. **التسميات**:

- `sar_type` - نوع تعيين الخادم: `authentication_timeout` أو `authentication_failure`.
- `outcome` - `name_cleared` عندما تم تحرير اسم S-CSCF، أو `kept_registered` الاسم عندما لم يكن المشترك مسجلاً، HSS عندما تم الحفاظ على ربط مسجل. يحرر I-CSCF مختلف عن المسجل. تعني الحالة الثانية أن S-CSCF من SAR وأيضًا عندما يأتي REGISTER أعاد توزيع لأنه لم يتمكن من الوصول إلى العقدة المسجلة، لذا فإن الاسم قديم.
- `origin_host` - S-CSCF الذي أرسل SAR.

استعلامات المثال:

```
# معدل التحديات المهجورة/الفاشلة في الثانية
rate(hss_cx_auth_abandon_total[5m])

# تقسيم حسب السبب
sum by (sar_type) (rate(hss_cx_auth_abandon_total[5m]))

# أعلى S-CSCFs حسب التحديات المهجورة
topk(5, sum by (origin_host)
(rate(hss_cx_auth_abandon_total[5m])))
```

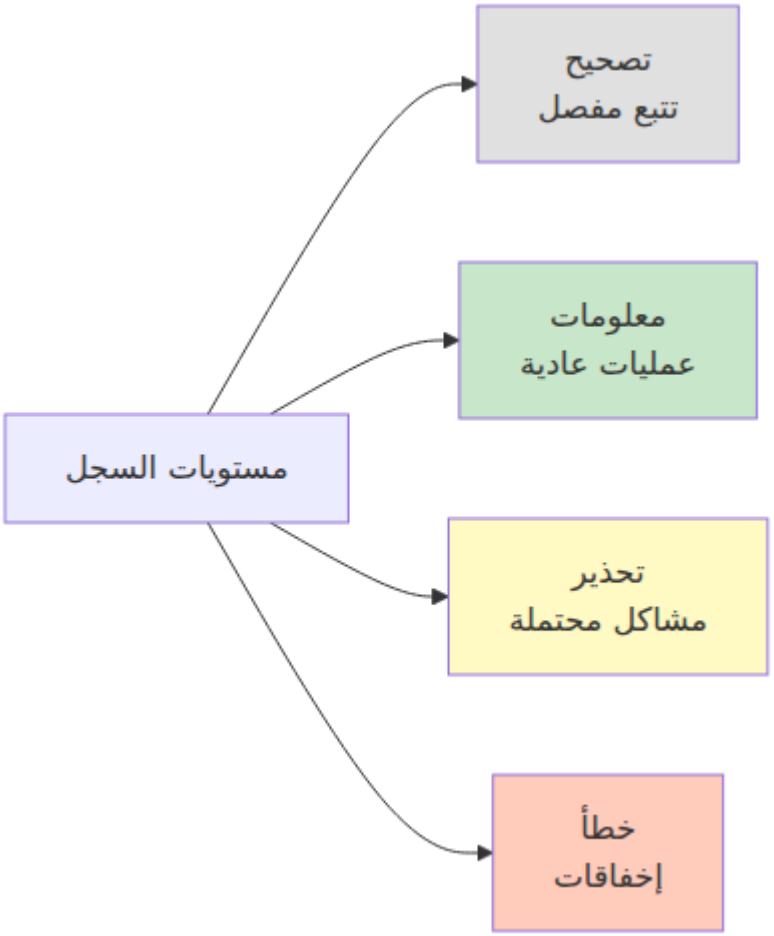
تفشل في التحديات، أو S-CSCF واحد إلى `origin_host` ي��كن أن يشير معدل مرتفع على مشتركين يتخلون عن التسجيل على تلك العقدة.

تكامل SNMP

المخصصة قاعدة البيانات SNMP يمكن أن تستعلم نصوص الامتداد، SNMP للمراقبة المعتمدة على OIDs SNMP للحصول على المقاييس وإرجاع القيم عبر API أو.

مؤشرات الأداء الرئيسية

مؤشرات الأداء التشغيلية



عتبات مؤشرات ال��داء الموصى بها

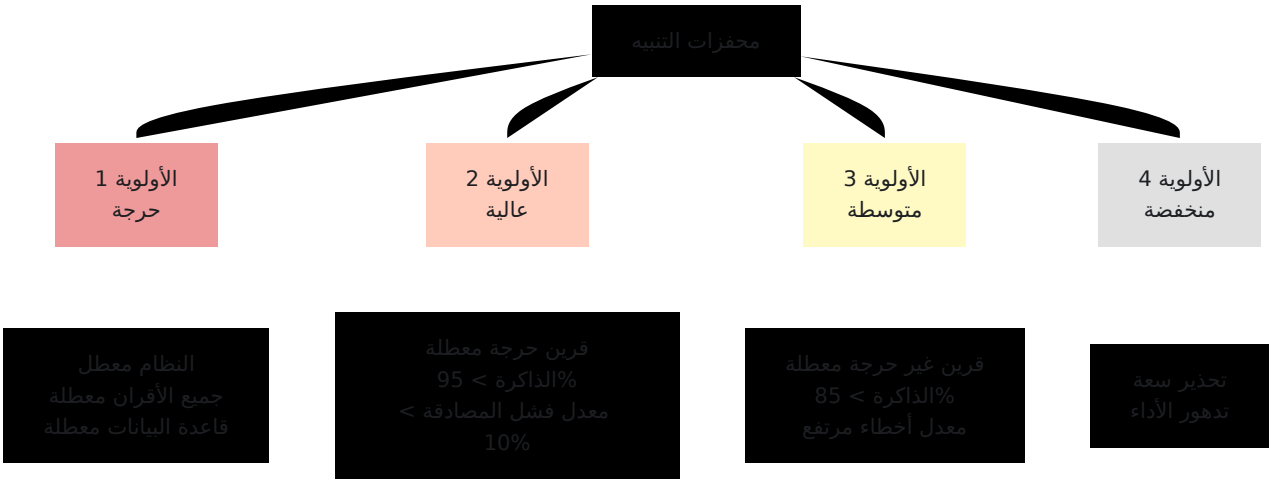
KPI	الهدف	تحذير	حرجة
وقت تشغيل النظام	99.99%	< 99.95%	< 99.9%
نسبة وقت تشغيل قرين Diameter	99.9%	< 99.5%	< 99%
نسبة نجاح المصادقة	> 99%	< 99%	< 95%
وقت استجابة Diameter	< 100ms	> 200ms	> 500ms
وقت استعلام قاعدة البيانات	< 50ms	> 100ms	> 500ms
نسبة الأخطاء	< 0.1%	> 0.5%	> 1%

مؤشرات الأداء للسعة

المقياس	المراقبة	خطة العمل عند
إجمالي المشتركين	العدد الحالي	80% من السعة المتوقعة
جلسات PDN المتزامنة	الجلسات النشطة	70% من الحد الأقصى المتوقع
حجم قاعدة البيانات	MB المستخدمة	80% من التخزين المخصص
اتصالات قاعدة البيانات	الاتصالات النشطة	80% من حجم التجمع

استراتيجيات التنبيه

أولويات التنبيه



تعريفات التنبيه

التنبيهات الحرجة (P1)

النظام غير متاح:

- فشل تحقق صحة API
- لوحة التحكم غير قابلة للوصول
- فشل اتصال قاعدة البيانات
- الإجراء: التحقيق الفوري والتصعيد

جميع أقران Diameter مفصولة:

- صفر أقران متصلة
- الإجراء: تحقق من الشبكة، أعد التشغيل إذا لزم الأمر

قاعدة البيانات معطلة:

- لا يمكن الاتصال بقاعدة بيانات SQL
- الإجراء: التحقيق في خادم قاعدة البيانات، أعد التشغيل إذا لزم الأمر

التنبيهات عالية الأولوية (P2)

حرجة معطلة Diameter قرين:

- فصل MME الأساسي
- فصل P-GW الأساسي
- فصل S-CSCF الأساسي
- الإجراء: التحقيق في اتصال القرين خلال 15 دقيقة

استخدام الذاكرة مرتفع:

- 95 < الذاكرة%
- الإجراء: التحقيق في تسرب الذاكرة، التخطيط لإعادة التشغيل

معدل فشل المصادقة مرتفع:

- 10% من طلبات المصادقة تفشل
- الإجراء: تحقق من توفير المشتركين، التحقيق في السبب

التنبيهات متوسطة الأولوية (P3)

قرين غير حرجة معطلة:

- فصل قرين ثانوي
- فصل خادم التطبيق
- الإجراء: التحقيق خلال ساعة واحدة

استخدام الذاكرة مرتفع:

- 85 < الذاكرة%
- الإجراء: مراقبة الاتجاه، التخطيط لترقية السعة

معدل الأخطاء مرتفع:

- 1 < معدل الأخطاء%
- الإجراء: مراجعة السجلات، تحديد السبب الجذري

التنبيهات منخفضة الأولوية (P4)

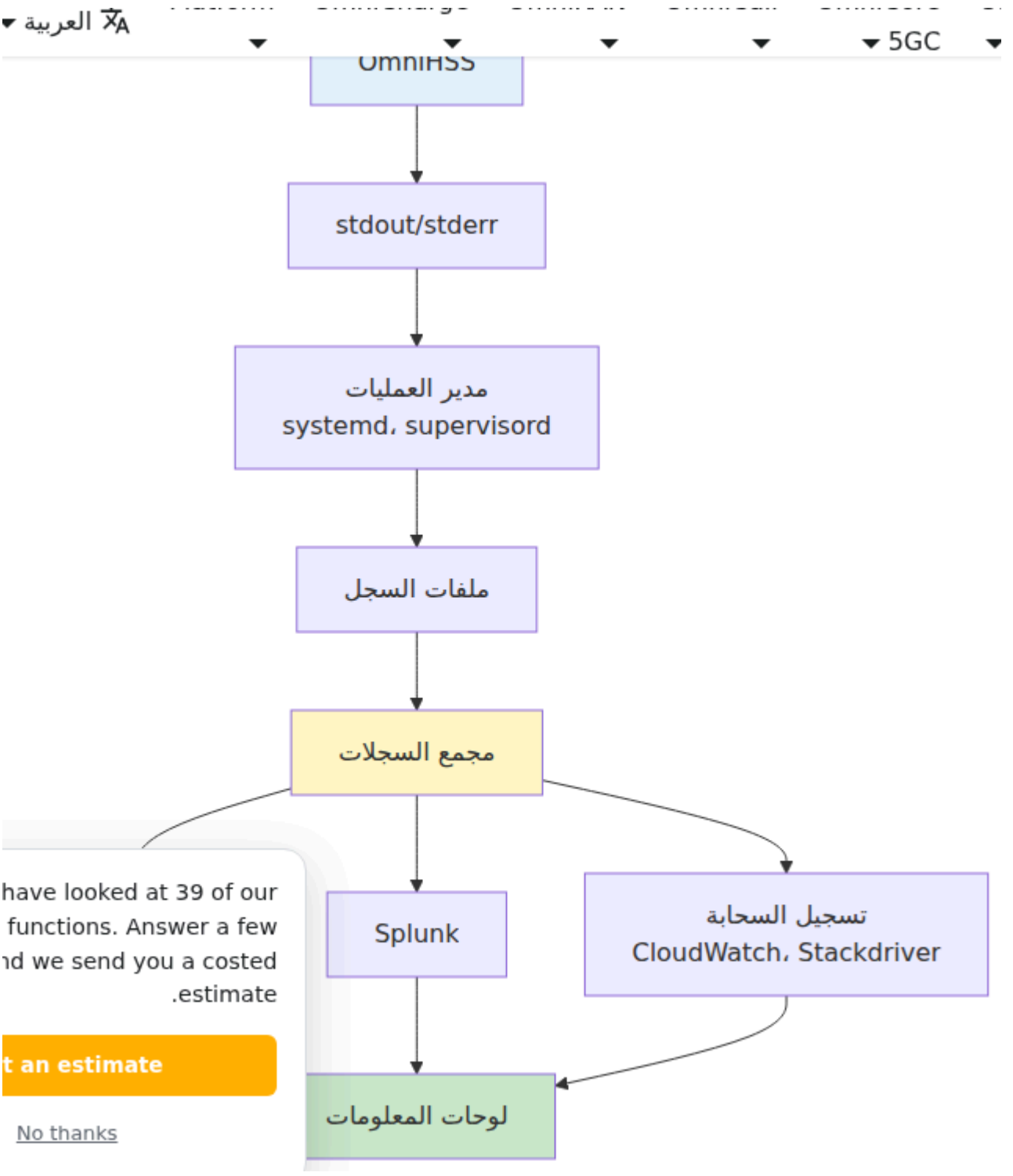
تحذير سعة:

- المشتركي�� > 80% من السعة
- قاعدة البيانات > 80% من التخزين المخصص
- الإجراء: التخطيط لتوسيع السعة

تدهور الأداء:

- أوقات الاستجابة مرتفعة ولكن مقبولة
- الإجراء: مراقبة وتحسين الاستعلامات

قنوات إشعار التنبيه



قائمة مراجعة المراقبة

الفحوصات اليومية

- [ ] مراجعة نظرة عامة على لوحة التحكم - عدد المشتركين طبيعي
- [ ] جميع الأقران الحرجة متصلة - مراجعة صفحة Diameter
- [ ] مراجعة صفحة التطبيق - الذاكرة والعمليات ضمن الحدود
- [ ] التحقق من سجلات الأخطاء - لا توجد أخطاء حرجة في آخر 24 ساعة
- [ ] التحقق من اكتمال النسخ الاحتياطي بنجاح

الفحوصات الأسبوعية

- [ ] مراجعة اتجاهات السعة - نمو المشتركين
- [ ] مراجعة اتجاهات الأداء - أوقات الاستجابة
- [ ] مراجعة حجم قاعدة البيانات - معدل النمو مقبول
- [ ] مراجعة معدلات الأخطاء - تحديد الأنماط
- [ ] اختبار إشعارات التنبيه - التأكد من العمل

الفحوصات الشهرية

- [ ] مراجعة تخطيط السعة - التخطيط لمدة 6 أشهر قادمة
- [ ] مراجعة تحسين الأداء - تحديد الاستعلامات البطيئة
- [ ] مراجعة الأمان - انتهاء صلاحية الشهادات، الثغرات
- [ ] مراجعة الوثائق - تحديث كتب التشغيل
- [ ] اختبار استعادة الكوارث - التحقق من استعادة النسخ الاحتياطية بشكل صحيح

← العودة إلى دليل العمليات | التالي: ميزات متعددة →

ميزات OmniHSS متعددة IMSI ومتعددة MSISDN

← العودة إلى دليل العمليات

جدول المحتويات

- نظرة عامة
- Multi-MSISDN: أرقام هواتف متعددة
- Multi-IMSI SIM: هويات شبكة متعددة
- سيناريوهات مجمعة
- حل MSISDN عبر الواجهات
- هوية المستخدم العامة المشتركة
- أمثلة على التكوين
- إجراءات التشغيل

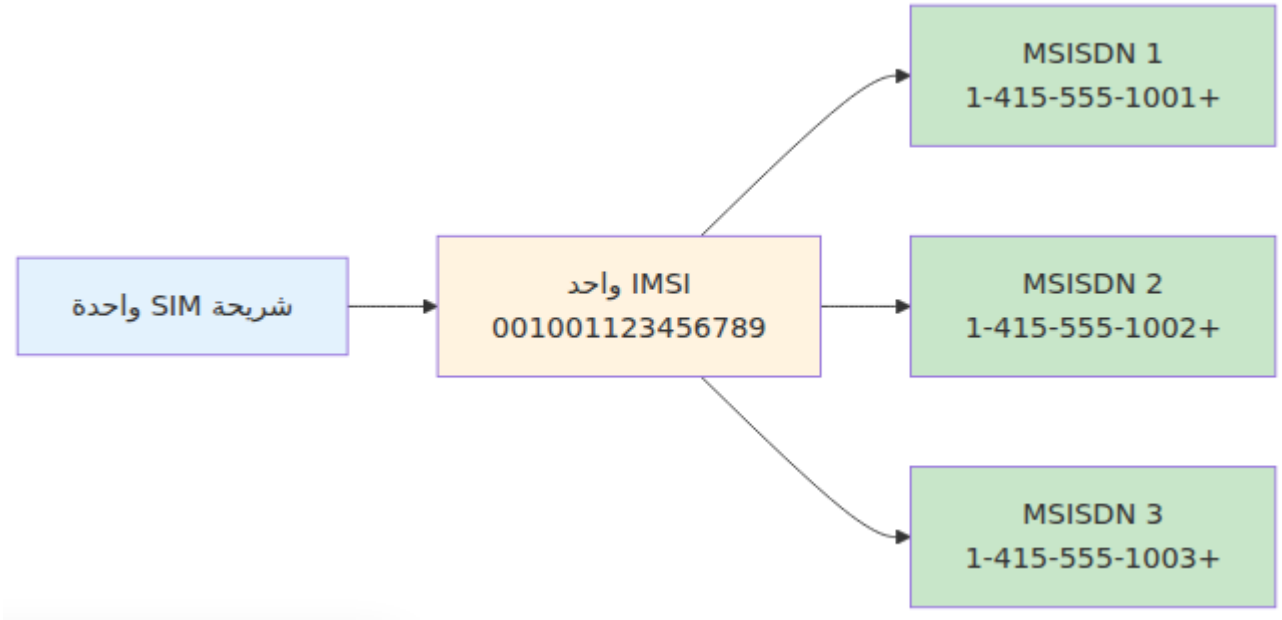
نظرة عامة

يدعم OmniHSS قدرات توفير متقدمة تتيح تكوينات خدمة مرنة:

دعم Multi-MSISDN

أرقام هواتف متعددة ← واحد IMSI

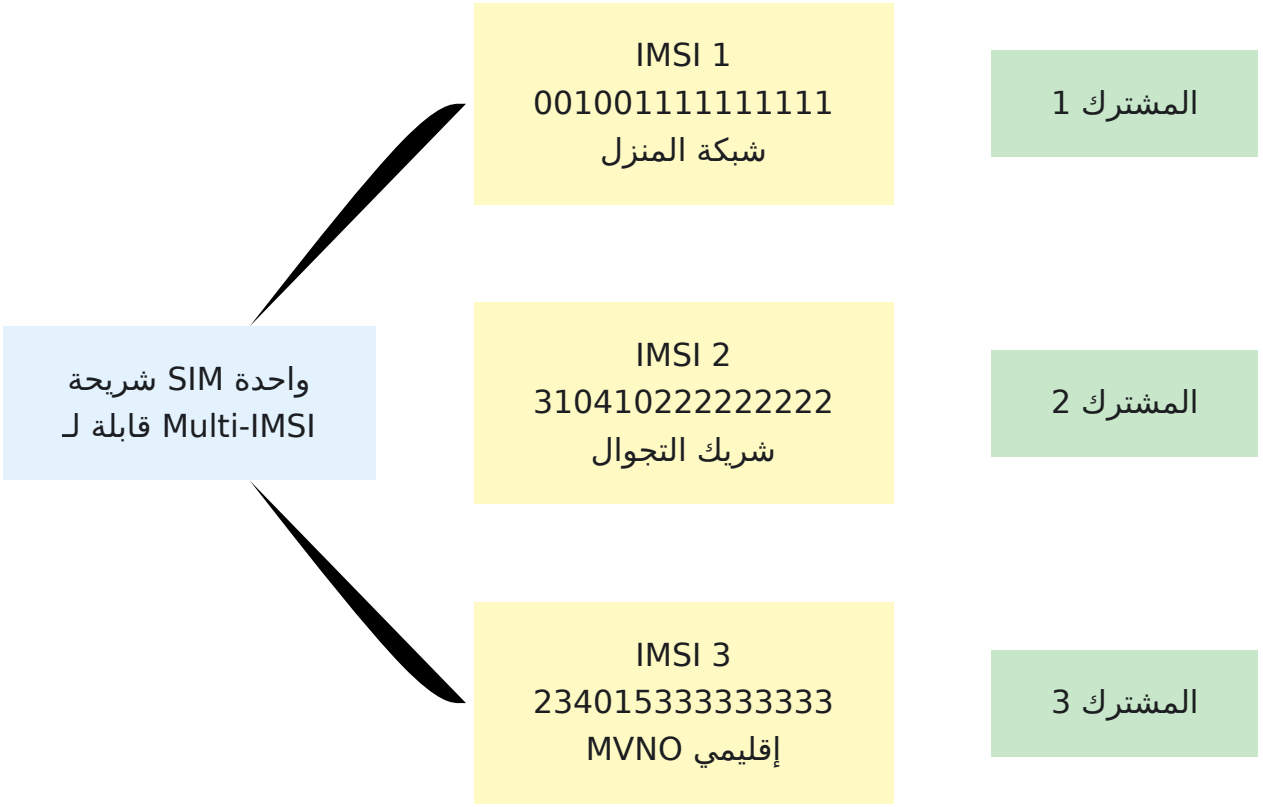
يمكن أن يكون لدى مشترك واحد (واحد IMSI محدد بواسطة) عدة MSISDNs (أرقام هواتف) مخصصة. جميع الأرقام ترن على نفس الجهاز وتشارك نفس ملفات تعريف الخدمة.



دعم Multi-IMSI SIM

شريحة SIM عدة ← واحدة IMSIs

مما يسمح للجهاز بالاتصال، IMSIs الفيزيائية الواحدة على عدة SIM يمكن أن تحتوي بطاقة بشبكات مختلفة باستخدام هويات شبكة مختلفة. هذا مفيد للتجوال الدولي وسيناريوهات MVNO.



Multi-MSISDN: أرقام هواتف متعددة

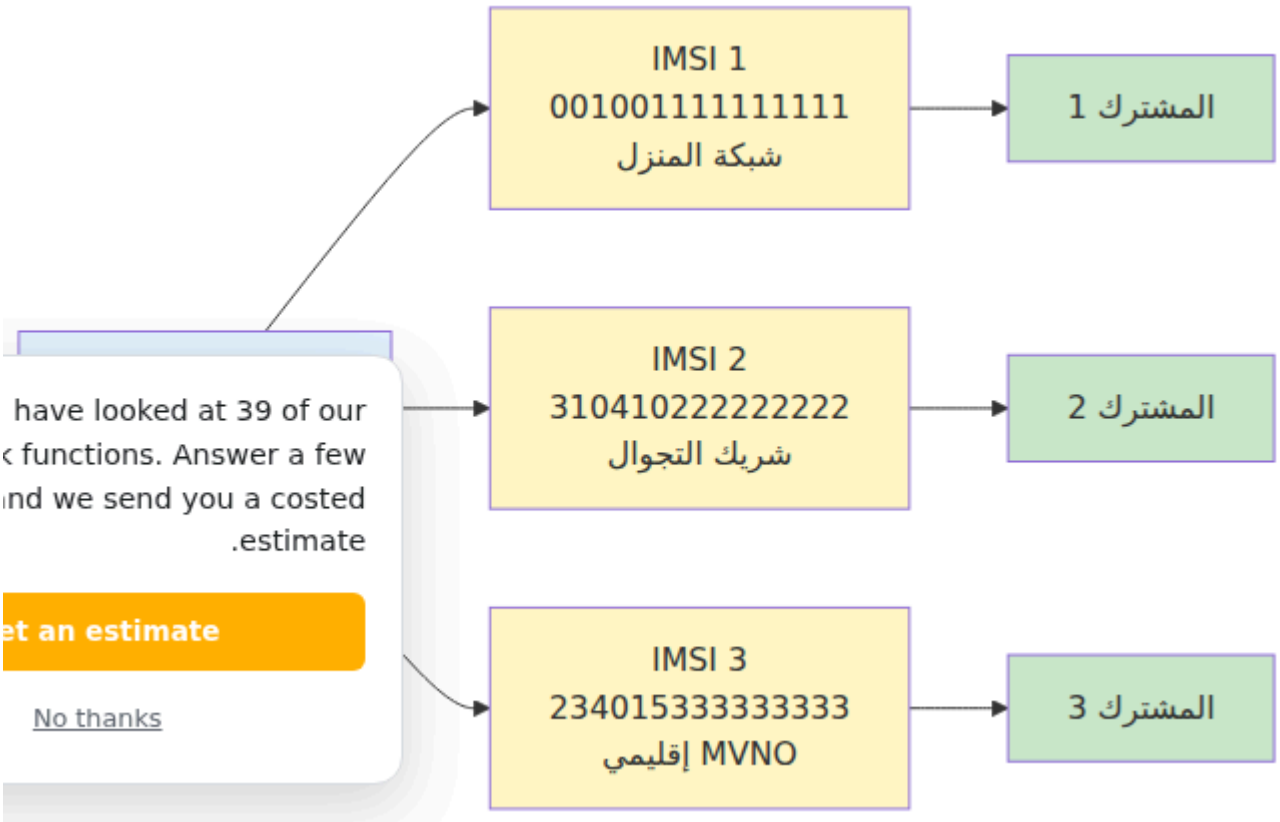
كيف يعمل

مرتبطة من خلال جدول انضمام. عندما MSISDNs على عدة HSS تحتوي سجل مشترك واحد في IMS، يسجل المشترك في IMS، مما يسمح MSISDNs في ملف تعريف IMS يتم تضمين جميع للمكالمات الواردة إلى أي رقم بالوصول إلى الجهاز.

الخصائص الرئيسية

- **IMSI واحد** - المشترك لديه IMSI واحد مرتبط ببطاقة SIM الخاصة به
- **MSISDNs عدة** - يمكن أن يكون لدى المشترك عدة أرقام هواتف
- **IMS تكامل** - يتم تسجيل جميع MSISDNs في IMS
- **خدمة مشتركة** - جميع الأرقام تشترك في نفس ملفات تعريف الخدمة (EPC، IMS، التجوال)

نموذج البيانات



واحدة فقط لمشترك واحد في وقت واحد. ومع ذلك، يمكن أن يكون MSISDN **مهم:** يمكن تعيين لدى مشترك واحد العديد من MSISDNs.

حالات الاستخدام

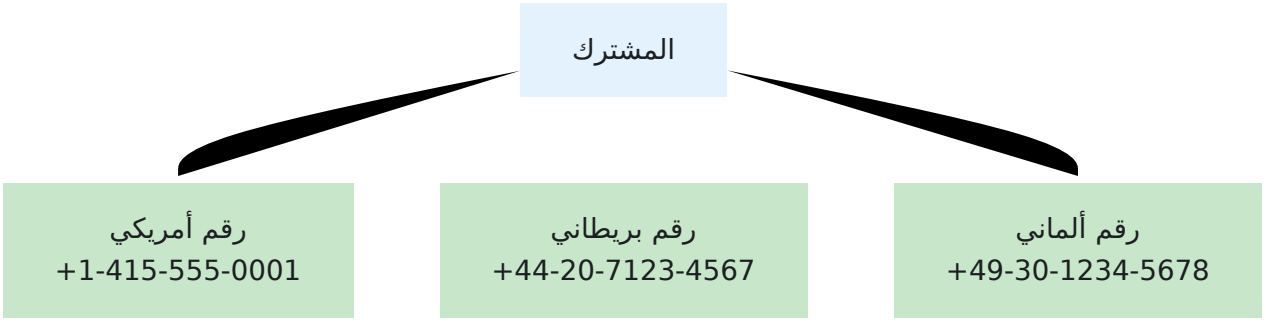
1. خطوط الأعمال والشخصية

يمتلك مشترك أرقام هواتف للأعمال والشخصية على نفس الجهاز:



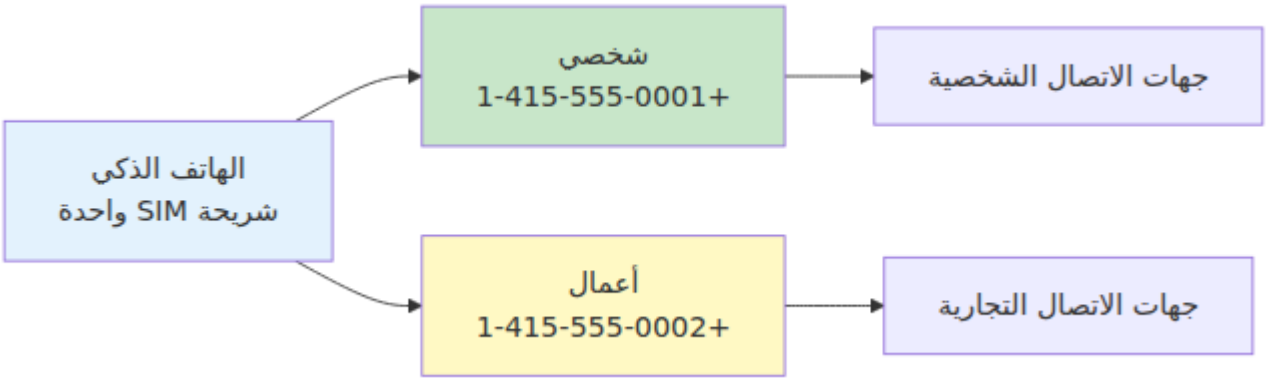
2. أرقام دولية

يمتلك مشترك يسافر كثيرًا أرقامًا في عدة دول:



3. خطط عائلية

يدير أحد الوالدين أرقام عدة أفراد من العائلة:



ملاحظة: في OmniHSS، كل منهم قد (SIM/IMSI واحد لكل) سيتطلب ذلك عدة مشتركين، يكون لديه عدة MSISDNs.

4. نقل الخطوط القديمة

عندما يغير المشترك أرقامه ولكنه يريد الاحتفاظ بالرقم القديم نشطًا أثناء الانتقال:



التكوين

إنشاء MSISDNs

يجب إنشاء MSISDNs قبل تعيينها للمشتركين.

```
# إنشاء أول MSISDN
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{"msisdn": {"msisdn": "14155551001"}}'

# إنشاء ثاني MSISDN
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{"msisdn": {"msisdn": "14155551002"}}'
```

تعيين MSISDNs للمشتركين

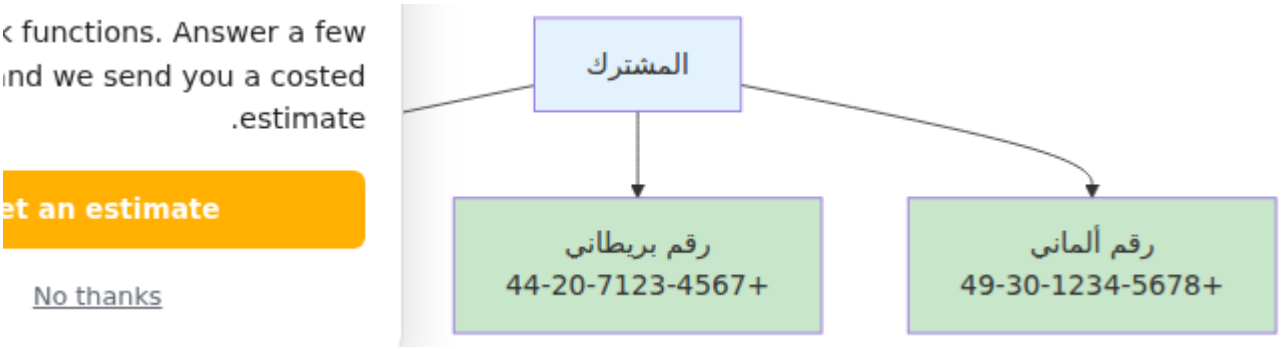
يتم التعيين من خلال جدول الانضمام في قاعدة البيانات.

طريقة قاعدة البيانات:

1. استعلام قاعدة البيانات للحصول على معرف المشترك لـ IMSI المستهدف
2. استعلام قاعدة البيانات للحصول على معرفات MSISDN لأرقام الهواتف
3. إدراج سجلات في جدول الانضمام تربط subscriber_id بكل msisdn_id

هذا ينشئ العلاقة بين المشترك وأرقام هواتفه.

سير عمل التوفير



التحقق من التعيين

استعلام قاعدة البيانات لاسترجاع المشترك مع جميع MSISDNs المرتبطة من خلال:

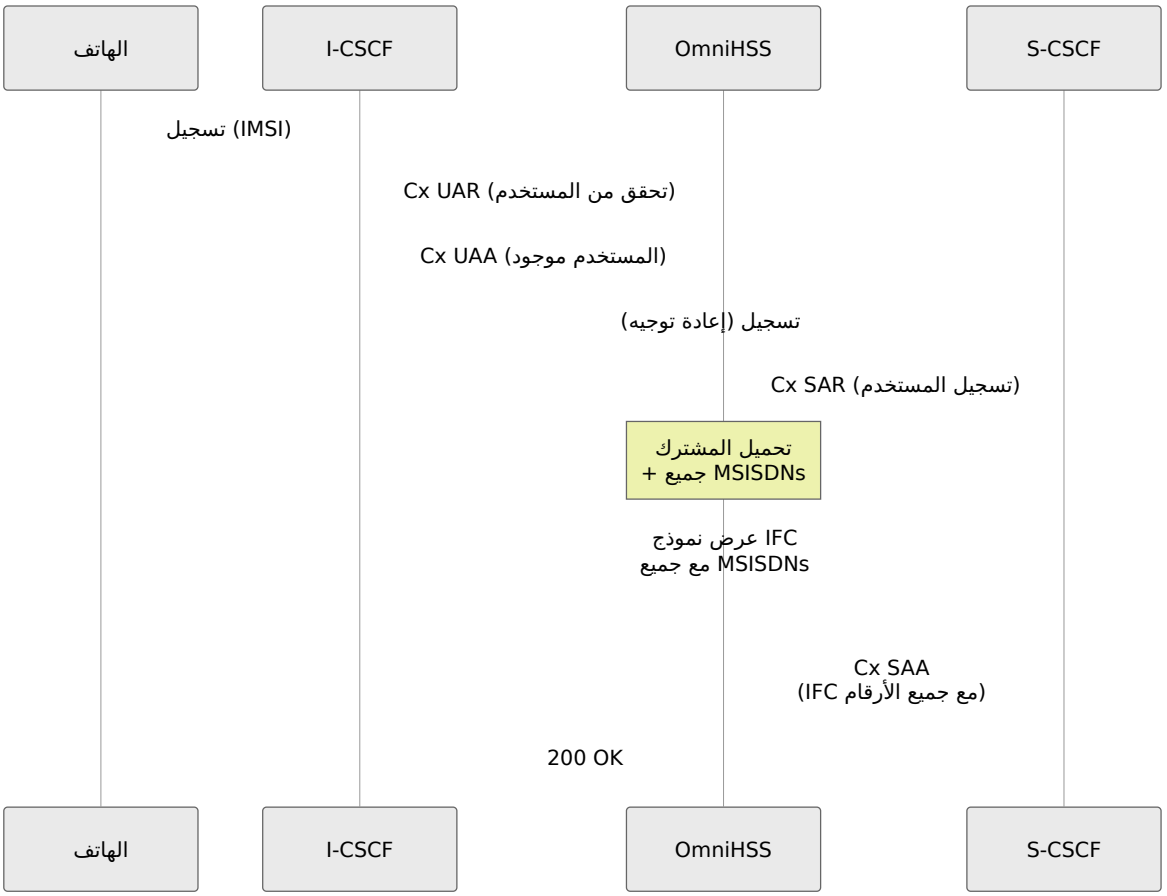
- الانضمام إلى جدول المشترك مع جدول الانضمام
- الانضمام إلى جدول الانضمام مع جدول msisdn
- تجميع النتائج حسب المشترك لرؤية جميع أرقام الهواتف معًا

سيظهر هذا معرف المشترك، IMSI، وقائمة بجميع MSISDNs المعينة.

تكامل IMS

تسجيل IMS

عندما يسجل المشترك في IMS، **يتم تضمين جميع MSISDNs المعينة** في ملف تعريف IMS المرسل إلى S-CSCF.



عرض نموذج IFC

يمكن لنموذج IMS IFC الإشارة إلى جميع MSISDNs باستخدام المتغير `{{msisdns}}`.

مثال على نموذج IFC:

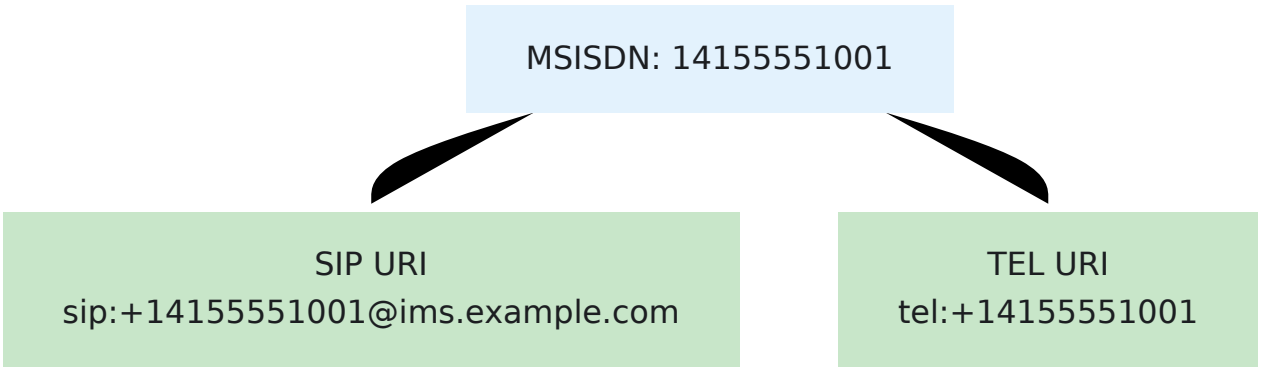
```
<ServiceProfile>
  <PublicIdentity>
    <Identity>sip:
{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <!-- تكرار لكل MSISDN -->
  <PublicIdentity>
    <Identity>sip:+14155551001@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551001</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>sip:+14155551002@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551002</Identity>
  </PublicIdentity>
  <!-- ... -->
</ServiceProfile>
```

متغير النموذج:

- `{{msisdns}}` - قائمة بجميع MSISDNs المعينة للمشترك

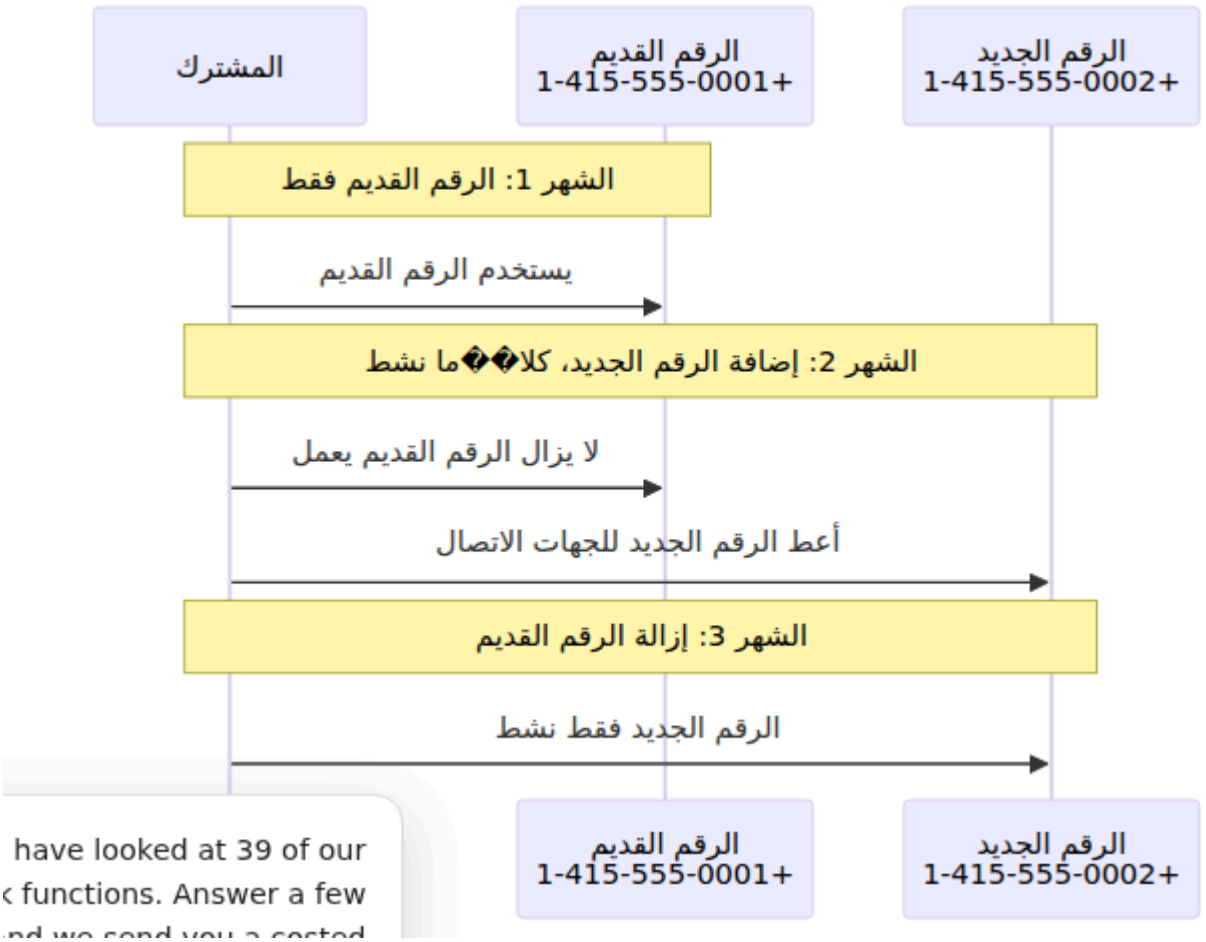
الهويات العامة

كل MSISDN عادةً ما ينتج عنه هويتان عموميتان IMS:



توجيه المكالمات الواردة

بتوجيه المكالمة إلى IMS عندما يتصل شخص ما بأحد أرقام المشترك، يقوم شبكة SIP URI الصحيح:



تقديم رقم المتصل للمكالمات الصادرة

يمكن للهاتف اختيار أي رقم لتقديمه كمعرف المتصل للمكالمات الصادرة.

مثال SIP INVITE:

```
INVITE sip:+15105551234@ims.example.com SIP/2.0
From: "+14155551002" <sip:+14155551002@ims.example.com>;tag=123
To: <sip:+15105551234@ims.example.com>
P-Asserted-Identity: <sip:+14155551002@ims.example.com>
```

تشير رؤوس `From` و `P-Asserted-Identity` إلى أي من أرقام المشترك يتم استخدامها.

استكشاف الأخطاء في Multi-MSISDN

المشكلة: MSISDN لا تظهر في تسجيل IMS

الأعراض:

- يظهر S-CSCF هوية عامة واحدة فقط
- تفشل المكالمات إلى الرقم الثاني

خطوات استكشاف الأخطاء:

1. **تحقق من تعيين MSISDN في قاعدة البيانات:**
    - استعلام قاعدة البيانات لاسترجاع جميع MSISDNs المرتبطة بـ IMSI المشترك
    - تحقق من جدول الانضمام لضمان وجود العلاقات
2. **تحقق من نموذج ملف IMS:**
    - تحقق من أن النموذج يتضمن المتغير `{{msisdns}}`
    - تأكد من أن بناء جملة النموذج هو XML صالح
3. **راجع سجلات HSS:**
    - ابحث عن رسائل تسجيل IMS (Cx SAR)
    - تحقق من تضمين جميع MSISDNs في الاستجابة
4. **اختبر تسجيل IMS:**
    - قم بتحفيز إعادة التسجيل على الهاتف
    - تحقق من سجلات S-CSCF لهويات العامة المسجلة

المشكلة: لا يمكن تعيين MSISDN للمشترك

الأعراض:

- فشل إدراج قاعدة البيانات
- خطأ: "إدخال مكرر" أو "قيود المفتاح الخارجي"

الأسباب المحتملة:

1. **تم تعيين MSISDN بالفعل:**
    - استعلام قاعدة البيانات للتحقق مما إذا كانت MSISDN مرتبطة بالفعل بمشترك آخر
    - **الحل:** قم بإزالة التعيين الحالي أولاً، ثم أنشئ التعيين الجديد
2. **MSISDN غير موجود:**
    - استعلام قاعدة البيانات للتحقق من وجود سجل MSISDN
    - **الحل:** قم بإنشاء سجل MSISDN أولاً عبر API أو إدراج قاعدة البيانات

المشكلة: المكالمات إلى رقم واحد تعمل، والآخر لا يعمل

الأعراض:

- تعمل المكالمات إلى الرقم الأساسي
- تفشل المكالمات إلى الرقم الثانوي أو تتجه بشكل غير صحيح

خطوات استكشاف الأخطاء:

1. **تحقق من كلا الرقمين في تسجيل IMS:**
    - تحقق من هويات العامة المسجلة في S-CSCF
    - تأكد من وجود كلا SIP URIs
2. **تحقق من قواعد توجيه IMS:**
    - تحقق من أن قواعد توجيه نموذج IFC تنطبق على جميع الهويات
    - تحقق مما إذا كان الرقم المحدد يحتاج إلى توجيه خاص
3. **اختبر كلا الرقمين:**

```
# اختبار من عميل SIP
sip:+14155551001@ims.example.com  # يجب أن يعمل
sip:+14155551002@ims.example.com  # يجب أن يعمل أيضًا
```

المشكلة: استعلام API عن MSISDN يعيد مشترك خاطئ

الأعراض:

- استعلام API `/api/subscriber/msisdn/:msisdn` يعيد مشترك غير متوقع

التحقق:

استعلام قاعدة البيانات لمعرفة أي مشترك تم تعيين MSISDN له. يجب أن يعيد هذا بالضبط مشترك واحد. إذا أعاد عدة مشتركين أو المشترك الخاطئ، فإن جدول الانضمام يحتوي على بيانات غير صحيحة تحتاج إلى تصحيح.

أفضل الممارسات

ترتيب التوفير

1. إنشاء جميع MSISDNs أولاً
2. إنشاء المشترك
3. تعيين MSISDNs للمشترك
4. التحقق من ��لتعيين قبل التفعيل

إدارة MSISDN

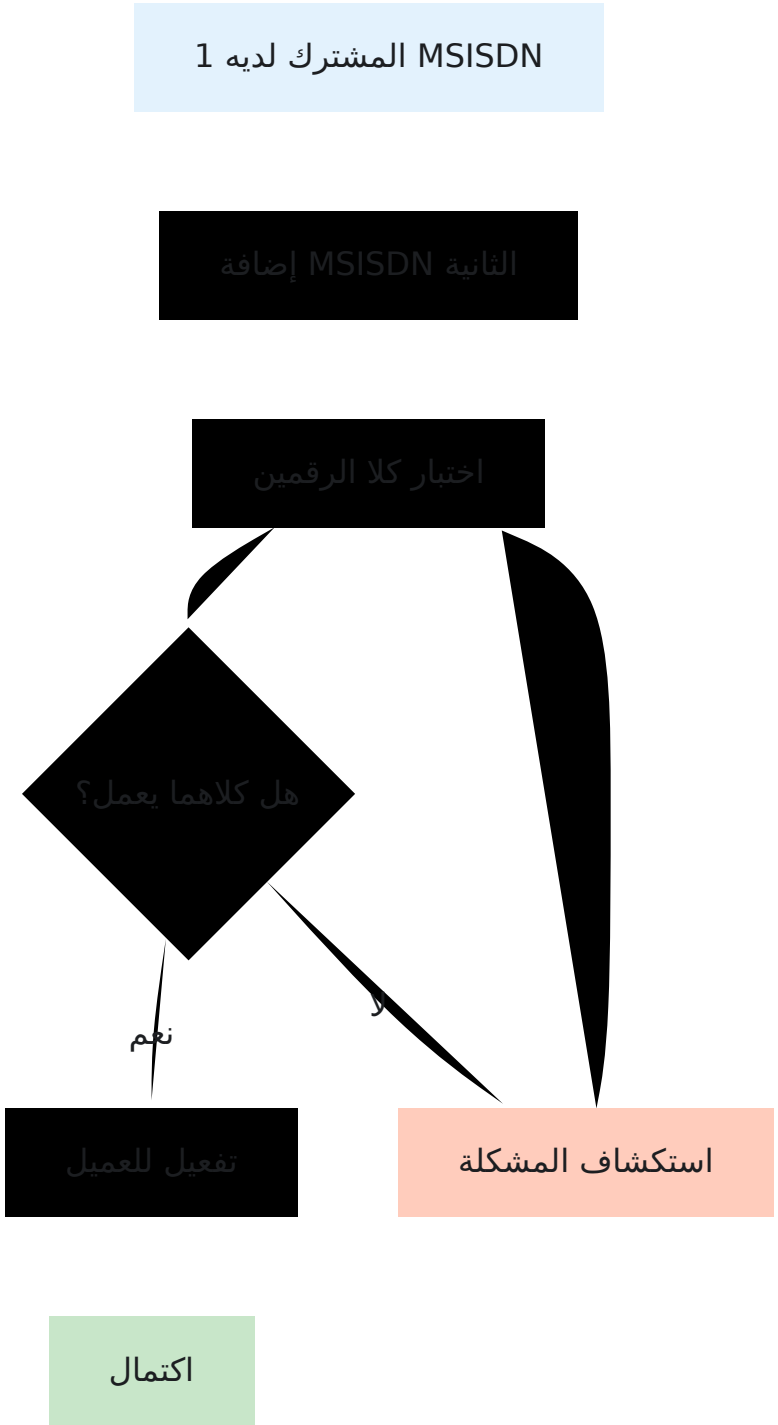
- **توثيق الأرقام الأساسية مقابل الثانوية** في custom_attributes للمشترك
- **نقل الأرقام بشكل متسلسل** عند النقل لتجنب انقطاع الخدمة
- **اختبار جميع الأرقام** بعد التوفير قبل إعطائها للعميل

تكوين IMS

- تأكد من أن نموذج IFC يتعامل مع عدة هويات عامة بشكل صحيح
- اختبار التوجيه الوارد لجميع الأرقام
- تحقق من تقديم معرف المتصل للمكالمات الصادرة

الهجرة

عند الانتقال من MSISDN واحدة إلى متعددة:



Multi-IMSI SIM: هويات شبكة متعددة

كيف يعمل

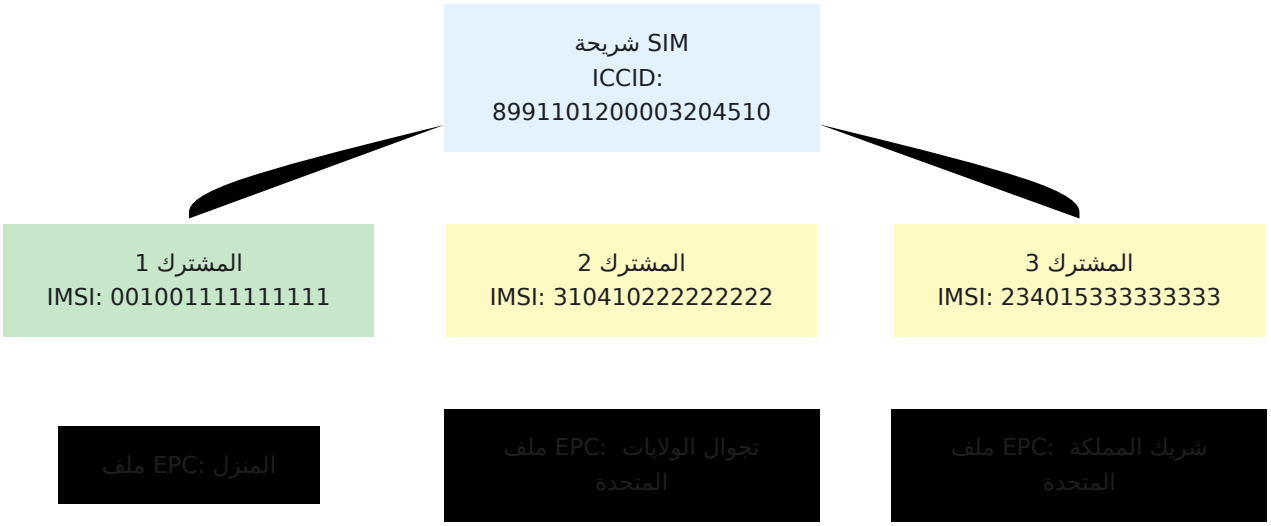
تحتوي شريحة SIM متعدد�� IMSI على عدة ملفات تعريف مشترك كاملة، كل منها مع IMSI خاص بها، ومفاتيح، وبيانات اعتماد. يمكن للجهاز التبديل بين

ما يتم ذلك تلقائيًا بناءً على الموقع أو توفر الشبكة.

IMSI **واحد فقط نشط في أي وقت**. عندما يتحول الجهاز إلى **IMSI مهم:** يمكن أن يكون النشط سابقًا IMSI تلقائيًا بإلغاء تسجيل HSS سيقوم، مختلف على نفس شريحة SIM.

تنفيذ OmniHSS

في OmniHSS، يتم توفير كل IMSI على شريحة SIM متعددة IMSI، كـ **سجل مشترك منفصل** ولكن جميعها تشير إلى **نفس شريحة SIM**:



حالات الاستخدام

1. تحسين التجوال الدولي

- المنزل: 001-001 (أسعار الشبكة المنزلية) IMSI
- تجوال الولايات المتحدة: 310-410 (أسعار محلية في الولايات المتحدة) IMSI
- تجوال الاتحاد الأوروبي: 234-015 (أسعار محلية في الاتحاد الأوروبي) IMSI
- بناءً على الموقع IMSI يتبدل الجهاز

2. خدمة MVNO

- MVNO (بائع) الأساسي: شبكة IMSI
- احتياطي: شبكة المضيف (المشغل الأم) IMSI
- غير متاحة MVNO فشل تلقائي إذا كانت تغطية

3. IoT/M2M متعددة الشبكات

- IMSI 1: الناقل الأساسي
- IMSI 2: الناقل الاحتياطي للموثوقية
- IMSI 3: احتياطي الطوارئ/منخفض التكلفة
- تحافظ الأجهزة الحرجة على الاتصال

4. الامتثال التنظيمي

- IMSIs مختلفة لمناطق تنظيمية مختلفة
- الامتثال لمتطلبات الإقامة المحلية للبيانات
- استخدام هوية الشبكة المحلية لكل ولاية قضائية

ميزات Multi-IMSI

مصادقة مستقلة

- كل IMSI لديه Ki و OPC ومجموعة مفاتيح خاصة به
- متجهات مصادقة منفصلة لكل IMSI
- بيانات اعتماد أمنية مختلفة لكل شبكة

ملفات تعريف خدمة منفصلة

- ملفات EPC مختلفة (عرض النطاق الترددي، APNs)
- ملفات IMS مختلفة (خدمات الصوت)
- قواعد تجوال مختلفة لكل IMSI

هوية مادية مشتركة

- جميع IMSIs تشير إلى نفس شريحة SIM (عبر sim_id)
- نفس ICCID عبر جميع سجلات المشترك
- تجميع منطقي عبر شريحة SIM

اختيار الشبكة

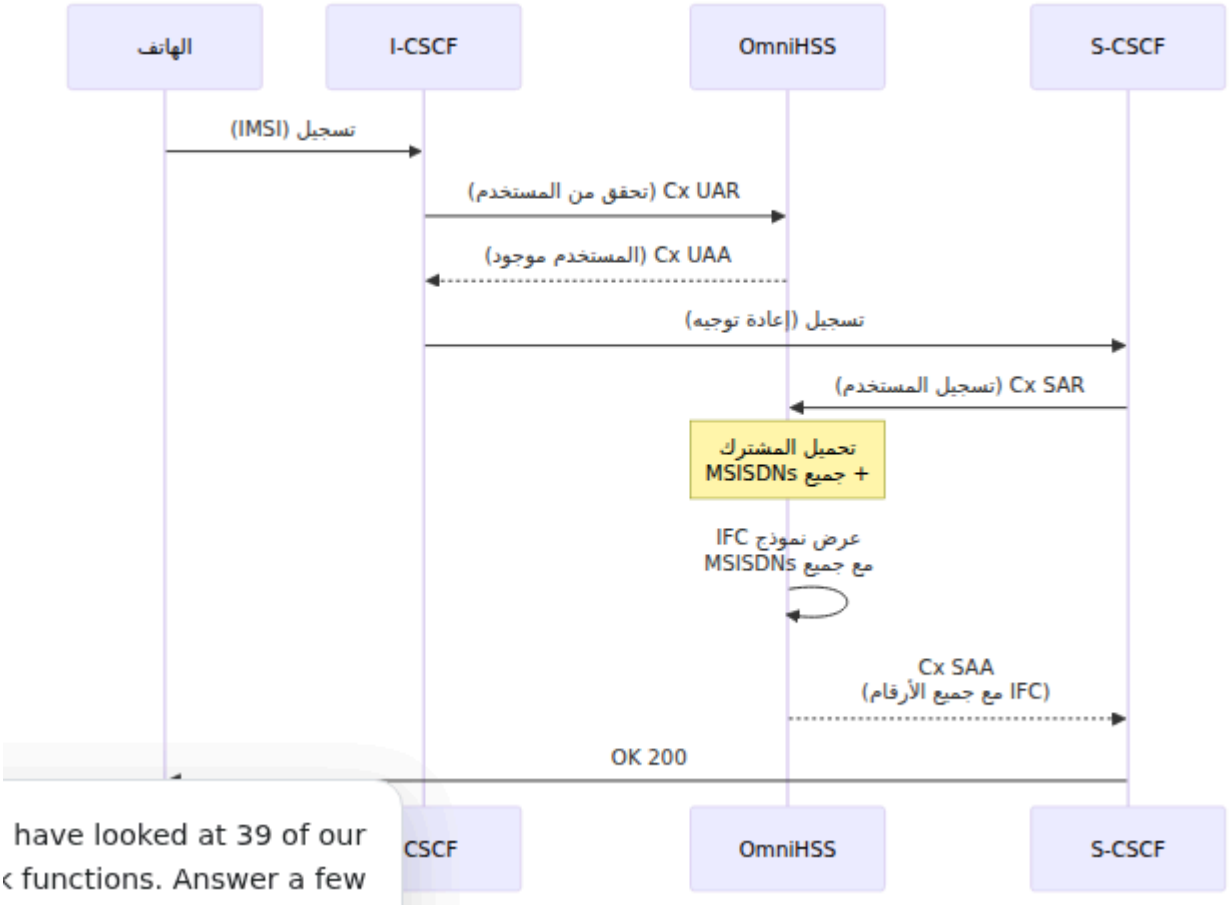
- يقرر الجهاز أو شريحة SIM أي IMSI يجب استخدامها
- بناءً على الشبكات المتاحة، الموقع، السياسة
- يقوم HSS بمصادقة أي IMSI يقدمها الجهاز

التكوين

```
# 1. إنشاء شريحة SIM (قابلة لـ multi-IMSI)
SIM_ID=$(curl -k -X POST https://hss.example.com:8443/api/sim \
  -d '{"sim": {"iccid": "8991101200003204510", "is_esim": false}}'
\
  | jq -r '.data.id')

# 2. إنشاء مجموعة مفاتيح لـ IMSI 1 (شبكة المنزل)
KEYSET1=$(curl -k -X POST https://hss.example.com:8443/api/key_set
\
  -d '{"key_set": {"ki": "0123456789ABCDEF...", "opc":
"FEDCBA9876..."}}' \
  | jq -r '.data.id')

# 3. إنشاء المشترك 1 (IMSI المنزل)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d "{\"subscriber\": {
    \"imsi\": \"001001111111111\",
    \"sim_id\": \"$SIM_ID\",
    \"key_set_id\": \"$KEYSET1\",
    \"epc_profile_id\": \"e58ed763-928c-4155-bee9-fdbaaadc15f3\"
  }}"

# 4. إنشاء مجموعة مفاتيح لـ IMSI 2 (شريك التجوال)
KEYSET2=$(curl -k -X POST https://hss.example.com:8443/api/key_set
\
  -d '{"key_set": {"ki": "1111111111111111...", "opc":
"2222222222..."}}' \
  | jq -r '.data.id')

# 5. إنشاء المشترك 2 (IMSI التجوال)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d "{\"subscriber\": {
    \"imsi\": \"310410222222222\",
    \"sim_id\": \"$SIM_ID\",
    \"key_set_id\": \"$KEYSET2\",
    \"epc_profile_id\": \"f47ac10b-58cc-4372-a567-0e02b2c3d479\"
  }}"

# 6. تكرار لـ IMSIs الإضافية على شريحة SIM...
```

تدفق المصادقة

عندما يتصل جهاز متعدد IMSI:



يقدمها الجهاز IMSI يقوم بمصادقة أي .IMSI متعددة SIM إلى معرفة أنه شريحة HSS لا يحتاج.

وإلغاء التسجيل التلقائي IMSI تبديل

واحد فقط IMSI إلى أخرى، يمكن أن يكون هناك IMSI من IMSI متعددة SIM عندما تتحول شريحة مع ذلك تلقائيًا عن طريق إرسال **طلب إلغاء** OmniHSS مسجل في الشبكة في أي وقت. يتعامل **الموقع (CLR)** جديد من نفس شريحة IMSI النشط سابقًا عندما يسجل IMSI لإلغاء تسجيل SIM.

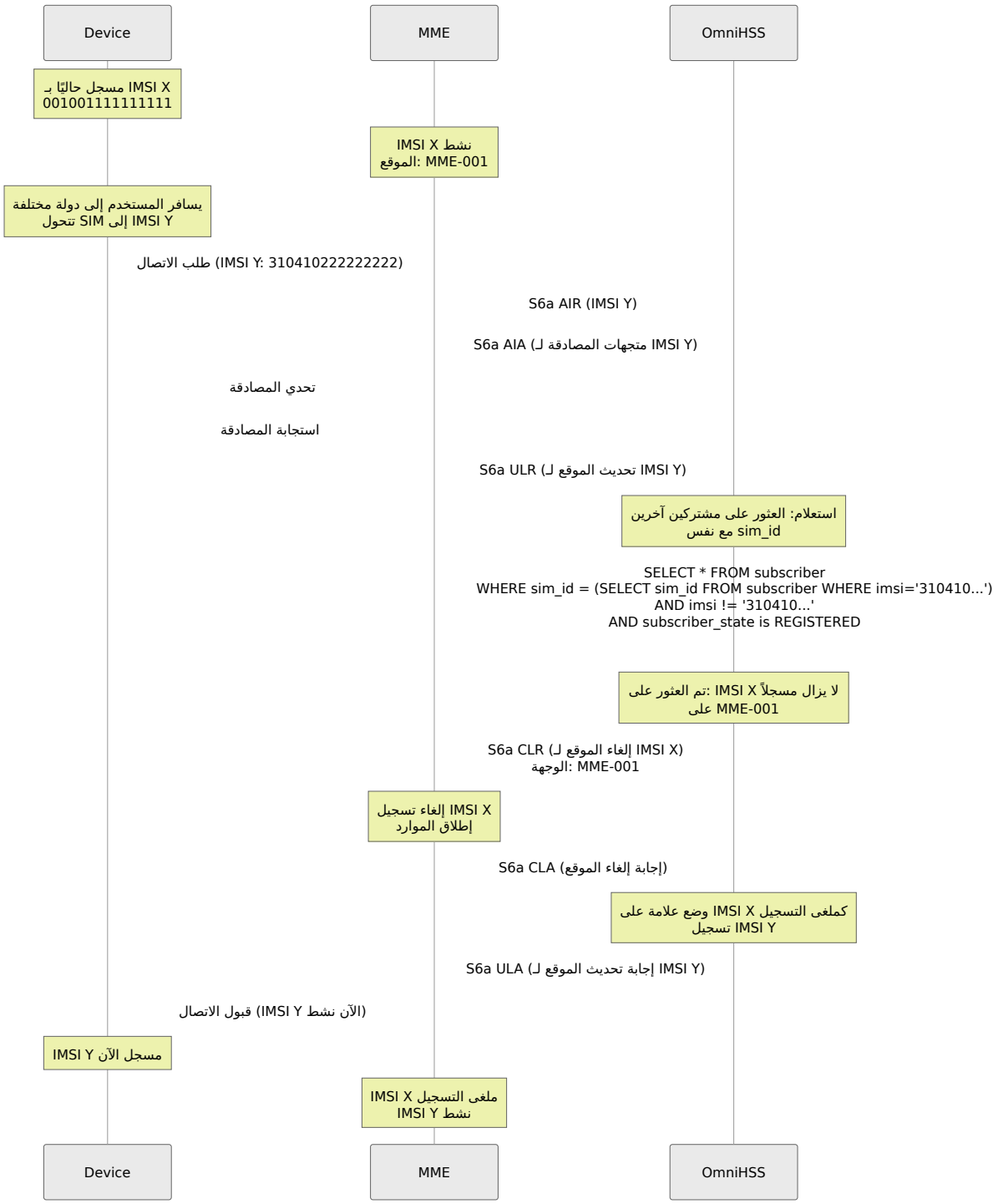
النشطة الواحدة IMSI قاعدة

نشطة في أي SIM لكل شريحة (IMSI) **المفهوم الرئيسي:** يمكن أن يكون هناك مشترك واحد وقت.

- **IMSI X** باستخدام MME إذا كان المشترك مسجلاً على
- **IMSI Y** طلب تحديث الموقع لـ HSS وتلقى (IMSI X مثل SIM على نفس شريحة)
- **IMSI X** تلقائيًا بإرسال **طلب إلغاء الموقع** لإلغاء تسجيل HSS يقوم

ويمنع حدوث تعارضات في الشبكة IMSIs هذا يضمن انتقالًا نظيفًا بين.

تدفق تبديل IMSI



لماذا هذا مهم

سلامة الشبكة:

- يمنع التسجيلات المكررة من نفس بطاقة SIM الفعلية

- يضمن تحرير موارد الشبكة بشكل صحيح
- يحافظ على بيانات موقع المشترك بدقة

دقة الفوترة:

- يتم فرض رسوم على IMSI واحد فقط للوصول إلى الشبكة في وقت واحد
- حدود جلسة واضحة بين تبديلات IMSI
- توليد دقيق لسجلات تفاصيل المكالمات (CDR)

إدارة الموارد:

- يتم تحرير موارد MME لـ IMSI القديم
- يتم تنظيف سياقات PDP وحوامل البيانات
- يبقى تتبع الموقع دقيقًا

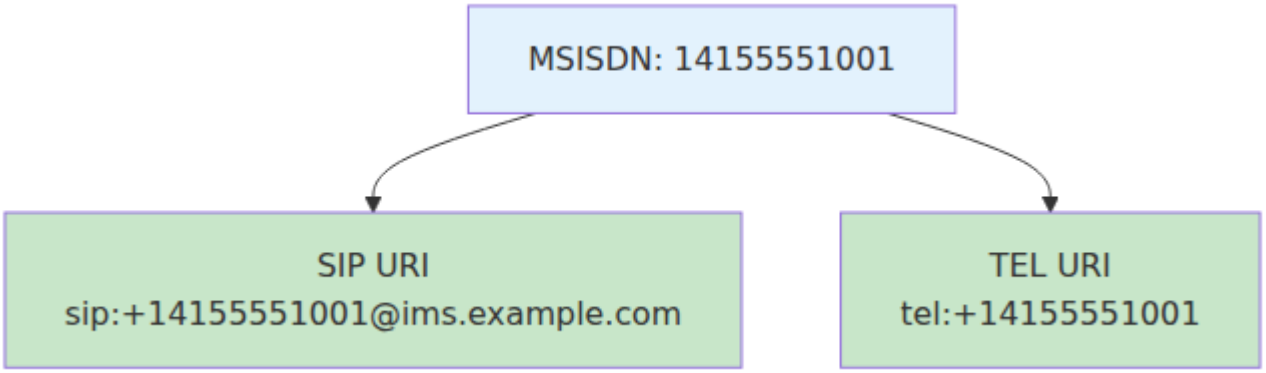
محفزات تبديل IMSI

يقرر الجهاز / SIM متى يتم تبديل IMSIs بناءً على:

1. **توفر الشبكة**
    - شبكة IMSI المنزلية غير متاحة
    - شريك التجوال IMSI التبديل إلى
2. **الاختيار اليدوي**
    - يختار المستخدم الشبكة يدويًا
    - المقابل IMSI إلى SIM يتبدل
3. **استنادًا إلى السياسات**
    - تحتوي بطاقة SIM على قواعد داخلية (مثل: تفضيل IMSI المحلي في دول معينة)
    - التبديل التلقائي استنادًا إلى MCC / MNC
4. **تحسين التكلفة**
    - بمعدلات تجوال أقل IMSI التبديل إلى
    - استخدام IMSI المحلي لتجنب رسوم التجوال

اعتبارات IMS

ينطبق نفس سلوك طلب إلغاء الموقع على تسجيل IMS:



الأثر التشغيلي

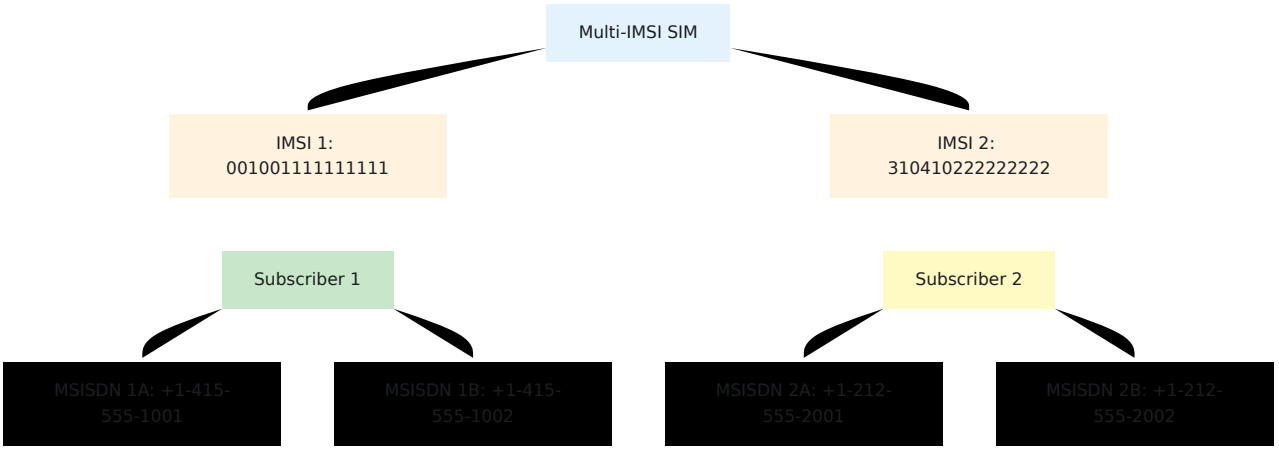
للعاملين في العمليات:

1. عندما يتم تبديل IMSI، سيظهر IMSI القديم كـ "غير مسجل" في HSS. هذا سلوك طبيعي. **يظهر المشترك غير متصل:**
2. ستحتوي بطاقات SIM متعددة IMSI على نفس `sim_id`. سيكون واحد فقط في حالة تشترك في سجلات مشتركين متعددة في وقت واحد "مسجل". **سجلين مشتركين لبطاقة SIM واحدة:**
3. تتبع جدول `subscriber_state` أي MME/SGSN تم تسجيل كل IMSI به. عندما يتم تبديل IMSI، يتم مسح الموقع القديم. **تتبع الموقع:**
4. إذا لم يكن بالإمكان الوصول إلى جهاز **استكشاف الأخطاء:**:
   - تحقق من أي IMSI مسجل حاليًا
   - تحقق من أن IMSI الصحيح يتم استخدامه للشبكة الحالية
   - تأكد من أن IMSI واحد فقط لكل SIM في حالة التسجيل

السيناريوهات المجمعة

Multi-IMSI + Multi-MSISDN

يمكنك دمج كلا الميزتين: عدة IMSIs على بطاقة SIM واحدة، كل منها مع عدة MSISDNs.



حالة استخدام مثال:

- **شبكة المنزل (IMSI 1):**
  - الرقم الشخصي: +1-415-555-1001
  - الرقم التجاري: +1-415-555-1002
- **شبكة التجوال الأمريكية (IMSI 2):**
  - الرقم الشخصي: +1-212-555-2001
  - الرقم التجاري: +1-212-555-2002

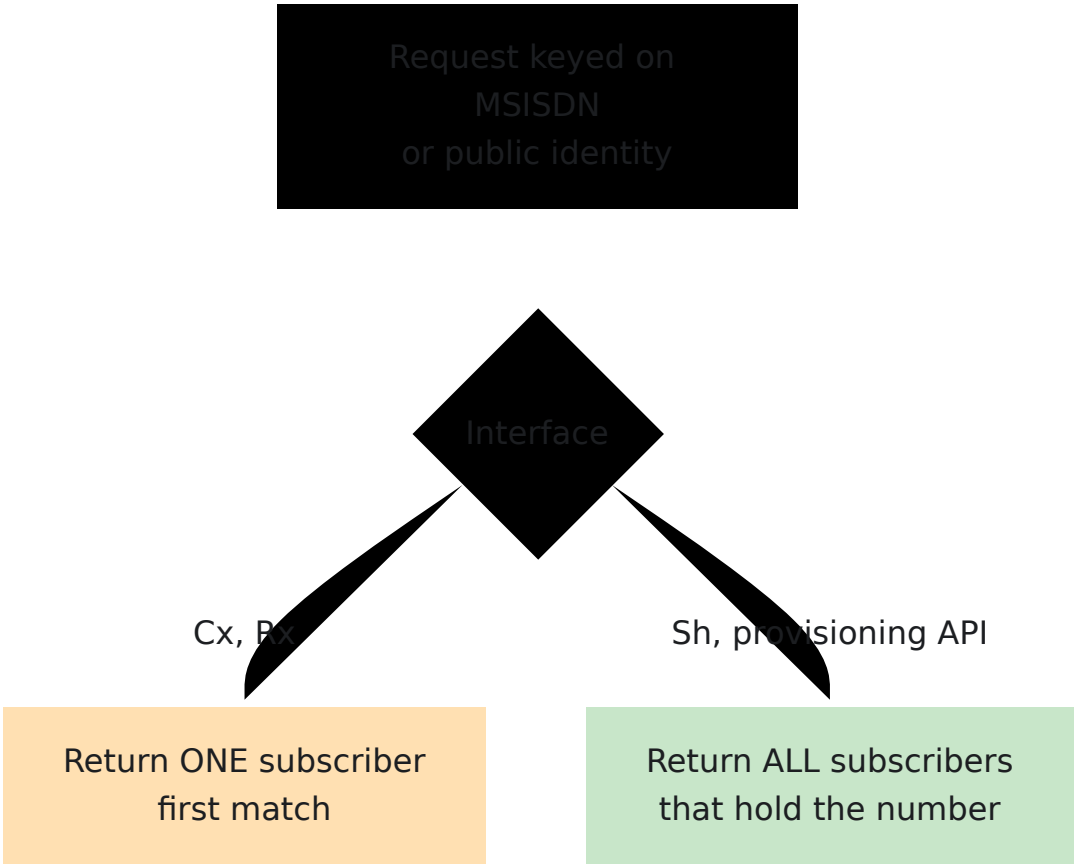
عندما يكون الجهاز في الإقليم المنزلي، يستخدم IMSI 1 مع MSISDNs الخاصة به. عند التجوال في الولايات المتحدة، يتبدل إلى IMSI 2 مع MSISDNs مختلفة محسّنة لشبكة الولايات المتحدة.

حل MSISDN عبر الواجهات

MSISDN هو كيان مشترك في نموذج البيانات. يمكن لمشترك واحد أن يحمل العديد من MSISDNs (IMSI واحد، عدة أرقام). يمكن أن يتم الاحتفاظ بـ MSISDN واحد من قبل العديد من المشتركين (عدة IMSIs، على سبيل المثال هاتف وساعة ذكية). انظر كيان (رقم واحد، Subscriber و MSISDN لنموذج البيانات.

نظرًا لأن الرقم ليس دائمًا فريدًا لمشترك واحد، يجب على كل واجهة أن تقرر كيفية حل الطلب الذي يصل مفاتيحه على MSISDN أو على هوية عامة تحتوي على MSISDN. يستخدم OmniHSS قاعدتين مختلفتين للحل، ويجب أن تعرف أي قاعدة تستخدمها واجهة.

قاعدتان للحل



- **إرجاع واحد.** تعيد عملية البحث مشتركًا واحدًا (أول تطابق). تستخدم واجهات **Cx** و **Rx** هذه القاعدة.
- **إرجاع الكل.** تعيد عملية البحث كل مشترك يحمل الرقم. تستخدم واجهة **Sh** وواجهة API الخاصة بالتزويد هذه القاعدة.

السلوك حسب الواجهة

الواجهة	مفاتيح على	Multi-MSISDN لكل IMSI	Multi-IMSI لكل MSISDN (رقم مشترك)
Cx UAR, MAR	الهوية الخاصة (IMSI)	صحيح. IMSI دقيق.	صحيح. كل IMSI منفصل.
Cx SAR	الهوية الخاصة، أو الهوية العامة	صحيح. تسرد IFC كل MSISDN للمشترك.	يتم حلها إلى مشترك واحد إذا كانت مفاتيحها على الرقم المشترك. استخدم الهوية الخاصة (IMSI) لاختيار مشترك معين.
Cx LIR	الهوية العامة	صحيح.	يتم حلها إلى مشترك **مسجل** (واحد لديه S-CSCF مخصص) عندما يكون الرقم مشتركًا، لذا تعيد الطلبات النهائية عقدة

الواجهة	مفاتيح على	Multi-MSISDN لكل IMSI	Multi-IMSI لكل MSISDN (رقم مشترك)
			خدمية قابلة للوصول.
Sh UDR, PUR, SNR	هوية المستخدم (MSISDN أو هوية عامة)	صحيح. البيانات لكل مشترك.	تعيد جميع المشتركين الذين يحملون الرقم. يقوم UDR بتجميع بياناتهم. يقوم PUR بتحديث جميعهم.
Rx AAR	مشترك جلسة الب��انات	يمكن أن يكون للمشترك العديد من الأرقام، لكن الإجابة تحمل MSISDN واحدًا كـ Subscription-Id (يسمح البروتوكول بواحد).	صحيح. يتم اختيار الرقم من جلسة البيانات، وليس عن طريق البحث العكسي.
API `GET /subscriber/msisdn/:msisdn`	MSISDN	تعيد المشترك.	تعيد جميع المشتركين الذين يحملون الرقم.

ماذا يعني هذا في الممارسة العملية

- **التسجيل والمصادقة دائمًا صحيحة.** مسار تسجيل IMS (Cx MAR، SAR، UAR) يسجل كل جهاز باستخدام IMSI. مفاتيحه على الهوية الخاصة، التي تحتوي على IMSI الخاص به، لذا يسجل الهاتف وساعة ذكية تشتركان في رقم ويصادقان بشكل مستقل.
- **يحتفظ المشترك بجميع أرقامه.** بالنسبة لـ IMSI واحد مع العديد من MSISDNs، تسرد بيانات مستخدم Cx SAR كل رقم كهوية عامة (`sip:` و `tel:`).
- **يتم حل الرقم المشترك إلى مشترك واحد على Cx وإلى جميع المشتركين المشتركين على Sh.** هذه هي الفرق في الحل في الجدول أعلاه. في لمسار S-CSCF الخدمي مشتركًا **مسجلًا** مشتركًا، لذا يعيد HSS يفضل (Cx LIR) النهائي لجهاز يمكن الوصول إليه. كيفية تسليم المكالمة بعد ذلك إلى الأجهزة المسجلة هي مسألة نواة IMS، وليست مسألة HSS.
- **استخدم IMSI أو ICCID للتصرف على مشترك معين.** البحث العكسي عن الرقم ليس فريدًا عندما يكون الرقم مشتركًا.

المواصفات

تمتلك النموذجان حالة معيارية مختلفة. اعرف أيهما تستخدم.

Multi-MSISDN لكل IMSI 3GPP **موحد.** يحدد أكثر من رقم واحد لاشتراك واحد:

- **خيار تعدد الأرقام** (3GPP TS 23.008، الفقرة 2.1.3). يخزن HLR/HSS MSISDN الأساسي إلى الرقم MSISDN إضافية. يشير مؤشر MSISDNs أساسي بالإضافة إلى SGSN و VLR الذي يستخدمه.
- **MSISDN إضافي (A-MSISDN)** (3GPP TS 23.003، الفقرة 18.9). يتم "تعيين MSISDNs المعينة مسبقًا" بالإضافة إلى PS لمستخدم لديه اشتراك A-MSISDN و"يجب أن يتم تعيينه بشكل فريد لكل IMSI".

Multi-IMSI لكل MSISDN يتم تحقيقه على **هو نمط تنفيذ، وليس معيار شبكة واحد.** يخزن عدة IMSI بواسطة تطبيق متعدد SIM بطاقة IMSIs ويتبدل بينها (مصطلح الصناعة: Multiple-IMSI-Multiple-MSISDN، MIMM). التوجيهات ذات الصلة من GSMA هي GSMA IR.73 Steering of Roaming، ولـ eSIM مواصفات ملف SGP.2x/SGP.32. على جانب الشبكة، لا يقوم 3GPP بتوحيد MSISDN واحد عبر عدة اشتراكات كخدمة؛ بدلاً من ذلك، يفرض ذلك:

- **Correlation MSISDN (C-MSISDN)** (3GPP TS 23.003، الفقرة 18.7). يتم تعيين C-MSISDN بشكل فريد لكل IMSI وهوية مستخدم IMS. يمكن أن "تعيين MSISDN الخاصة" الذي لا يتم مشاركته من قبل أكثر من هوية مستخدم IMS يعمل فقط

لذا لا يمكن استخدام رقم مشترك لمطابقة جلسة SRVCC. C-MSISDN خاصة" كـ
خطط لـ SRVCC و CS fallback برقم لكل IMSI، وليس الرقم المشترك.

مواصفات الواجهة:

- Cx (MAR، SAR، UAR، LIR): 3GPP TS 29.228 3 وGPP TS 29.229.
- Sh (UDR، PUR، SNR): 3GPP TS 29.328 3 وGPP TS 29.329.

النموذج	الحالة	المرجع
Multi-MSISDN لكل IMSI	موحد	TS 23.008 §2.1.3 (تعدد الأرقام)؛ TS 23.003 §18.9 (A-MSISDN، فريد لكل IMSI)
Multi-IMSI لكل MSISDN	نمط تطبيق (MIMM)؛ مقيد على الشبكة	GSMA IR.73؛ TS 23.003 §18.7 (لا يمكن أن يكون MSISDN مشتركًا C-MSISDN)

هوية المستخدم العامة المشتركة (رقم واحد، عدة أجهزة)

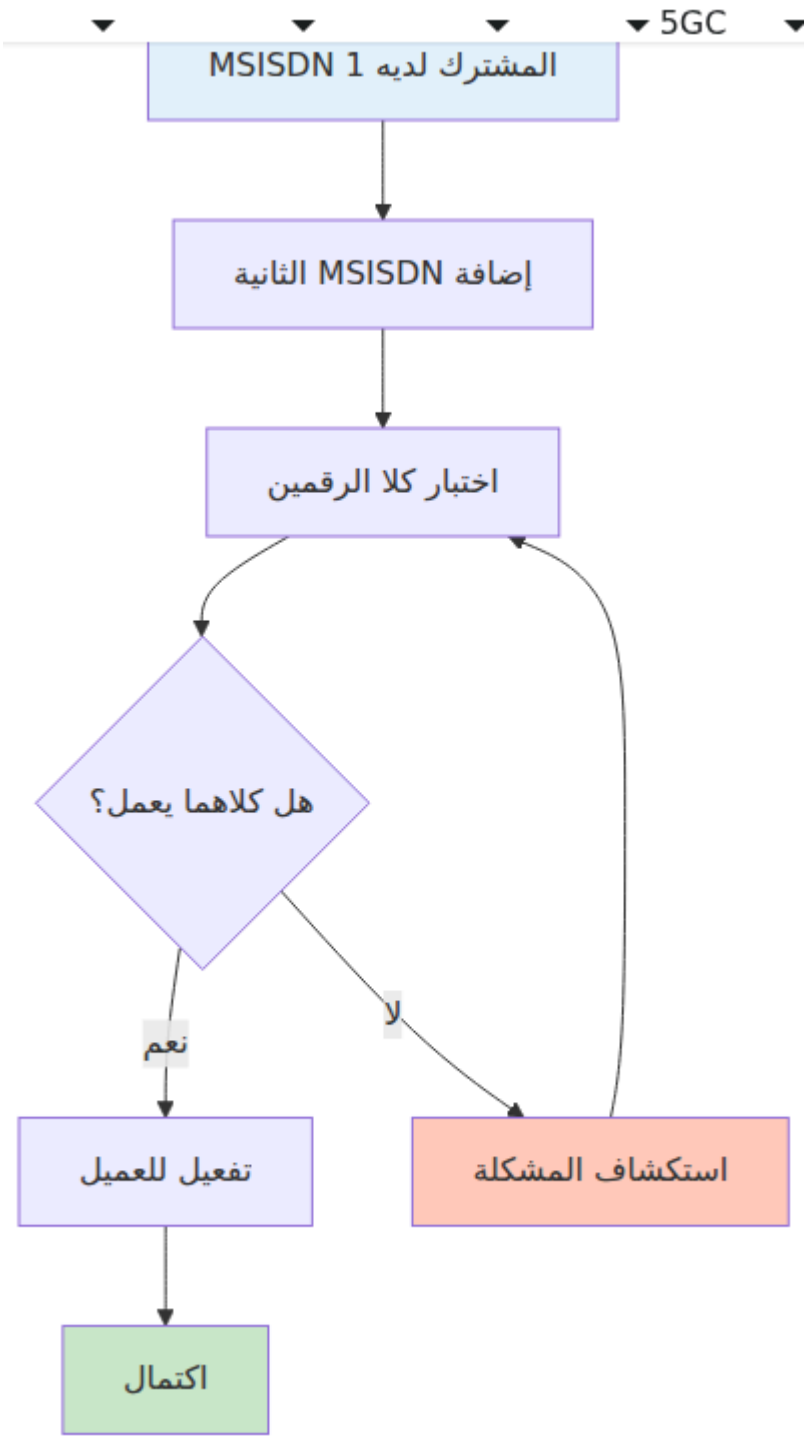
على سبيل المثال هاتف وساعة ذكية رفيقة على بطاقات) لجعل رقم واحد يرن على عدة أجهزة لهوية مستخدم GPPواحد. هذا هو نموذج 3 **IMS** قم بتجميع الأجهزة في **اشتراك**، (منفصلة SIM عامة مشتركة (3GPP TS 23.228): عدة هويات مستخدم خاصة (IMPIs، واحدة لكل IMSI) بتوجيه S-CSCF خدمية واحدة. ثم يقوم S-CSCF، تشترك في هوية عامة واحدة، والأهم من ذلك مكالمة نهائية إلى كل جهاز مسجل.

منفصلان. يمكن تعيينهم إلى IMS بدون مجموعة، فإن مشتركين يشاركون رقمًا فقط هما اشتراكان مختلفة، لذا تصل المكالمة النهائية فقط إلى الأجهزة على أحدهما. تزيل مجموعة S-CSCFs `ims_subscription` هذه الفجوة من خلال منح الأعضاء S-CSCF مشترك.

كيف يعمل

- تحتوي `ims_subscription` على S-CSCF المشترك للمجموعة (`assigned_scscf`).
- يشير كل مشترك عضو إلى المجموعة (`ims_subscription_id`).

- المجموعة على تلك HSS واحدًا. يثبت HSS S-CSCF عندما يسجل العضو الأول، يختار أيًا S-CSCF، تسجيلها. يتم توجيه كل عضو لاحق إلى نفس Cx SAR العقدة عندما يؤكد كانت S-CSCF التي تدعي تسجيله.
- حقيقية. مع S-CSCF دائمًا ما يحمل المثبت عقدة `selection_method: :pool_uri`، يعيد HSS اسم المجموعة في أول REGISTER، لكنه يثبت العقدة التي اختارها DNS، انظر وليس اسم المجموعة. One Serving S-CSCF Per Subscription.
- تعيد إعادة التسجيل العقدة المثبتة، وليس اسم المجموعة أبدًا.
- يتم تحرير S-CSCF عضو **آخر** إلغاء تسجيل المشترك فقط عندما يتم.
- عند طلب نهائي (Cx LIR) يعيد HSS S-CSCF المشترك بينما يكون أي عضو مسجلاً.
- عضو (مجموعة التسجيل الضمنية)، لذا يسجل IMPI كل Cx SAR تسرد بيانات مستخدم S-CSCF المجموعة بالكامل. يقدم ملف خدمة مشترك اختياري على المجموعة iFC واحدة للهويات المشتركة.
- عند طلب Sh لهوية المستخدم العامة المشتركة (مرجع البيانات `IMSPublicIdentity`)، يتضمن HSS `<IMSPrivateUserIdentity>` واحدة لكل IMSI على سبيل المثال) عضو في بيانات المستخدم. يعد خادم التطبيق MMTel TAS) لذا يسمح IMSI، هذه لاكتشاف رقم مشترك: يعد العد أكبر من واحد رقمًا مشتركًا متعدد للمكالمة النهائية بالتفرع إلى كل جهاز. يُعيد الرقم العادي AS `<IMSPrivateUserIdentity>` واحدة فقط ويتم تسليمه إلى جهة اتصال واحدة.



التزويد

قم بإنشاء المجموعة، واربط كل مشترك جهاز بها، وخصص الرقم المشترك لكل عضو.

```
# 1. إنشاء اشتراك IMS (المجموعة). يحدد ims_profile_id الاختياري ملف
خدمة مشترك
#    للهويات المشتركة للمجموعة.
GROUP_ID=$(curl -k -X POST
https://hss.example.com:8443/api/ims_subscription \
  -H "Content-Type: application/json" \
  -d '{"name": "Smith family - shared number"}' | jq -r
'.response.id')

# 2. ربط كل مشترك عضو بالمجموعة ومنحه MSISDN المشترك.
curl -k -X PATCH
https://hss.example.com:8443/api/subscriber/$PHONE_SUBSCRIBER_ID \
  -H "Content-Type: application/json" \
  -d "{\"ims_subscription_id\": \"$GROUP_ID\", \"msisdns\":
[\"$SHARED_MSISDN_ID\"]}"

curl -k -X PATCH
https://hss.example.com:8443/api/subscriber/$WATCH_SUBSCRIBER_ID \
  -H "Content-Type: application/json" \
  -d "{\"ims_subscription_id\": \"$GROUP_ID\", \"msisdns\":
[\"$SHARED_MSISDN_ID\"]}"
```

المعلمات:

المعلمة	النوع	مطلوب	الوصف
`name`	سلسلة	نعم	اسم قابل للقراءة البشرية لاشتراك IMS (فريد).
`ims_profile_id`	UUID	لا	ملف خدمة مشترك (iFC) للهويات المشتركة للمجموعة. عند عدم وجوده، يقدم كل عضو ملف IMS الخاص به.
`ims_subscription_id`	UUID	لا	على مشترك: المجموعة التي ينتمي إليها. عند عدم وجوده، يكون المشترك خاص به، S-CSCF مستقلًا (الافتراضي).

على المجموعة حالة وقت `last_seen_scscf_timestamp` و `assigned_scscf` تكون التشغيل التي كتبها HSSلا تقوم بتعيينها؛.

ملاحظات

- هو مستقل ويتصرف تمامًا `ims_subscription_id` المشترك الذي لا يحتوي على كما كان من قبل.
- بحيث يتم حل الرقم المشترك إلى المجموعة. يمكن MSISDN أعط الأعضاء نفس للأعضاء الاحتفاظ بأرقام إضافية خاصة بهم.
- `ims_subscription_id` لا يؤدي حذف مجموعة إلى حذف مشتركيها؛ يتم مسح الخاصة بهم ويصبحون مستقلين.

الإجراءات التشغيلية

إدارة المشت��كين Multi-MSISDN

عرض جميع MSISDNs لمشترك:

```
استعلام عبر API: GET /api/subscriber/imsi/:imsi
```

تتضمن الاستجابة جميع MSISDNs المرتبطة.

استكشاف الأخطاء Multi-IMSI

الجهاز لا يتصل بـ IMSI الثاني:

1. تحقق من وجود سجل مشترك ثاني لذلك IMSI
2. تحقق من تكوين key_set بشكل صحيح لذلك IMSI
3. تحقق من تعيين ملف EPC
4. تأكد من أن قواعد التجوال تسمح بالاتصال

الجهاز يتبدل بين IMSIs بشكل غير متوقع:

- يتم التحكم في ذلك بواسطة منطق الجهاز / SIM، وليس HSS

- يقوم HSS بمصادقة أي IMSI يتم تقديمه
- تحقق من إعدادات اختيار IMSI للجهاز

استكشاف الأخطاء Multi-MSISDN

الرقم الثاني لا يرن:

1. تحقق من ربط MSISDN في جدول الانضمام
2. تحقق من أن قالب ملف IMS يتضمن متغير `{{msisdns}}`
3. تأكد من أن تسجيل IMS يتضمن جميع الهويات العامة
4. راجع سجلات S-CSCF للهويات المسجلة

المكالمات الصادرة تظهر رقمًا واحدًا فقط:

- يختار الجهاز الرقم الذي سيظهر كمعرف المتصل
- هذا هو تكوين الجهاز، وليس HSS
- يوفر HSS جميع الهويات؛ يختار الجهاز

ملخص الفوائد

فوائد Multi-MSISDN

✓ بطاقة SIM واحدة، عدة أرقام هاتفية ✓ خطوط تجارية وشخصية منفصلة ✓ وجود محلي دولي ✓ تبسيط إدارة الأجهزة ✓ جميع الأرقام تشترك في نفس خدمة البيانات ✓ فوترة مركزية لكل IMSI

فوائد SIM Multi-IMSI

✓ تكاليف تجوال محسّنة ✓ اختيار تلقائي للشبكة ✓ تكرار وفشل ✓ هوية شبكة محلية ✓ الامتثال التنظيمي ✓ استمرارية الخدمة عبر الشبكات

فوائد مجمعة

✓ ✓ أقصى مرونة ✓ مجموعات أرقام مختلفة لكل شبكة ✓ محسّنة لكل حالة استخدام سيناريوهات أعمال معقدة ✓ تحسين دولي ومحلي

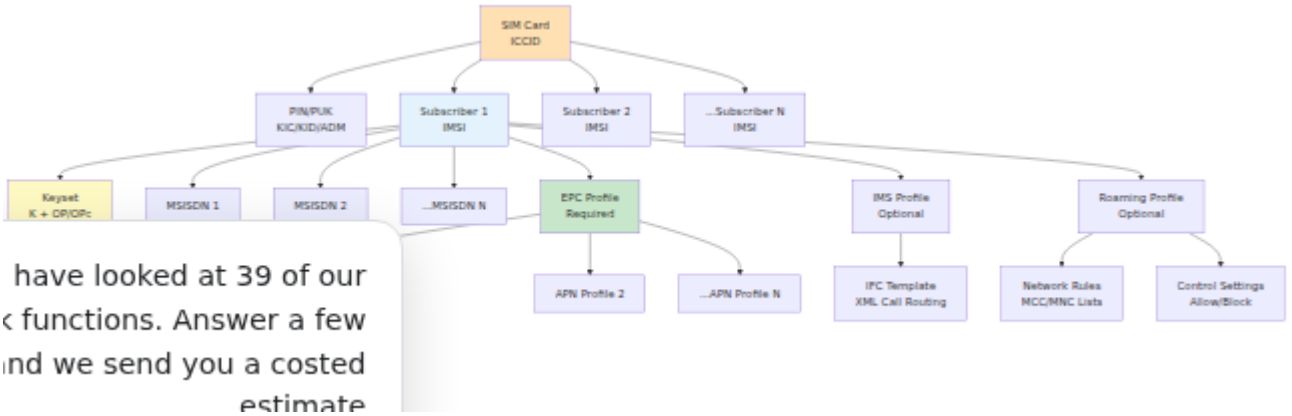
العودة إلى دليل العمليات ←

إدارة ملفات OmniHSS

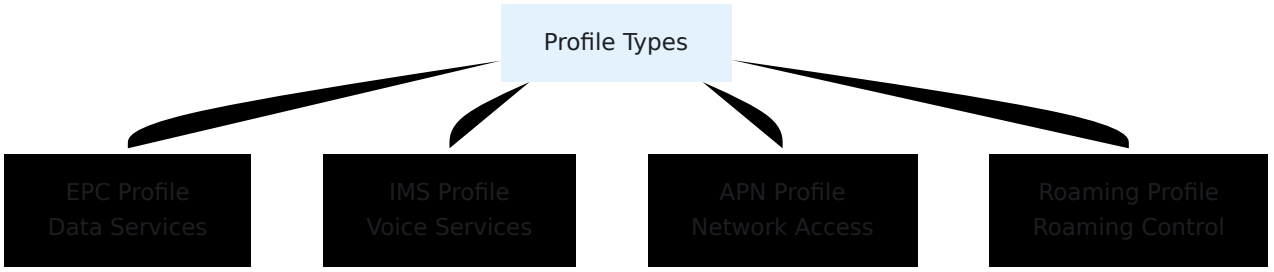
← العودة إلى دليل العمليات

نظرة عامة

تستخدم OmniHSS **الملفات الشخصية** لتعريف خصائص الخدمة للمشتركين. تتيح الملفات الشخصية لك إنشاء قوالب خدمة قابلة لإعادة الاستخدام يمكن تعيينها لعدة مشتركين، مما يبسط عملية التزويد ويضمن التناسق.



أنواع الملفات الشخصية



ملفات EPC

تحدد ملفات EPC (Evolved Packet Core) خصائص خدمة البيانات لمشتركي LTE.

المعلمات الرئيسية

المعلمة	الوصف	القيم النموذجية
`ue_ambr_dl_kbps`	حد سرعة التنزيل	10,000 - 1,000,000 Kbps
`ue_ambr_ul_kbps`	حد سرعة الرفع	5,000 - 500,000 Kbps
`network_access_mode`	نوع الخدمة	"packet_only" أو "packet_and_circuit"
`tracking_area_update_interval_seconds`	مؤقت TAU	54 ثانية (نموذجي)

إنشاء ملفات EPC

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_profiles": [],
    "name": "Premium 100Mbps",
    "network_access_mode": "packet_only",
    "tracking_area_update_interval_seconds": 600,
    "ue_ambr_dl_kbps": 100000,
    "ue_ambr_ul_kbps": 50000
  }'
```

قوالب ملفات EPC الشائعة

إنترنت أساسي:

- التنزيل: 10 ميجابت في الثانية (10,000 كيلوبت في الثانية)
- الرفع: 5 ميجابت في الثانية (5,000 كيلوبت في الثانية)

قياسي:

- التنزيل: 50 ميجابت في الثانية (50,000 كيلوبت في الثانية)
- الرفع: 25 ميجابت في الثانية (25,000 كيلوبت في الثانية)

متميز:

- التنزيل: 100 ميجابت في الثانية (100,000 كيلوبت في الثانية)
- الرفع: 50 ميجابت في الثانية (50,000 كيلوبت في الثانية)

غير محدود:

- التنزيل: 1 جيجابت في الثانية (1,000,000 كيلوبت في الثانية)
- الرفع: 500 ميجابت في الثانية (500,000 كيلوبت في الثانية)

ملفات IMS

تحدد ملفات IMS خصائص خدمة الصوت، بشكل أساسي من خلال قوالب IFC (معايير التصفية الأولية).

قوالب IFC

تعد قوالب IFC مستندات XML تحدد قواعد توجيه المكالمات لـ S-CSCF.

متغيرات القالب:

- `{{imsi}}` - IMSI المشترك
- `{{msisdns}}` - قائمة بأرقام الهواتف
- `{{mcc}}` - رمز الدولة المنزلية
- `{{mnc}}` - رمز الشبكة المنزلية

إنشاء ملفات IMS

```
curl -k -X POST https://hss.example.com:8443/api/ims/profile \
  -H "Content-Type: application/json" \
  -d '{
    "ims_profile": {
      "name": "Standard VoLTE",
      "ifc_template": "<InitialFilterCriteria>...
</InitialFilterCriteria>"
    }
  }'
```

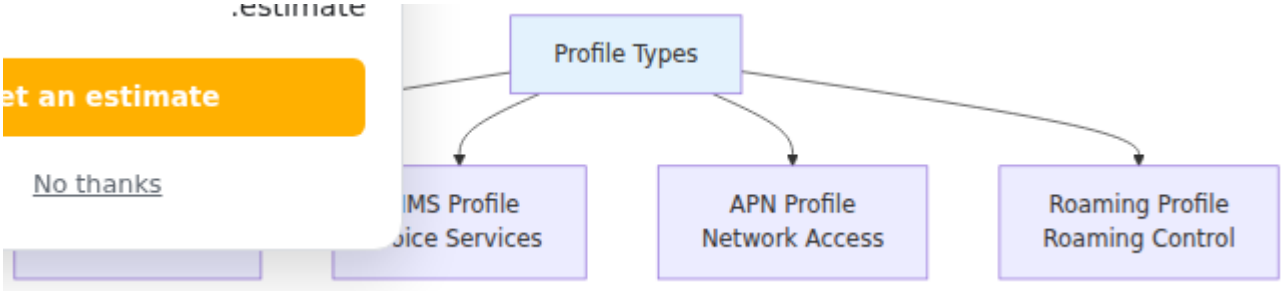
مثال على قالب IFC

```
<ServiceProfile>
  <PublicIdentity>
    <Identity>sip:
{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <InitialFilterCriteria>
    <Priority>0</Priority>
    <TriggerPoint>
      <ConditionTypeCNF>0</ConditionTypeCNF>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
      </SPT>
    </TriggerPoint>
    <ApplicationServer>
      <ServerName>sip:as.ims.example.com</ServerName>
      <DefaultHandling>0</DefaultHandling>
    </ApplicationServer>
  </InitialFilterCriteria>
</ServiceProfile>
```

ملفات APN

تحدد ملفات APN (اسم نقطة الوصول) نقاط الوصول الشبكية لعمليات الاتصال بالبيانات.

مكونات APN



معرف APN

يحدد اسم APN وبروتوكول IP.

APNs الشائعة:

- `internet` - وصول عام إلى الإنترنت
- `ims` - إشارات IMS/VoLTE
- `mms` - الرسائل متعددة الوسائط
- `vzwadmin` - محدد من قبل الناقل

خيارات إصدار IP:

- `"ipv4"`: IPv4 فقط
- `"ipv6"`: IPv6 فقط
- `"ipv4v6"`: IPv4v6 (دعم مزدوج)
- `"ipv4_or_ipv6"`: IPv4 أو IPv6 (اختيار الشبكة)

ملف QoS لـ APN

يحدد معلمات جودة الخدمة.

قيم QCI (معرف فئة جودة الخدمة):

QCI	النوع	حالة الاستخدام	الأولوية
1	GBR	صوت محادثة	الأعلى
2	GBR	فيديو محادثة	عالي
4	GBR	بث الفيديو	عالي
5	Non-GBR	إشارات IMS	متوسط
9	Non-GBR	الإنترنت (افتراضي)	الأدنى

طريقة شحن مستوى الجلسة (اختياري):

يمكن أن يحدد ملف QoS لـ APN أيضًا طريقة الشحن الافتراضية لجلسة IP-CAN، كـ المرسلة في Gx CCA-I. `Online`/`Offline` AVPs

الحقل	النوع	الافتراضي	الوصف
`online_charging_enabled`	boolean	`null`	عند التعيين، يجبر AVP `Online` على مستوى الجلسة (`true` = تمكين، `false` = تعطيل). عندما يكون `null`، يعكس القيمة التي أرسلها PCRF في CCR-I. PGW
`offline_charging_enabled`	boolean	`null`	عند التعيين، يجبر AVP `Offline` على مستوى الجلسة (`true` = تمكين، `false` = تعطيل). عندما يكون `null`، يعكس القيمة التي أرسلها PCRF في CCR-I. PGW

انظر PCRF: شحن مستوى الجلسة عبر الإنترنت/خارج الإنترنت للسلوك الكامل ومرجع قيمة AVP.

إنشاء تكوين APN كامل

```
# 1. إنشاء معرف APN
APN_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{"apn": "internet", "ip_version": "ipv4v6"}' \
  | jq -r '.response.id')

# 2. إنشاء ملف QoS لـ APN
QOS_ID=$(curl -k -X POST
https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "name": "Best Effort",
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 50000,
    "apn_ambr_ul_kbps": 25000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true,
    "qci": 9
  }' | jq -r '.response.id')

# 3. إنشاء ملف APN
curl -k -X POST https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_identifier_id\": \"$APN_ID\",
    \"apn_qos_profile_id\": \"$QOS_ID\",
    \"name\": \"Internet APN\"
  }"
```

ربط APNs بملف EPC

ترتبط APNs بملفات EPC من خلال جدول `join_epc_profile_to_apn_profile`.

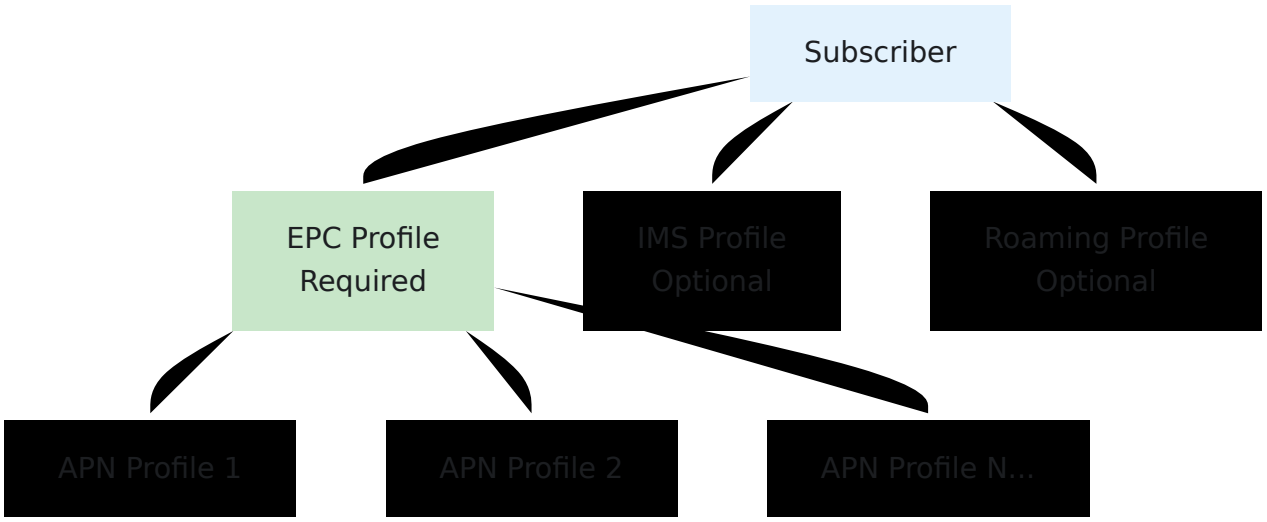
أدخل سجلات في جدول الربط لربط معرفات ملفات APN بمعرف ملف EPC. يمكن تعيين ملفات EPC متعددة إلى ملف APN واحد.

ملفات التجوال

انظر الوثائق التفصيلية في د��يل التحكم في التجوال.

تعيين الملفات الشخصية

علاقات ملف المشترك



تعيين الملفات الشخصية للمشتركين

```
# تعيين ملفات EPC و IMS أثناء إنشاء المشترك
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "epc_profile_id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
      "ims_profile_id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
      "roaming_profile_id": "9c858901-8a57-4791-81fe-4c455b099bc9"
    }
  }'

# تحديث ملف المشترك
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-4b01-
90e6-d701748f0851 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "epc_profile_id": "f47ac10b-58cc-4372-a567-0e02b2c3d479"
    }
  }'
```

أفضل الممارسات لإدارة الملفات الشخصية

مبادئ التصميم

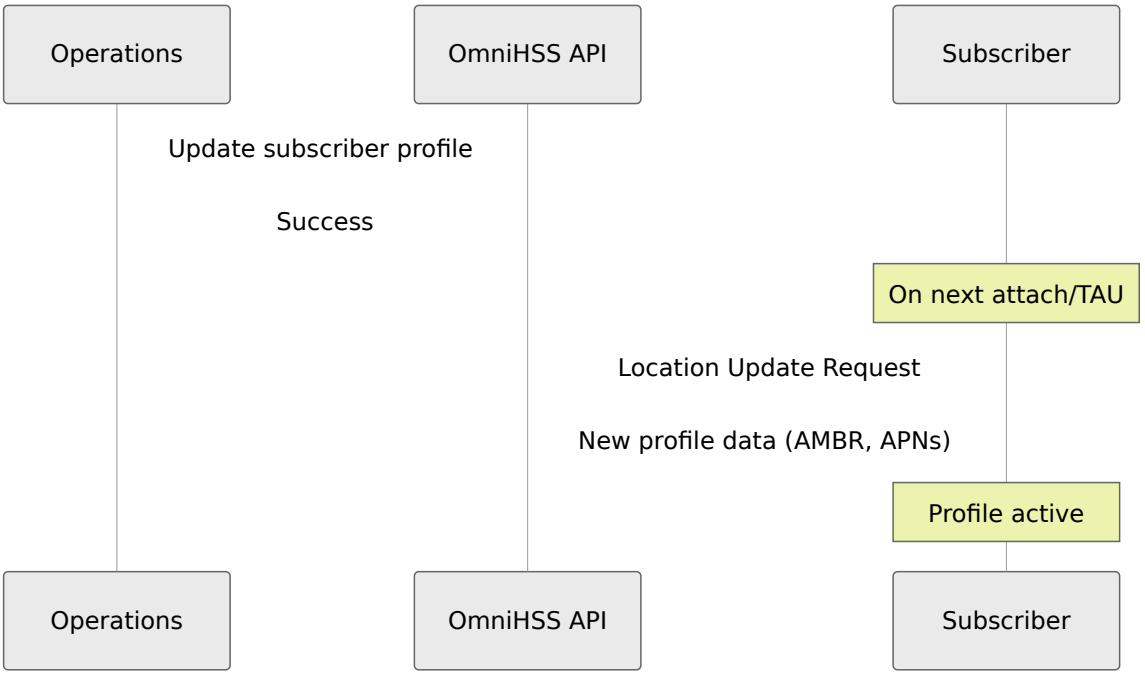
1. **إنشاء ملفات قياسية** - تحديد مستويات الخدمة الشائعة (أساسي، قياسي، متميز)
2. **إعادة استخدام الملفات** - تعيين نفس الملف لعدة مشتركين
3. **توثيق التغييرات** - تتبع تعديلات الملفات
4. **اختبار قبل الإنتاج** - التحقق من عمل الملف مع مشترك اختبار أولاً

قاعدة تسمية الملفات الشخصية

```
[Service Tier]-[Speed]-[Features]

أمثلة:
- "Basic-10Mbps-Internet"
- "Premium-100Mbps-VoLTE"
- "Enterprise-1Gbps-MultiAPN"
```

ترحيل الملفات الشخصية

عند تغيير ملف مشترك:



مهم: تدخل تغييرات الملف حيز التنفيذ في التالي:

- تحديث منطقة التتبع (TAU)
- الاتصال
- تسجيل IMS (لتغييرات ملف IMS)

استكشاف مشاكل الملف الشخصي

المشترك لا يحصل على السرعة المتوقعة:

1. تحقق من قيم AMBR للملف EPC المعين
2. تحقق من قيم AMBR لملف QoS لـ APN
3. تحقق من أن MME/P-GW يفرض QoS بشكل صحيح
4. تحقق من وجود ازدحام في الشبكة

فشل تسجيل IMS:

1. تحقق من تعيين ملف IMS
2. تحقق من صحة XML لقالب IFC
3. مراجعة سجلات S-CSCF لأخطاء معالجة IFC
4. تأكيد تكوين اختيار S-CSCF

غير متاح APN:

1. تحقق من ربط ملف APN بملف EPC
2. تحقق من تطابق معرف APN مع طلب الشبكة
3. مراجعة طلب الاتصال PDN من UE

← التالي: التحكم في التجوال | العودة إلى دليل العمليات →

تدفقات بروتوكول OmniHSS

← العودة إلى دليل العمليات

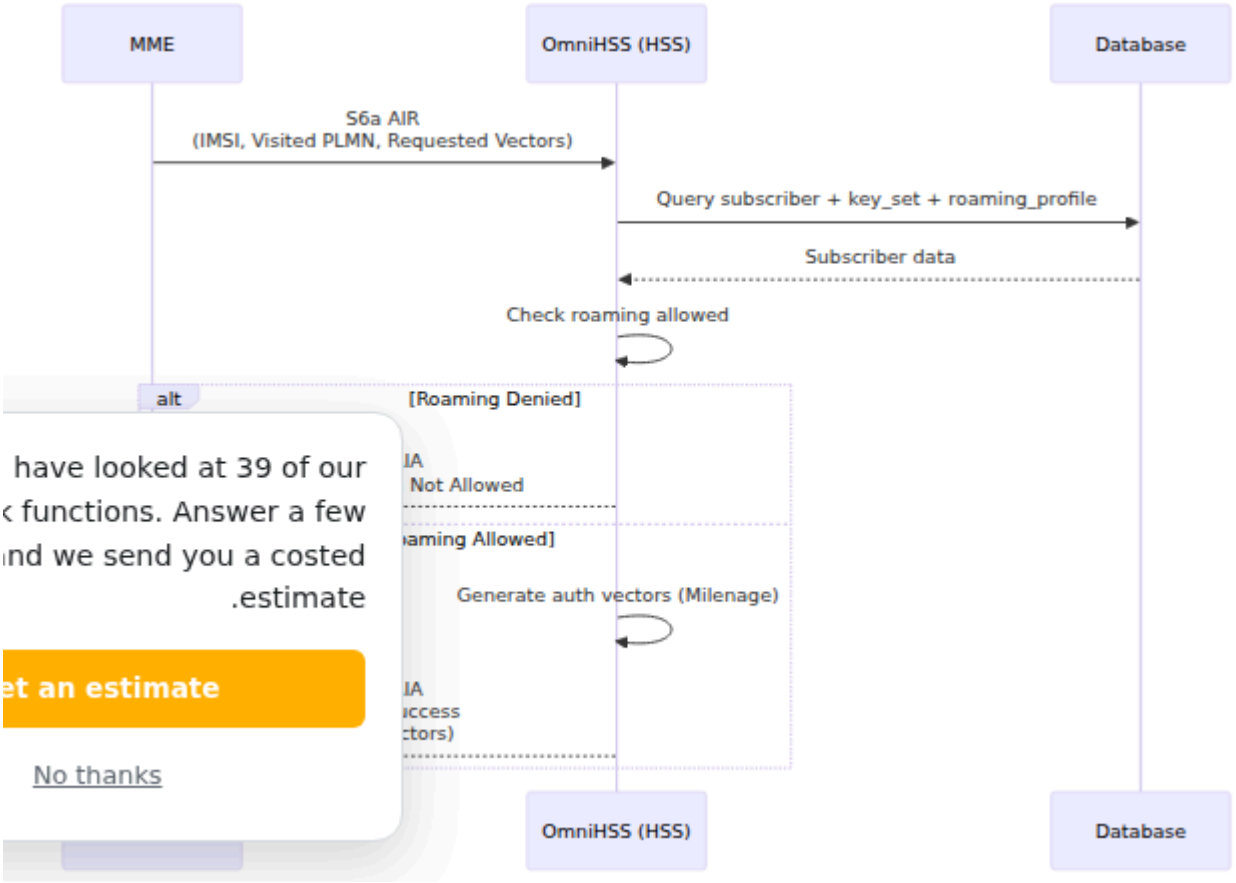
نظرة عامة

توضح هذه الوثيقة تدفقات رسائل بروتوكول Diameter المدعومة من قبل OmniHSS. فهم هذه التدفقات أمر أساسي لاستكشاف الأخطاء وإصلاحها والعمليات.

واجهة S6a (LTE/EPC)

طلب معلومات المصادقة (AIR/AIA)

يطلب MME متجهات المصادقة للاشتراك.

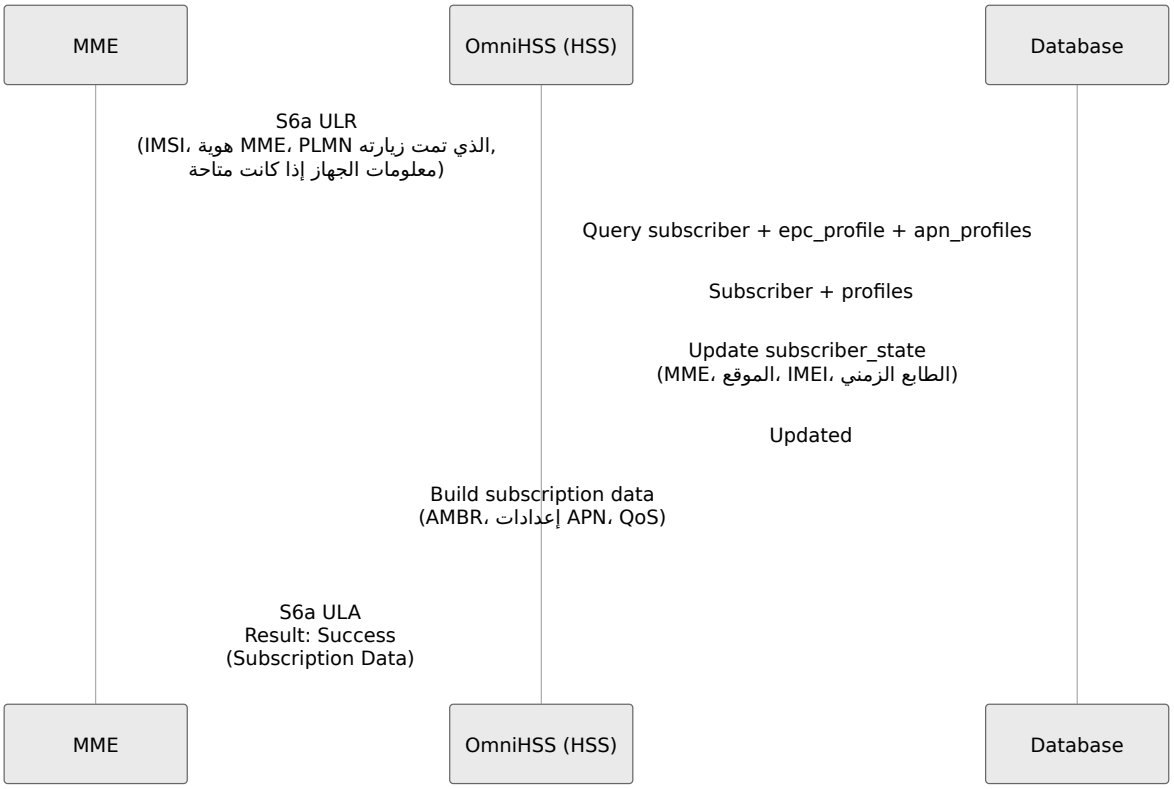


المتغيرات الرئيسية:

- الطلب: اسم المستخدم (IMSI)، معرف PLMN الذي تمت زيارته، عدد المتجهات المطلوبة
- الاستجابة: معلومات المصادقة (RAND، AUTN، XRES، KASME)

طلب تحديث الموقع (ULR/ULA)

يُخطر MME HSS بموقع المشترك ويسترجع بيانات الاشتراك.

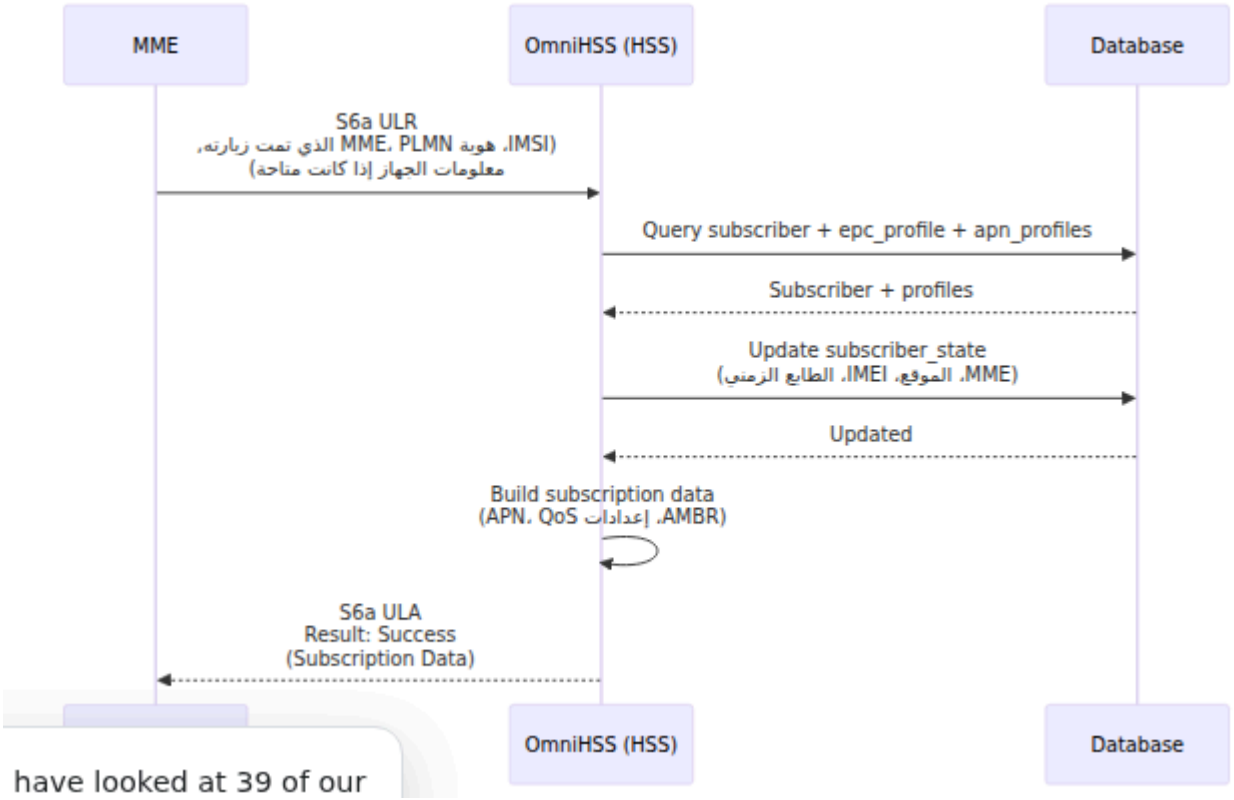


المتغيرات الرئيسية:

- الطلب: اسم المستخدم (IMSI)، نوع RAT، ULR-Flags، معرف PLMN الذي تمت زيارته، قدرة UE-SRVCC، معلومات الجهاز (IMEI، اختياري؛ إصدار البرنامج)
- الاستجابة: بيانات الاشتراك (AMBR، إعدادات APN، وضع الوصول إلى الشبكة)

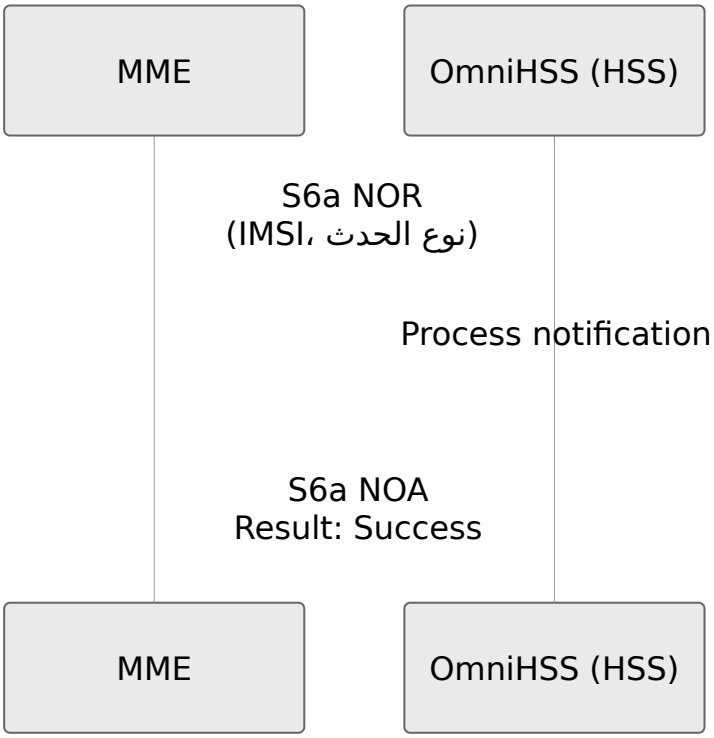
طلب تطهير UE (PUR/PUA)

يُخطر MME HSS عندما يتم حذف سياق المشترك.



طلب الإخطار (NOR/NOA)

يُبلغ MME HSS بالأحداث المختلفة.

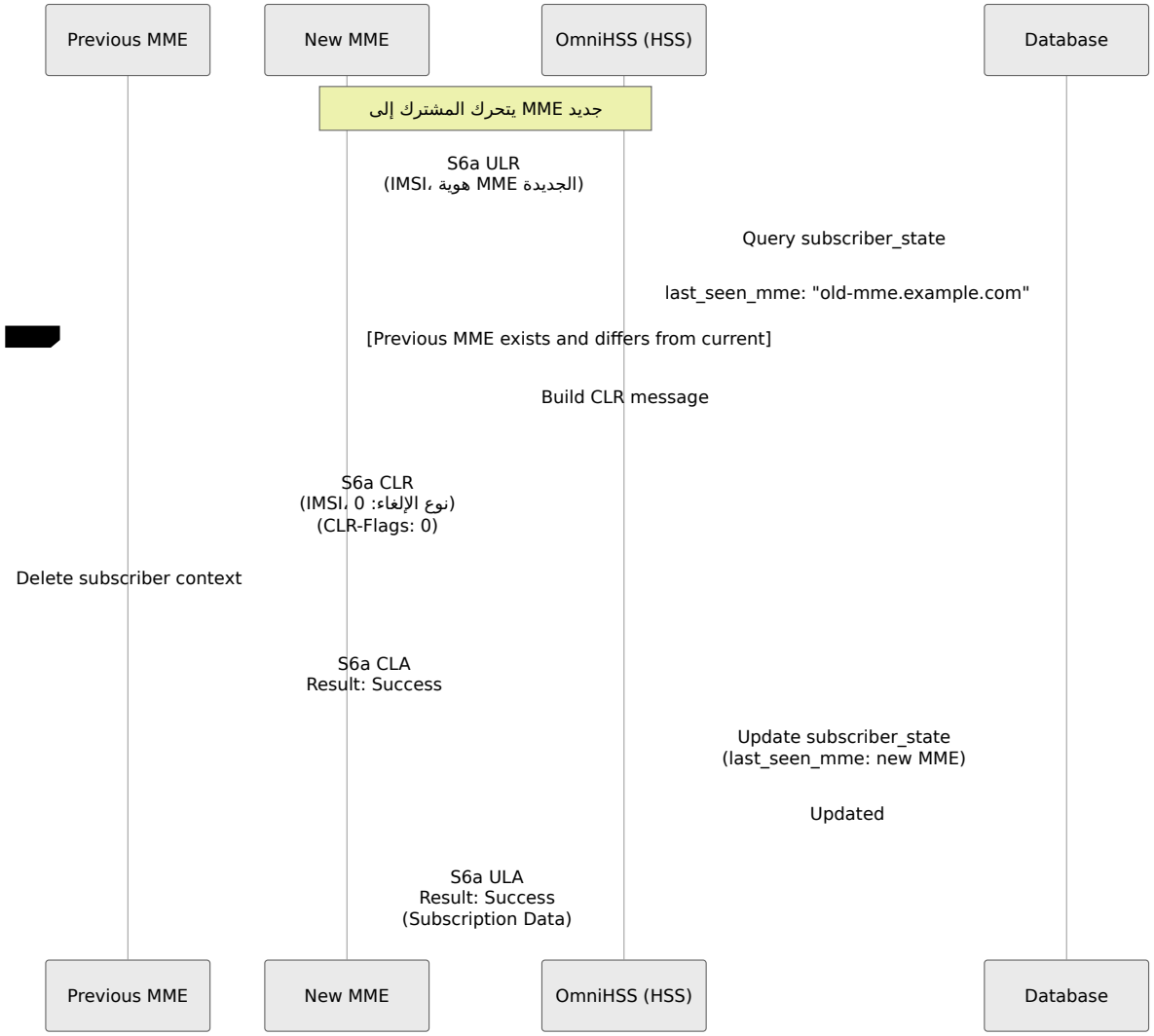


طلب إلغاء الموقع (CLR/CLA)

يبدأ HSS إلغاء الموقع لإبلاغ MME بأنه يجب فصل المشترك. يدعم OmniHSS إرسال CLR تلقائيًا وبرمجيًا.

CLR التلقائي (تسليم MME)

عندما يقوم المشترك بإجراء طلب تحديث الموقع من MME جديد، يقوم OmniHSS تلقائيًا بإرسال CLR إلى MME السابق لتنظيف التسجيلات القديمة.



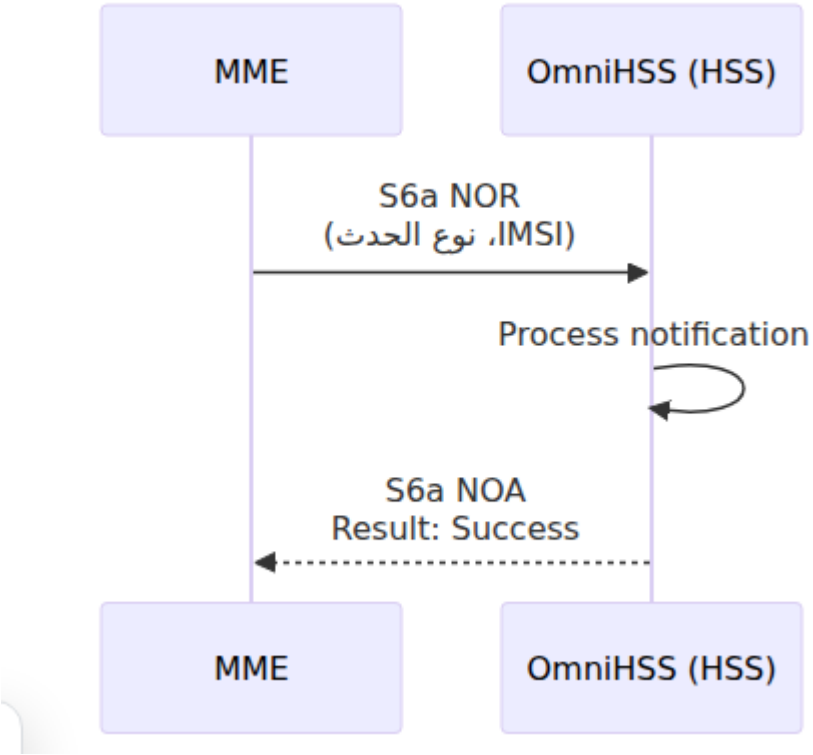
المتغيرات الرئيسية (CLR التلقائي):

- اسم المستخدم: IMSI للمشترك
- اسم مضيف: وجهة المضيف السابق MME
- مجال الوجهة: مجال MME السابق
- نوع الإلغاء: 0 (إجراء تحديث MME)
- CLR-Flags: 0

- بيانات الاشتراك: ملف الاشتراك الكامل

CLR البرمجي (مُحفز API)

عبر واجهة برمجة التطبيقات البرمجية لفصل المشتركين بالقوة (على CLR يمكن للمسؤولين تحفيز سبيل المثال، لسحب الاشتراك، منع الاحتيال، أو الإجراءات الإدارية).



المتغيرات الرئيسية (CLR البرمجي):

- اسم المستخدم: IMSI للمشترك
- اسم مضيف: وجهة المضيف MME الذي تم رؤيته آخر مرة
- مجال الوجهة: مجال MME الذي تم رؤيته آخر مرة
- نوع الإلغاء: `:subscription_withdrawal` (3 مشفرة كعدد صحيح وفقًا لـ GPP TS 29.272)
- CLR-Flags:
  - s6a_indicator: 1 (تشير إلى استخدام واجهة S6a)
  - reattach_required: 1 (يجب على UE إعادة المصادقة لإعادة الاتصال)

أنواع الإلغاء

يدعم OmniHSS 3 أنواع إلغاء متعددة وفقًا لـ GPP TS 29.272:

حالة الاستخدام	الوصف	القيمة	النوع
جديد MME من ULR تلقائي أثناء	تغيير MME عادي	0	إجراء تحديث MME
3 سيناريوهات تسليم G/2G	تسليم SGSN	1	إجراء تحديث SGSN
فصل يدوي عبر API	إنهاء إداري	2	سحب الاشتراك
تداخل الشبكة القديمة	تحديث وظيفة التداخل	3	إجراء تحديث IWF
فرض إعادة المصادقة	تسجيل جديد	4	إجراء الاتصال الأولي

CLR-Flags

متغير CLR-Flags هو قناع بت يحتوي على الحقول التالية:

الوصف	البت	العلم
1 = تم استخدام واجهة S6a	0	مؤشر S6a/S6d
1 = يجب على UE إجراء اتصال جديد	1	إعادة الاتصال المطلوبة

مثال على تكوين CLR-Flags:

```
clr_flags: %{
  s6a_indicator: 1,        # استخدام واجهة S6a
  reattach_required: 1     # فرض إعادة المصادقة
}
```

سيناريوهات متعددة IMSI

يتتبع OmniHSS تسجيل MME **لكل مشترك (IMSI)**، وليس لكل MSISDN. هذا أمر حاسم لفهم سلوك CLR في سيناريوهات متعددة IMSI:

السيناريو 1: عدة MSISDNs، IMSI واحد

```
المشترك A:
  - IMSI: 999000123456789
  - MSISDNs: ["+1234567890", "+9876543210"]
  - last_seen_mme: "mme01.operator.com"
```

عندما ينتقل هذا المشترك إلى MME جديد:

- **تم إرسال CLR** إلى **واحد** "mme01.operator.com" مع IMSI 999000123456789
- كلا MSISDNs يتأثران (نفس المشترك، نفس SIM)
- يحتوي متغير اسم المستخدم على IMSI، وليس MSISDNs

السيناريو 2: مشتركين متعددين (IMSI مختلفة)، نفس MSISDN

يفرض OmniHSS **قيود MSISDN الفريدة** (لا يمكن أن ينتمي MSISDN واحد إلى عدة مشتركين في نفس الوقت). ومع ذلك، أثناء النقل/الهجرة:

```
المشترك A:
  - IMSI: 999000111111111
  - MSISDN: "+1234567890"
  - last_seen_mme: "mme01.operator.com"

المشترك B (بعد النقل):
  - IMSI: 999000222222222
  - MSISDN: "+1234567890"  # نفس MSISDN، SIM/IMSI مختلفة
  - last_seen_mme: "mme02.operator.com"
```

عندما يسجل المشترك B:

- **لم يتم إرسال CLR** (IMSI مختلف = مشترك مختلف)
- يبقى المشترك مسجلاً في A mme01
- يسجل المشترك في B mme02
- يمكن أن يكون كلاهما نشطين في نفس الوقت (أجهزة مادية مختلفة)

السيناريو 3: CLR برمجي لمشترك متعدد MSISDN

النتيجة:

- **تم إرسال CLR** إلى **واحد** last_seen_mme للمشترك
- **جميع MSISDNs** المرتبطة بتلك IMSI مفصولة بشكل فعال
- IMSI هو المفتاح الأساسي لتتبع تسجيل MME

ملاحظات هامة

1. **IMSI** عمليات **هو المفتاح:** CLR **لكل** تكون دائمًا **IMSI**، وليس لكل MSISDN. تتبع جدول `subscriber_state` `last_seen_mme` حسب المشترك (IMSI).

2. **عملية ذرية:** يمكن تسجيل كل مشترك في MME واحد فقط في وقت واحد. يضمن التلقائي ذلك من خلال تنظيف التسجيل القديم CLR.

3. **لا CLR إذا لم يكن هناك MME سابق:** إذا كان `last_seen_mme` هو `nil` (لم يسجل المشترك أبدًا)، فلا يتم إرسال CLR أثناء ULR.

4. **تضمين بيانات الاشتراك:** يتضمن CLR التلقائي (أثناء ULR) متغير `Subscription-Data` الكامل لمساعدة MME القديم على تنظيف السياق بشكل صحيح.

5. **غير متزامن:** يتم إرسال CLR بشكل غير متزامن (إطلاق ونسيان). لا تنتظر استجابة MME القديم من CLA الجديد MME لـ ULA.

6. **معالجة CLA:** يتلقى OmniHSS استجابات CLA ولكنه حاليًا يتجاهلها. يمنع ذلك حلقات الرسائل وهو سلوك قياسي لـ HSS.

واجهة SWx (3GPP / الوصول غير مكالمات WiFi)

تمكن واجهة SWx مكالمات WiFi من خلال ربط ePDG (بوابة بيانات الحزمة المتطورة) بـ HSS لمصادقة وتفويض المشتركين عبر شبكات الوصول غير 3GPP.

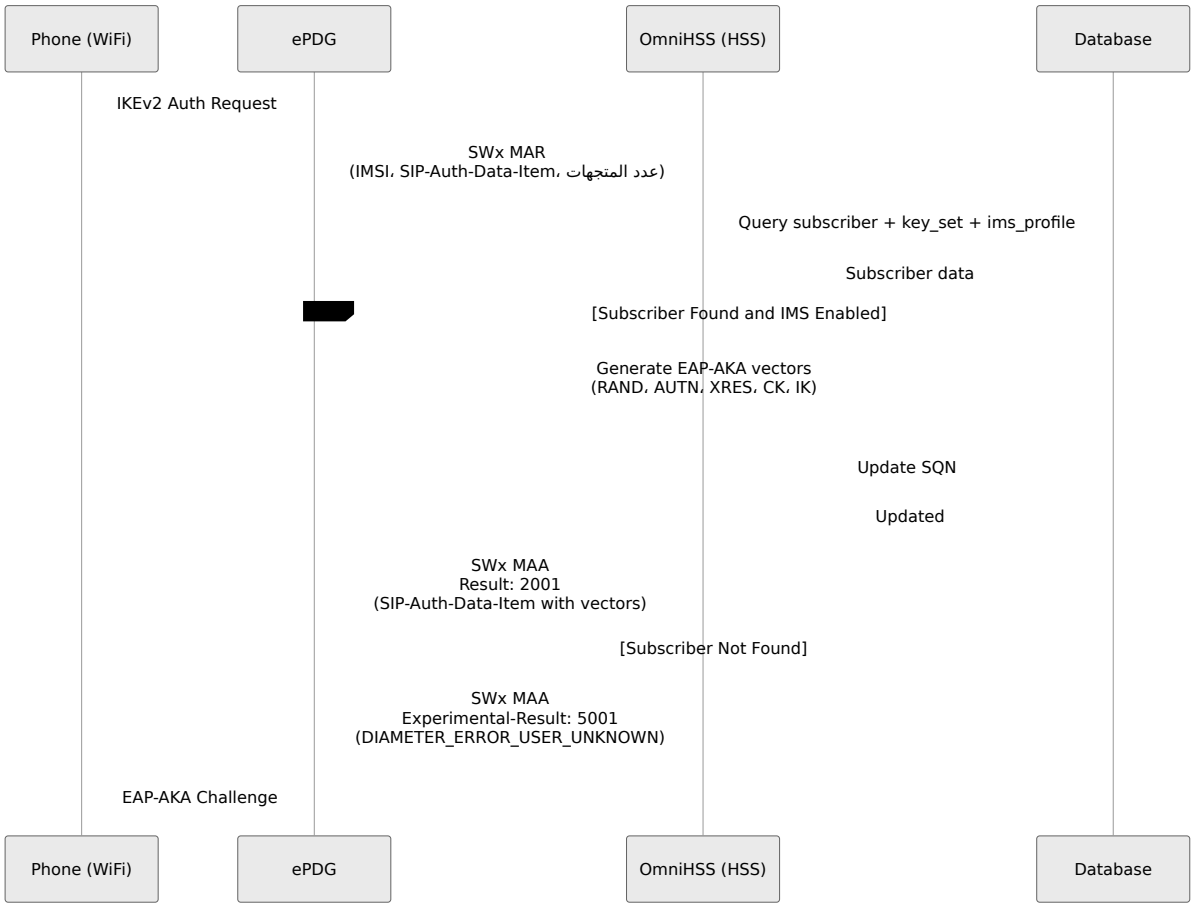
طلب مصادقة الوسائط المتعددة (MAR/MAA)

يطلب ePDG متجهات مصادقة EAP-AKA لتسجيل مكالمات WiFi. يطلب TWAG (موثوق WLAN) متجهات EAP-AKA' الواجهة عبر نف��.

يحدد `SIP-Authentication-Scheme` في الطلب نوع المتجه (3GPP TS 29.273 الفقرة 8.1.2.1):

المخطط	ANID	المتجه المعاد
`EAP-AKA`	تم تجاهله	بت فصل AMF 0. يحمل `Confidentiality-Key` و `Integrity-Key` CK و IK.
`EAP-AKA'`	مطلوب	بت فصل AMF 1. يحمل `Confidentiality-Key` و `Integrity-Key` CK' و IK'، المستمدة من CK و IK و SQN xor AK و ANID 3 وفقًا لـ 3GPP TS 33.402 الملحق A.2. لا تترك CK و IK HSS.

يتم الرد على طلب يحتوي على `EAP-AKA'` وبدون `ANID` برمز النتيجة 5005 (DIAMETER_MISSING_AVP). يتم الرد على أي مخطط آخر برمز 5004 (DIAMETER_INVALID_AVP_VALUE). ANID لشبكة وصول WLAN هو `WLAN` (3GPP TS 24.302 الفقرة 8.1.1.2).



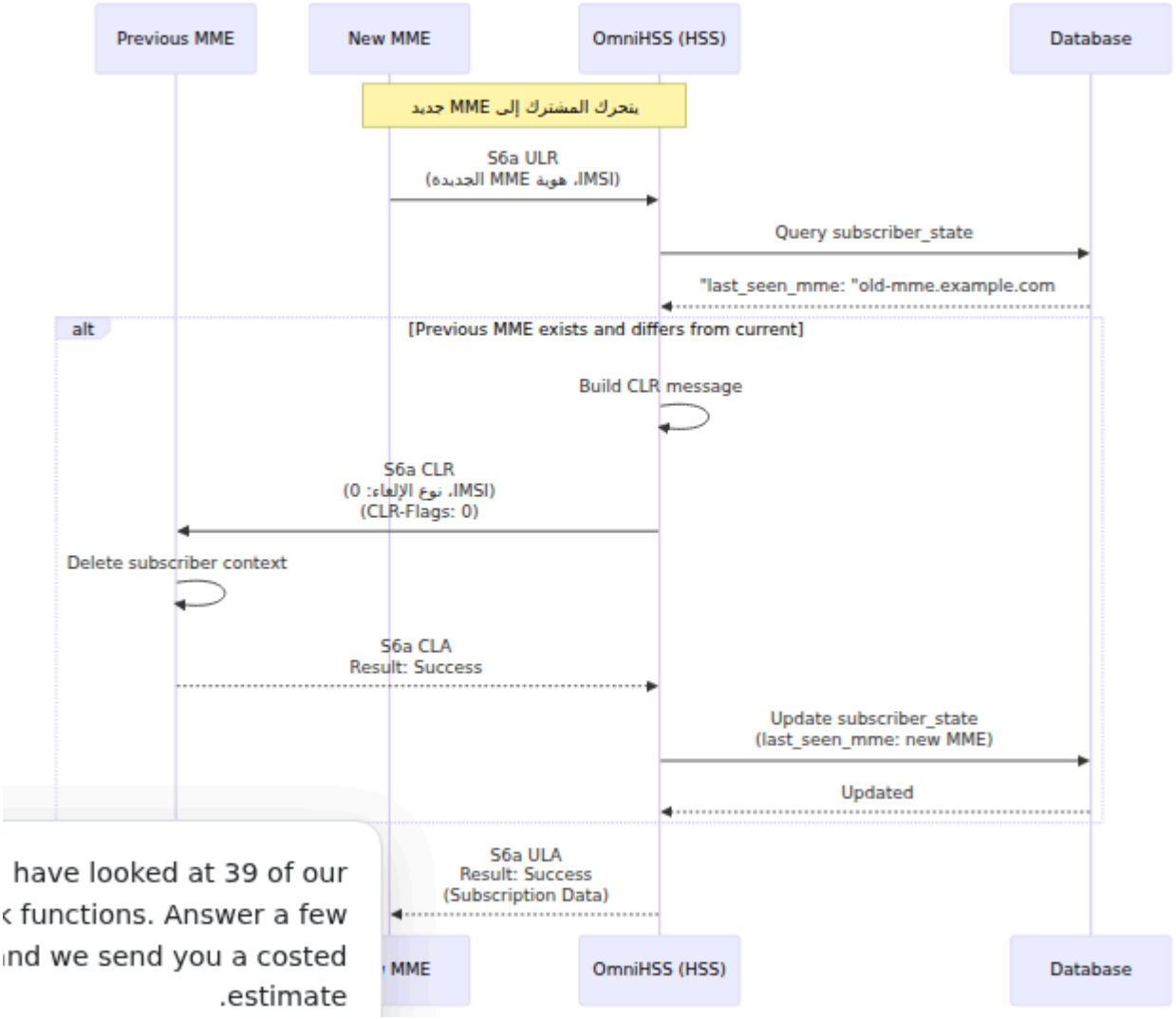
المتغيرات الرئيسية:

- الطلب: اسم المستخدم (IMSI أو IMSI@realm)، SIP-Auth-Data-Item (مخطط المصادقة)، SIP-Number-Auth-Items
- الاستجابة: SIP-Auth-Data-Item (SIP-Authenticate، SIP-Authorization، Confidentiality-Key، Integrity-Key)

إعادة مزامنة SQN: عندما يكتشف UE أن فشل المصادقة بسبب عدم تطابق SQN، يتضمن ePDG بيانات إعادة المزامنة في متغير SIP-Authorization. يستخرج OmniHSS AUTS من هذا الحقل باستخدام حساب واعٍ لطول IND 3 وفقًا لـ 3GPP TS 33.102. ويعيد حساب SQN.

طلب تعيين الخادم (SAR/SAA)

يسجل ePDG المشترك أو يلغي تسجيله لخدمات مكالمات WiFi.



أنواع تعيين الخادم:

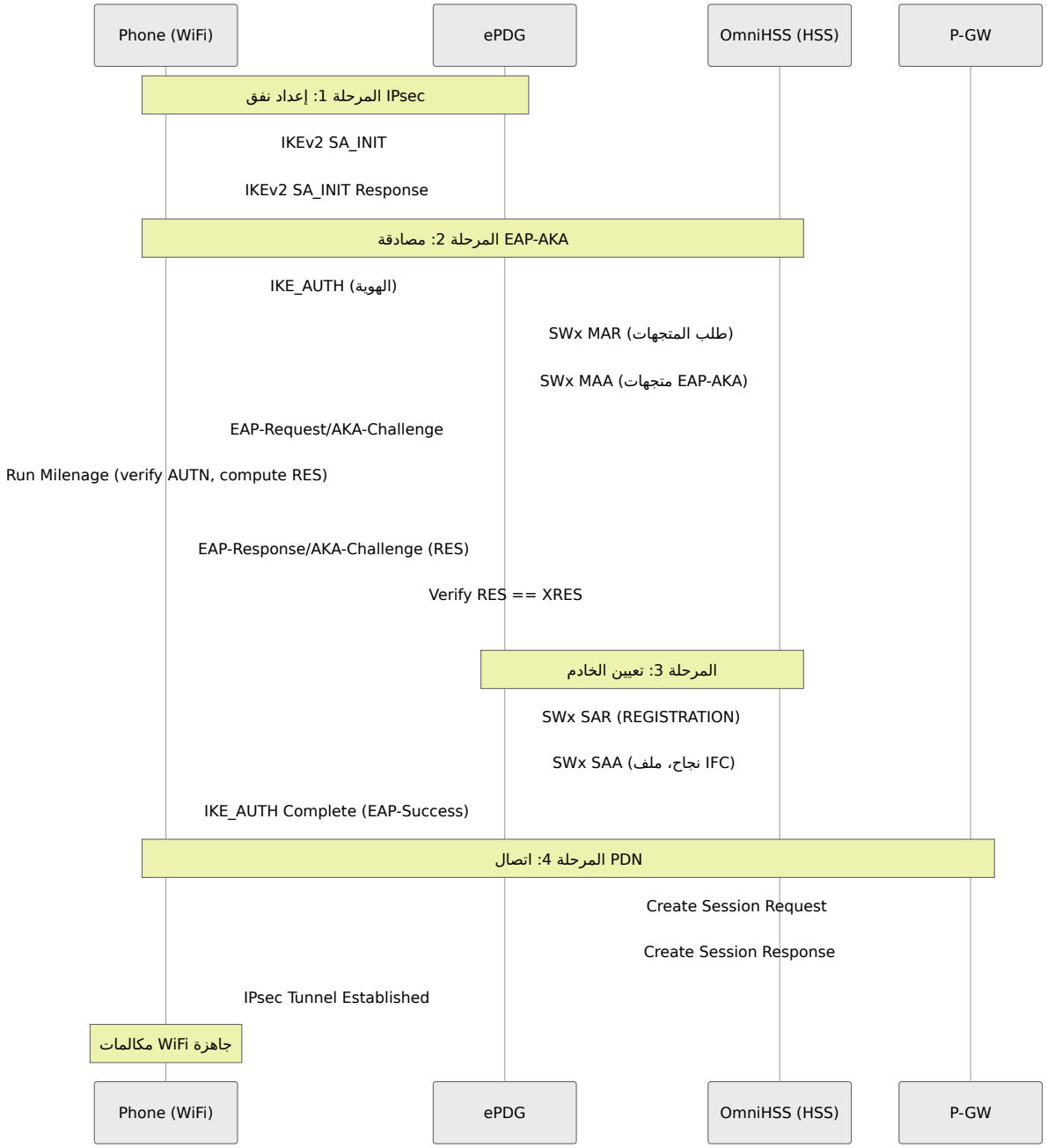
الوصف	القيمة	النوع
استعلام فقط، لا تغيير في الحالة	0	NO_ASSIGNMENT
تسجيل مكالمات WiFi الأولي	1	REGISTRATION
تحديث التسجيل	2	RE_REGISTRATION
خدمات للمستخدم غير المسجل	3	UNREGISTERED_USER
انتهاء التسجيل	4	TIMEOUT_DEREGISTRATION
إلغاء التسجيل الذي بدأه المستخدم	5	USER_DEREGISTRATION
فشل المصادقة، مسح الحالة	7	AUTHENTICATION_FAILURE
لغاء التسجيل الذي بدأه�� المسؤول	8	ADMINISTRATIVE_DEREGISTRATION

المتغيرات الرئيسية:

- اختيار ePDG (هوية) نوع تعيين الخادم، اسم الخادم، الطلب: اسم المستخدم (IMSI)، الخدمة (APN)
- بيانات المستخدم غير 3GPP، الاستجابة: بيانات المستخدم (ملف IFC XML)

تدفق تسجيل مكالمات WiFi

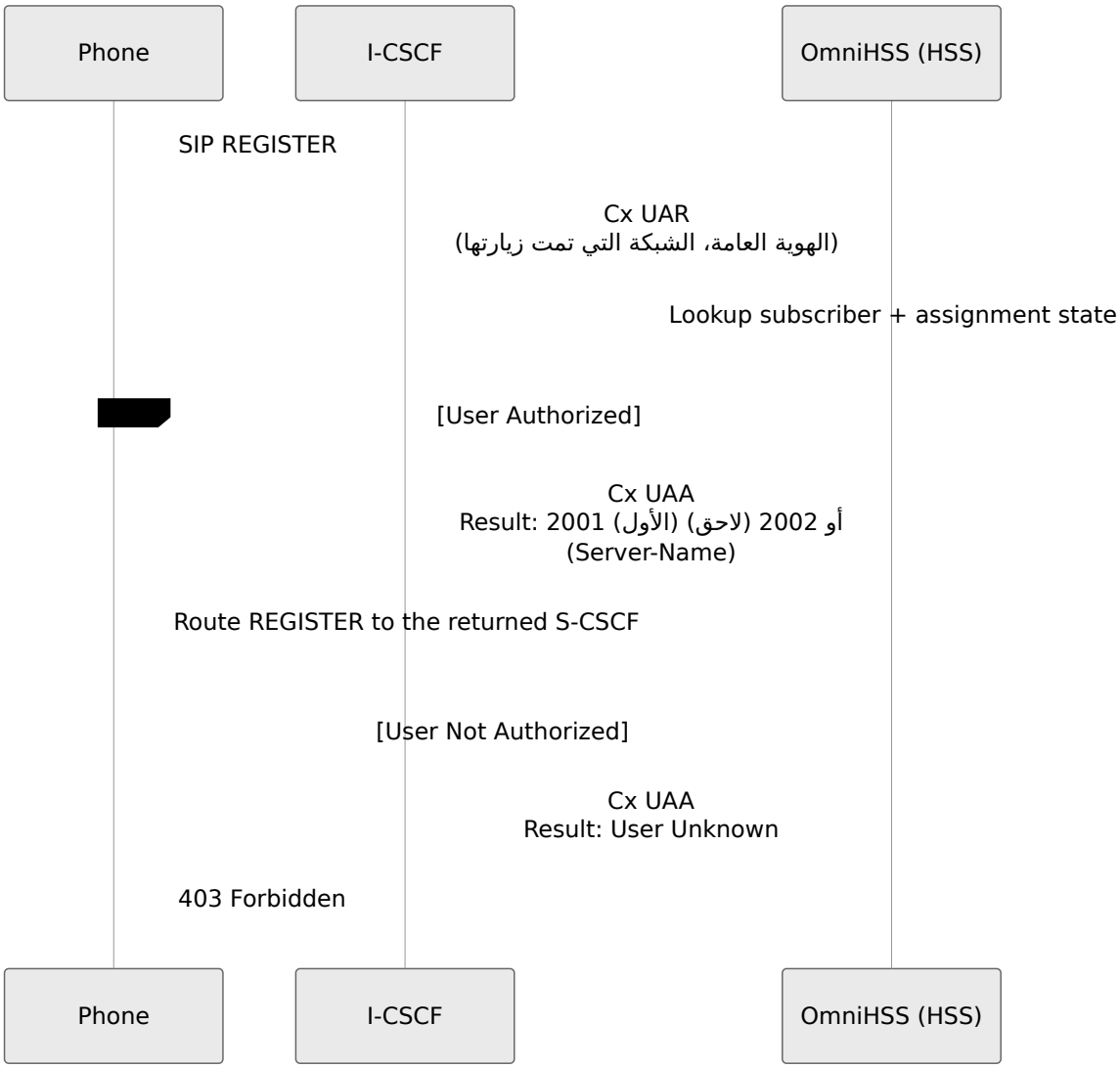
تسجيل مكالمات WiFi من النهاية إلى النهاية.



واجهة Cx (IMS)

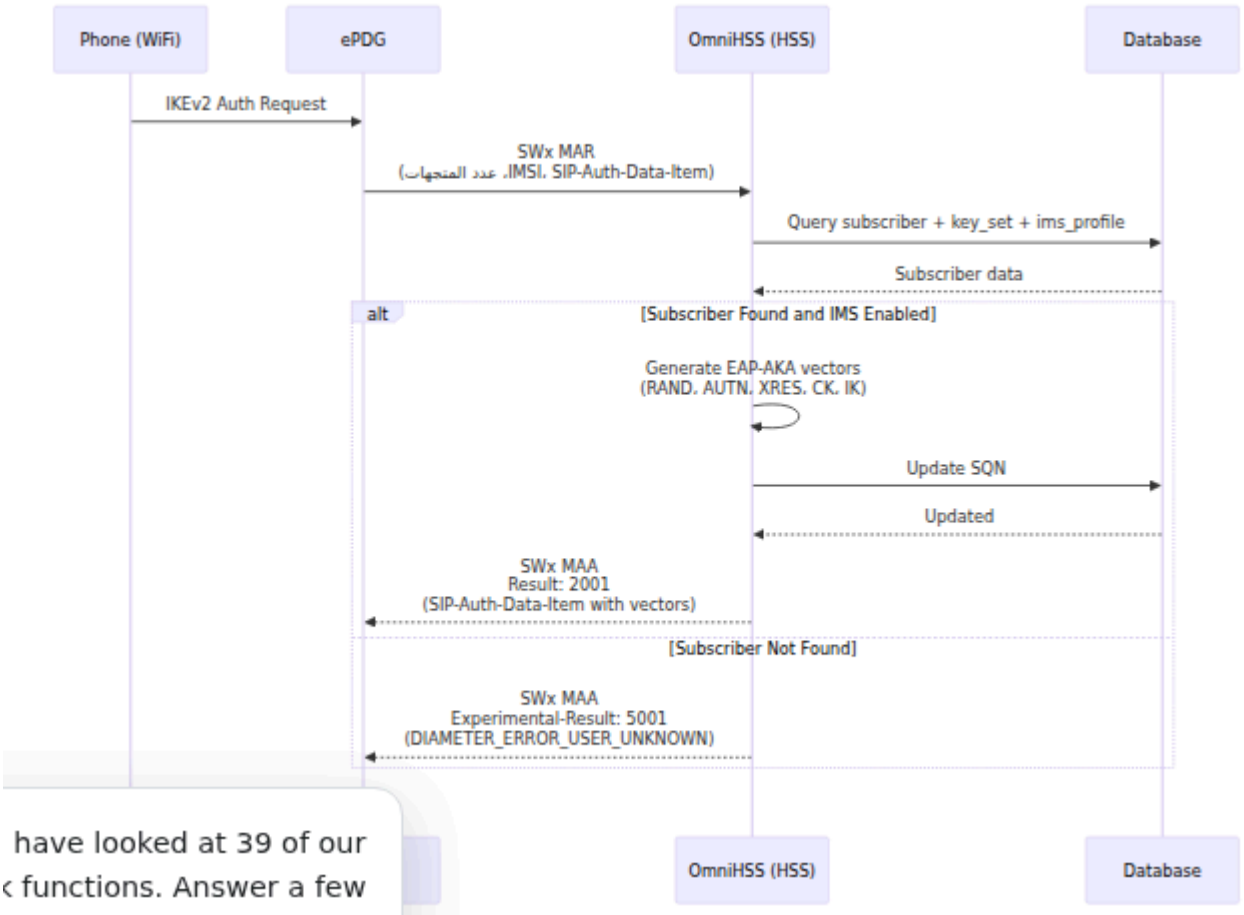
طلب تفويض المستخدم (UAR/UAA)

يسأل I-CSCF عما إذا كان يمكن للمستخدم التسجيل، وأي S-CSCF يجب استخدامه. يعيد HSS اسم S-CSCF (اسم خادم)، ورمز النتيجة قواعد حالة تعيين وليس مجموعة قدرات. يتبع الاسم S-CSCF.



طلب تعيين الخادم (SAR/SAA)

يسجل S-CSCF/يلغي تسجيل المستخدم ويسترجع ملف IMS.



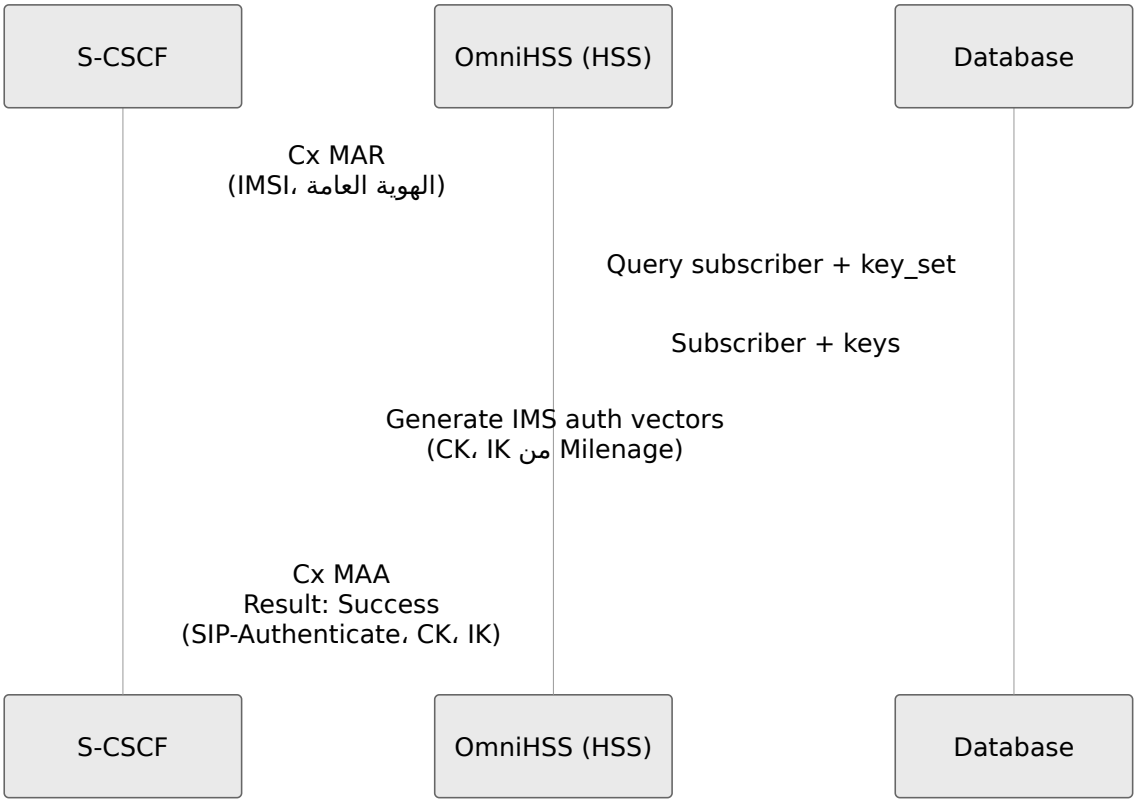
عرض قالب IFC:

- `{{imsi}}` → IMSI الفعلي
- `{{msisdns}}` → قائمة بأرقام الهواتف
- `{{mcc}}`، `{{mnc}}` → رموز PLMN المنزلية

لحالة التسجيل وحالة الانتظار للمصادقة، وكيفية التعامل مع SAR للحصول على كيفية تحديث `AUTHENTICATION_FAILURE` و `AUTHENTICATION_TIMEOUT`، انظر حالة تعيين S-CSCF.

طلب مصادقة الوسائط المتعددة (MAR/MAA)

يطلب S-CSCF متجهات المصادقة لتسجيل IMS.



حالة تعيين S-CSCF

لكل مشترك. حالة التسجيل وحالة الانتظار للمصادقة IMS قطعتين منفصلتين من حالة HSS يمتلك مستقلة، وفقًا لـ 3GPP TS 29.228 §3.1.

حقل الحالة	تم تعيينه في	تم مسحه في	المعنى
`assigned_scscf`	نجاح SAR (التسجيل)	فشل المصادقة/ SAR، إلغاء انتهاء الوقت عندما لا يكون مسجلاً، أو فشل المصادقة/ انتهاء الوقت الذي يتقاعد اسمًا قديمًا	المشترك مسجل على هذا S-CSCF.
`auth_pending_scscf`	MAR	نجاح أو فشل المصادقة (/SAR إلغاء UAR، أو انتهاء الوقت)، انتهاء TTL	تحدي IMS-AKA قيد ال��قدم على هذا S-CSCF.
`auth_pending_since`	MAR	مع `auth_pending_scscf`	الوقت الذي بدأ فيه التحدي. يستخدم HSS ذلك لإنتهاء تحدٍ لم يكتمل أبدًا.

تخزن MAR اسم S-CSCF وتحدد حالة الانتظار للمصادقة، وفقًا لـ TS 29.228 §6.3. أو SAR يؤكد يمسحها، وفقًا لـ TS 29.228 §6.1.2.

ترتيب اختيار S-CSCF. UAA لكل UAR، يعيد HSS اسم S-CSCF ورمز نتيجة مع هذا الترتيب:

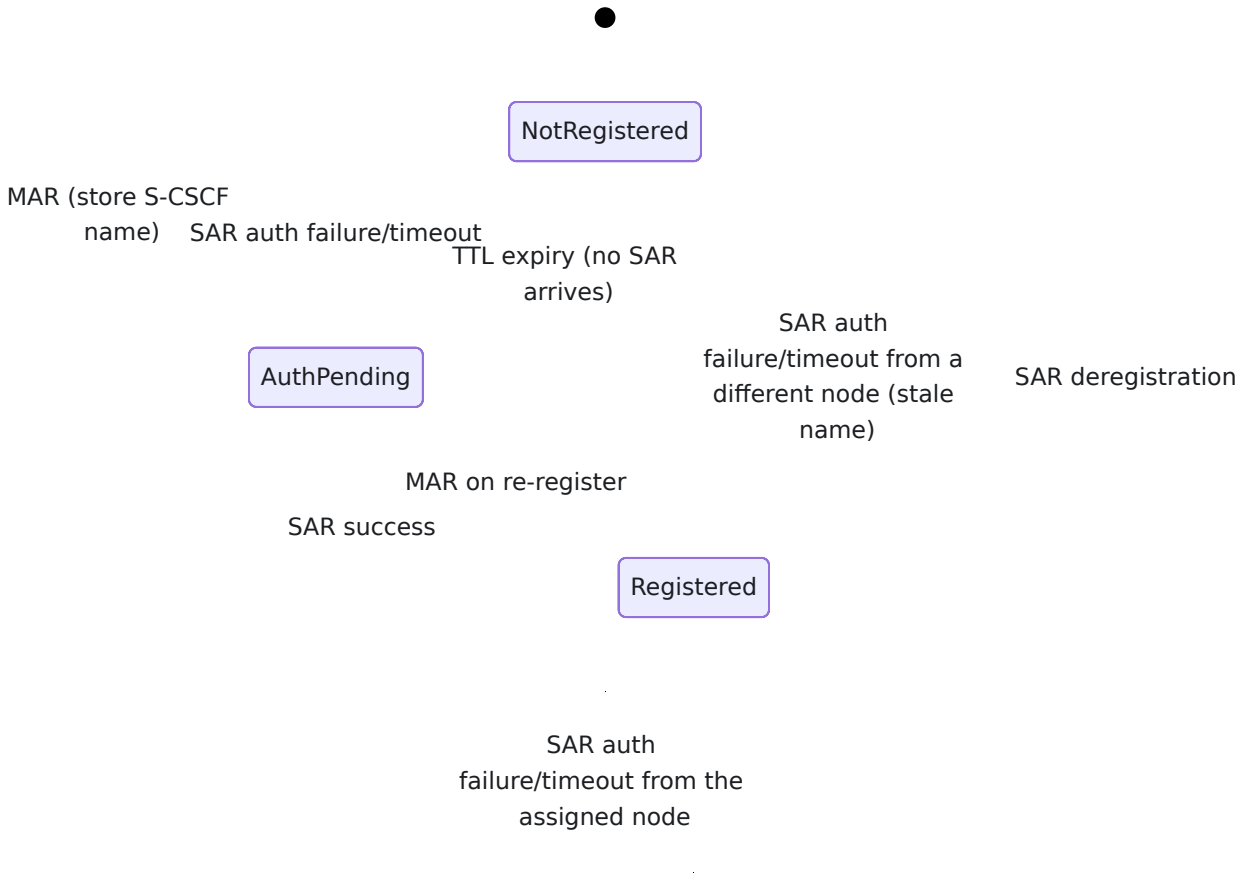
1. قيد المصادقة الحية: أعده، مع S-CSCF يوجد `DIAMETER_SUBSEQUENT_REGISTRATION` (2002). التحدي حي طالما تم تعيين `auth_pending_scscf` و `auth_pending_since` داخل `auth_pending_ttl_seconds`.
2. حقيقية: أعدها، مع S-CSCF عقدة يحمل `assigned_scscf` `DIAMETER_SUBSEQUENT_REGISTRATION` (2002).
3. جديد S-CSCF لا ينطبق أي منهما: اختر (انظر تكوين اختيار S-CSCF)، مع `DIAMETER_FIRST_REGISTRATION` (2001).

المجموعة هو اسم للمجموعة بأكملها، لذا لا URI. تختبر القاعدة 2 وجود عقدة حقيقية عن عمد HSS المجموعة مسجلاً من إصدار سابق، يعامل URI يحدد أبدًا العقدة التي تخدم المشترك. إذا كان التالي العقدة الحقيقية SAR المشترك على أنه غير مخدم ويجيب بـ 2001. ثم يخزن.

الخادم. تجعل القاعدة 2 التعيين لزجًا. بعد أن **S-CSCF تسجيل إعادة التسجيل دائمًا يعيد** منتهي تلك العقدة. يعيد LIR إعادة تسجيل وكل UAR تأخذ العقدة التسجيل، تعيد كل HSS URI المجموعة فقط لمشترك لم تخدمه أي عقدة بعد.

يجعل هذا دورة التحدي الجارية. `assigned_scscf` قيد المصادقة على HSS S-CSCF يفضل تتقارب على العقدة التي أصدرتها. بالنسبة لمشترك مسجل صحي، العقدة التي تتحدى هي العقدة S-CSCF المعينة، لذا فإن التفضيل ليس له تأثير. يهم فقط أثناء استرداد فشل.

يمسح SAR **تنتهي حالة الانتظار للمصادقة.** تكتمل دورة التحدي في ثوانٍ، ويرسل كل نتيجة اسمًا HSS يبقى الاسم المعلق مسجلاً. يتجاهل SAR، المتحدية تلك S-CSCF الحالة. إذا لم ترسل MAR سيحتل، بدون TTL. (الافتراضي 30 ثانية) `auth_pending_ttl_seconds` معلقًا أكبر من ضا�ً أو مهجور مرتبة التسجيل المسجلة إلى الأبد. ستذهب حركة المرور الأصلية إلى عقدة لا تحمل شيئًا، بينما لا تزال حركة المرور المنتهية تذهب إلى `assigned_scscf`.



رموز نتائج Cx:

الرمز	الاسم	المعنى	المرجع
2001	DIAMETER_FIRST_REGISTRATION	لا يوجد S-CSCF في السجل. الاسم المعاد هو اختيار.	TS 29.229
2002	DIAMETER_SUBSEQUENT_REGISTRATION	يوجد S-CSCF في السجل. تعيد HSS الاسم المخزن.	TS 29.229

قيم نوع تعيين الخادم ذات الصلة (SAR):

القيمة	الاسم	إجراء HSS
0	NO_ASSIGNMENT	مسح اسم S-CSCF والتسجيل.
1	REGISTRATION	تعيين حالة التسجيل إلى مسجل. مسح الانتظار للمصادقة.
2	RE_REGISTRATION	الاحتفاظ بالتسجيل. مسح الانتظار للمصادقة.
4	TIMEOUT_DEREGISTRATION	مسح اسم S-CSCF والتسجيل.
5	USER_DEREGISTRATION	مسح اسم S-CSCF والتسجيل.
6	TIMEOUT_DEREGISTRATION_STORE_SERVER_NAME	إنهاء التسجيل. الاحتفاظ باسم S-CSCF في السجل.
7	USER_DEREGISTRATION_STORE_SERVER_NAME	إنهاء التسجيل. الاحتفاظ باسم S-CSCF في السجل.
8	ADMINISTRATIVE_DEREGISTRATION	مسح اسم S-CSCF

القيمة	الاسم	إجراء HSS
		والتسجيل.
9	AUTHENTICATION_FAILURE	الاحتفاظ بربط مسجل، ما لم يكن الاسم في السجل قديمًا. مسح اسم S-CSCF عند عدم التسجيل.
10	AUTHENTICATION_TIMEOUT	الاحتفاظ بربط مسجل، ما لم يكن الاسم في السجل قديمًا. مسح اسم S-CSCF عند عدم التسجيل.
11	DEREGISTRATION_TOO_MUCH_DATA	مسح اسم S-CSCF والتسجيل.

تستمر تلك TS 29.228 §6.1.2. وفقًا لـ S-CSCF، تنهي الأنواع 6 و 7 التسجيل ولكن تحتفظ باسم ال��قدة في خدمة حالة المشترك غير المسجل، لذا لا يزال يتم حل UAR لاحقًا إليها.

`AUTHENTICATION_FAILURE` **كشف الاسم القديم عند فشل المصادقة.** عادةً ما يحتفظ SAR بربط المشترك المسجل. هناك استثناء واحد. إذا جاء SAR `AUTHENTICATION_TIMEOUT` أو قد أعادت توزيع I-CSCF مختلف عن الموجود في السجل، يجب أن تكون S-CSCF من HSS بمسح إلى المجموعة، لأنها لم تتمكن من الوصول إلى العقدة المسجلة. ثم تقوم REGISTER العقدة الميتة HSS ستعيد: S-CSCF ذلك الاسم كقديم. بدون هذه القاعدة، لا يتقارب استرداد فشل SAR قبل أي UE لاحق، وفقط تحدٍ يكمله UAR في كل مهلة سيستعيد المشترك.

راجع مقياس hss_cx_auth_abandon_total لرؤية التحديات المهجورة أو الفاشلة.

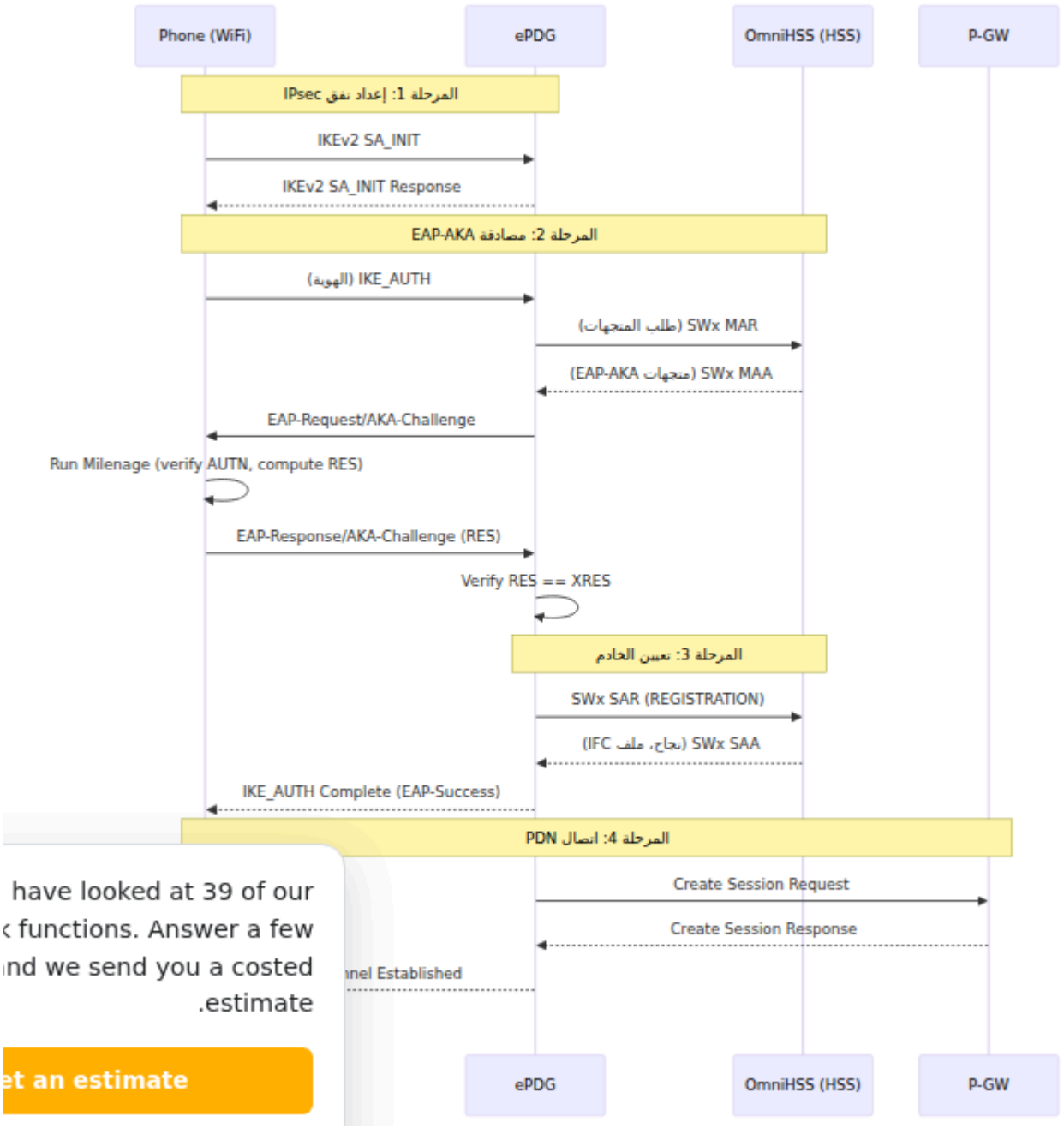
S-CSCF واحد لكل اشتراك

انظر ميزات) تحت هوية واحدة، MSISDNs أو عدة IMSIs، المشتركة عدة IMS تجمع اشتراكات واحد فقط الاشتراك بالكامل. إذا سجل S-CSCF يجب أن يخدم Multi-IMSI و Multi-MSISDN). عضوان ��لى عقدتين مختلفتين، فإن مكالمة إنهاء ستصل إلى عقدة لا تحتفظ بأي ربط للطرف المطلوب.

تحتفظ HSS باسم S-CSCF مشترك على اشتراك IMS، يسمى المرساة:

1. يسجل العضو الأول. لا يتم تعيين مرساة، لذلك تعيد UAA اختيارًا (URI أو مجموعة، عقدة تحت `:random_peer`).
2. تأخذ عقدة حقيقية التسجيل وترسل SAR تقوم بها. الخاص HSS على بتثبيت الاشتراك تلك العقدة.
3. يقرأ كل عضو UAA الخاصة به العقدة المثبتة، لذا تهبط كل عضو لاحق المرساة. تعيد على نفس S-CSCF.
4. يتم تحرير المرساة عندما يتم deregister العضو الأخير.

لا تقوم HSS أبدًا بتثبيت URI مجموعة. URI مجموعة يسمي المجموعة، وليس عقدة، لذا تحتفظ به فقط لفترة كافية لتقوم I-CSCF بحله. إذا كانت المرساة تحمل URI مجموعة من إصدار HSS التالي يستبدله بالعقدة الحقيقية التي تخدم SAR سابق، فإن.

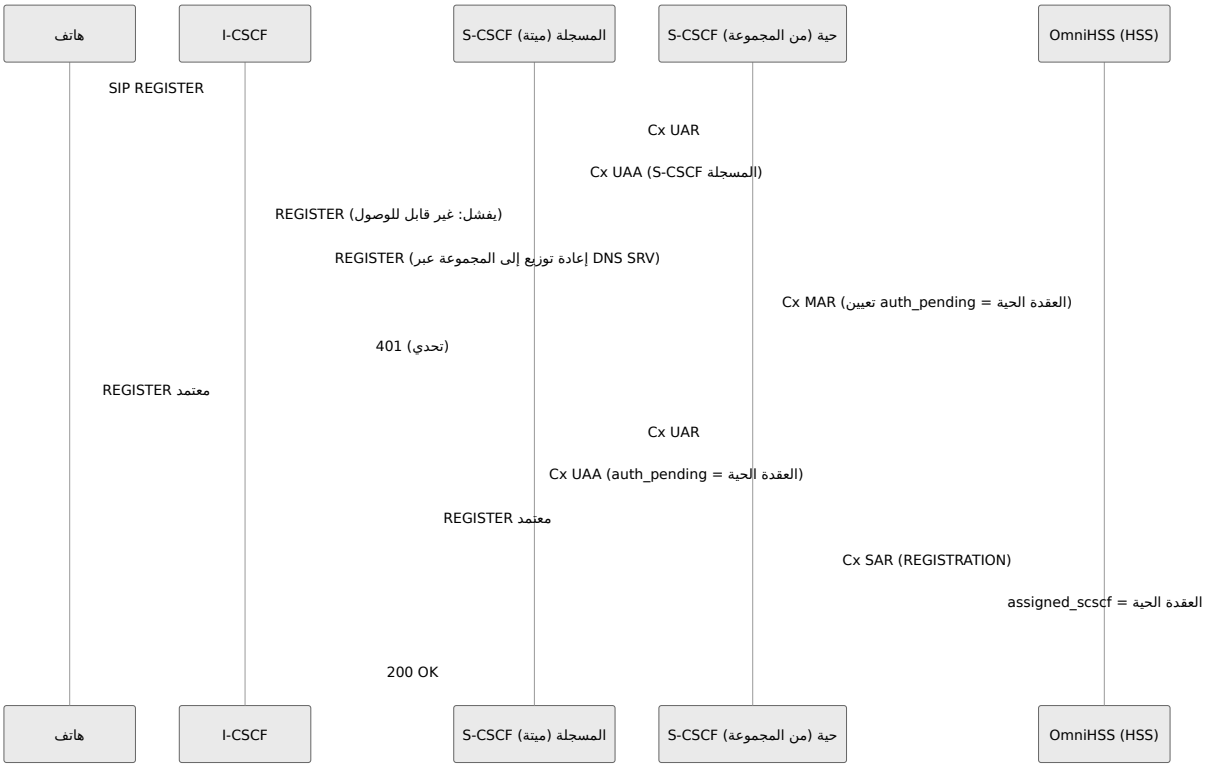


استرداد فشل S-CSCF

إذا كانت S-CSCF المسجلة غير قابلة للوصول، تعيد I-CSCF إرسال REGISTER إلى مجموعة S-CSCF حية المشترك. يتطلب ذلك مسار تراجع مجموعة S-CSCF وتفضيل I-CSCF ثم تخدم S-CSCF. معًا في HSS `auth_pending_scscf`.

هناك وضعان للفشل:

وضع الفشل	كيف يظهر	الاسترداد
اسم S-CSCF غير قابل للحل (اسم تم إيقافه أو قديم في بيانات HSS)	تعيد DNS NXDOMAIN. يفشل التوجيه من I-CSCF قبل أن ينشئ فرعًا.	I-CSCF تعيد URI إرسال إلى المجموعة. تختار DNS SRV S-CSCF حية.
S-CSCF قابل للحل ولكنه ميت (S-CSCF خدمة معطلة)	TCP. تم رفض اتصال يفشل الفرع بشكل غير متزامن.	I-CSCF تعيد URI إرسال إلى المجموعة من مسار الفشل الخاص بها. تجعل `use_dst_blocklist` و `use_dns_failover` DNS يتجاوز العقدة الميتة.



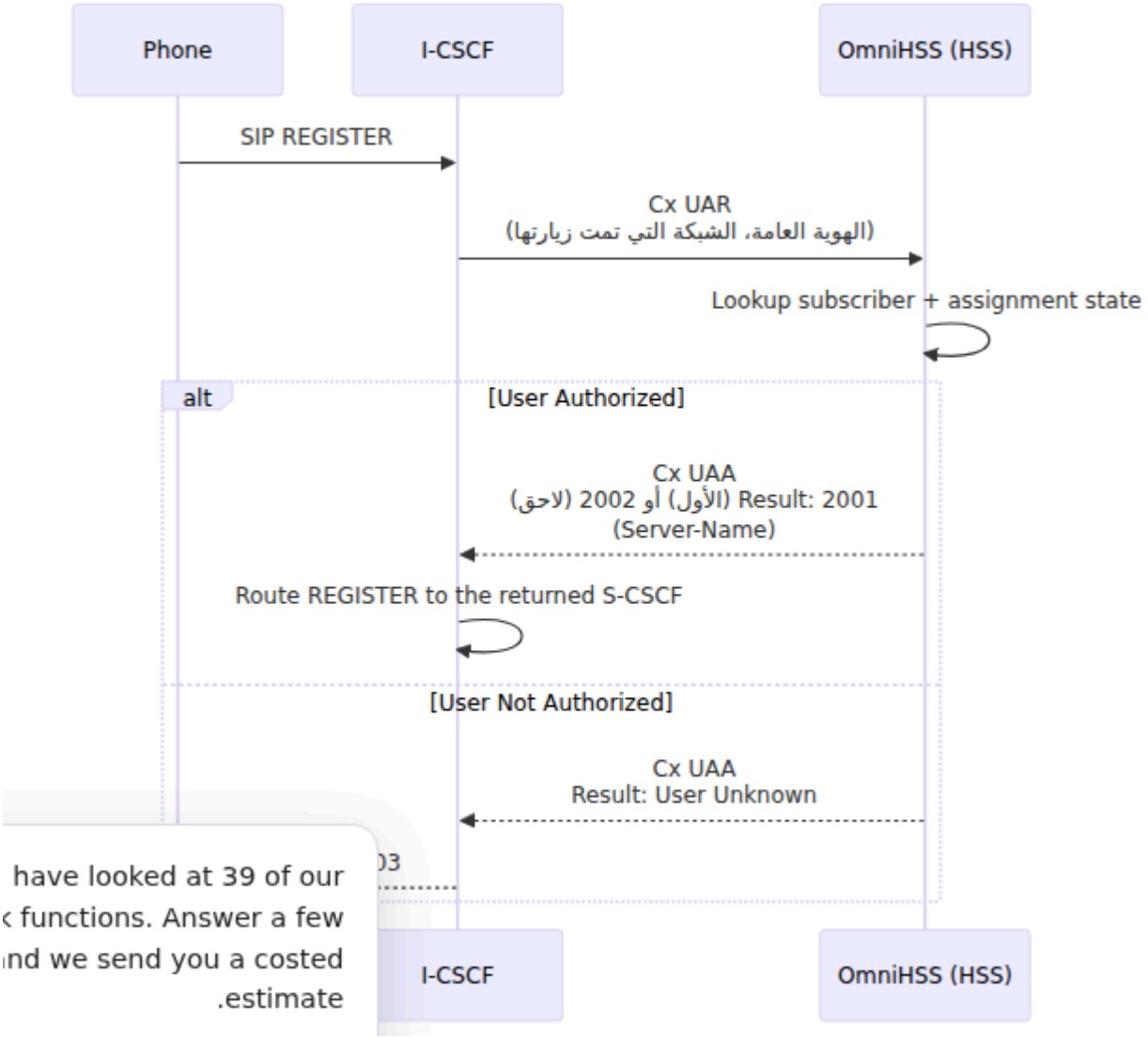
الحية التي أصدرت التحدي. تجعل تفضيل S-CSCF المعتمد إلى نفس REGISTER يجب أن يصل الخاص بها، MAR هذا يحدث: بعد أن ترسل العق��ة الحية UAA في `auth_pending_scscf` التالي، وليس العقدة الميتة المسجلة. بدون التفضيل، ستذهب الـ UAR تلك العقدة في HSS تعيد إلى أعضاء مجموعة مختلفين ولن يتقارب الدورة REGISTERs.

S-CSCF بواسطة UE يتم إعادة تحدي IMS-AKA، أثناء دورة تحدي S-CSCF **القيود.** إذا تم قتل في منتصف S-CSCF في تسجيله التالي. هذا متأصل في تغيير UE جديد. يستعيد nonce الجديد مع مختلف S-CSCF التحدي، لأن متجه المصادقة الجاري لا يمكنه الانتقال إلى.

انظر تكوين اختيار S-CSCF) لتمكين هذا الاسترداد، قم بتعيين `selection_method: :pool_uri` ونشر مسار تراجع مجموعة I-CSCF.

طلب معلومات الموقع (LIR/LIA)

يخدم المستخدم S-CSCF عن أي I-CSCF تستفسر.

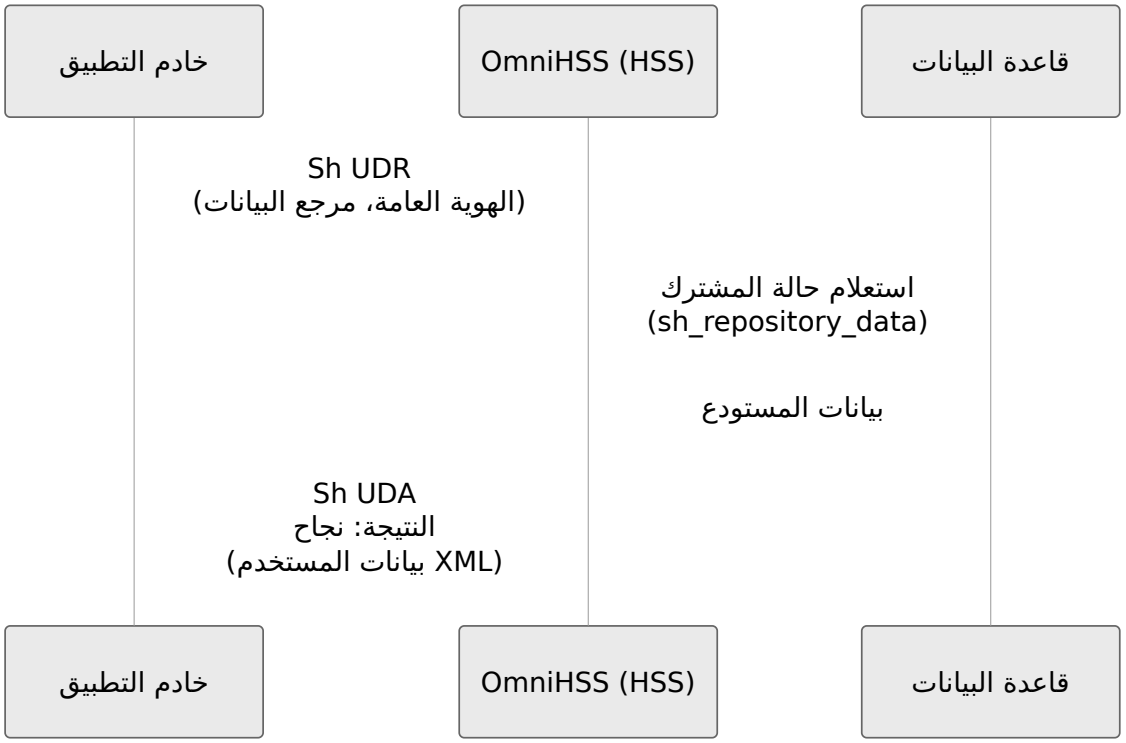


واجهة Sh (بيانات ملف تعريف IMS)

انظر Sh RepositoryData (بيانات شفافة) لنموذج البيانات، قواعد التزامن، وواجهة برمجة REST لتوفير خدمات MMTEL / SequenceNumber/ معلومات IMS-ODB.

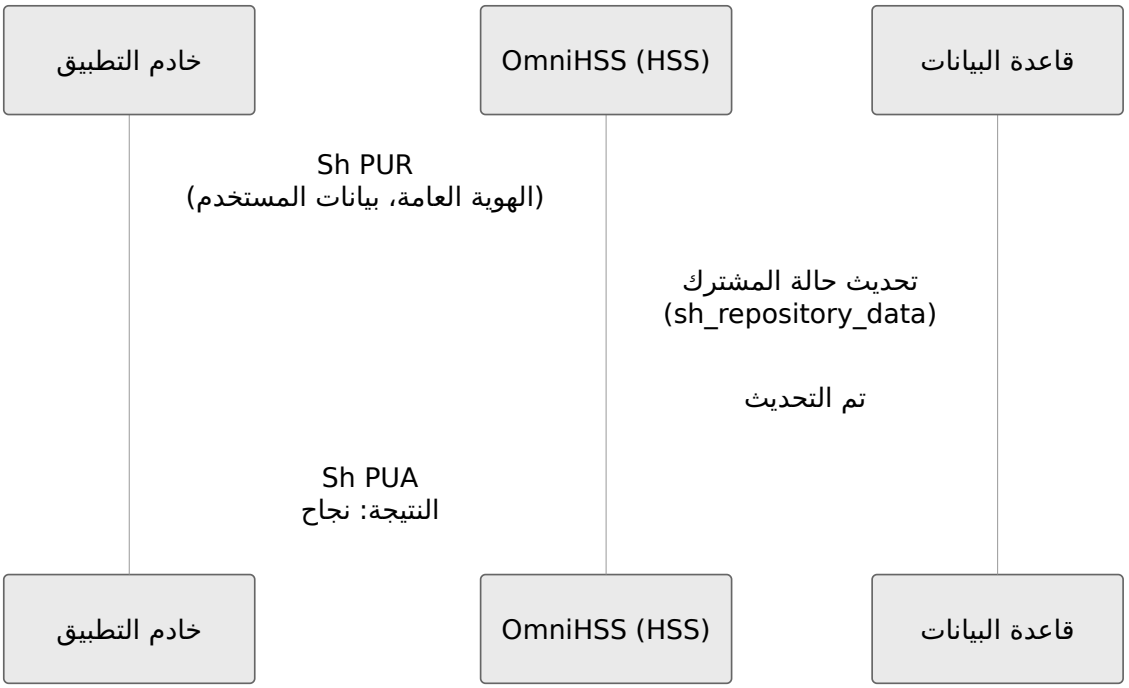
طلب بيانات المستخدم (UDR/UDA)

يطلب خادم التطبيق بيانات ملف تعريف المشترك.



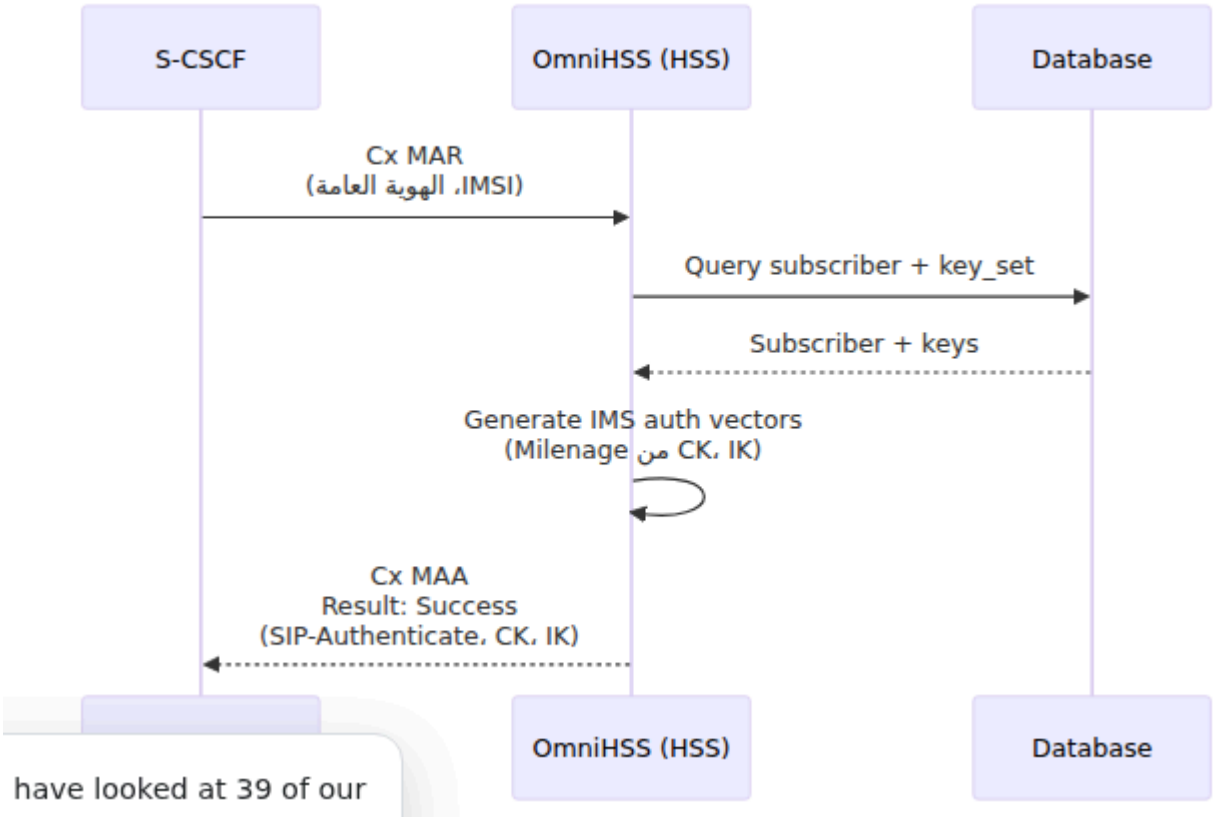
طلب تحديث الملف الشخصي (PUR/PUA)

يحدث خادم التطبيق بيانات ملف تعريف المشترك.



طلب إشعارات الاشتراك (SNR/SNA)

يشتري خادم التطبيق تغييرات الملف الشخصي.



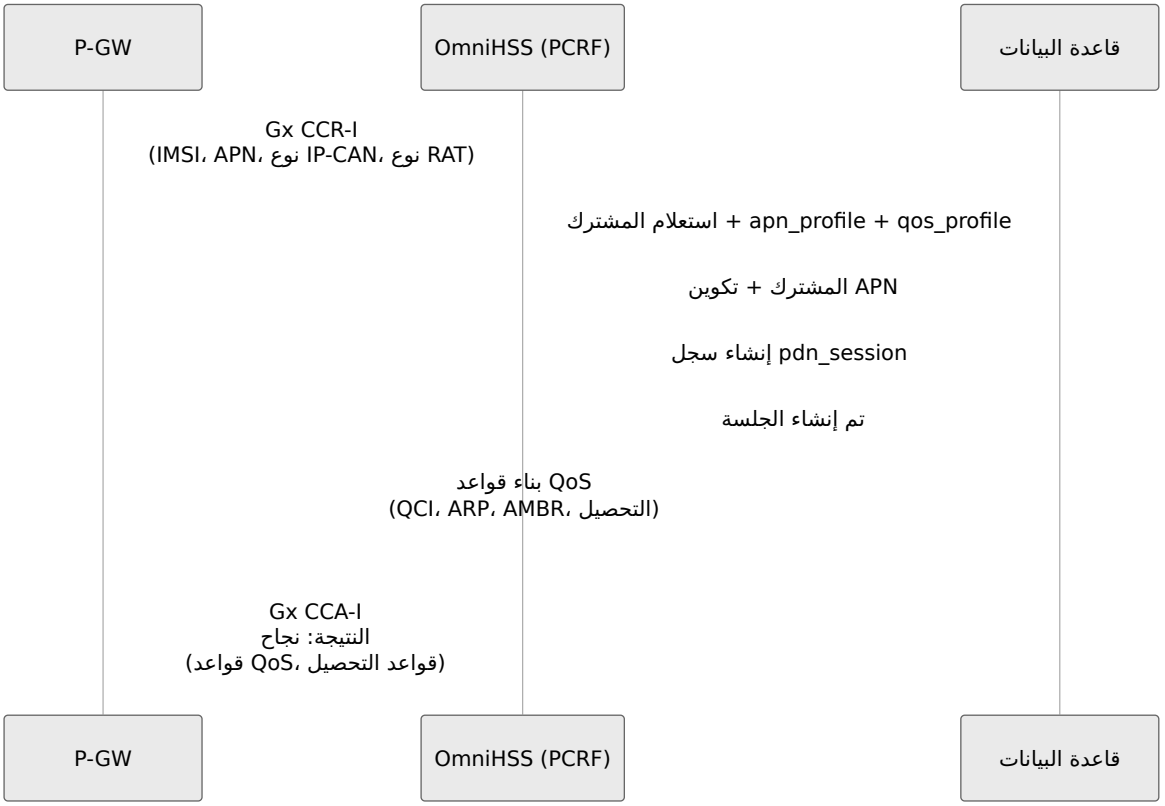
واجهة Gx (التحكم في السياسة)

تعمل OmniHSS كـ PCRF (وظيفة قواعد السياسة والتحصيل) عبر واجهة Gx.

انظر وثائق PCRF للمعمارية التفصيلية، تكوين السياسة، وإدارة جودة الخدمة.

طلب التحكم في الائتمان - أولي (CCR-I/CCA-I)

يطلب P-GW قواعد السياسة عند إنشاء جلسة PDN.

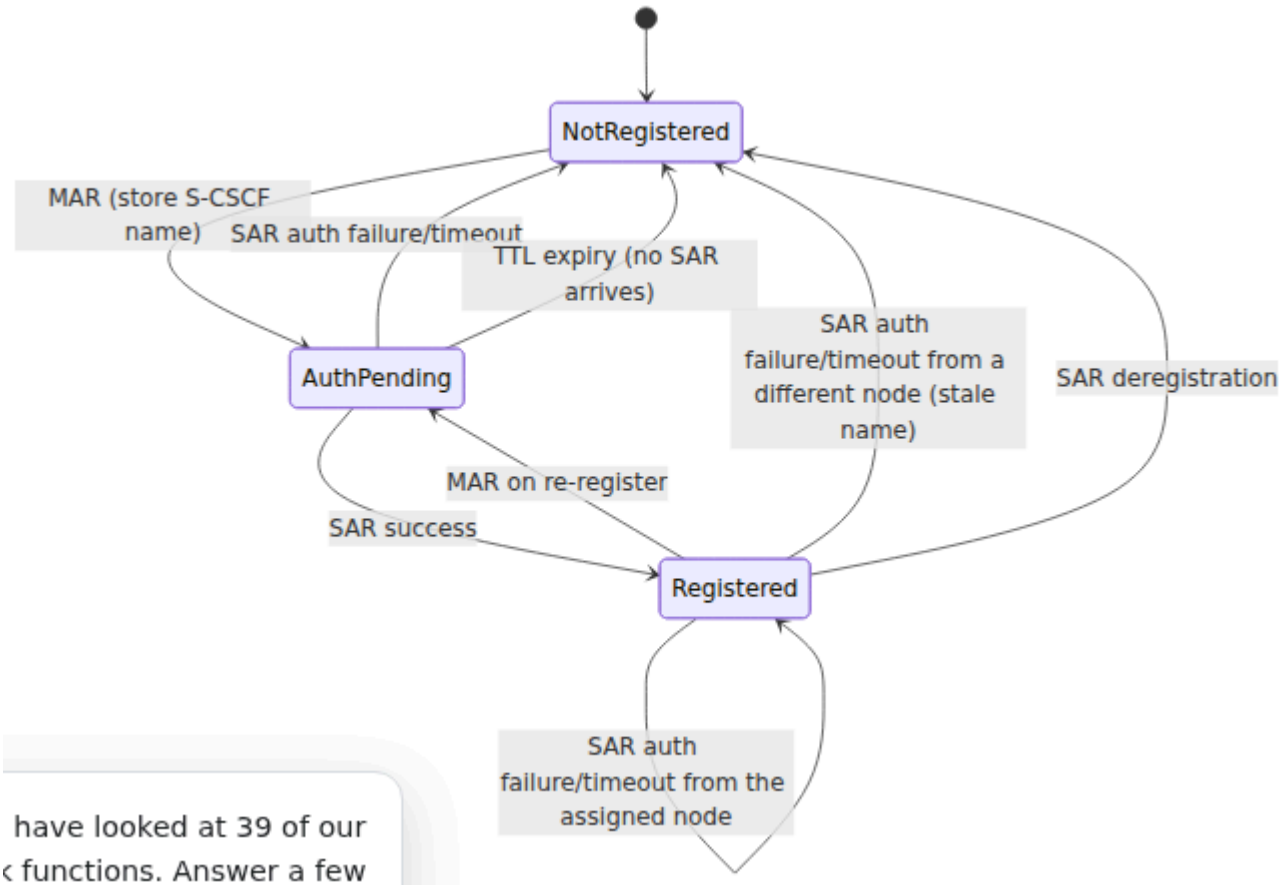


المفاتيح AVPs:

- الطلب: Subscription-Id (IMSI)، Called-Station-Id (APN)، RAT-Type، IP-CAN-Type
- الاستجابة: QoS-Information (QCI، ARP، AMBR)، Charging-Rule-Install

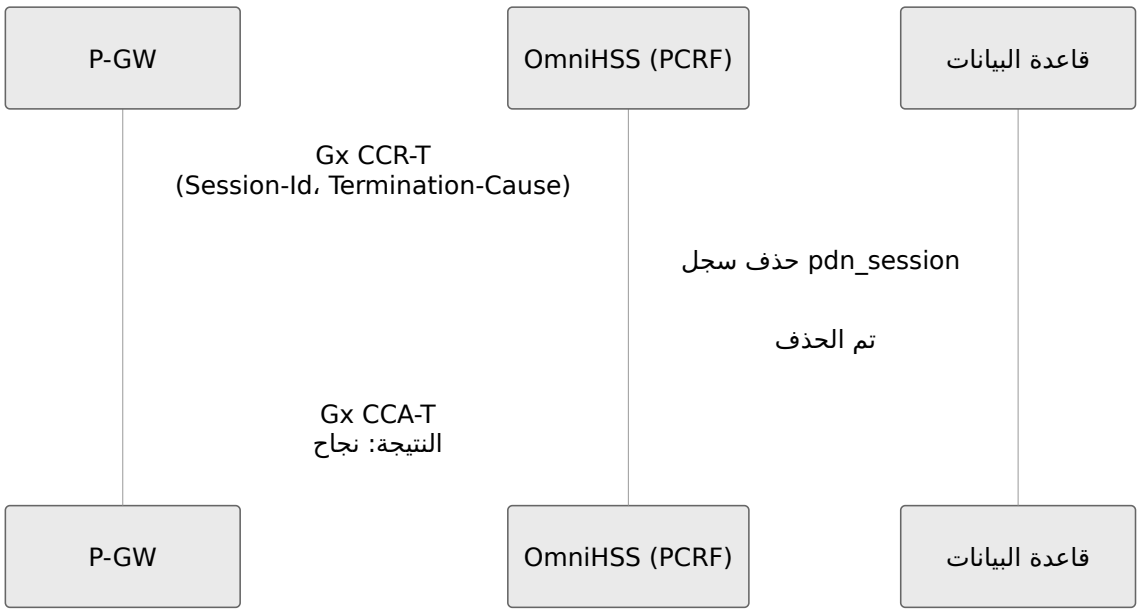
طلب التحكم في الائتمان - تحديث (CCR-U/CCA-U)

يبلغ P-GW عن تغييرات الجلسة.



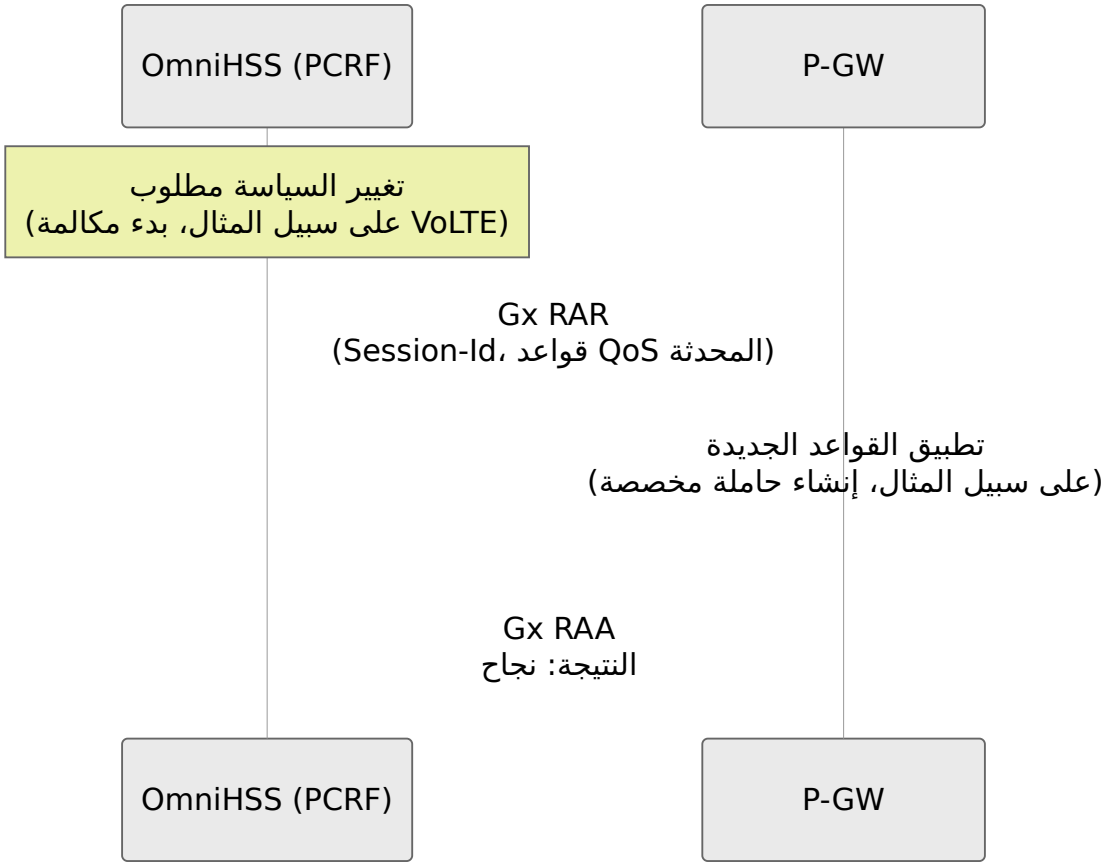
طلب التحكم في الائتمان - إنهاء (CCR-T/CCA-T)

يبلغ P-GW عند انتهاء جلسة PDN.



طلب إعادة المصادقة (RAR/RAA)

تبدأ OmniHSS (PCRF) تحديث السياسة إلى P-GW.



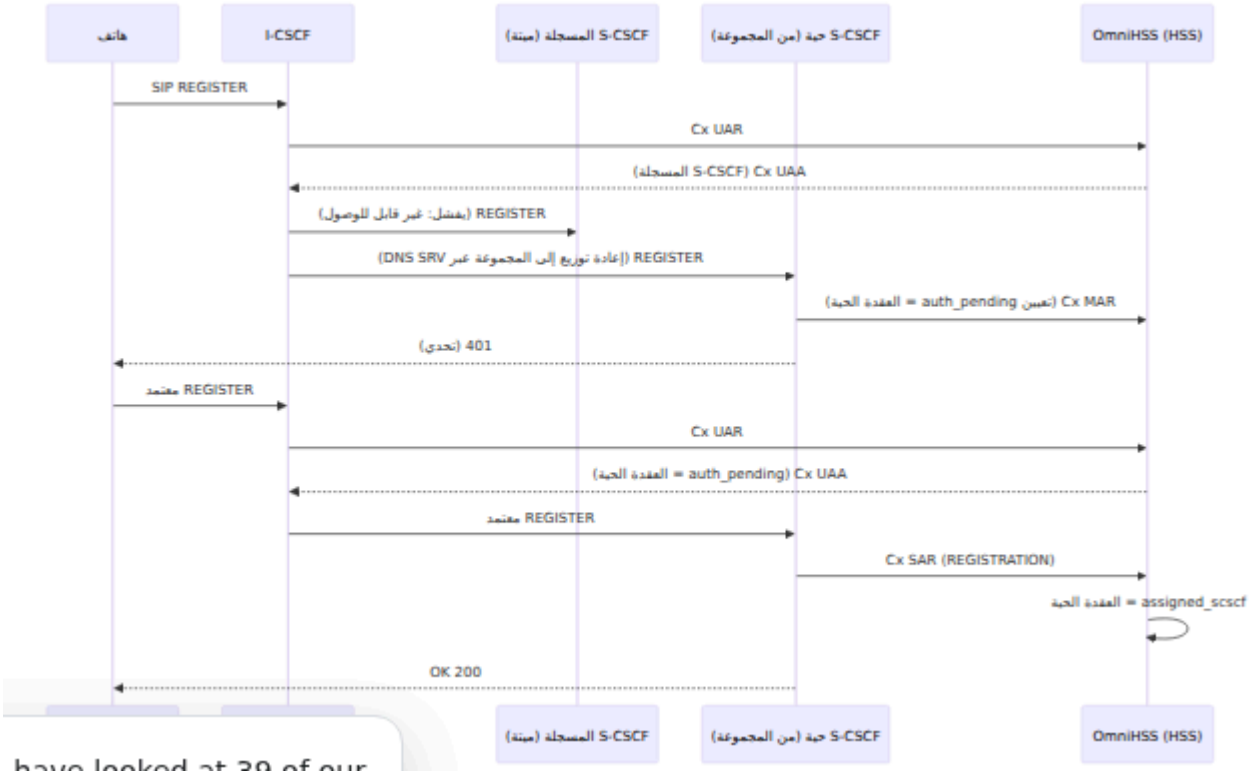
واجهة Rx (سياسة وسائط IMS)

تعمل OmniHSS كـ PCRF عبر واجهة Rx لتفويض وسائط IMS.

انظر وثائق PCRF لتفاصيل تدفقات مكالمات VoLTE وتفويض الوسائط.

طلب AA (AAR/AAA)

يطلب P-CSCF تفويض الوسائط لجلسة IMS.

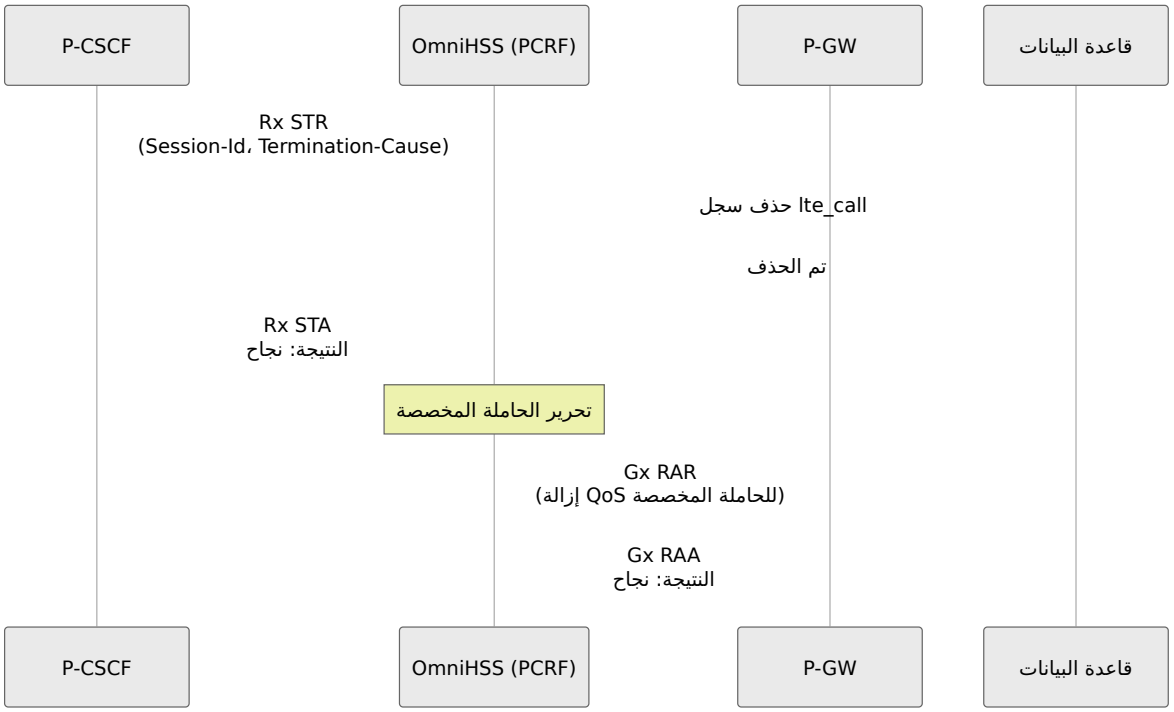


المعلومات الرئيسية:

- تحليل SDP لتحديد الترميز وعرض النطاق الترددي
- حساب عرض النطاق الترددي المطلوب (UL/DL)
- إنشاء مرشحات SDF لتدفقات الوسائط
- بدء الحاملة المخصصة عبر Gx RAR

طلب إنهاء الجلسة (STR/STA)

يبلغ P-CSCF عند انتهاء جلسة IMS.

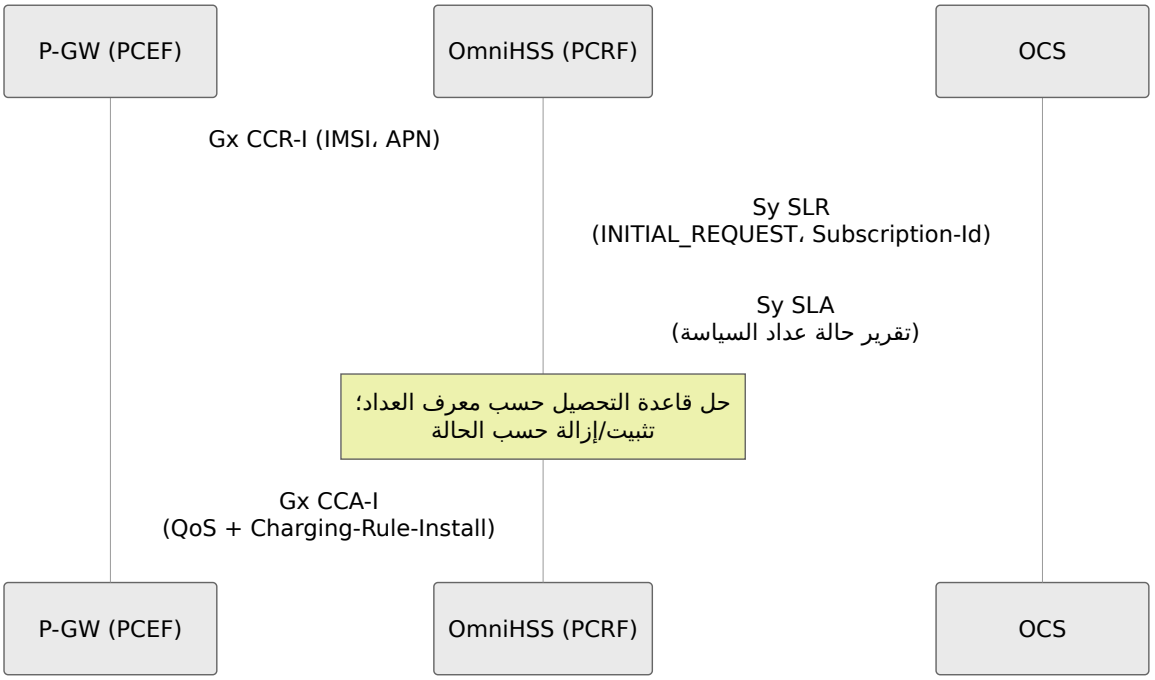


واجهة Sy (التحكم في حدود الإنفاق)

للحصول على حالة حد الإنفاق للمشترك من Sy واجهة، PCRF التي تعمل كـ OmniHSS، تستخدم Sy تستخدم Gx. خارجي (نظام التحصيل عبر الإنترنت) وتطبيق سياسة مدفوعة بالإنفاق عبر OCS هو Sy؛ OCS هو عميل HSS. (3GPP TS 29.219) `16777302` Diameter معرف تطبيق (التكوين، AVPs، تعيين عداد السياسة) للمرجع الكامل Sy الخادم. انظر واجهة.

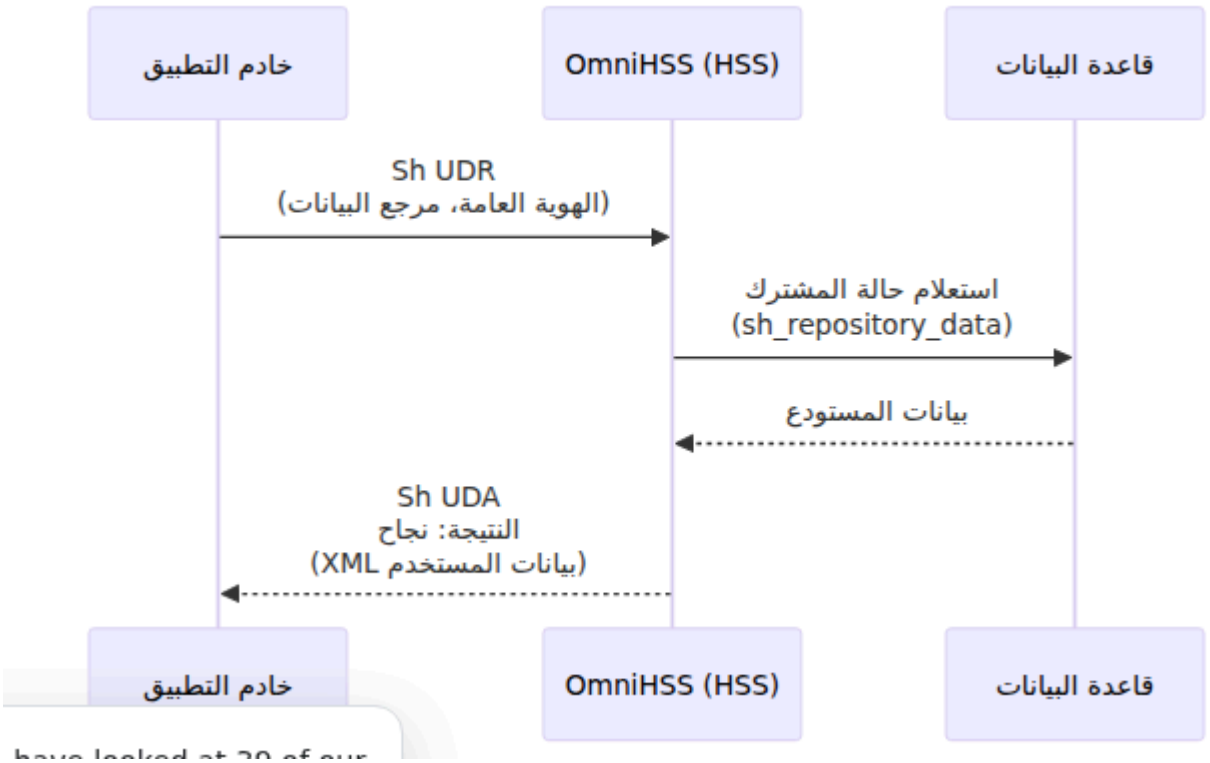
طلب حد الإنفاق (SLR/SLA)

يفتح PCRF جلسة Sy لكل مشترك لجلب الحالة الحالية لعدادات سياسة OCS، ثم يدمج القواعد الذي يعيده بالفعل Gx CCA الناتجة في.



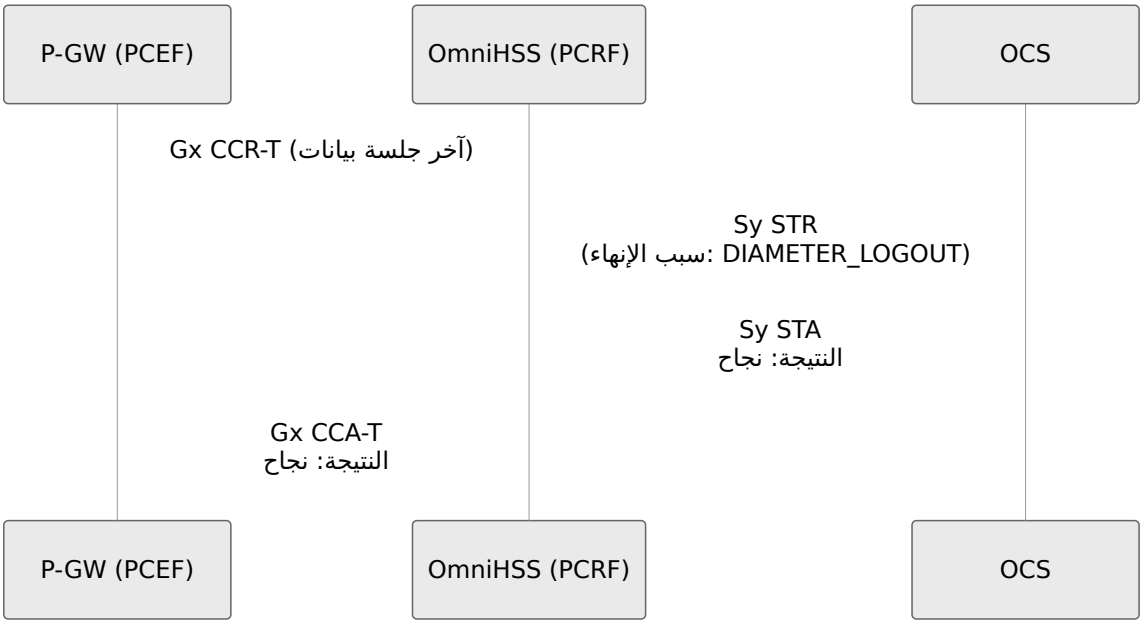
إشعار حالة الإنفاق (SNR/SNA)

عندما تتغير حالة عداد (على سبيل المثال، يتم استنفاد بدل البيانات)، يقوم PCRF، بإخطار OCS الذي يدفع تغيير السياسة إلى PGW عبر Gx RAR.



إنهاء الجلسة (STR/STA)

جلسة Sy. عندما تنتهي آخر جلسة بيانات للمشترك، يغلق PCRF



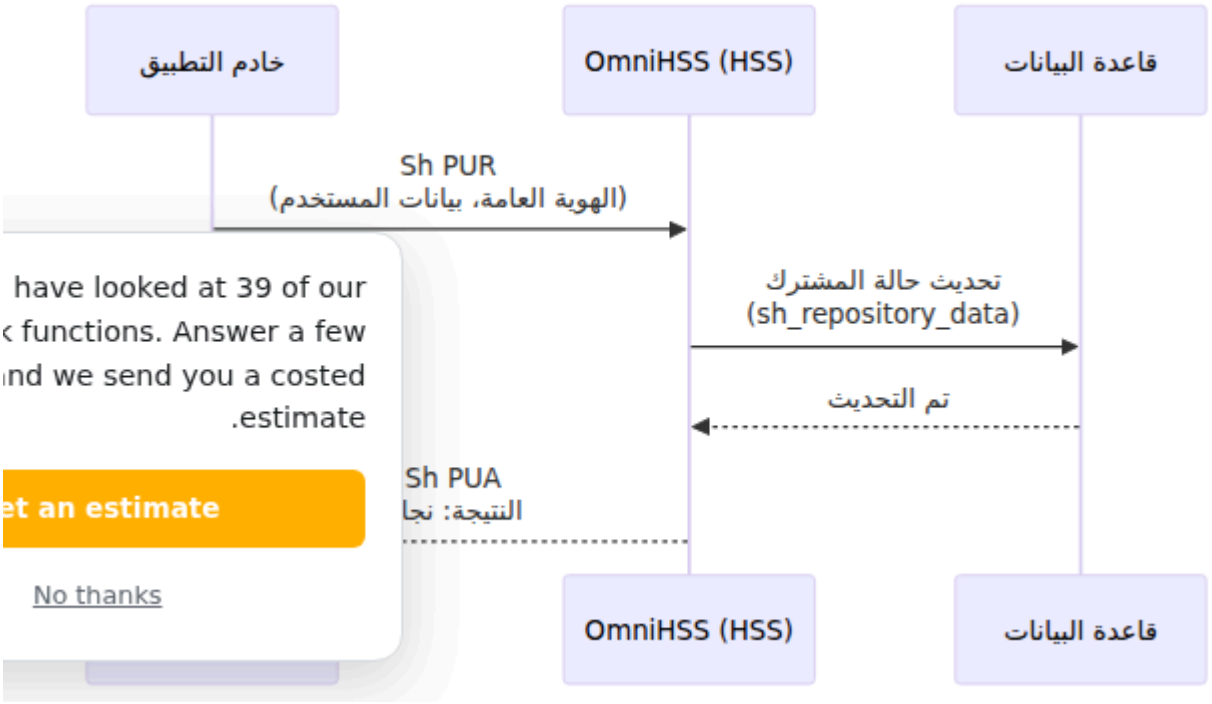
واجهة S13 (EIR)

تعمل OmniHSS كـ EIR (سجل هوية المعدات) عبر واجهة S13.

انظر وثائق EIR للتحقق التفصيلي من هوية المعدات، والتحقق من IMEI، وإدارة القائمة السوداء، وأولوية القواعد.

طلب التحقق من هوية ME (ECR/ECA)

يطلب عميل EIR الخارجي (أو MME) التحقق من المعدات.



قيم حالة المعدات:

- مدرج في القائمة البيضاء **(0)** - الجهاز مسموح
- مدرج في القائمة السوداء **(1)** - الجهاز محظور
- مدرج في القائمة الرمادية **(2)** - الجهاز مسموح ولكن يتم تتبعه

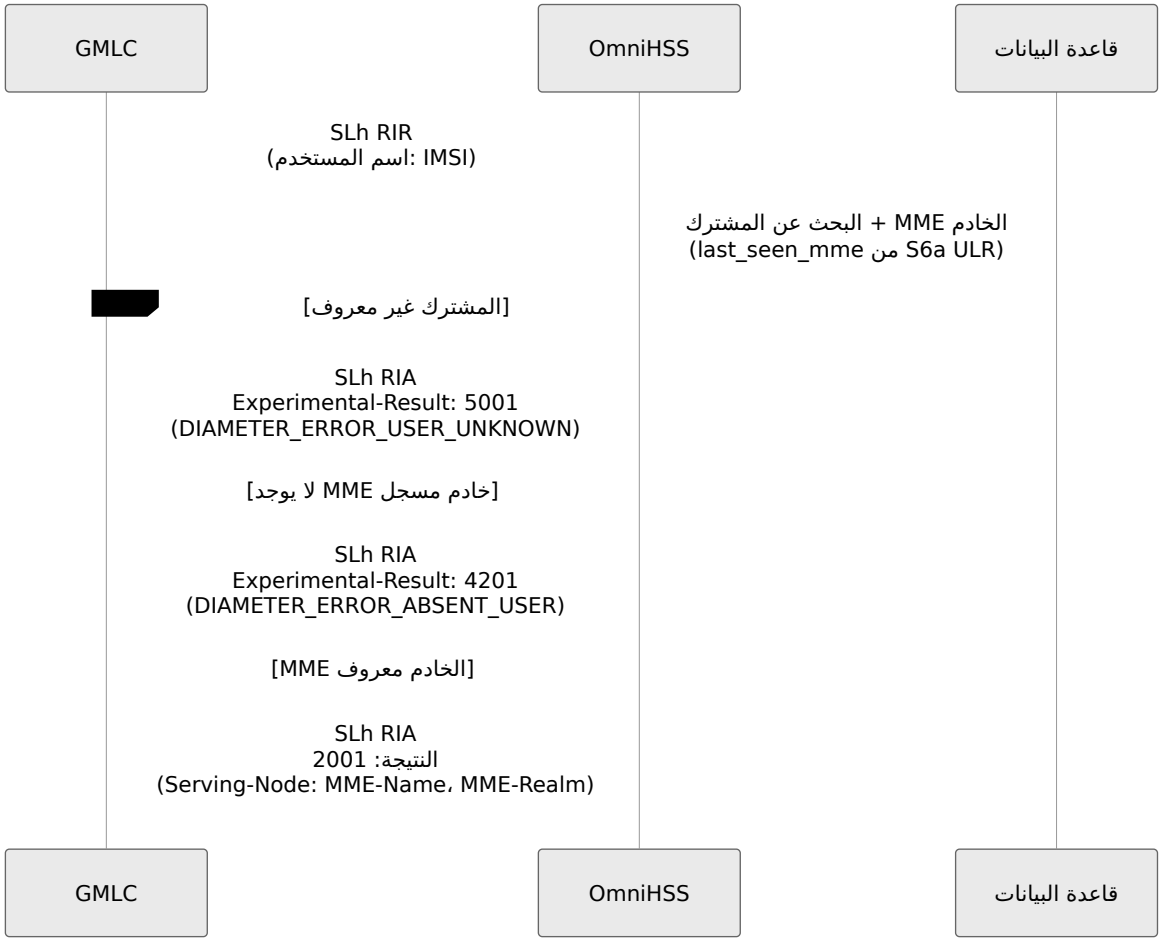
في الطلب غير معروف أو معطل، أو لم يتطابق أي قاعدة و IMSI إذا كان `unknown_equipment_behaviour` هو `:reject_unknown_equipment`، فإن ECA يحمل بدلاً من حالة (DIAMETER_ERROR_EQUIPMENT_UNKNOWN) رمز نتيجة تجريبية 5422 المعدات.

واجهة SLh (LCS / خدمات الموقع)

تجيب OmniHSS على SLh `LCS-Routing-Info-Request` (RIR) حتى يتمكن GMLC من اكتشاف أي MME يخدم مشتركًا حاليًا قبل طلب موقعهم عبر SLg. MME الخادم هو الذي تم تسجيله في تسجيل S6a (تحديث الموقع). تستخدم SLh معرف تطبيق Diameter `16777291` (3GPP TS 29.173).

طلب معلومات توجيه LCS (RIR/RIA)

يطلب GMLC العقدة الخادمة لمشترك.



ملاحظات:

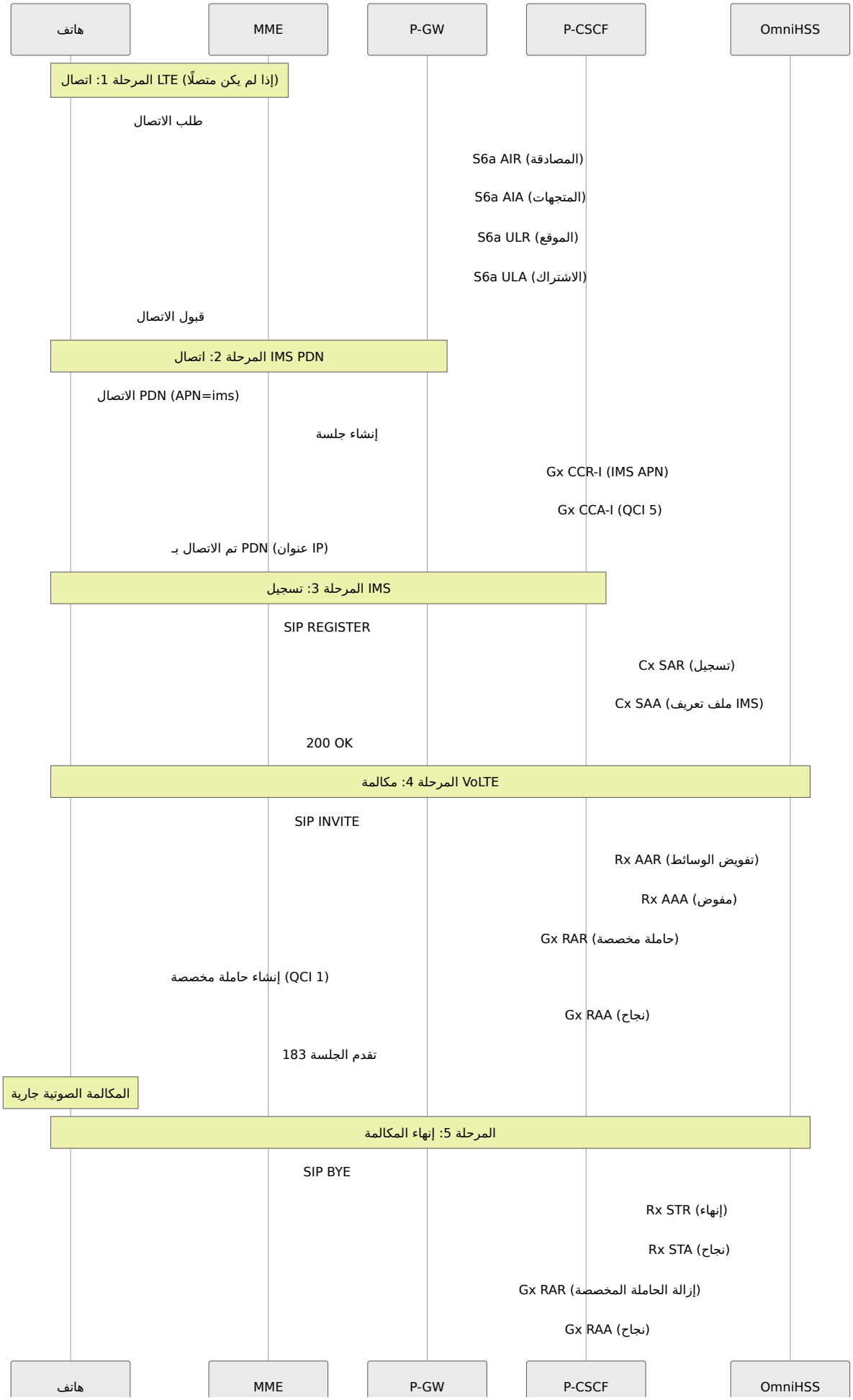
- يتم أخذ IMSI بحث استخدام يتم ؛`اسم المستخدم` من MSISDN كخيار احتياطي.
- تحمل `Serving-Node` المعادة `MME-Name`/`MME-Realm` المسجلة آخر مرة بواسطة معالجات S6a AIR/ULR (`subscriber_state.last_seen_mme` / `last_seen_realm`) - لا يتطلب الأمر توفيرًا إضافيًا.
- يتبع GMLC عادةً RIA ناجحة مع طلب SLg Provide-Location إلى MME المعاد.

رموز النتائج:

- **2001** - نجاح؛ تم إرجاع `Serving-Node`.
- **5001** - `DIAMETER_ERROR_USER_UNKNOWN`؛ IMSI/MSISDN غير موفر.
- **4201** - `DIAMETER_ERROR_ABSENT_USER` المشترك معروف ولكن لا يوجد ؛ MME خادم في السجل (لم يتصل أبدًا، أو تم إلغاء الموقع).

VoLTE تدفق المكالمة الكامل: مكالمة

إعداد مكالمة VoLTE من النهاية إلى النهاية يظهر واجهات متعددة.

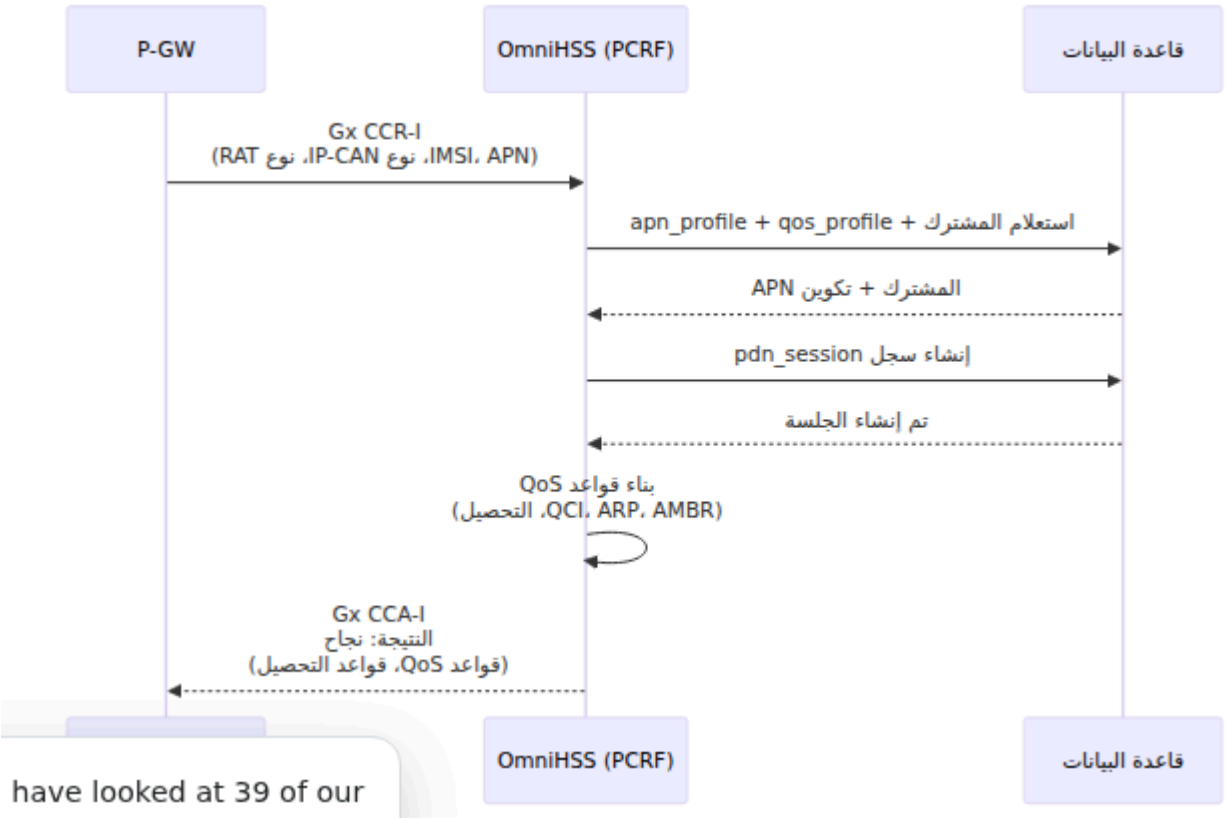

هاتف
MME
P-GW
P-CSCF
OmniHSS
المرحلة 1: اتصال LTE (إذا لم يكن متصلًا)
طلب الاتصال
S6a AIR (المصادقة)
S6a AIA (المتجهات)
S6a ULR (الموقع)
S6a ULA (الاشتراك)
قبول الاتصال
المرحلة 2: اتصال IMS PDN
الاتصال PDN (APN=ims)
إنشاء جلسة
Gx CCR-I (IMS APN)
Gx CCA-I (QCI 5)
تم الاتصال بـ PDN (عنوان IP)
المرحلة 3: تسجيل IMS
SIP REGISTER
Cx SAR (تسجيل)
Cx SAA (ملف تعريف IMS)
200 OK
المرحلة 4: مكالمة VoLTE
SIP INVITE
Rx AAR (تفويض الوسائط)
Rx AAA (مفوض)
Gx RAR (حاملة مخصصة)
إنشاء حاملة مخصصة (QCI 1)
Gx RAA (نجاح)
تقدم الجلسة 183
المكالمة الصوتية جارية
المرحلة 5: إنهاء المكالمة
SIP BYE
Rx STR (إنهاء)
Rx STA (نجاح)
Gx RAR (إزالة الحاملة المخصصة)
Gx RAA (نجاح)
هاتف
MME
P-GW
P-CSCF
OmniHSS

واجهة Zh (معمارية التمهيد العامة)

تمكن واجهة Zh معمارية التمهيد العامة (GBA) من خلال ربط وظيفة خادم التمهيد (BSF) بنظام HSS لمصادقة المشتركين واستخراج المفاتيح.

طلب مصادقة الوسائط المتعددة (MAR/MAA)

يطلب BSF متجهات مصادقة GBA للتمهيد.



المتغيرات الأساسية:

- الطلب: اسم المستخدم (IMPI)، الهوية العامة، SIP-Auth-Data-Item (نظام المصادقة)، مجال الوجهة
- الاستجابة: SIP-Auth-Data-Item (SIP-Authenticate، SIP-Authorization، Confidentiality-Key، Integrity-Key)، GBA-UserSecSettings

حالات استخدام GBA:

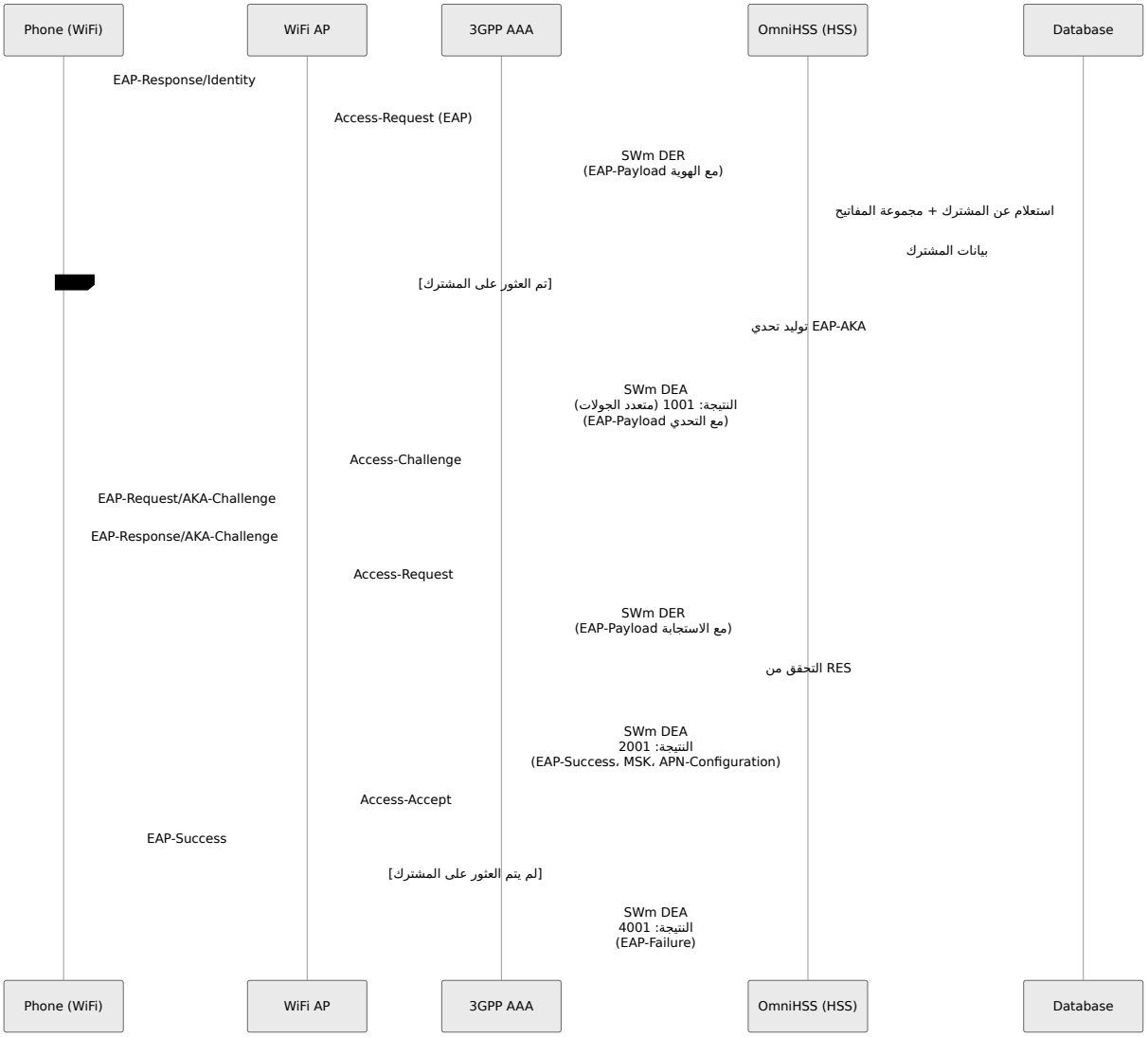
التطبيق	الوصف
MBMS	إدارة مفاتيح خدمة البث المتنقل المتعدد
HTTPS	توفير الشهادات المعتمدة على GBA
NAF	مصادقة وظيفة تطبيق الشبكة العامة
الحضور	مصادقة خدمة الحضور الآمن

واجهة SWm (الوصول غير الموثوق وغير 3GPP)

تمكن واجهة SWm مصادقة EAP-AKA 3 لشبكات الوصول غير الموثوقة وغير 3GPP (مثل WiFi عبر ePDG) من خلال ربط خادم AAA 3GPP بنظام HSS.

طلب Diameter-EAP (DER/DEA)

تبادل مصادقة EAP للوصول عبر WiFi.

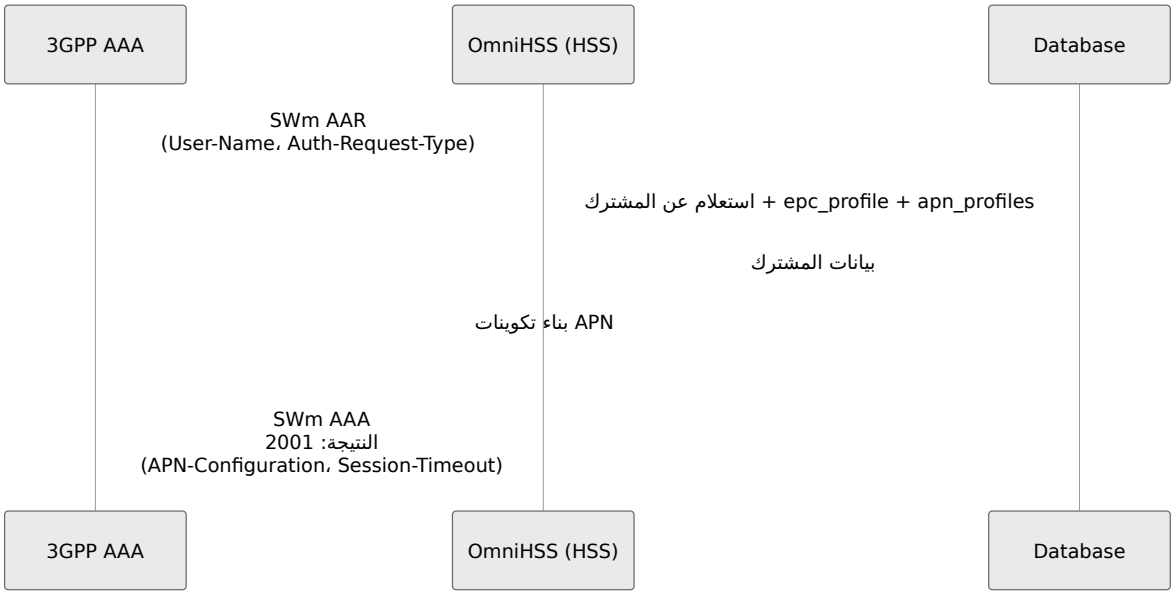


المتغيرات الأساسية:

- الطلب: Session-Id، Auth-Application-Id، EAP-Payload، Auth-Request-Type، User-Name (اختياري)
- الاستجابة: EAP-Payload، EAP-Master-Session-Key (MSK)، APN-Configuration، Session-Timeout

طلب AA (AAR/AAA)

التفويض بعد نجاح مصادقة EAP.

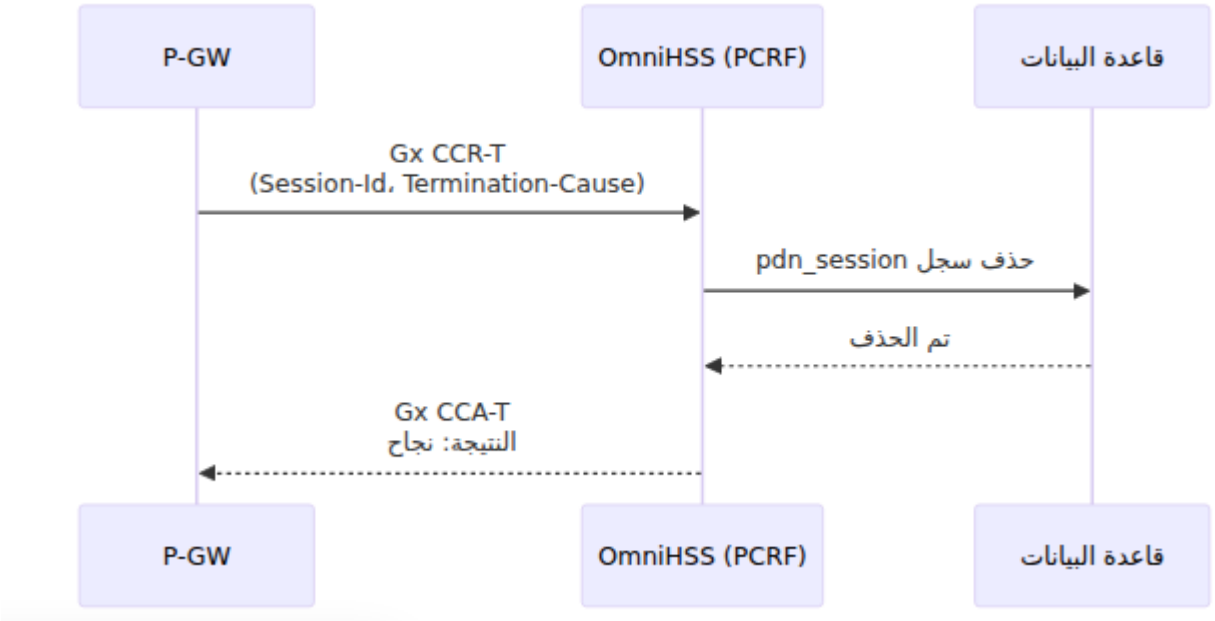


المتغيرات الأساسية:

- الطلب: Session-Id، Auth-Application-Id، User-Name، Auth-Request-Type، AAR-Flags
- الاستجابة: APN-Configuration، 3GPP-Charging-Characteristics، Session-Timeout

طلب إنهاء الجلسة (STR/STA)

إشعار إنهاء جلسة WiFi.



أسباب الإنهاء:

الوصف	القيمة	السبب
تسجيل خروج المستخدم	1	DIAMETER_LOGOUT
الخدمة غير متاحة	2	DIAMETER_SERVICE_NOT_PROVIDED
خطأ في البروتوكول	3	DIAMETER_BAD_ANSWER
إنهاء إداري	4	DIAMETER_ADMINISTRATIVE
فقدان الاتصال	5	DIAMETER_LINK_BROKEN
انتهاء صلاحية المصادقة	6	DIAMETER_AUTH_EXPIRED
انتقل المستخدم إلى وصول آخر	7	DIAMETER_USER_MOVED
انتهاء الجلسة	8	DIAMETER_SESSION_TIMEOUT

استكشاف مشكلات البروتوكول

فشل المصادقة (S6a AIR)

تحقق:

1. تم تكوين مجموعة المفاتيح بشكل صحيح (Ki، OPC، AMF)
2. مزامنة SQN (إذا كانت هناك فشلات متكررة)
3. قواعد التجوال تسمح بالشبكة التي تمت زيارتها

فشل تحديث الموقع (S6a ULR)

تحقق:

1. ملف EPC موجود وله APNs مكونة
2. التجوال مسموح لخدمات البيانات

3. تنسيق هوية MME صحيح

فشل تسجيل IMS (Cx SAR)

تحقق:

1. تم تعيين ملف IMS للمشترك
2. قالب IFC XML صالح
3. تم تكوين اختيار S-CSCF
4. تم تعيين MSISDNs إذا تم استخدامها في القالب

فشل اتصال PDN (Gx CCR-I)

تحقق:

1. APN موجود في قائمة APN لملف EPC
2. تم تكوين ملف QoS لـ APN
3. جدول جلسات PDN ليس ممتلئًا (إذا كانت هناك حدود موجودة)

← العودة إلى دليل العمليات

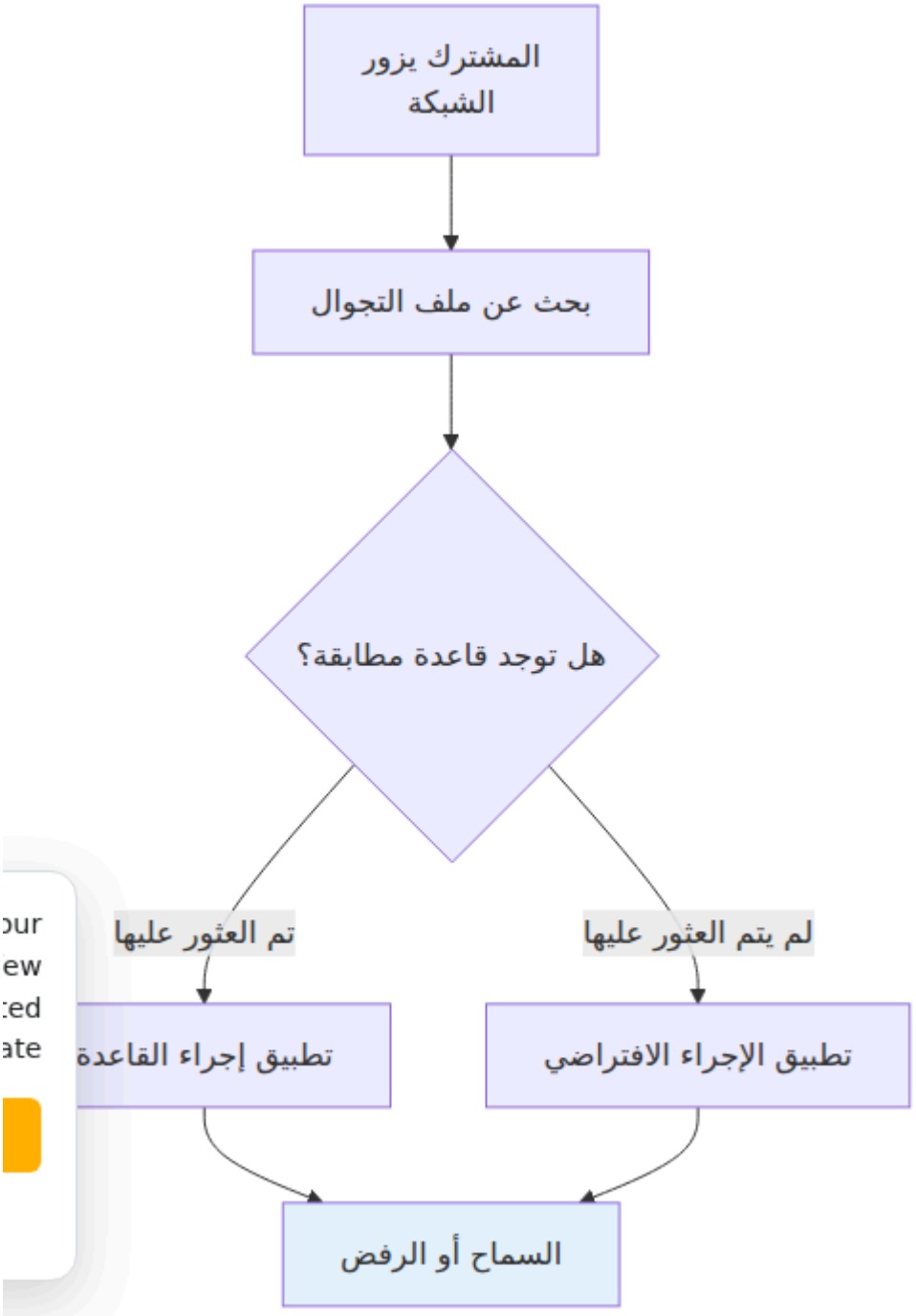
التحكم في التجوال لـ OmniHSS

← العودة إلى دليل العمليات

نظرة عامة

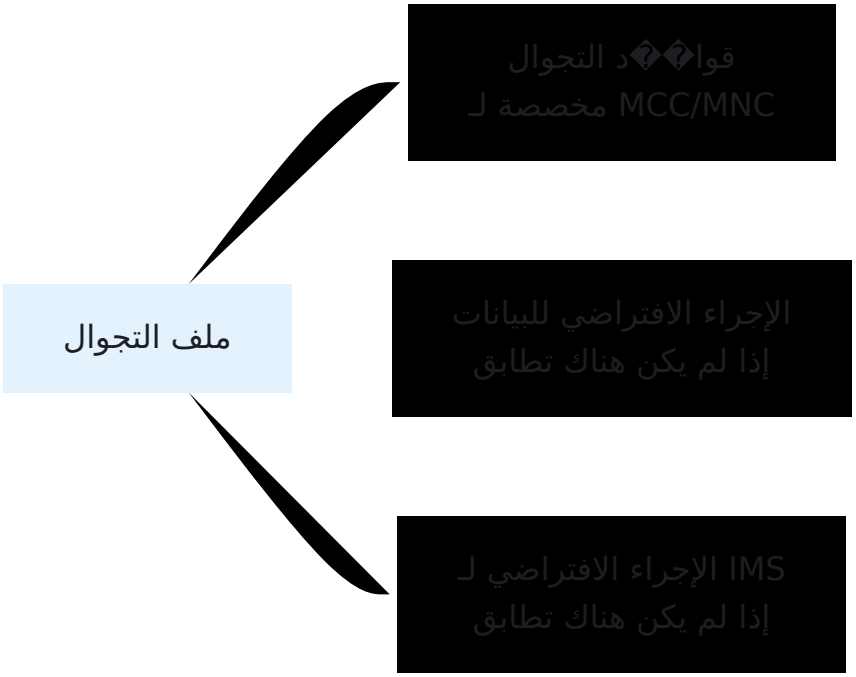
يوفر OmniHSS تحكمًا دقيقًا في التجوال، مما يسمح لك بتحديد الشبكات التي يمكن للمشتركين الوصول إليها لخدمات البيانات و IMS عند التجوال.

تدفق التحكم في التجوال



هيكل ملف التجوال

المكونات



قاعدة التجوال

تحدد كل قاعدة إجراء لشبكة معينة (مزيج MCC/MNC).

الحقول:

- `name` - اسم وصفي
- `mcc` - رمز الدولة المحمول (3 أرقام)
- `mnc` - رمز الشبكة المحمولة (2-3 أرقام)
- `data_action` - "السماح" أو "الرفض"
- `ims_action` - "السماح" أو "الرفض"

ملف التجوال

يحدد السلوك الافتراضي ويرتبط بالقواعد.

الحقول:

- `name` - اسم الملف
- `data_action_if_no_rules_match` - "السماح" أو "الرفض"
- `ims_action_if_no_rules_match` - "السماح" أو "الرفض"

أمثلة على التكوين

السماح بجميع التجوال

```
# إنشاء ملف يسمح بكل شيء
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "السماح للجميع",
      "data_action_if_no_rules_match": "السماح",
      "ims_action_if_no_rules_match": "السماح",
      "roaming_rules": []
    }
  }'
```

رفض جميع التجوال

```
# إنشاء ملف يمنع كل شيء
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "لا تجوال",
      "data_action_if_no_rules_match": "رفض",
      "ims_action_if_no_rules_match": "رفض",
      "roaming_rules": []
    }
  }'
```

السماح بشبكات محددة (القائمة البيضاء)

```
# إنشاء قاعدة AT&T
RULE1=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "السماح بـ AT&T",
      "mcc": "310",
      "mnc": "410",
      "data_action": "السماح",
      "ims_action": "السماح"
    }
  }' | jq -r '.response.id')

# إنشاء قاعدة Verizon
RULE2=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "السماح بـ Verizon",
      "mcc": "311",
      "mnc": "480",
      "data_action": "السماح",
      "ims_action": "السماح"
    }
  }' | jq -r '.response.id')

# إنشاء ملف مع رفض افتراضي وربط القواعد
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"roaming_profile\": {
      \"name\": \"شركات الولايات المتحدة فقط\",
      \"data_action_if_no_rules_match\": \"رفض\",
      \"ims_action_if_no_rules_match\": \"رفض\",
      \"roaming_rules\": [$RULE1, $RULE2]
    }
  }"
```

السماح بالبيانات، حظر الصوت

```
# إنشاء قاعدة تسمح بالبيانات ولكن تحظر IMS
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "بيانات فقط - T-Mobile",
      "mcc": "310",
      "mnc": "260",
      "data_action": "السماح",
      "ims_action": "رفض"
    }
  }'
```

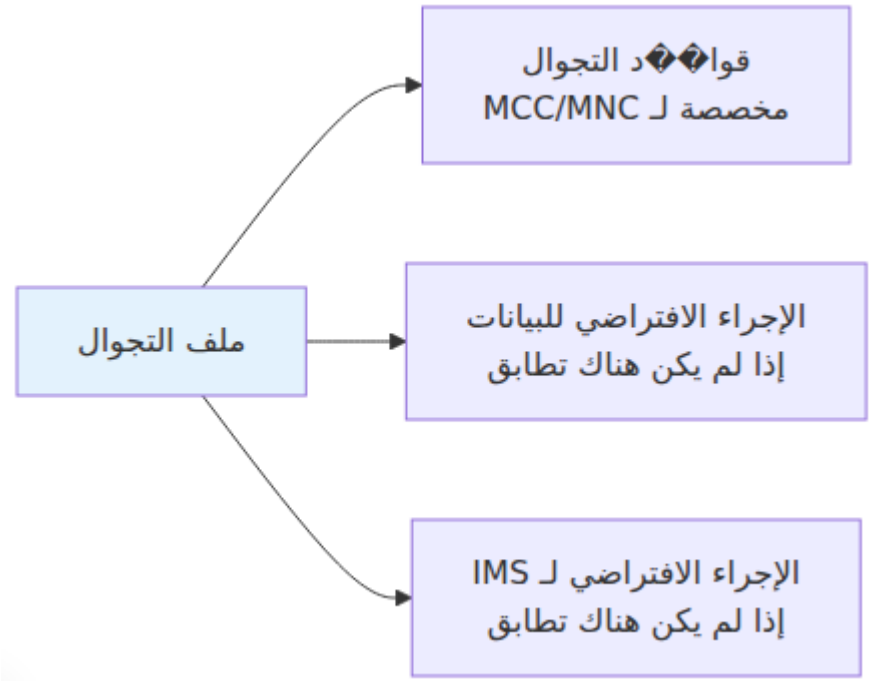
حظر شبكات محددة (القائمة السوداء)

```
# إنشاء قاعدة حظر الشبكة المكلفة
RULE=$(curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "حظر الشبكة المكلفة",
      "mcc": "206",
      "mnc": "01",
      "data_action": "رفض",
      "ims_action": "رفض"
    }
  }' | jq -r '.response.id')

# إنشاء ملف مع السماح افتراضي
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"roaming_profile\": {
      \"name\": \"حظر الشبكات المكلفة\",
      \"data_action_if_no_rules_match\": \"السماح\",
      \"ims_action_if_no_rules_match\": \"السماح\",
      \"roaming_rules\": [$RULE]
    }
  }"
```

سيناريوهات التجوال الشائعة

السيناريو 1: التجوال المحلي فقط

يمكن للمشترك التجوال داخل بلده الأم ولكن ليس دوليًا.

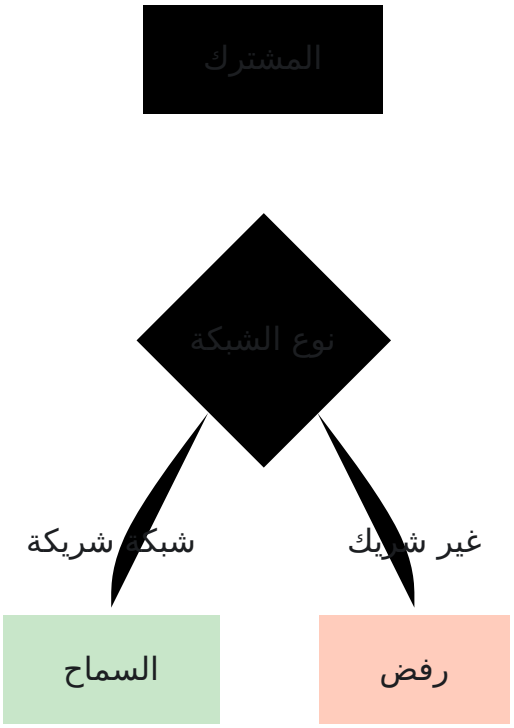


التكوين:

- الافتراضي: رفض الكل
- القواعد: السماح لجميع رموز MCC، 315، 314، 313، 312، 311، 310) الأمريكية (316)

السيناريو 2: فقط شركاء التجوال

يمكن للمشترك التجوال فقط على الشبكات التي لديها اتفاقيات تجارية.

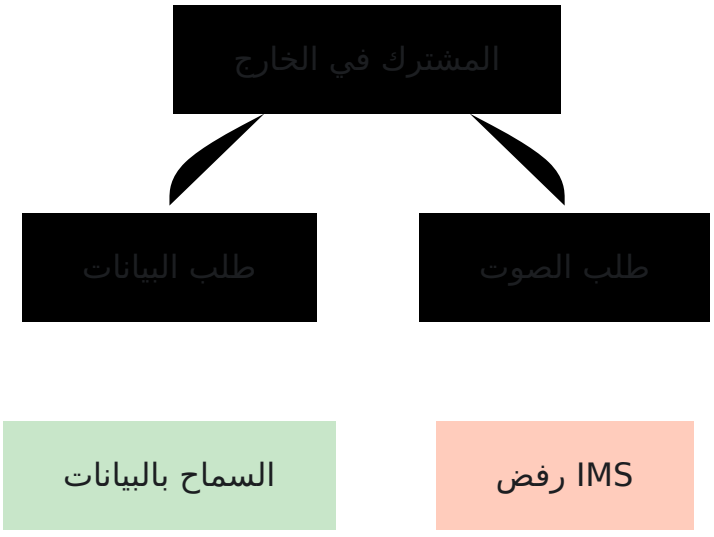


التكوين:

- الافتراضي: رفض الكل
- القواعد: السماح لكل شبكة شريكة بشكل صريح (حسب MCC/MNC)

السيناريو 3: التجوال للبيانات، بدون تجوال صوتي

يمكن للمشترك استخدام البيانات في الخارج ولكن يجب استخدام WiFi للمكالمات الصوتية.



التكوين:

- القواعد: `data_action: "السماح"`, `ims_action: "رفض"`

السيناريو 4: الوصول إلى خدمات الطوارئ

السماح دائمًا لخدمات الطوارئ، حتى إذا تم حظر التجوال.

ملاحظة: يتم التعامل مع خدمات الطوارئ عادةً على مستوى MME/التجوال قواعد تنطبق. الشبكة على الخدمات العادية OmniHSS لـ.

مرجع MCC/MNC

رموز الدول الشائعة (MCC)

MCC	الدولة	الشبكات
310-316	الولايات المتحدة	AT&T، Verizon، T-Mobile، إلخ.
302	كندا	Rogers، Bell، Telus
234-235	المملكة المتحدة	Vodafone، O2، EE
262	ألمانيا	Deutsche Telekom، Vodafone
208	فرنسا	Orange، SFR، Bouygues
222	إيطاليا	TIM، Vodafone، Wind
214	إسبانيا	Movistar، Vodafone

شركات الاتصالات الأمريكية الشائعة (MCC 310-316)

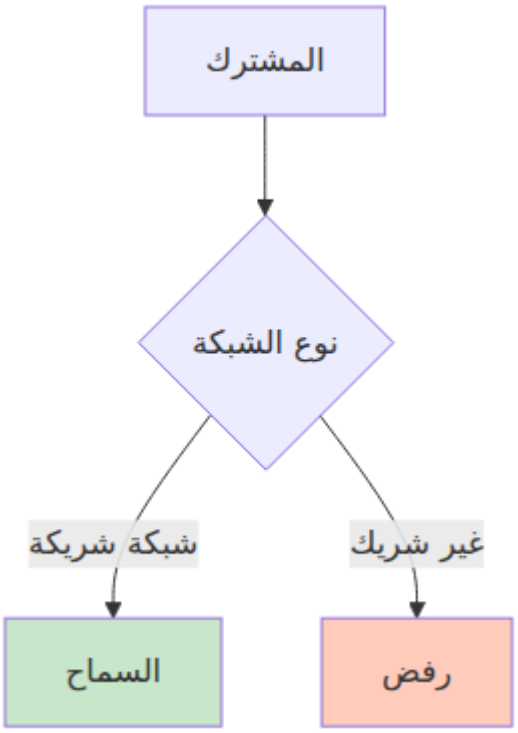
MCC	MNC	شركة الاتصالات
310	410	AT&T
311	480	Verizon
310	260	T-Mobile
310	120	Sprint
313	380	(شبكة اختبار مثال)

القوائم الكاملة: انظر ITU-T E.212 قوا��د بيانات أو MCC/MNC

نقاط تنفيذ التجوال

واجهة S6a (البيانات)

عند اتصال المشترك بالشبكة الزائرة:



واجهة Cx (IMS)

في الشبكة الزائرة IMS عند تسجيل المشترك في:



استكشاف مشاكل التجوال

المشترك لا يمكنه الاتصال في الشبكة الزائرة

تحقق من تعيين ملف التجوال:

- استعلام عن قاعدة البيانات لعرض ملف التجوال المعين للمشترك
- تحقق من اسم الملف وإعدادات الإجراء الافتراضي

تحقق مما إذا كانت القاعدة موجودة للشبكة الزائرة:

- استعلام عن قاعدة البيانات لقواعد التجوال المطابقة لـ MCC/MNC الشبكة الزائرة
- تحقق مما إذا كانت هناك قاعدة موجودة لملف التجوال الخاص بالمشترك
- تحقق من قيمة `data_action` لتلك الشبكة المحددة

المشترك يمكنه الاتصال ولكن لا يمكنه تسجيل IMS

تحقق من إجراء IMS بشكل منفصل:

- استعلام عن قواعد التجوال للشبكة ��لزائرة
- تحقق من قيم `ims_action` و `data_action`
- ابحث عن الحالات التي يتم فيها السماح بالبيانات ولكن يتم رفض IMS

سلوك التجوال غير المتوقع

راجع السجلات للتحقق من التجوال:

```
[info] تحقق من التجوال: IMSI 001001123456789، PLMN 410-310 الزائر
[info] القاعدة التجوال المطابقة: "السماح بـ AT&T"
[info] إجراء البيانات: السماح، إجراء IMS: السماح
```

أفضل الممارسات

تصميم الملف

1. **ابدأ بشكل تقييدي** - افتراضيًا رفض، السماح بشكل صريح للشركاء
2. **اختبر بشكل شامل** - تحقق من القواعد في المختبر قبل الإنتاج
3. **وثق القواعد** - احتفظ بقائمة بالشبكات المسموح بها ولماذا
4. **راجع بانتظام** - تحديث عند تغيير اتفاقيات التجوال

إدارة القواعد

1. السماح" - **استخدم أسماء وصفية**-ATT-1قاعدة" وليس "بيانات-فقط"
2. تحقق من الرموز مقابل قواعد البيانات الرسمية - **تحقق من MCC/MNC**
3. بشكل منفصل IMS - فكر في البيانات و **اعتبر كلا الخدمتين**
4. تتبع الشبكات التي يزورها المشتركون فعليًا - **راقب الاستخدام**

إجراءات التشغيل

1. وجود إجراء لتمكين/تعطيل التجوال بسرعة - **تغييرات الطوارئ**
2. خطط لتحديث ملفات التجوال لعدة مشتركين - **تحديثات جماعية**
3. تتبع استخدام التجوال ومحاولات الرفض - **التقارير**
4. إخطار العملاء بتغييرات سياسة التجوال - **التواصل مع العملاء**

← التالي: تدفقات البروتوكول | العودة إلى دليل العمليات →

بيانات Sh (بيانات مستودع شفافة)

يعمل OmniHSS كمستودع (AS) ضد **شفاف** لبيانات الخدمة التي تخزنها خوادم التطبيقات (الخدمات التكميلية / تحويل **MMTEL**) المشترك عبر واجهة Sh. **خدمات** تُكتب مستندات مثل (الحظر المحدد من **IMS-ODB** و **معلومات** (الحظر، OIP/OIR، المكالمات، انتظار المكالمات وتُقرأ عند الطلب، وتحتفظ بها HSS، بواسطة AS (قبل المشغل.

هذه البيانات **بشكل نحوي ولكن** تفهم HSS: 3GPP TS 29.328 لـ "شفاف" معنى دقيق في 3. يخزن OmniHSS ويعيد تحميل `ServiceData` غير شفافة مملوكة لـ AS. XML **ليس دلاليًا**. إنها بتحديده أو AS **بايتًا بايتًا**. لا يعيد تحليل أو إعادة تسلسل الحمولة أبدًا. يتم إرجاع مستند يقوم تمامًا كما كُتب (على سبيل المثال XCAP/MMTel) التحقق من صحته.

يمكن أيضًا إدارة نفس المستندات خارج النطاق بواسطة أنظمة التزويد / CRM من خلال REST Provisioning API.

جدول المحتويات

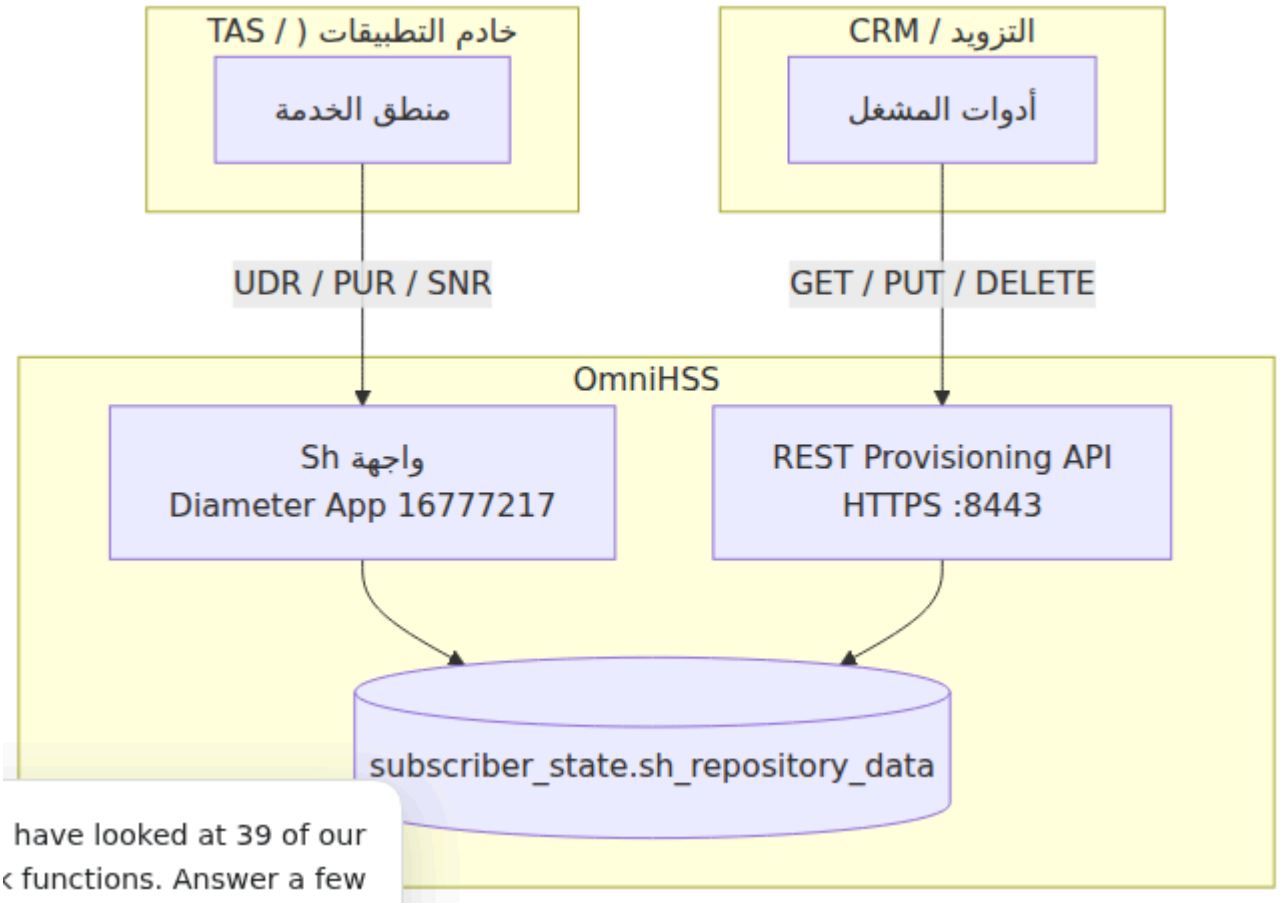
- المفاهيم
- نموذج البيانات
- تدفقات رسائل Sh
- SequenceNumber والتزامن
- REST Provisioning API
- الجداول المرجعية
- استكشاف الأخطاء وإصلاحها

المفاهيم

يمكن أن يحتفظ المشترك بعدد غير محدود من **المستندات الشفافة** المستقلة، كل منها مُعرف بواسطة **Service-Indication** (اسم الملف). يتكون المستند من ثلاثة أجزاء:

العنصر	المالك	المعنى
Service-Indication	مُدار بواسطة HSS	يُسمى المستند (مثل `MMTEL-Services`، `IMS-ODB-Information`).
SequenceNumber	مُدار بواسطة HSS	عداد النسخة المستخدم للتزامن المتفائ��. انظر SequenceNumber والتزامن.
ServiceData	مملوك لـ AS (غير شفاف)	الحمولة XML مخزنة ومُعادة كما هي نفسها.

تقوم HSS بتفسير Service-Indication وSequenceNumber فقط. يتم التعامل مع جسم `ServiceData` كبايتات غير شفافة.



have looked at 39 of our
‹ functions. Answer a few

نموذج البيانات

تُحتفظ جميع المستندات الشفافة للمشترك في حقل واحد، `subscriber_state.sh_repository_data`، ككائن JSON مُفاتيح بواسطة Service-Indication. يخزن كل إدخال النسخة والحمولة كما هي:

```
{
  "MMTEL-Services":      { "sequence_number": "0", "service_data":
"<MMTelServices …>…</MMTelServices>" },
  "IMS-ODB-Information": { "sequence_number": "1", "service_data":
"<OdbForImsOrientedServices xmlns=\"odb.mmtel.omnitou.ch\"/>" }
}
```

الحقل	الوصف
`sequence_number`	النسخة الحالية من هذا المستند، كما تم قبولها آخر مرة بواسطة HSS. يتم إرجاعها في كل `UDA` وتستخدم للتحقق من صحة التحديثات.
`service_data`	جسم XML غير الشفاف، مخزنة تمامًا كما أرسلها AS (بدون مساحة بيانات). يتم حذف حقل `ServiceData` المستند الذي لا يحتوي على عنصر (اسم، ترتيب سمات أو تطبيع المسافات البيضاء المستودع الفارغة وفقًا للمواصفات).

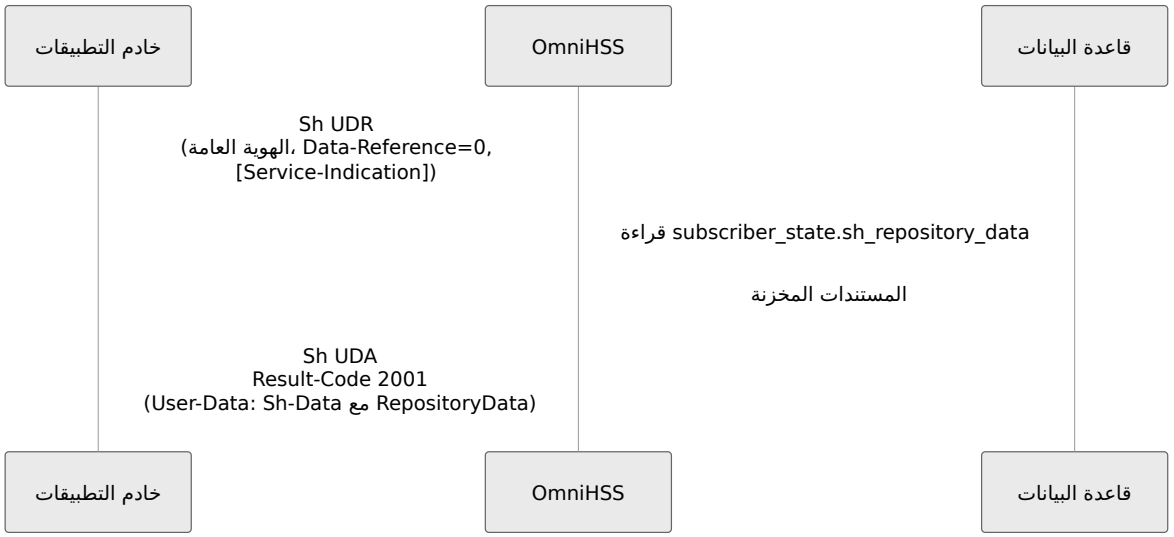
يعني هذا النموذج أن مشتركًا واحدًا يمكن أن يحتفظ بالعديد من المستندات المتميزة، كل منها مُرقم بشكل مستقل، دون فرض مخطط ثابت من قبل HSS.

تدفقات رسائل Sh

تُحمل RepositoryData في AVP `User-Data` كمستند XML `Sh-Data`. يتم اختيار RepositoryData باستخدام **قيمة Data-Reference 0**. AVP **Service-Indication** الاختياري يضيق الطلب إلى مستند واحد.

طلب بيانات المستخدم (UDR/UDA): قراءة

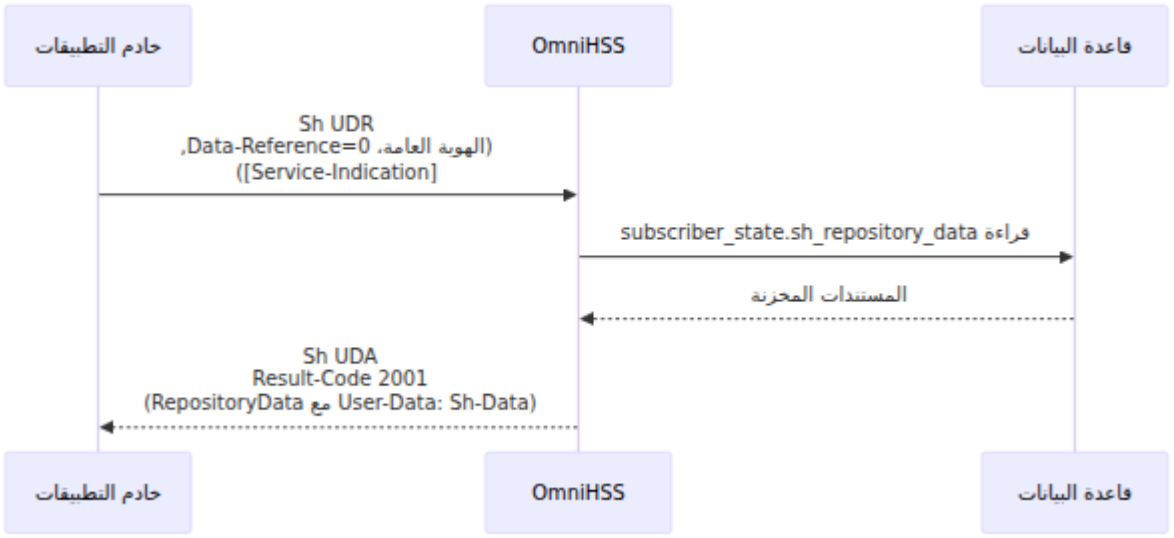
يتم إرجاع Service-Indication، مستندًا واحدًا أو جميع المستندات الشفافة. مع وجود AS يقرأ المستند المطابق فقط؛ بدونها، يتم إرجاع كل مستند مخزن، كل منها كعنصر `<RepositoryData>` خاص به.



يتم الرد على مشترك غير معروف أو غير مُفعل بـ IMS **Experimental-Result 5001 (DIAMETER_ERROR_USER_UNKNOWN)**.

طلب تحديث الملف الشخصي (PUR/PUA): كتابة

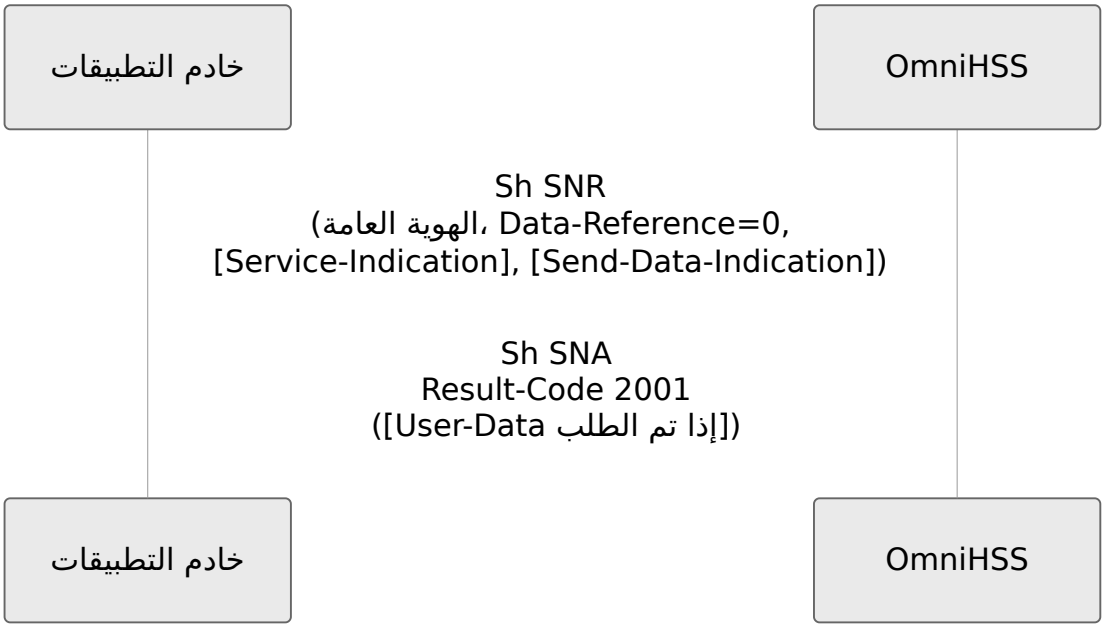
ينشئ AS أو يحدث مستندًا واحدًا. يتم تخزين الحمولة `ServiceData` كما هي. يتم قبول التحديث صالحة (انظر أدناه) SequenceNumber فقط إذا كانت.



عندما يتم حل PUR إلى عدة مشتركين (هوية عامة مُعطاة بشكل عشوائي)، يتم تطبيق التحديث بشكل ذري: إذا كان أي مستند خارج التزامن، فلن يتم حفظ أي منها.

الاشتراك: طلب إشعارات الاشتراك (SNR/SNA)

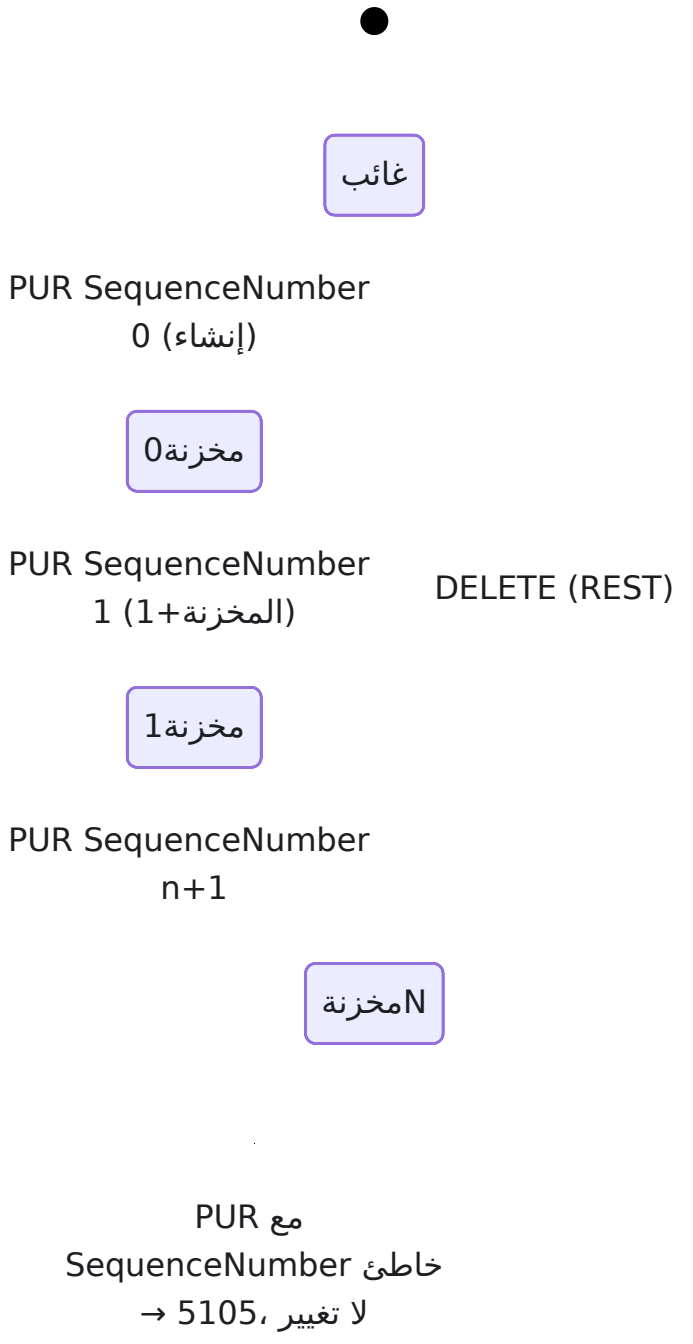
يشترك AS في بيانات المشترك وقد يطلب إرجاع القيمة الحالية على الفور (`Send-Data-Indication`). يجيب OmniHSS على SNR، يتضمن، وعند الطلب، RepositoryData الحالي.



SequenceNumber والتزامن

يوفر SequenceNumber تحكمًا في التزامن المتفائل بحيث لا يمكن لخادمي تطبيقات الكتابة فوق بعضهما البعض بصمت، وفقًا لـ 3GPP TS 29.328.

- **إنشاء SequenceNumber 0** (القيمة `0` محجوزة حصريًا للبيانات المضافة حديثًا).
- **تحديث** SequenceNumber لـ **الخلف المباشر** مستند موجود يجب أن يحمل (المخزنة + 1) المخزنة.
- العداد **يلف من 65535 إلى 1** (ليس 0، لأن 0 محجوز).
- يتم رفض تحديث لا يكون SequenceNumber الخاص به هو الخلف المتوقع مع **Experimental-Result 5105 (DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC)** ويترك المستند المخزن دون تغيير.



مثال: يتم تخزين مستند عند SequenceNumber `0`. يتم رفض PUR الذي يحمل SequenceNumber `5105` ولا يتغير شيء. يتم قبول PUR الذي يحمل SequenceNumber `1` `1` ويتقدم المستند إلى النسخة.

REST Provisioning API

يتم توجيه المشترك. يمكن قراءة وكتابة نفس المستندات مباشرة بواسطة أنظمة التزويد / CRM بواسطة IMSI في المسار؛ يتم تعريف المستند بواسطة `service_indication` في جسم

غير `service_data` يتم إعادة .(الطلب للتحديثات، أو سلسلة الاستعلام للقراءات / الحذف الشفاف بايتًا بايتًا، تمامًا كما هو الحال عبر Sh.

تستخدم جميع الاستجابات غلاف API القياسي:

```
{ "status": "success", "response": { } }
```

على عكس مسار Sh، فإن REST API تحقق **يطبق** ولا هو وصول موثوق للتزويد خارج التزامن. يقوم الكتابة بتعيين المستند مباشرة SequenceNumber.

قائمة جميع المستندات

ترجع كل مستند مخزن للمشترك.

نقطة النهاية: `GET /api/subscriber/repository_data/:imsi`

```
curl -k
https://hss.example.com:8443/api/subscriber/repository_data/001001123
```

```
{
  "status": "success",
  "response": {
    "MMTEL-Services":      { "sequence_number": "0",
"service_data": "<MMTelServices …/>" },
    "IMS-ODB-Information": { "sequence_number": "1",
"service_data": "<OdbForImsOrientedServices
xmlns=\"odb.mmtel.omnitou.ch\"/>" }
  }
}
```

الحصول على مستند واحد

ترجع مستندًا واحدًا بواسطة Service-Indication.

نقطة النهاية: `GET /api/subscriber/repository_data/:imsi?service_indication=:service_indication`

```
curl -k
"https://hss.example.com:8443/api/subscriber/repository_data/00100112
service_indication=MMTEL-Services"
```

```
{
  "status": "success",
  "response": { "sequence_number": "0", "service_data": "
<MMTelServices …/>" }
}
```

إنشاء أو تحديث مستند

ينشئ المستند إذا كان غائبًا، أو يستبدله.

نقطة النهاية: `PUT /api/subscriber/repository_data/:imsi`

```
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/repository_data/001001123
\
  -H "Content-Type: application/json" \
  -d '{
        "service_indication": "MMTEL-Services",
        "service_data": "<MMTelServices version=\"1\"/>",
        "sequence_number": "0"
      }'
```

الحقل	النوع	مطلوب	الافتراضي	الوصف
`service_indication`	سلسلة	نعم	-	اسم المستند الذي سيتم إنشاؤه / تحديثه (مثل `MMTEL-Services`).
`service_data`	سلسلة	لا	-	حمولة XML غير الشفافة، المخزنة كما هي. احذف لتخزين مستند فارغ (Service-Indication وSequenceNumber فقط).
`sequence_number`	سلسلة	لا	`0`	النسخة التي سيتم تسجيلها للمستند.

تكرر الاستجابة المستند المخزن:

```
{
  "status": "success",
  "response": { "sequence_number": "0", "service_data": "
<MMTelServices version=\"1\"/>" }
}
```

حذف مستند

يُزيل مستندًا واحدًا بواسطة Service-Indication.

نقطة النهاية: `DELETE /api/subscriber/repository_data/:imsi`

```
curl -k -X DELETE
https://hss.example.com:8443/api/subscriber/repository_data/001001123
\
  -H "Content-Type: application/json" \
  -d '{ "service_indication": "MMTEL-Services" }'
```

الحقل	الن��ع	مطلوب	الافتراضي	الوصف
`service_indication`	سلسلة	نعم	-	المستند الذي سيتم إزالته.

ترجع الاستجابة المستندات المتبقية للمشترك.

الجداول المرجعية

قيم Data-Reference (RepositoryData)

القيمة	الاسم	الوصف	المرجع
0	RepositoryData	بيانات الخدمة الشفافة المحددة بواسطة Service-Indication	3GPP TS 29.328 §7.6

رموز النتيجة وExperimental-Result

الرمز	الاسم	المعنى
2001	DIAMETER_SUCCESS	تم معالجة UDR/PUR/SN بنجاح
5001	DIAMETER_ERROR_USER_UNKNOWN	يتم العثور على مشترك أو غير مُفعل IMS
5105	DIAMETER_ERROR_TRANSPARENT_DATA_OUT_OF_SYNC	SequenceNu ث ليس الخلف للقيمة المخزنة

معرف التطب��ق

المعرف	الواجهة	الوصف	المرجع
16777217	Sh	بيانات المستخدم AS ↔ HSS	3GPP TS 29.329

Service-Indications الشائعة

Service-Indication	المحتوى النموذجي
`MMTEL-Services`	خدمات MMTel التكميلية (تحويل المكالمات، انتظار/حجز/حظر، مؤتمرات، OIP/OIR، الاتصالات): XML simservs
`IMS-ODB-Information`	معلومات الحظر المحددة من قبل المشغل لخدمات IMS-oriented

> يتم تعريف قيم Service-Indication بواسطة خادم التطبيقات ومخططه XML؛ لا المقابل. تفرض HSS قائمة ثابتة.

استكشاف الأخطاء وإصلاحها

يتلقى خادم التطبيقات 5105 عند التحديث

الأعراض: يتم الرد على PUR مع Experimental-Result `5105` ولا يتغير المستند.

الأسباب المحتملة:

- HSS (نسخته المخزنة قديمة) أرسل AS SequenceNumber ليس الخلف المباشر للقيمة المخزنة في.
- AS آخر تقدم تحديث متزامن من SequenceNumber.

الحل:

1. اقرأ المستند الحالي باستخدام UDR للحصول على SequenceNumber المحدث.

2. أعد إصدار PUR مع SequenceNumber = 1 + المخزنة.
3. لفرض قيمة إداريًا، قم بتعيينها عبر REST API، التي لا تطبق تحقق التزامن.

المعادة عن ما تم كتابته ServiceData تختلف

الأعراض: يعتقد AS أن الحمولة تم تعديلها بواسطة HSS.

الأسباب المحتملة:

- `ServiceData` بايتًا بايتًا. عادةً ما تأتي OmniHSS ويعيد يجب ألا يحدث هذا. يخزن التي تعيد تسلسل المستند (تغيير AS الخاصة بـ XML الاختلافات الظاهرة من مكتبة بادئات المساحة، ترتيب السمات أو المسافات البيضاء) قبل المقارنة.

الحل:

1. `UDA` / REST، مع البايتات الخام المرسلة قارن البايتات الخام المعادة في استجابة وليس تمثيلًا معاد تحليله.
2. تأكد من أن AS لا يقوم بتطبيع XML على جانبه قبل المقارنة.

REST لم يتم العثور على المستند عبر

الأعراض: `GET …/repository_data/:imsi?service_indication=…` يعيد خطأ.

الأسباب المحتملة:

- لا يوجد مستند مع تلك Service-Indication مخزنة للمشترك.
- IMSI لا يتوافق مع مشترك موجود.

الحل:

1. `GET /api/subscriber/repository_data/:imsi` قائمة بجميع المستندات باستخدام لرؤية ما هو مخزن.
2. تحقق من IMSI الحصول على المشترك بواسطة باستخدام IMSI.

SRVCC - استمرارية مكالمة الصوت عبر راديو واحد

← العودة إلى دليل العمليات

نظرة عامة

SRVCC (استمرارية مكالمة الصوت عبر راديو واحد) يسمح لجهاز المستخدم (UE) بنقل مكالمة VoLTE نشطة إلى حامل CS (الدائرة المبدلة) 2G/3G عندما تفشل تغطية LTE. يقوم MME بتنظيم النقل عبر **واجهة Sv** (TS 29.280). لبناء طلب Sv PS-to-CS، يحتاج MME إلى قيمتين مأخوذتين من HSS:

AVP	الرمز	الغرض
`STN-SR`	1433	رقم نقل الجلسة لـ SRVCC. يقوم خادم MSC بالاتصال بهذا الرقم لنقل SIP REFER الذي ينفذ TAS/S-CSCF، للوصول إلى E.164 جلسة VoLTE النشطة إلى حامل CS.
`C-MSISDN`	1452	رقم MSISDN المرتبط. يستخدم TAS هذا لمطابقة مكالمة STN-SR الواردة مع الجلسة النشطة الصحيحة عندما يكون لدى المشترك عدة مكالمات قيد التشغيل.

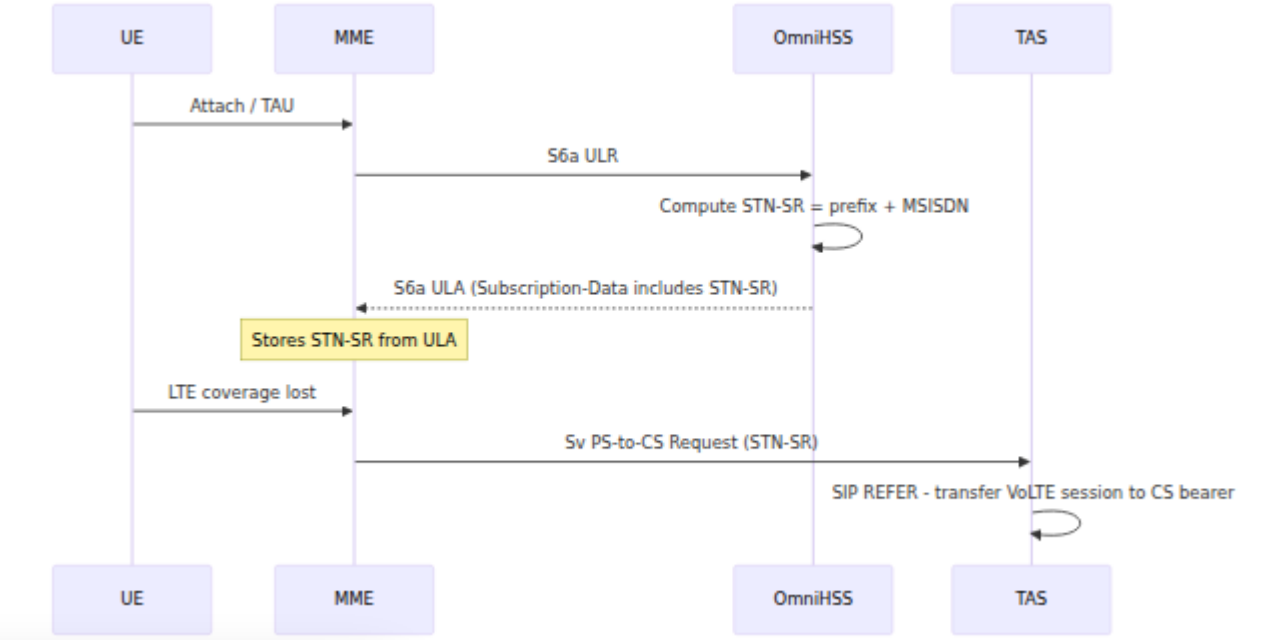
يوفر OmniHSS `STN-SR` في **إجابة تحديث الموقع** (ULA) `Subscription-Data` AVP. يقوم MME بقراءته من ULA وإعادة توجيهه في طلب Sv PS-to-CS.

المواصفات المرجعية:

العنوان	المواصفة
إجراء SRVCC PS-to-CS	TS 23.216
واجهة S6a (STN-SR §7.3.89، Subscription-Data §7.3.2)	TS 29.272
تنسيق رقم STN-SR (§13.4)	TS 23.003

كيفية العمل

يستخدم OmniHSS واحدة على مستوى STN-SR نهجًا قائمًا على البادئات. تقوم بتكوين بادئة STN-SR بحساب الرقم الكامل لـ HSS المشغل. يقوم عن طريق دمج البادئة مع ULA في وقت داخل AVP `STN-SR` وتوضع في TBCD للمشترك. يتم ترميز النتيجة بتنسيق MSISDN `Subscription-Data`.



يتلقون نفس البادئة، HSS يتطلب هذا النهج عدم وجود إعدادات لكل مشترك. جميع المشتركين في لقاعدة المشتركين بالكامل SRVCC لذا فإن تغيير تكوين واحد يمكّن.

غير متأثرة. لا ULA تمامًا. تظل `STN-SR` AVP بإغفال OmniHSS إذا لم يتم تكوين البادئة، يقوم أي تغيير في السلوك SRVCC ترى عمليات النشر غير.

التكوين

أضف المفتاح `srvcc` إلى تكوين تطبيق `:hss` في `config/runtime.exs`.

```
config :hss, :srvcc,
  stn_sr_prefix: "9"
```

المعلمات

المعلمة	النوع	مطلوب	الافتراضي	الوصف
`stn_sr_prefix`	سلسلة	لا	(لا شيء)	بادئة STN-SR المعينة من قبل المشغل والتي تضاف إلى MSISDN لكل مشترك لتشكيل الرقم الكامل E.164 لـ STN-SR. عند عدم تعيينها، يقوم OmniHSS بإغفال AVP `STN-SR` من جميع استجابات ULA.

تنسيق رقم STN-SR

الرقم الكامل لـ STN-SR هو:

```
STN-SR = stn_sr_prefix + subscriber MSISDN
```

يتم ترميز الرقم بتنسيق **TBCD** (الرقم الثنائي المشفر هاتفيًا، وفقًا لـ TS 24.008 §10.5.4.7) ويتم وضعه في AVP `STN-SR` (الرمز 1433، البائع 10415).

مثال:

المدخلات	القيمة
البادئة المكونة	`9`
MSISDN المشترك	`61412345678`
STN-SR المحسوب	`961412345678`

يقوم خادم MSC إلى `961412345678` بالاتصال بـ TAS، جزء الذي يستخدم تصل المكالمة. CS لنقلها إلى حامل SIP REFER النشطة ويصدر IMS لتحديد جلسة MSISDN

مثال على التكوين

مفعل SRVCC

```
# config/runtime.exs

config :hss, :srvcc,
  # البادئة التي يتصل بها خادم MSC للوصول إلى TAS عبر PSTN/CS.
  # STN-SR = stn_sr_prefix + subscriber MSISDN.
  stn_sr_prefix: "9"
```

كيف يعمل: تتضمن كل استجابة ULA `STN-SR` في `Subscription-Data`. القيمة هي ترميز بتخزين القيمة وإعادة توجيهها في MME للمشترك. يقوم MSISDN للبادة المدمجة مع TBCD طلبات Sv PS-to-CS عند تفعيل SRVCC.

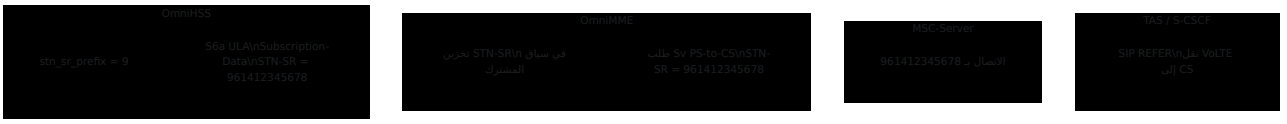
معطل SRVCC (افتراضي)

عندما يكون المفتاح `srvcc` غائبًا أو لم يتم تعيين `stn_sr_prefix`، يقوم OmniHSS بإغفال AVP `STN-SR`. تظل ULA متطابقة. استخدم هذا للعمليات التي لا تتطلب SRVCC.

التفاعل مع MME

يقوم MME (OmniMME) بقراءة `STN-SR` من ULA `Subscription-Data` ويخزنها في سياق المشترك. عندما يتم تفعيل SRVCC، يتضمن `STN-SR` في **طلب Sv PS-to-CS** المرسل إلى

خادم MSC. انظر Omnitouch/omnimme#426 لتنفيذ MME.



استكشاف الأخطاء وإصلاحها

STN-SR غير موجود في ULA

الأعراض: لا يمكن لـ MME ملء طلب Sv PS-to-CS. تفشل عمليات نقل SRVCC.

الأسباب المحتملة:

- لم يتم تعيين `stn_sr_prefix` في `config/runtime.exs`.
- بدأت خدمة HSS قبل أن يدخل تغيير التكوين حيز التنفيذ.

الحل:

1. تحقق من وجود كتلة `srvcc` في `config/runtime.exs` مع `stn_sr_prefix` غير فارغ.
2. أعد تشغيل خدمة OmniHSS لتطبيق تغيير التكوين.
3. قم بتحفيز ULR جديدة من MME (على سبيل المثال عن طريق إجبار TAU). تأكد من أن ULA `Subscription-Data` تحتوي الآن على `STN-SR`.

قيمة STN-SR غير صحيحة

الأعراض: يتلقى خادم MSC رقمًا مشوهًا أو غير قابل للتوجيه.

الأسباب المحتملة:

- البادئة غير صحيحة أو تفتقر إلى الأرقام الرائدة.
- MSISDN المخزنة في HSS للمشترك ليست بتنسيق E.164 (أرقام فقط، لا الدولي `+`).

الحل:

1. تحقق من MSISDN للمشترك عبر API (`GET /api/subscriber/imsi/:imsi`).
2. تحقق من STN-SR المتوقع: دمج `stn_sr_prefix` مع MSISDN المخزنة.
3. تأكد من أن جدول توجيه خادم MSC يتعامل مع تلك النطاقات من الأرقام.

← العودة إلى دليل العمليات

واجهة Sy (تحكم حد الإنفاق)

نظرة عامة

تربط واجهة Sy نظام HSS (الذي يعمل كـ **PCRF**، وظيفة قواعد السياسة والفوترة) بنظام **OCS** (نظام الفوترة عبر الإنترنت). تتيح لـ PCRF للتحكم في **حد الإنفاق للمشتركين** اتخاذ قرارات السياسة الخاصة بها - على سبيل المثال، أي قاعدة فوترة يجب تطبيقها، أو ما إذا كان يجب تقليل سرعة المشترك - بناءً على حالة **عدادات السياسة** التي يحتفظ بها OCS لكل مشترك (حصة البيانات المستهلكة، الإنفاق مقابل حد شهري، وما إلى ذلك).

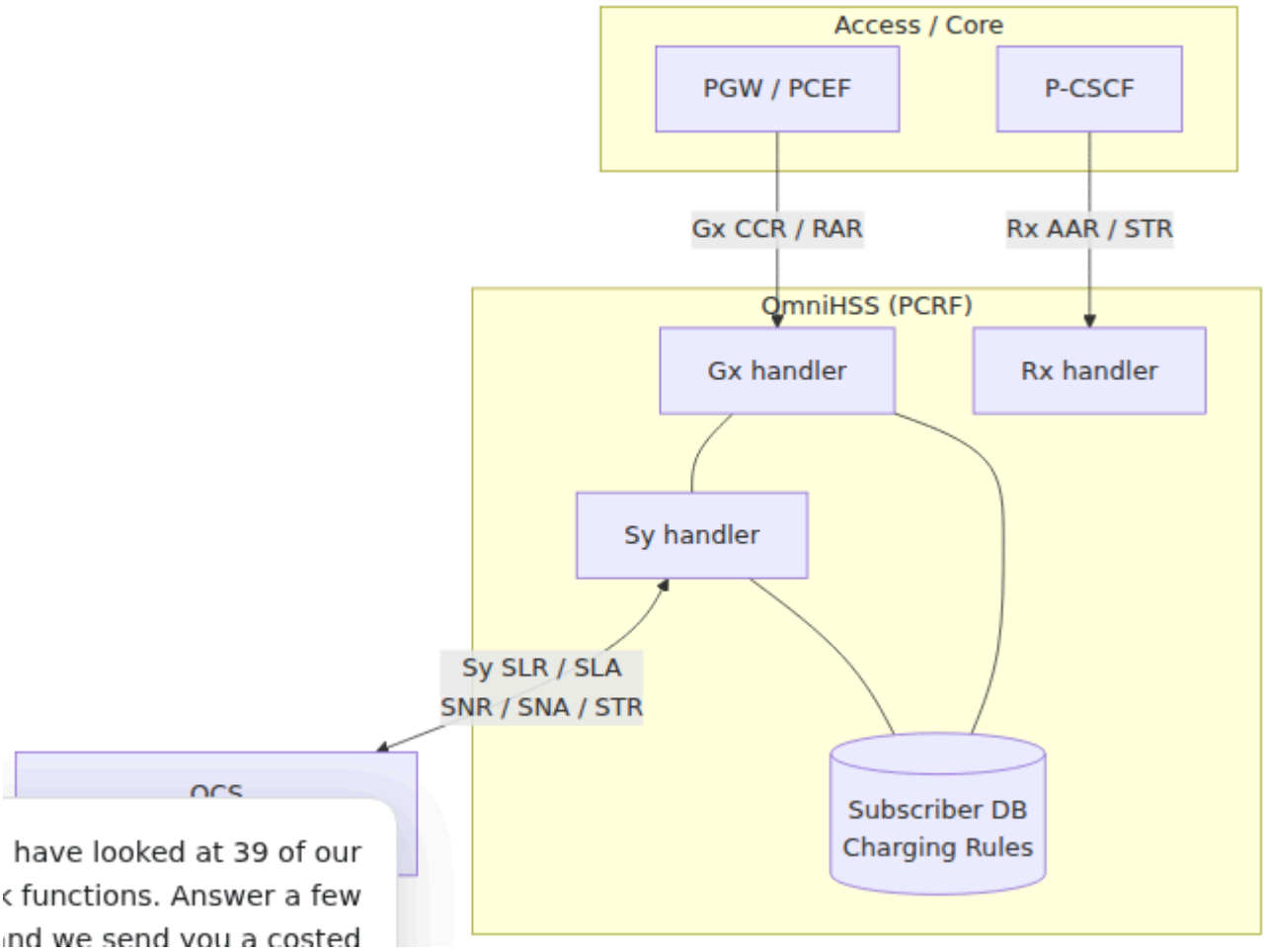
يقوم PCRF في OmniHSS بتثبيت قواعد الفوترة وجودة الخدمة عبر Gx ويصرح بوسائط IMS عبر Sy، ويتم إخطاره عند OCS يشترك في حالة عدادات السياسة الخاصة بالمشترك في Rx. في الاعتبار الإنفاق الحالي والمخصص للمشترك Gx تغييرها، بحيث يمكن أن تأخذ قرارات.

تم تعريف Sy 3 بواسطةGPP TS 29.219 ويستخدم معرف تطبيق Diameter **16777302**.

الخاصية	القيمة
معرف التطبيق	16777302
المواصفة	3GPP TS 29.219
دور HSS	PCRF (عميل Diameter لـ SLR/STR، خادم لـ SNR)
النظير	OCS (نظام الفوترة عبر الإنترنت)
النقل	TCP أو SCTP، المنفذ 3868

> **Sy مقابل Gy.** Sy ليست فوترة عبر الإنترنت. Gy (TS 32.299) هو المكان الذي يطلب فيه PGW من OCS منح الائتمان لحركة المرور الحية. Sy هي واجهة منفصلة وخفيفة حيث يشترك **PCRF** في **الحالة** لعدادات السياسة الخاصة بـ OCS ويتم إخطاره عند تغييرها، بحيث يمكنه تعديل السياسة. OCS هو الخادم في كلا الحالتين.

الهيكلية



عندما يحتاج أولاً إلى حالة الإنفاق لمشترك، OCS مع Sy يفتح جلسة: **Sy** هو **عميل** HSS يعد يجيب على طلبات الحالة، : **Sy** هو **خادم** OCS. ويغلقها عندما تنتهي آخر جلسة بيانات للمشترك Gx. حتى يتمكن من إعادة تطبيق السياسة عبر PCRF وعندما تتغير حالة أي عداد، يخطر

عدادات السياسة وقواعد الفوترة

يحافظ OCS على عداد أو أكثر من **عدادات السياسة** لكل مشترك. يحتوي كل عداد على:

- **معرف عداد السياسة** (AVP 2901) - و اسم ثابت للعداد،
- **حالة عداد السياسة** (AVP 2902) - على سبيل) تسمية تصف أين يقع العداد حاليًا لم يتم تعريف مجموعة قيم الحالة). المثال `active`، `over_quota`، `throttled` ؛ OCS يتم تكوينها بشكل مشترك من قبل المشغل على كل منGPPبـ3 اسطة وPCRF (TS 29.219 §3.1).

يربط OmniHSS الموجودة بالفعل في قاعدة بياناته قواعد الفوترة بـ هذه:

Sy AVP	الطبيعة	يطابق	الدور
`Policy-Counter-Identifier` (2901)	ثابت - يسمي العداد	اسم **قاعدة فوترة** في قاعدة بيانات HSS	يحدد *أي* قاعدة فوترة يحكمها العداد
`Policy-Counter-Status` (2902)	ديناميكي - يتغير عند العتبات	إجراء **تنفيذ**	يحدد *ماذا تفعل* بهذه القاعدة الآن: تثبيت، إزالة، أو اختيار مستوى

المعرف ثابت طوال فترة حياة العداد، لذلك بمفرده لا يمكنه التعبير عن "تحت الحصة" مقابل "فوق الحصة". **الحالة** هي القيمة التي تتغير عندما يتجاوز المشترك عتبة، لذا فهي تقود الإجراء:

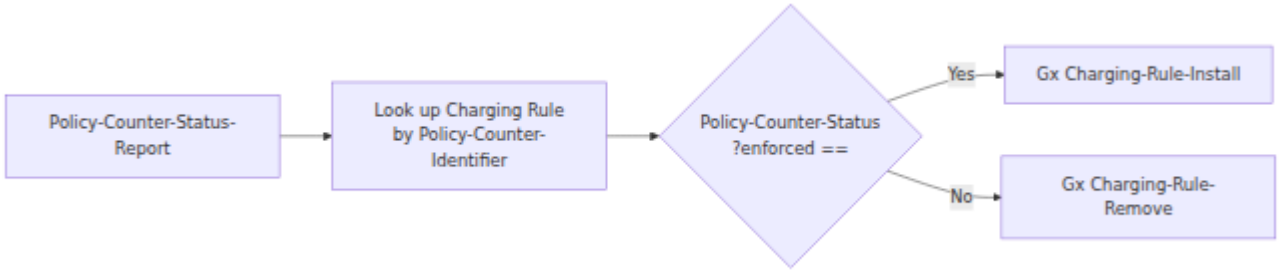
- الحالة الثابتة `enforced` تثبت قاعدة الفوترة المسماة (`Charging-Rule-Install` عبر Gx)؛
- أي حال أخرى تزيلها (`Charging-Rule-Remove`).

> **Sy** ليس لدى **لا يحمل قواعد فوترة خاصة به.** أي AVPs Sy أو QoS لقواعد الفوترة أو تسليم تعريف قاعدة إلى OCS لذلك لا يمكن لـ Gx. تلك موجودة فقط على PCRF؛ يمكنه فقط *تسمية* القاعدة (عبر معرف العداد) وإشارة متى يتم تطبيقها (عبر الحالة). يتم توفير تعريف القاعدة نفسها في HSS. هذه هي السبب في أن `Policy-Counter-Identifier` يجب أن يتطابق مع اسم قاعدة فوترة، ويجب على OCS إصدار تلك الأسماء عندما يجب تطبيق القاعدة `enforced` الدقيقة مع الحالة.



دورة حياة جلسة Sy

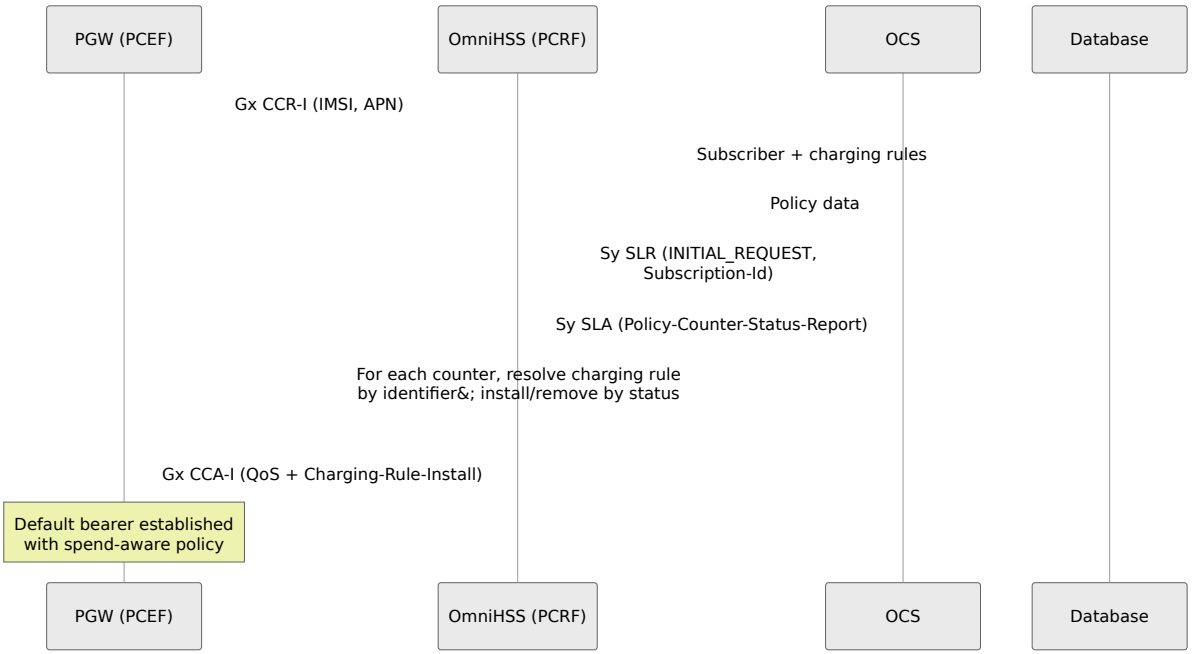
تكون جلسة Sy بجلسة Sy واحدة (معرفه بواسطة `Session-Id` واحد من Diameter) لمشترك طالما أن أي من جلسات البيانات الخاصة بذلك المشترك تعتمد على حالة الإنفاق (TS 29.219 §4.4.1). PCRF **لكل مشترك**، وليس لكل حامل بيانات. يحتفظ



- **إنشاء (SLR، INITIAL_REQUEST).** في أول Gx CCR-I حيث تعتمد سياسة ويطلب عدادات السياسة ذات Sy جلسة PCRF المشترك على حالة الإنفاق، يفتح بحالة كل منها في OCS الصلة. يجيب SLA.
- **تحديث (SLR، INTERMEDIATE_REQUEST).** إذا احتاج PCRF لاحقًا إلى مع طلب وسيط Sy عدادات إضافية، فإنه يعيد استخدام نفس جلسة.
- **إخطار (SNR / SNA).** عندما تتغير حالة عداد، يرسل OCS طلب إخطار حالة الإنفاق. ويطبق التغيير عبر SNA بذلك مع PCRF يعترف Gx.
- **إنهاء (STR / STA).** عندما تنتهي آخر جلسة بيانات للمشترك، يغلق Sy جلسة PCRF مع طلب إنهاء الجلسة.

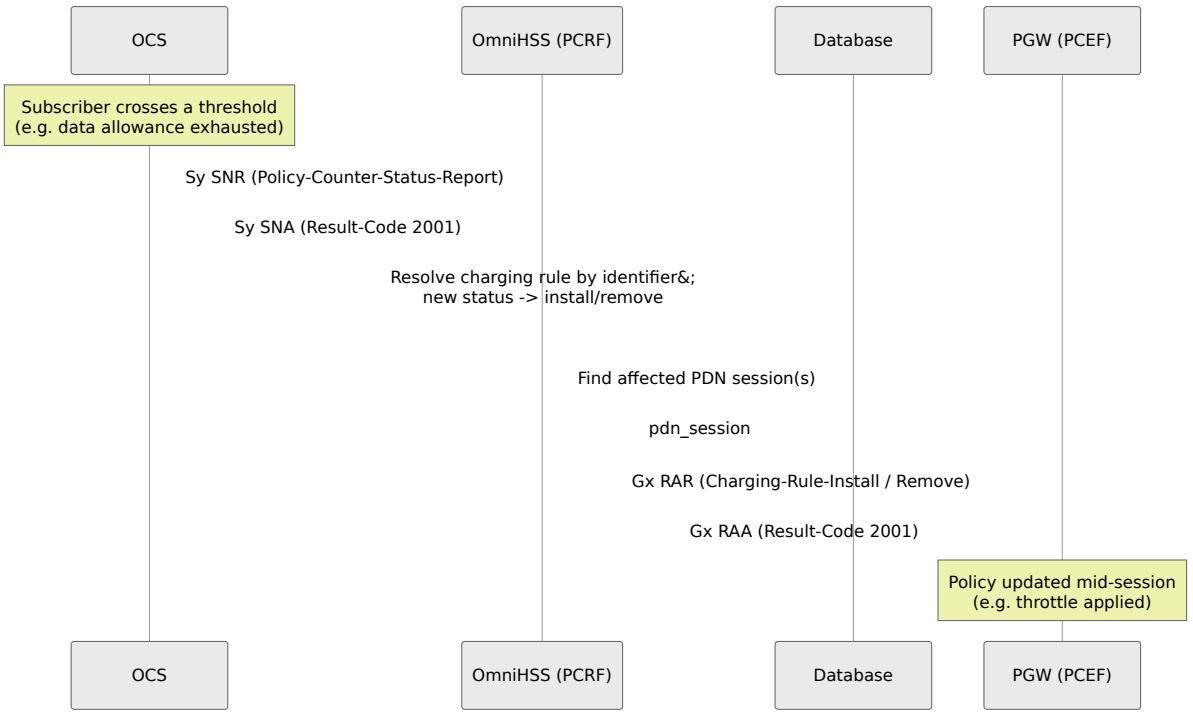
تدفقات الرسائل

التدفق 1: تقرير حد الإنفاق الأولي عند إعداد PDN



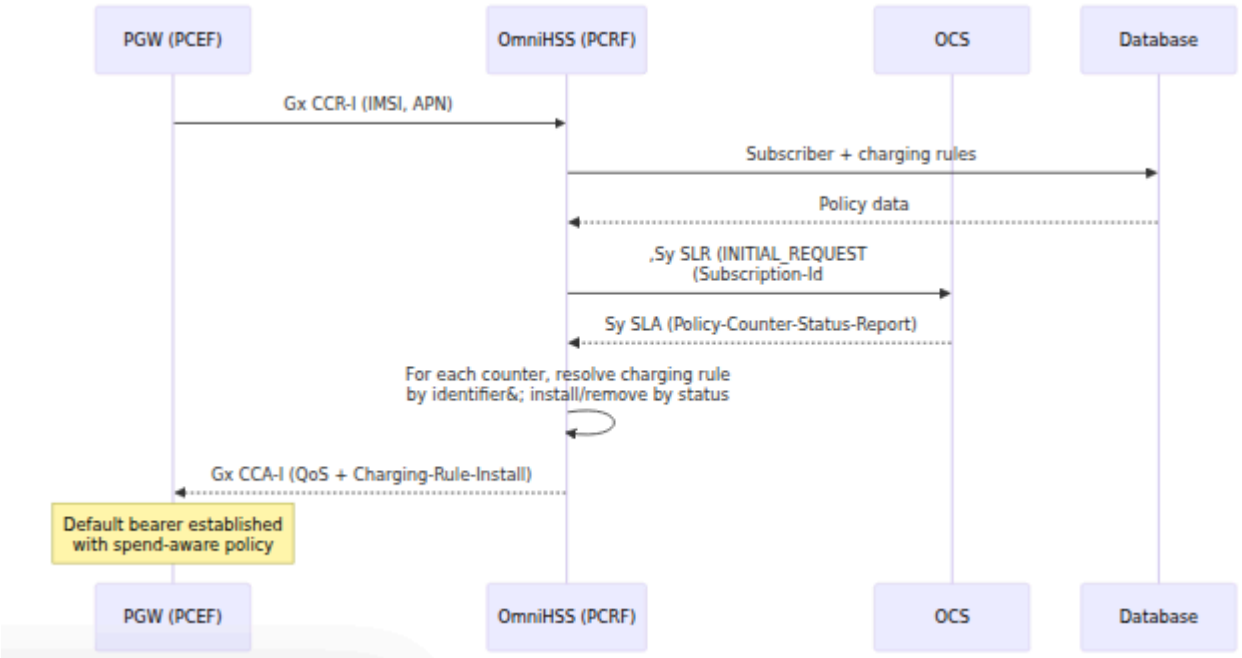
يجمع PCRF **نفس** قواعد الفوترة المستمدة من الإنفاق في **CCA-I** الذي يبنيه بالفعل لجلسة Gx. الافتراضية بحيث لا تعيق APN إلى سياسة PCRF في الوقت المناسب، يعود OCS إذا لم يرد عملية الاتصال Sy انقطاع.

التدفق 2: تغيير حالة الإنفاق (OCS -> PCRF -> Gx RAR)



نفس المسار الذي يثبت حاملات PCRF - الموجودة في Gx Re-Auth تستخدم هذه العملية آلية VoLTE التالي CCR دون انتظار PGW المخصصة - لدفع تغيير السياسة المدفوع بالإنفاق إلى.

التدفق Sy 3: إنهاء جلسة



التكوين

تطبيق Sy

يتم تسجيل تطبيق Sy على خدمة Diameter في HSS جنبًا إ��ى جنب مع Gx وRx (`config/runtime.exs`):

```
%{
  application_name: :sy,
  application_dictionary: :diameter_gen_3gpp_sy,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_302,
acct_application_id: nil}
  ]
}
```

المعامل	النوع	مطلوب	الافتراضي	
`application_name`	Atom	نعم	-	نهة. يجب أن يكون
`application_dictionary`	Atom	نعم	-	ة قاموس أن تكون `:diame` (3GPP T
`vendor_specific_application_ids`	قائمة	نعم	-	ن تطبيق نظر أدناه
`vendor_id`	عدد صحيح	نعم	-	`10415` لـ 3GPP.
`auth_application_id`	عدد صحيح	نعم	-	لمصادقة. `302_7` لـ
`acct_application_id`	عدد صحيح | nil	لا	`nil`	حاسبة. لا يستخدمه `nil`.

إعدادات Sy

يتم تكوين سلوك Sy تحت المفتاح `:hss, :sy` (`config/runtime.exs`):

```
config :hss,
  sy: %{
    enabled: false
  }
```

المعامل	النوع	مطلوب	الافتراضي	الوصف
`enabled`	Boolean	لا	`false`	المفتاح الرئيسي. عندما يكون `true`، يفتح PCRF جلسة Sy لكل مشترك عند Gx CCR-I. عندما يكون `false`، يتم تجاوز Sy تمامًا.

التي تثبت قاعدة الفوترة المسماة هي الاتفاق الثابت `Policy-Counter-Status` تكون قيمة `enforced` مع الاتفاق على ذلك. تم الاتفاق ؛ أي قيمة أخرى تزيل القاعدة. OCS وليس قابلًا للتكوين.

توجيه OCS

لا يقوم HSS بتثبيت مضيف OCS أو مجال. تحمل طلبات STR و SLR الخاصة بـ HSS ويتم توجيهها بواسطة `Destination-Host`، الخاصة بها ولا تحمل `Destination-Realm` في ذلك Sy أي نظير يعلن عن تطبيق Sy (16777302). المجال بالإضافة إلى معرف تطبيق المتاح. يعمل هذا بشكل متطابق سواء OCS الذي يوجهه إلى **DRA**، المجال يتلقى الطلب - عادةً أو تم التوصيل مباشرة، ويسمح لطبقة التوجيه بالاختيار بين DRA من خلال OCS تم الوصول إلى عدة OCSs.

يكون هذا هو نظير DRA، في المجال. في نشر Sy المتطلب الوحيد هو وجود نظير يعلن عن تطبيق Sy. ؛ لا حاجة لإدخال نظير محدد لـHSS الذي تم تكوينه بالفعل لـ DRA

ربط عدادات السياسة

لكي يعمل ربط المعرف إلى القاعدة، يقوم المشغل بتكوين **كلا** الطرفين بشكل متسق:

- على **OCS**: يتم تعيين `Policy-Counter-Identifier` لكل عداد سياسة إلى الاسم `enforced` عندما HSS، ويبلغ العداد عن الحالة الدقيق لـ قاعدة فوترة المعرفة في يجب تطبيق تلك القاعدة.
- على **HSS**: توجد قواعد الفوترة المشار إليها في قاعدة البيانات.

انظر عدادات السياسة وقواعد الفوترة لنموذج الربط.

المقاييس

تقوم Sy بعرض مقاييس Prometheus جنبًا إلى جنب مع المقاييس الأخرى لواجهة HSS (انظر Metrics & Monitoring).

المقياس: `hss_sy_messages_total` رسائل **الوصف**: عداد **النوع**: Sy المعالجة، حسب الأمر، الاتجاه والنتيجة. **التسميات**:

- `command` - `slr`، `sla`، `snr`، `sna`، `str`، أو `sta`
- `direction` - `incoming` (تم استلامه من OCS) أو `outgoing` (تم إرساله إلى OCS)
- `result` - `sent`، `received`، `success`، أو `error`

المقياس: `hss_sy_policy_updates_total` تغييرات قواعد الفوترة **الوصف**: عداد **النوع**: Sy، المدفوعة بحالة عداد سياسة Gx. **التسميات**: حسب الإجراء والنتيجة:

- `action` - `install` أو `remove`
- `result` - `success` أو `error` (نتيجة Gx RAR إلى PGW)

استعلامات المثال:

```
# معدل إشعارات Sy من OCS
rate(hss_sy_messages_total{command="snr", direction="incoming"}
[5m])

# معدل تثبيت قواعد التخفيف/التنفيذ المدفوعة بحدود الإنفاق
rate(hss_sy_policy_updates_total{action="install",
result="success"}[5m])

# نسبة فشل Sy Gx RAR
sum(rate(hss_sy_policy_updates_total{result="error"}[5m]))
  / sum(rate(hss_sy_policy_updates_total[5m]))
```

المرجع

الأوامر

الأمر	الاختصار	الرمز	الاتجاه	الغرض
طلب حد الإنفاق	SLR	8388635	PCRF -> OCS	طلب حالة عداد السياسة؛ الاشتراك في التغييرات
إجابة حد الإنفاق	SLA	8388635	OCS -> PCRF	إرجاع الحالة الحالية للعداد
طلب إشعار حالة الإنفاق	SNR	8388636	OCS -> PCRF	إخطار بتغيير حالة عداد
إجابة إشعار حالة الإنفاق	SNA	8388636	PCRF -> OCS	الاعتراف بإشعار
طلب إنهاء الجلسة	STR	275	PCRF -> OCS	إغلاق جلسة Sy (التقرير النهائي)
إجابة إنهاء الجلسة	STA	275	OCS -> PCRF	تأكيد إغلاق الجلسة

المعاد استخدامها STR/STA تحمل جميع الأوامر معرف التطبيق `16777302`، بما في ذلك (RFC 6733 لإنهاء الجلسة).

AVPs الرئيسية

AVP	الرمز	النوع	الوصف
`Policy-Counter-Identifier`	2901	UTF8String	يسمي عداد السياسة. مرتبط باسم قاعدة فوترة في OmniHSS.
`Policy-Counter-Status`	2902	UTF8String	تسمية الحالة المعرفة من قبل المشغل للعداد. تقود إجراء التنفيذ.
`Policy-Counter-Status-Report`	2903	Grouped	معرف عداد واحد + الحالة (+ أي حالات معلقة).
`SL-Request-Type`	2904	Enumerated	`INITIAL_REQUEST (0)` للطلب الأول، `INTERMEDIATE_REQUEST (1)` بعد ذلك.
`Pending-Policy-Counter-Information`	2905	Grouped	حالة مستقبلية والوقت الذي تصبح فيه الحالة الحالية.
`Pending-Policy-Counter-Change-Time`	2906	Time	متى تصبح الحالة المعلقة سارية.
`SN-Request-Type`	2907	Unsigned32	قناع بت على SNR. بت 0 = تقرير عادي، بت 1 = إلغاء (OCS يطلب إنهاء جلسة Sy).
`Subscription-Id`	443	Grouped	هوية المشترك (MSISDN و/أو IMSI) على SLR.

رموز النتيجة

الرمز	الاسم	المعنى
2001	DIAMETER_SUCCESS	تم معالجة الطلب بنجاح
5030	DIAMETER_USER_UNKNOWN	لا يعرف OCS المشترك؛ لم يتم إنشاء جلسة Sy
5570	DIAMETER_ERROR_UNKNOWN_POLICY_COUNTERS	واحد أو أكثر من عدادات السياسة المطلوبة غير معروفة لـ OCS
4241	DIAMETER_ERROR_NO_AVAILABLE_POLICY_COUNTERS	لا يوجد لدى OCS عدادات سياسة للمشترك

؛ 5030 معرف(TS 29.219 §5.5) Sy الرموز 5570 و4241 هي قيم رموز نتائج تجريبية خاصة بـ بواسطة RFC 4006.

الوثائق ذات الصلة

- PCRF - التحكم في السياسة Gx وRx الذي تغذيه Sy
- بروتوكولات Diameter - تدفقات الرسائل عبر جميع واجهات HSS
- الهيكلية HSS - الهيكل العام لـ

دليل استكشاف الأخطاء وإصلاحها لـ OmniHSS

← العودة إلى دليل العمليات

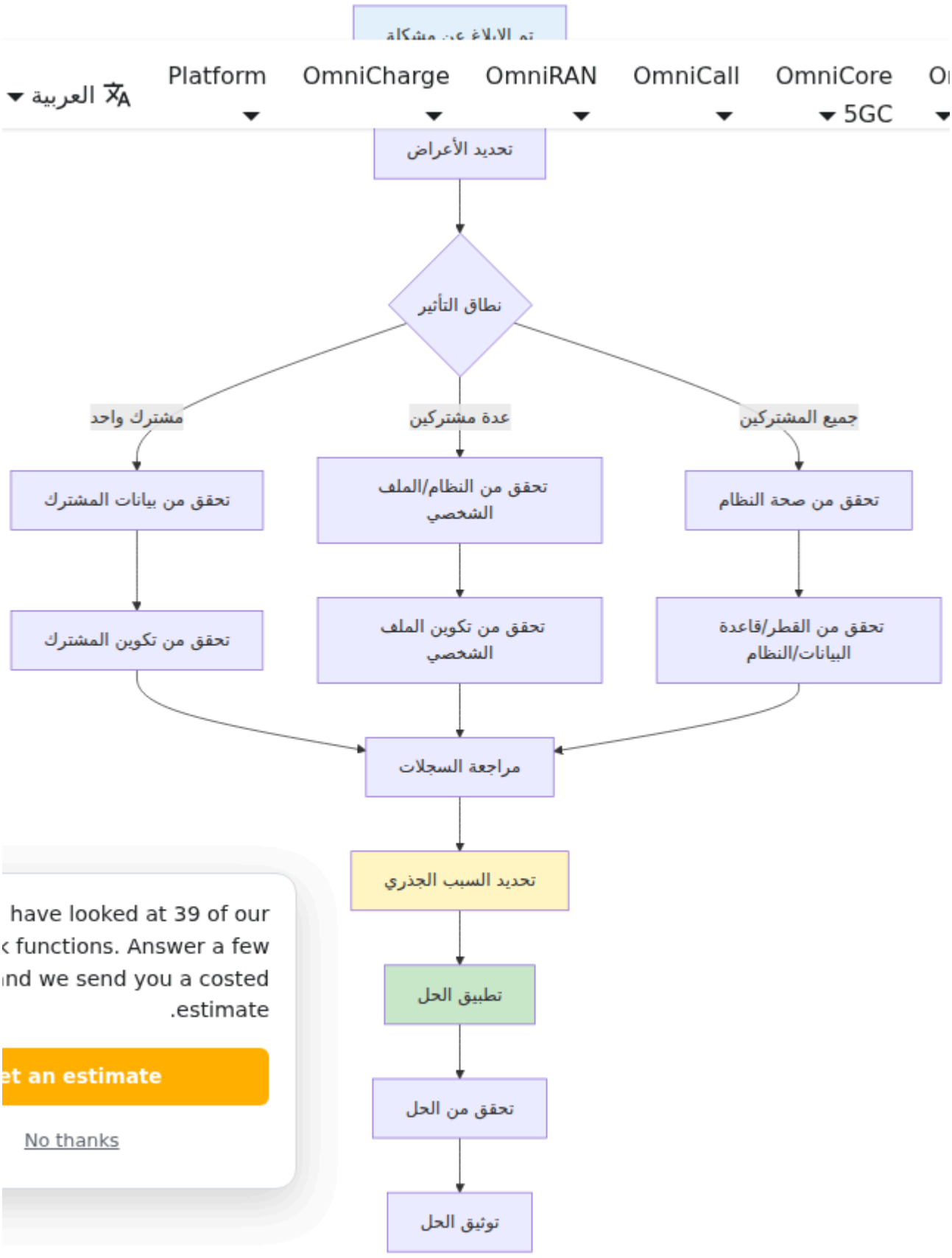
جدول المحتويات

- نظرة عامة على استكشاف الأخطاء وإصلاحها
- فشل المصادقة
- مشكلات الاتصال بالقطر
- مشكلات قاعدة البيانات
- فشل تسجيل EPC
- فشل تسجيل IMS
- فشل مكالمات VoLTE
- مشكلات التجوال
- مشكلات EIR
- مشكلات الأداء
- مشكلات المشتركين
- مشكلات API
- أدوات وأوامر التشخيص

نظرة عامة على استكشاف الأخطاء

وإصلاحها

النهج العام لاستكشاف الأخطاء وإصلاحها



المعلومات التي يجب جمعها

قبل استكشاف أي مشكلة، اجمع:

1. **معلومات المشترك** (إذا كانت محددة للمشترك)
    - IMSI
    - MSISDN (رقم الهاتف)
    - آخر حالة معروفة
    - رسائل الخطأ من الجهاز
2. **معلومات التوقيت**
    - متى بدأت المشكلة؟
    - هل هي متقطعة أم ثابتة؟
    - وقت آخر عملية ناجحة
3. **نطاق التأثير**
    - مشترك واحد أم عدة مشتركين؟
    - شبكة محددة أم جميع الشبكات؟
    - خدمة محددة (بيانات/صوت) أم كلاهما؟
4. **حالة النظام**
    - تحقق من لوحة التحكم لحالة النظام
    - مراجعة حالة نظير القطر
    - تحقق من اتصال قاعدة البيانات

فشل المصادقة

الأعراض

- لا يمكن للمشترك الاتصال بالشبكة
- أخطاء "تم رفض المصادقة"
- محاولات مصادقة متكررة

الأسباب والحلول الشائعة

السبب 1: مجموعة مفاتيح غير صحيحة

الأعراض:

- فشل المصادقة بشكل متكرر لمشترك محدد
- تعمل مع مشتركين آخرين بنفس الملف الشخصي

خطوات التشخيص:

1. استعلام عن المشترك للتحقق من key_set_id:

```
curl -k
https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
```

2. تحقق من وجود مجموعة المفاتيح والقيم الصحيحة:

```
curl -k
https://hss.example.com:8443/api/key_set/[KEY_SET_ID]
```

3. قارن بين قيم Ki و OPC مع وثائق بطاقة SIM

الحل:

- تحديث المشترك بمجموعة المفاتيح الصحيحة key set
- إذا كانت المفاتيح صحيحة، قد تكون بطاقة SIM معطلة

السبب 2: SQN خارج التزامن

الأعراض:

- فشل المصادقة بعد أن كانت تعمل سابقًا
- خطأ: "فشل تزامن SQN"
- تعمل بشكل متقطع

خطوات التشخيص:

1. تحقق من حالة المشترك لقيمة SQN في قاعدة البيانات
2. ابحث عن أخطاء متعلقة بـ SQN في السجلات
3. تحقق من قيمة SQN لمجموعة مفاتيح المشترك

الحل:

- سيتم إعادة تزامن SQN المشترك تلقائيًا بعد أن يرسل AUTS
- إلى 0 في مجموعة المفاتيح (يتطلب SQN إذا كانت المشكلة مستمرة، قم بإعادة تعيين إعادة اتصال المشترك)

تحذير: إعادة تعيين SQN يجب القيام بذلك فقط أثناء الصيانة. يمكن أن تسبب مشاكل أمنية.

السبب 3: المشترك معطل

الأعراض:

- تم رفض المصادقة على الفور
- لم يتم إنشاء أي مت��هات مصادقة

خطوات التشخيص:

1. تحقق من حالة تمكين المشترك:

```
curl -k
https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
```

2. تحقق من أن حقل `enabled` هو `true`

الحل:

- تمكين المشترك:

```
curl -k -X PUT
https://hss.example.com:8443/api/subscriber/[ID] \
  -H "Content-Type: application/json" \
  -d '{"subscriber": {"enabled": true}}'
```

السبب 4: ملف EPC مفقود

الأعراض:

- نجاح البحث عن المشترك ولكن فشل المصادقة
- خطأ: "لا يوجد ملف EPC مخصص"

خطوات التشخيص:

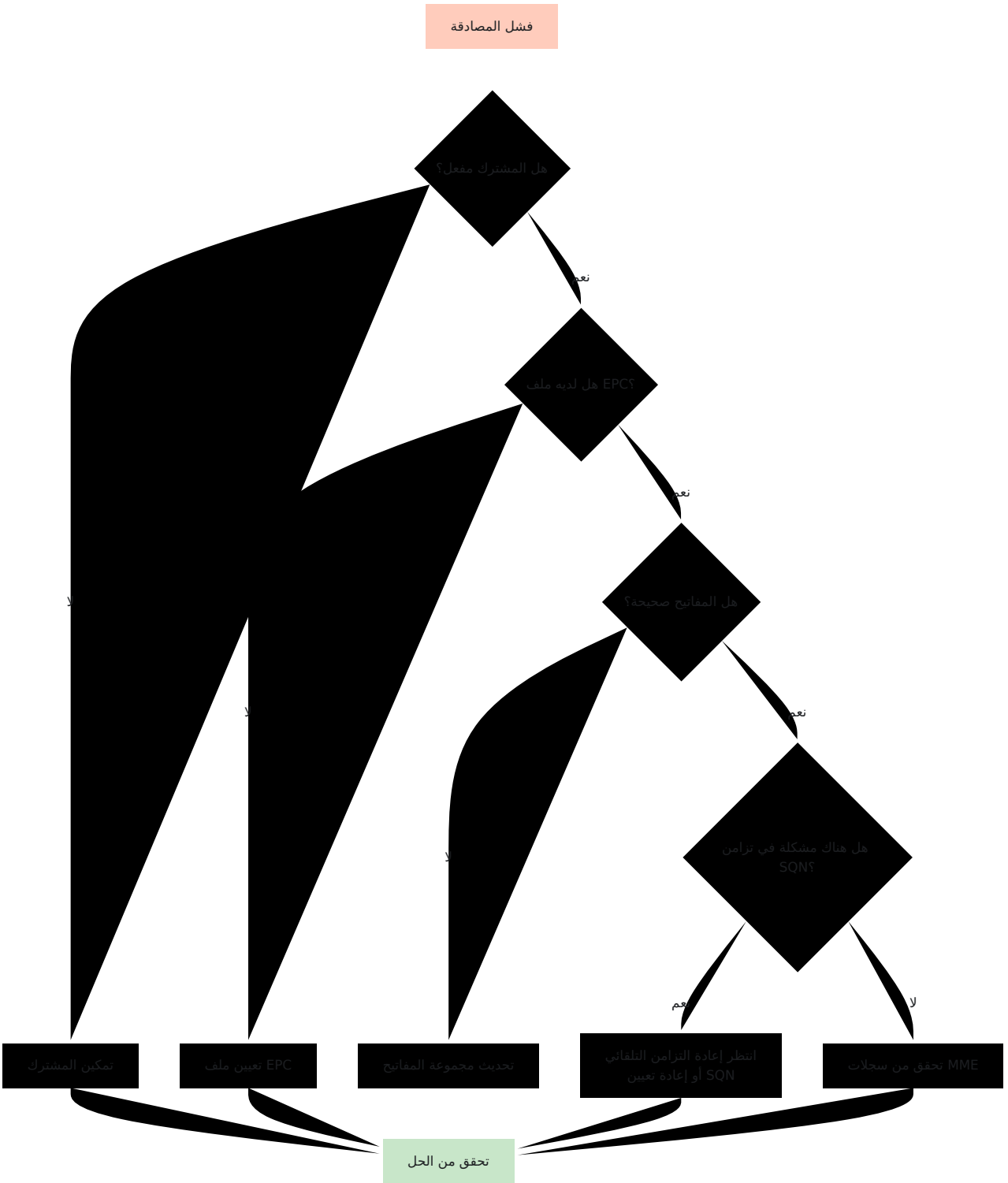
1. تحقق من حقل `epc_profile_id` للمشترك
2. تحقق من وجود ملف EPC:

```
curl -k
https://hss.example.com:8443/api/epc/profile/[PROFILE_ID]
```

الحل:

- تعيين ملف EPC صالح للمشترك

مخطط تدفق استكشاف الأخطاء في المصادقة



مشكلات الاتصال بالقطر

الأعراض

- تظهر نظائر القطر كغير متصلة في لوحة التحكم
- أخطاء "لا يوجد مسار إلى المضيف"
- فشل الخدمات لجميع المشتركين

الأسباب والحلول الشائعة

السبب 1: اتصال الشبكة

الأعراض:

- النظير لا يتصل أبدًا
- أخطاء انتهاء مهلة الاتصال
- فشل ping إلى النظير

خطوات التشخيص:

1. تحقق من اتصال الشبكة من OmniHSS إلى النظير:

   ```
   ping [PEER_IP]
   ```

2. تحقق مما إذا كان منفذ القطر قابل للوصول:

   ```
   telnet [PEER_IP] 3868
   ```

3. تحقق من أن قواعد جدار الحماية تسمح بحركة مرور القطر (المنفذ 3868)

الحل:

- إصلاح توجيه الشبكة
- تحديث قواعد جدار الحماية
- تحقق من أن النظير يعمل ويستمع

السبب 2: تكوين القطر غير صحيح

الأعراض:

- فشل محاولات الاتصال
- فشل تبادل CER/CEA
- يرفض النظير الاتصال

خطوات التشخيص:

1. مراجعة تكوين القطر في runtime.exs:
    - تحقق من أن origin_host للنظير يتطابق مع القيمة المتوقعة للنظير
    - تحقق من تكوين origin_realm
    - تحقق من أن عنوان IP للنظير صحيح
2. تحقق من السجلات بحثًا عن أخطاء CER/CEA
3. تحقق من أن تكوين النظير يتوقع origin_host لـ OmniHSS

الحل:

- تحديث runtime.exs بتكوين القطر الصحيح
- إعادة تشغيل OmniHSS بعد تغيير التكوين
- التنسيق مع مسؤول النظير للتحقق من الإعدادات

السبب 3: مشكلات الشه��دات (TLS Diameter)

الأعراض:

- فشل الاتصال أثناء مصافحة TLS
- أخطاء التحقق من الشهادة
- أخطاء "الشهادة منتهية الصلاحية" أو "الشهادة غير صالحة"

خطوات التشخيص:

1. تحقق من وجود ملفات الشهادة في `priv/cert/`
2. تحقق من انتهاء صلاحية الشهادة:

```
openssl x509 -in priv/cert/diameter.crt -noout -dates
```

3. تحقق من أن سلسلة الشهادات كاملة
4. تحقق من شهادة النظير إذا كان هناك TLS متبادل

الحل:

- تجديد الشهادات المنتهية
- تثبيت سلسلة الشهادات الصحيحة
- تحديث ملفات الشهادات وإعادة تشغيل OmniHSS

السبب 4: عدم تطابق دعم تطبيق النظير

الأعراض:

- يتصل النظير ولكن لا يدعم التطبيقات المطلوبة
- ينجح تبادل القدرات ولكن العمليات تفشل
- أخطاء "التطبيق غير مدعوم"

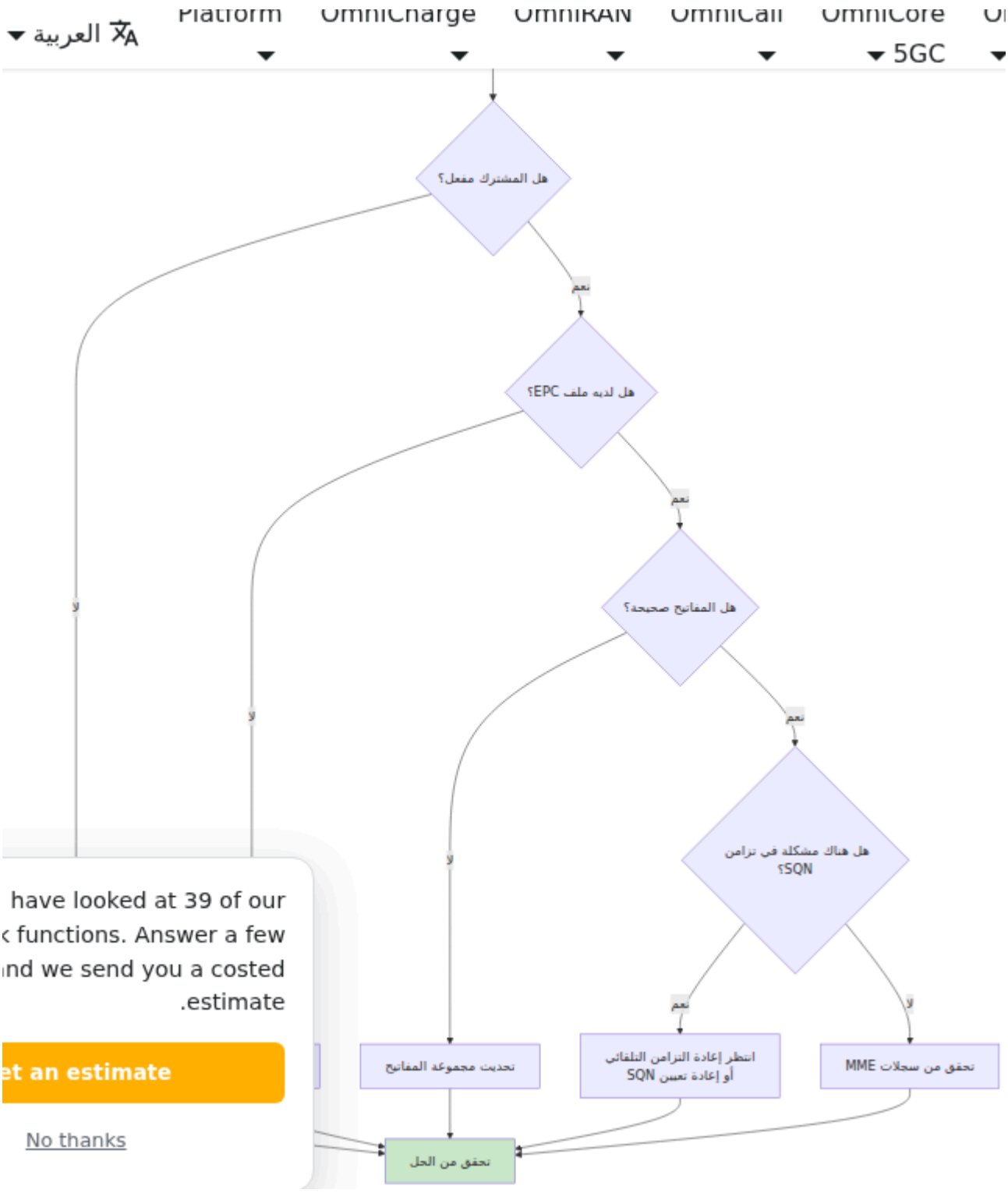
خطوات التشخيص:

1. تحقق من صفحة القطر في لوحة التحكم لتطبيقات النظير
2. تحقق مما إذا كان النظير يدعم التطبيق المطل��ب (S6a، Cx، Sh، إلخ)
3. مراجعة تبادل CER/CEA في السجلات

الحل:

- تحقق من أن تكوين النظير يتضمن التطبيقات المطلوبة للقطر
- تحقق من أن نوع النظير يتطابق مع الوظائف المتوقعة:
  - يجب أن يدعم MME S6a (16777251)
  - يجب أن يدعم S-CSCF Cx (16777216)
  - يجب أن يدعم P-GW Gx (16777238)

مخطط تدفق استكشاف الأخطاء في القطر



مشكلات قاعدة البيانات

الأعراض

- أخطاء API 500 ترجع
- فشل تحميل لوحة التحكم
- أخطاء "فشل الاتصال بقاعدة البيانات"
- أداء استعلام بطيء

الأسباب والحلول الشائعة

السبب 1: خادم قاعدة البيانات معطل

الأعراض:

- API تفشل جميع استدعاءات
- تظهر لوحة التحكم خطأ
- أخطاء "تم رفض الاتصال"

خطوات التشخيص:

1. اختبار اتصال قاعدة البيانات:

   ```
   # الاتصال بقاعدة البيانات
   psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME]
   ```

2. تحقق من حالة خدمة قاعدة البيانات على خادم قاعدة البيانات

3. تحقق من اتصال الشبكة بخادم قاعدة البيانات

الحل:

- بدء خدمة قاعدة البيانات
- إصلاح مشكلات خادم قاعدة البيانات
- تحقق من توجيه الشبكة إلى خادم قاعدة البيانات

السبب 2: ��يانات اعتماد قاعدة البيانات غير صحيحة

الأعراض:

- أخطاء "فشل المصادقة"
- لا يمكن لـ OmniHSS الاتصال عند بدء التشغيل

خطوات التشخيص:

1. مراجعة تكوين قاعدة البيانات في runtime.exs
2. اختبار بيانات الاعتماد يدويًا باستخدام عميل قاعدة البيانات
3. تحقق من أذونات مستخدم قاعدة البيانات

الحل:

- تحديث runtime.exs في تكوين قاعدة البيانات
- منح الأذونات الصحيحة لمستخدم قاعدة البيانات
- إعادة تشغيل OmniHSS بعد تغيير التكوين

السبب 3: استنفاد مجموعة الاتصالات

الأعراض:

- أخطاء 500 متقطعة
- أخطاء "لا توجد اتصالات متاحة"
- فترات الحمل العالية تؤدي إلى الفشل

خطوات التشخيص:

1. تحقق من عدد الاتصالات الحالية في قاعدة البيانات
2. مراجعة حجم مجموعة قاعدة البيانات في runtime.exs
3. مراقبة استخدام الاتصالات خلال فترات الحمل الذروة

الحل:

- زيادة حجم المجموعة في تكوين runtime.exs
- التحقيق في تسرب الاتصالات إذا تم استنفاد المجموعة بشكل متكرر
- النظر في توسيع قاعدة البيانات إذا كان الحمل مرتفعًا باستمرار

السبب 4: استعلامات بطيئة

الأعراض:

- استجابات API بطيئة جدًا
- انتهاء المهلة في عمليات البحث عن المشتركين
- ارتفاع CPU لقاعدة البيانات

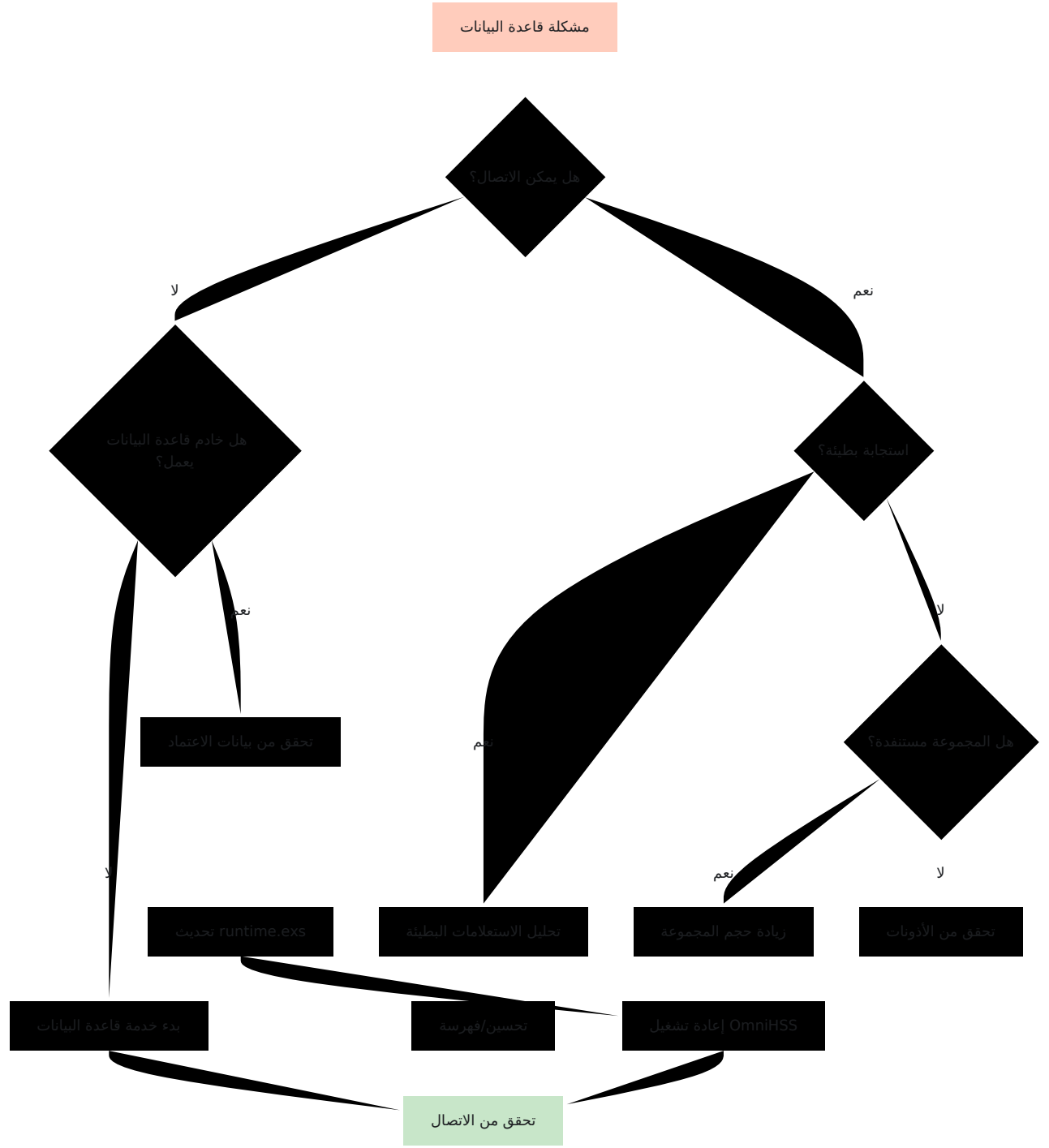
خطوات التشخيص:

1. استعلام قاعدة البيانات عن سجل الاستعلامات البطيئة
2. تحديد الاستعلامات البطيئة المحددة
3. التحقق من وجود فهارس مفقودة
4. التحقق من عدد المشتركين وأحجام الجداول

الحل:

- تحسين الاستعلامات البطيئة
- إضافة الفهارس المفقودة
- النظر في تحسين أداء قاعدة البيانات
- التخطيط لتوسيع قاعدة البيانات إذا لزم الأمر

مخطط تدفق استكشاف الأخطاء في قاعدة البيانات



فشل تسجيل EPC

الأعراض

- لا يمكن للمشترك الاتصال بشبكة LTE
- يرفض MME الاتصال
- لم يتم إنشاء جلسة PDN

الأسباب والحلول الشائعة

السبب 1: التجوال مرفوض

الأعراض:

- يعمل المشترك على الشبكة المنزلية ولكنه يفشل عند التجوال
- أخطاء "التجوال غير مسموح"
- يعمل لبعض الشبكات ولكن ليس لأخرى

خطوات التشخيص:

1. تحقق من `roaming_profile_id` للمشترك
2. استعلام عن ملف التجوال والقواعد
3. تحقق من MCC/MNC للشبكة التي تمت زيارتها
4. تحقق مما إذا كانت قاعدة التجوال موجودة لتلك الشبكة

الحل:

- إضافة MCC/MNC للشبكة التي تمت زيارتها قاعدة تجوال
- أو تحديث الإجراء الافتراضي لملف التجوال للسماح
- انظر وثائق التجوال للتكوين

السبب 2: تكوين APN مفقود

الأعراض:

- ينجح الاتصال ولكن تفشل جلسة PDN
- أخطاء "APN غير معروف" من MME

- لا يمكن للمشترك الحصول على اتصال بيانات

خطوات التشخيص:

1. تحقق من أن ملف EPC يحتوي على ملفات APN مرتبطة
2. تحقق من أن معرف APN يتطابق مع ما يطلبه الجهاز
3. استعلام عن تكوين ملف APN

الحل:

- ربط ملفات APN بملف EPC الخاص بالمشترك
- تأكد من أن اسم APN يتطابق مع تكوين الجهاز
- تحقق من وجود ملف QoS لـ APN

السبب 3: MME غير متصل

الأعراض:

- جميع المشتركين يفشلون في الاتصال
- لا يوجد اتصال مع MME
- النظير القطر معطل

خطوات التشخيص:

1. تحقق من صفحة القطر في لوحة التحكم
2. تحقق من أن حالة النظير MME متصل" هي"
3. تحقق من أن MME يدعم تطبيق S6a

الحل:

- استكشاف اتصال القطر
- تحقق من تكوين MME
- اتصل MME بمسؤول

السبب 4: فساد حالة المشترك

الأعراض:

- يظهر المشترك كمتصل ولكنه لا يمكنه الاتصال مرة أخرى

- الحالة لا تتطابق مع الواقع
- فشل فصل وإعادة الاتصال

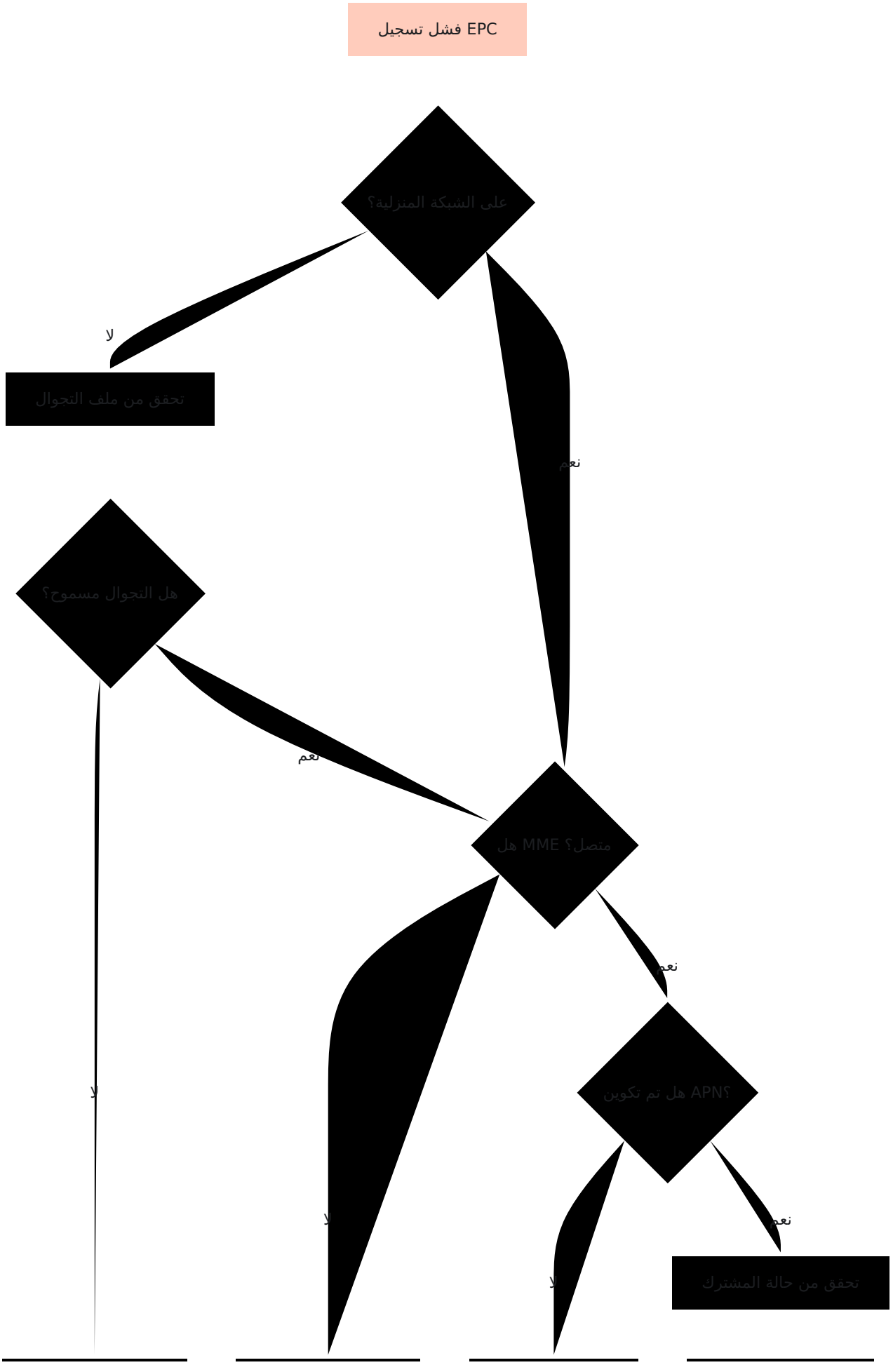
خطوات التشخيص:

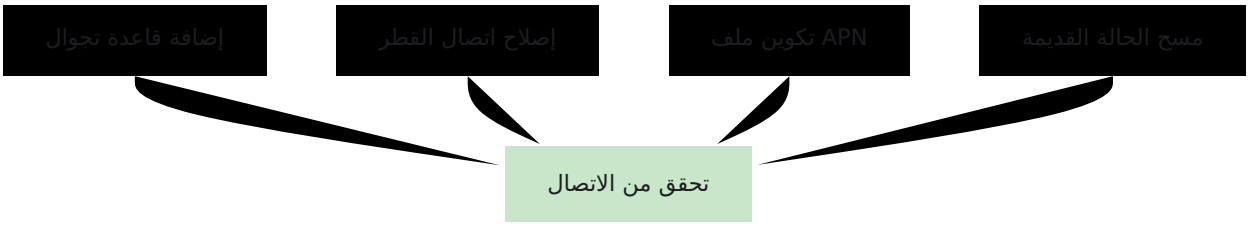
1. استعلام عن حالة المشترك من قاعدة البيانات
2. تحقق من تعيينات MME القديمة
3. تحقق من طابع الوقت لآخر تحديث

الحل:

- مسح حالة المشترك (إجراء الفصل)
- إعادة تعيين MME الخادم في حالة المشترك
- قد يتطلب إعادة تشغيل المشترك

مخطط تدفق استكشاف الأخطاء في تسجيل EPC


فشل تسجيل EPC
على الشبكة المنزلية؟
لا
تحقق من ملف التجوال
نعم
هل التجوال مسموح؟
نعم
هل MME متصل؟
نعم
هل تم تكوين APN؟
نعم
تحقق من حالة المشترك
لا
لا
لا



فشل تسجيل IMS

الأعراض

- لا يمكن للمشترك التسجيل لـ VoLTE
- على الجهاز "فشل تسجيل IMS"
- البيانات تعمل ولكن الصوت لا يعمل

الأسباب والحلول الشائعة

السبب 1: IMS معطل للمشترك

الأعراض:

- لدى المشترك بيانات ولكن لا يوجد IMS
- تم رفض التسجيل على الفور

خطوات التشخيص:

1. استعلام عن المشترك والتحقق من حقل `ims_enabled`
2. تحقق من أن المشترك لديه `ims_profile_id` معين

الحل:

- تمكين IMS للمشترك
- تعيين ملف IMS

السبب 2: S-CSCF غير متصل

الأعراض:

- تفشل جميع تسجيلات IMS

- لا توجد حركة مرور قطر مرتبطة بـ IMS

خطوات التشخيص:

1. تحقق من صفحة القطر في لوحة التحكم
2. تحقق من أن نظير S-CSCF متصل
3. تحقق من أن S-CSCF يدعم تطبيق Cx

الحل:

- إصلاح S-CSCF إلى اتصال القطر
- تحقق من تكوين S-CSCF

السبب 3: قالب IFC مفقود أو غير صالح

الأعراض:

- يفشل التسجيل أثناء User-Authorization-Answer
- أخطاء متعلقة بـ IFC في السجلات

خطوات التشخيص:

1. استعلام عن ملف IMS الخاص بالمشترك
2. تحقق من وجود قالب IFC
3. تحقق من بناء جملة XML لـ IFC

الحل:

- تحديث ملف IMS بقالب IFC صالح
- انظر وثائق الملفات الشخصية لأمثلة IFC

السبب 4: التجوال مرفوض لـ IMS

الأعراض:

- يعمل IMS على الشبكة المنزلية
- يفشل عند التجوال
- يعمل التجوال للبيانات ولكن ليس IMS

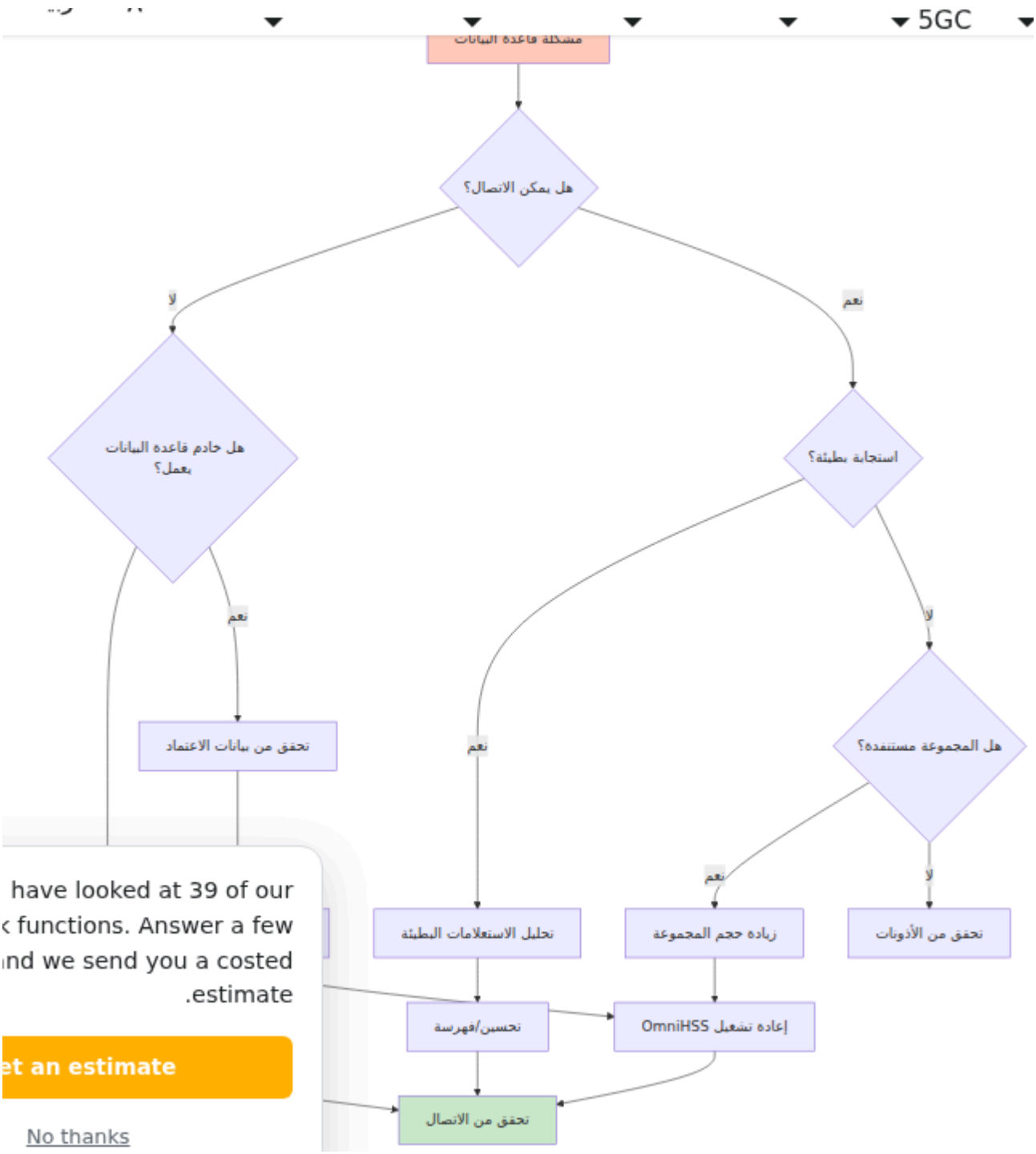
خطوات التشخيص:

1. في ملف التجوال IMS تحقق من إجراء
2. الصحيح `ims_action` تحقق من أن قواعد التجوال تحتوي على

الحل:

- IMS تحديث قواعد التجوال للسماح بـ
- IMS أو تحديث الإجراء الافتراضي لملف التجوال لـ

IMS مخطط تدفق استكشاف الأخطاء في تسجيل



فشل مكالمات VoLTE

الأعراض

- ولكن المكالمات تفشل IMS ينجح تسجيل
- صوت من اتجاه واحد
- انقطاع المكالمة على الفور
- خطأ "فشلت المكالمة" على الجهاز

الأسباب والحلول الشائعة

السبب 1: P-CSCF غير متصل

الأعراض:

- يعمل التسجيل ولكن المكالمات تفشل
- فشل تفويض الوسائط

خطوات التشخيص:

1. تحقق من صفحة القطر في لوحة التحكم
2. تحقق من أن نظير P-CSCF متصل
3. تحقق من أن P-CSCF يدعم تطبيق Rx (وظيفة OmniHSS PCRF)

الحل:

- إصلاح P-CSCF إلى اتصال القطر
- تحقق من أن تكوين P-CSCF يشير إلى OmniHSS لـ Rx

السبب 2: تفويض الوسائط مفقود

الأعراض:

- يبدأ إعداد المكالمة ولكن يفشل
- فشل تبادل AAR/AAA
- أخطاء في واجهة Rx

خطوات التشخيص:

1. تحقق من السجلات بحثًا عن رسائل قطر Rx
2. تحقق من تلقي AAR (AA-Request)
3. تحقق من استجابة AAA (AA-Answer)

الحل:

- تحقق من أن P-CSCF يرسل AAR لتفويض الوسائط
- تحقق من تكوين تطبيق Rx لـ OmniHSS
- تحقق من أن المشترك لديه تسجيل IMS نشط

مشكلات السبب 3: QoS/الناقل

الأعراض:

- تتصل المكالمة ولكن لا يوجد صوت
- صوت من اتجاه واحد
- مشكلات في الجودة

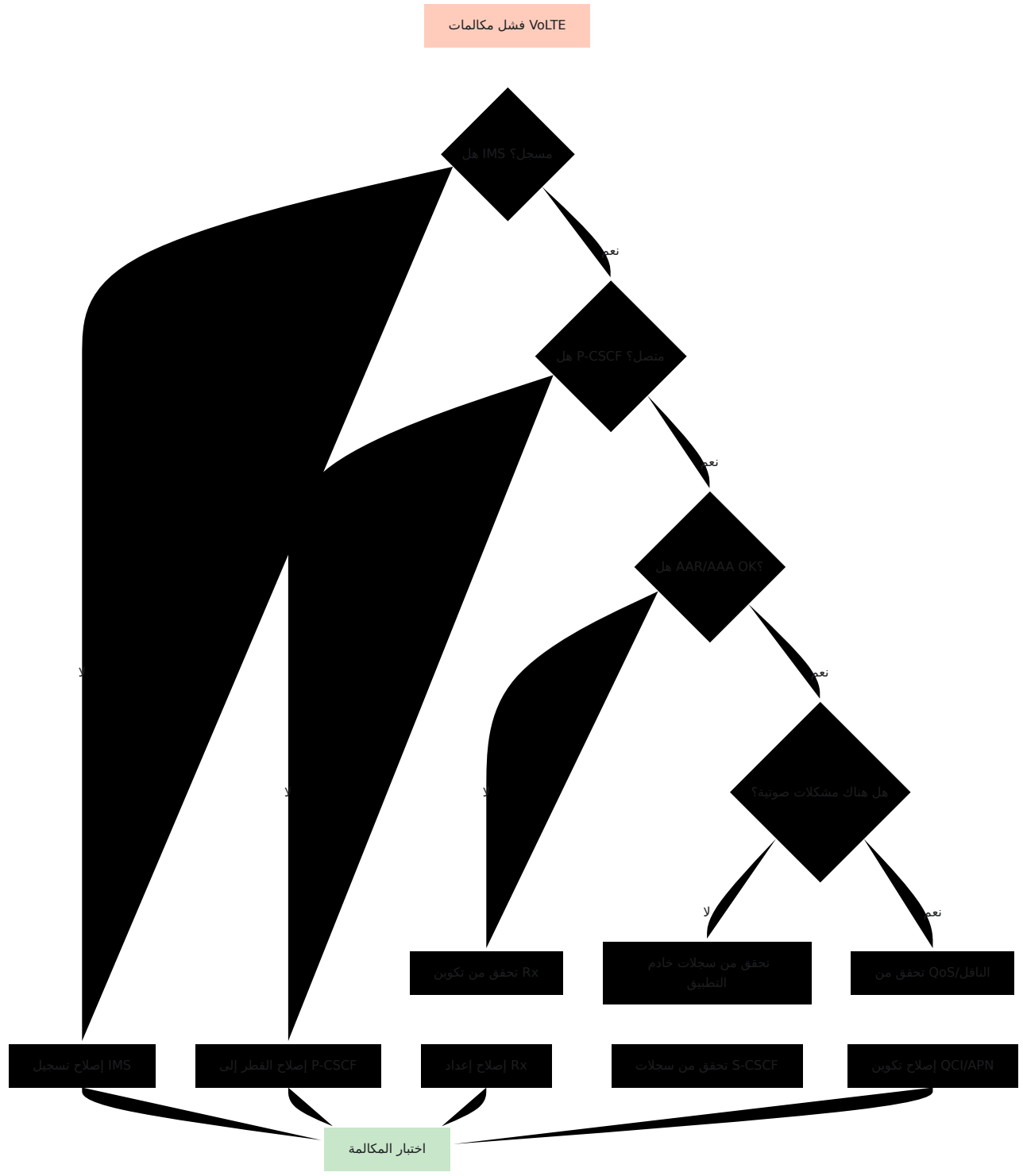
خطوات التشخيص:

1. تحقق من ملف QoS لـ APN للصوت
2. تحقق من تعيين QCI بشكل صحيح (عادة QCI 1 للصوت)
3. تحقق من أن P-GW متصل لـ Gx (وظيفة PCRF)

الحل:

- تحقق من ملف QoS لـ APN لـ APN IMS
- تأكد من تكوين QCI 1 للناقل الصوتي
- إذا لزم الأمر إصلاح P-GW إلى اتصال القطر

مخطط تدفق استكشاف الأخطاء في مكالمات VoLTE



مشكلات التجوال

الأعراض

- يعمل المشترك في المنزل ولكن لا يعمل عند التجوال
- بعض الشبكات أثناء التجوال تعمل، والبعض الآخر لا يعمل
- يعمل التجوال للبيانات ولكن ليس الصوت (أو العكس)

الأسباب والحلول الشائعة

السبب 1: عدم تعيين ملف تعريف التجوال

الأعراض:

- فشل التجوال للمشترك
- مشتركين آخرين يتجولون بنجاح

خطوات التشخيص:

1. استعلام عن `roaming_profile_id` للمشترك
2. تحقق مما إذا كان الحقل فارغًا

الحل:

- تعيين ملف تعريف التجوال للمشترك

السبب 2: تم رفض التجوال بواسطة السياسة

الأعراض:

- فشل التجوال باستمرار على شبكة معينة
- الخطأ يشير إلى رفض السياسة

خطوات التشخيص:

1. تحديد MCC/MNC أو MME للشبكة التي تم زيارتها من جهاز المشترك
2. استعلام عن ملف تعريف التجوال للمشترك
3. تحقق من قواعد التجوال لمطابقة MCC/MNC

4. تحقق من الإجراء الافتراضي للملف الشخصي

الحل:

- إضافة قاعدة التجوال للسماح للشبكة التي تم زيارتها:

```
curl -k -X POST
https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Allow Visited Network",
      "mcc": "310",
      "mnc": "410",
      "data_action": "allow",
      "ims_action": "allow"
    }
  }'
```

السبب 3: البيانات مسموح بها ولكن IMS مرفوض

الأعراض:

- يعمل تجوال البيانات
- فشل تجوال الصوت/IMS
- توفر الخدمة مقسوم

خطوات التشخيص:

1. استعلام عن قواعد التجوال للشبكة التي تم زيارتها
2. تحقق من قيم `data_action` مقابل `ims_action`
3. تحقق من الإجراءات الافتراضية لملف تعريف التجوال

الحل:

- تحديث قاعدة التجوال للسماح بـ IMS:
  - تعيين `ims_action: "allow"`
- أو تحديث `ims_action_if_no_rules_match` للملف الشخصي إلى `"allow"`

راجع وثائق التجوال للحصول على تكوين مفصل.

مشاكل EIR

الأعراض

- الأجهزة محظورة بشكل غير متوقع
- الأجهزة المسروقة غير محظورة
- فشل فحص EIR

الأسباب والحلول الشائعة

السبب 1: تعيير IMEI غير صحيح

الأعراض:

- حظر/السماح بأجهزة خاطئة
- تطابق القاعدة بشكل غير صحيح

خطوات التشخيص:

1. استعلام عن قواعد EIR (`GET /api/eir/rule`). يتم إرجاع القائمة بترتيب `id`، لذا قم بفرزها حسب `precedence` لرؤية ترتيب التقييم
2. تحديد أي قاعدة تتطابق. يتم اختبار القواعد ضد IMEISV (IMEI + إصدار البرمجيات) إذا كانت الطلب تحمل واحدة. ضمن كل خطوة، القاعدة IMSI ثم IMEI، ثم أولاً، ذات IMSI الأدنى تفوز، لذا لا يتم الوصول إلى قاعدة `precedence` المطابقة ذات الأولوية المنخفضة إذا تطابقت أي قاعدة مع IMEI أو IMEISV. راجع منطق مطابقة المعدات
3. اختبار نمط التعبير العادي ضد IMSI و IMEI و IMEISV الفعلي. الأنماط غير مثبتة، لذا تتطابق أيضًا مع `35979139461650` IMEISV `3597913946165008`
4. تحقق من أولوية القاعدة (القيم المنخفضة يتم تقييمها أولاً)

الحل:

- تحديث قاعدة EIR بتعبير عادي صحيح
- اختبار التعبير العادي بدقة قبل التطبيق
- مراعاة أولوية القاعدة (القاعدة المطابقة ذات الأولوية المنخفضة تفوز)

السبب 2: MME لا يرسل طلبات S13

الأعراض:

- لم يحدث فحص EIR أبدًا
- جميع الأجهزة مسموح بها بغض النظر عن القواعد

خطوات التشخيص:

1. تحقق مما إذا كان MME مُعدًا لاستخدام واجهة S13
2. تحقق من اتصال نظير Diameter لـ MME
3. تحقق من دعم تطبيق S13
4. مراجعة تكوين MME

الحل:

- تكوين MME لإجراء فحوصات EIR عبر S13
- تحقق من دعم نظير Diameter لتطبيق S13 (16777252)
- إذا لزم الأمر MME الاتصال بمدير

السبب 3: عدم وجود قاعدة افتراضية

الأعراض:

- الأجهزة التي لا تتطابق مع أي قاعدة لديها سلوك غير متوقع

خطوات التشخيص:

1. استعلام عن جميع قواعد EIR
2. تحقق مما إذا كانت قاعدة catch-all موجودة
3. تحقق من أولوية القاعدة

الحل:

- المعدات التي لا تتطابق مع أي قاعدة تحصل على إعداد `unknown_equipment_behaviour` من `config :hss, :eir` (انظر تكوين EIR). تحقق من ذلك أولاً.
- صريحة، أضف قاعدة بتعبير عادي `*.` والإجراء catch-all إذا كنت تفضل قاعدة حتى يتم اختبارها آخرًا ضمن كل خطوة `precedence` المطلوب، وامنحها أعلى رقم
- عندما يحمل IMEI أو IMEISV، قاعدة `*.` تتطابق في الخطوة الأولى التي تعمل والقيمة الافتراضية IMSI لذا لا يتم الوصول إلى قواعد، (الطلب لا إصدار برمجيات

المكونة للطلبات التي تحمل IMEI

مشاكل الأداء

الأعراض

- استجابات API بطيئة
- مهلات طلب Diameter
- استخدام مرتفع لوحدة المعالجة المركزية أو الذاكرة
- تحميل لوحة التحكم ببطء

الأسباب والحلول الشائعة

السبب 1: تحميل قاعدة بيانات مرتفع

الأعراض:

- جميع العمليات بطيئة
- وحدة المعالجة المركزية لقاعدة البيانات مرتفعة
- مهلات الاستعلامات

خطوات التشخيص:

1. تحقق من استخدام موارد خادم قاعدة البيانات
2. تحديد الاستعلامات البطيئة
3. تحقق من وجود فهارس مفقودة
4. مراقبة أنماط الاستعلام

الحل:

- تحسين الاستعلامات البطيئة
- إضافة فهارس قاعدة البيانات
- زيادة موارد قاعدة البيانات
- النظر في توسيع قاعدة البيانات
- انظر مشاكل قاعدة البيانات

السبب 2: عدد المشتركين مرتفع

الأعراض:

- تدهور الأداء مع مرور الوقت
- البطء يتزامن مع نمو عدد المشتركين
- عمليات القائمة بطيئة بشكل خاص

خطوات التشخيص:

1. استعلام عن إجمالي عدد المشتركين
2. تحقق من أحجام الجداول
3. مراجعة خطط تنفيذ الاستعلام
4. مراقبة اتجاهات استخدام الموارد

الحل:

- التخطيط لترقية السعة
- تحسين الاستعلامات لمجموعات البيانات الكبيرة
- النظر في الترقيم للنتائج الكبيرة
- تنفيذ التخزين المؤقت إذا لزم الأمر

السبب 3: مشا��ل نظير Diameter

الأعراض:

- عمليات Diameter بطيئة
- مهلات على نظير معين
- بعض النظائر سريعة، والبعض الآخر بطيء

خطوات التشخيص:

1. تحقق من صفحة Diameter في لوحة التحكم
2. تحديد النظير البطيء
3. اختبار زمن الانتقال الشبكي إلى النظير
4. تحقق من استخدام موارد النظير

الحل:

- التحقيق في مشاكل أداء النظير
- تحقق من مسار الشبكة للازدحام
- النظر في إضافة نظائر احتياطية
- إذا لزم الأمر Diameter زيادة مهلة

السبب 4: مشاكل الذاكرة

الأعراض:

- مرتفع OmniHSS استخدام ذاكرة
- أخطاء نفاد الذاكرة
- تدهور الأداء مع مرور الوقت

خطوات التشخيص:

1. في صفحة التطبيق OmniHSS تحقق من استخدام ذاكرة
2. مراقبة اتجاه الذاكرة
3. تحقق من وجود تسريبات في الذاكرة
4. مراجعة إعدادات VM Erlang

الحل:

- لمسح الحالة المؤقتة OmniHSS إعادة تشغيل
- التحقيق في تسرب الذاكرة إذا استمر الاستخدام في الارتفاع
- في runtime.exs ضبط إعدادات ذاكرة VM Erlang
- التخطيط لترقية الأجهزة إذا كانت مرتفعة باستمرار

مشاكل حالة المشترك

الأعراض

- يظهر المشترك كمتصل لكنه ليس كذلك
- معلومات الحالة قديمة
- معلومات الموقع غير صحيحة
- لا يمكن فصل المشترك

الأسباب والحلول الشائعة

السبب 1: تعطل/إعادة تشغيل MME

الأعراض:

- يظهر المشترك MME يخدم لم يعد يخدم
- لا يمكن للمشترك الاتصال بعد إعادة تشغيل MME
- الحالة قديمة

خطوات التشخيص:

1. تحقق من حالة المشترك لـ MME الخادم
2. تحقق مما إذا كان MME قد أعيد تشغيله
3. تحقق من آخر وقت اتصال لـ MME

الحل:

- الانتظار حتى يتصل المشترك مرة أخرى (ستتحدث الحالة)
- أو مسح حالة المشترك يدويًا
- عند إعادة التشغيل Cancel-Location إرسال MME يجب على

السبب 2: عدم استلام فصل الشبكة

الأعراض:

- تم إيقاف تشغيل المشترك ولكنه يظهر كمتصل
- تبقى جلسات PDN في قاعدة البيانات
- لم يتم مسح الموقع

خطوات التشخيص:

1. تحقق من الطابع الزمني last_seen للمشترك
2. تحقق مما إذا كانت الحالة قديمة (ساعات أو أيام)
3. تحقق مما إذا كان جهاز المشترك قابلًا للوصول

الحل:

- ستتم مسح الحالة عندما يتصل المشترك مرة أخرى

- أو الانتظار حتى انتهاء مهلة الحالة (إذا تم تنفيذها)
- قد تكون هناك حاجة لتنظيف يدوي للحالة القديمة جدًا

السبب 3: تلف قاعدة البيانات

الأعراض:

- حالة غير متسقة عبر الجداول
- انتهاكات المفتاح الأجنبي
- الحالة لا معنى لها

خطوات التشخيص:

1. استعلام عن حالة المشترك مباشرة من قاعدة البيانات
2. تحقق من وجود سجلات يتيمة
3. تحقق من سلامة المرجعية

الحل:

- تحديد وإصلاح البيانات غير المتسقة
- قد يتطلب تنظيف قاعدة البيانات يدويًا
- الاتصال بالدعم إذا كان التلف واسع النطاق

مشاكل API

الأعراض

- تعيد أخطاء API
- استجابات API بطيئة
- لا يمكن إنشاء/تحديث الكيانات
- أخطاء 500

الأسباب والحلول الشائعة

السبب 1: بيانات الطلب غير صالحة

الأعراض:

- أخطاء 400 أو 422
- رسائل خطأ التحقق
- تم رفض الحقل

خطوات التشخيص:

1. مراجعة استجابة الخطأ للحقول المحددة
2. تحقق من تنسيق طلب API
3. تحقق من وجود الحقول المطلوبة
4. تحقق من أنواع البيانات

الحل:

- إصلاح بيانات الطلب لتتوافق مع مرجع API
- التأكد من تضمين جميع الحقول المطلوبة
- التحقق من وجود مراجع المفتاح الأجنبي (معرفات الملفات الشخصية، إلخ.)

السبب 2: قيود المفتاح الأجنبي

الأعراض:

- لا يمكن إنشاء مشترك
- خطأ: "key_set_id does not exist"
- الكيان المرجع غير موجود

خطوات التشخيص:

1. تحديد أي مفتاح أجنبي يفشل
2. تحقق من وجود الكيان المرجع:
    - key_set_id → مجموعات المفاتيح
    - epc_profile_id → ملفات تعريف EPC
    - ims_profile_id → ملفات تعريف IMS

الحل:

- إنشاء الكيان المرجع أولاً

- أو استخدام معرف كيان موجود
- اتبع سير العمل الكامل للتزويد

السبب 3: اتصال قاعدة البيانات

الأعراض:

- أخطاء 500
- تفشل جميع مكالمات API
- أخطاء اتصال قاعدة البيانات

الحل:

- انظر مشاكل قاعدة البيانات

أدوات وأوامر التشخيص

فحوصات سريعة في لوحة التحكم

1. **نظرة عامة على النظام**
   - URL: `https://[hostname]:7443/overview`
   - تحقق: عدد المشتركين، الجلسات النشطة، حالة النظام
2. **حالة Diameter**
   - URL: `https://[hostname]:7443/diameter`
   - تحقق: جميع النظائر الحرجة متصلة
3. **صحة التطبيق**
   - URL: `https://[hostname]:7443/application`
   - تحقق: استخدام الذاكرة، عدد العمليات، وقت التشغيل

أوامر تشخيص API

تحقق من صحة النظام:

```
curl -k https://hss.example.com:8443/api/status
```

استعلام عن المشترك:

```
# بواسطة IMSI
curl -k
https://hss.example.com:8443/api/subscriber/imsi/001001123456789

# بواسطة MSISDN
curl -k
https://hss.example.com:8443/api/subscriber/msisdn/14155551234

# بواسطة ID
curl -k https://hss.example.com:8443/api/subscriber/d290f1ee-6c54-
4b01-90e6-d701748f0851
```

قائمة بجميع المشتركين:

```
curl -k https://hss.example.com:8443/api/subscriber
```

تحقق من تكوين الملف الشخصي:

```
# ملف تعريف EPC
curl -k https://hss.example.com:8443/api/epc/profile/e58ed763-
928c-4155-bee9-fdbaaadc15f3

# ملف تعريف IMS
curl -k https://hss.example.com:8443/api/ims/profile/7c9e6679-
7425-40de-944b-e07fc1f90ae7

# ملف تعريف الـتجوال
curl -k https://hss.example.com:8443/api/roaming/profile/9c858901-
8a57-4791-81fe-4c455b099bc9
```

أوامر تشخيص الشبكة

اختبار اتصال منفذ Diameter:

```
telnet [PEER_IP] 3868
```

تحقق من شهادة TLS:

```
openssl s_client -connect [hostname]:8443 -showcerts
```

اختبار اتصال قاعدة البيانات:

```
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME] -c "SELECT COUNT(*)
FROM subscriber;"
```

تحليل السجلات

البحث في السجلات عن IMSI محدد:

```
grep "001001123456789" /var/log/omnihss/omnihss.log
```

العثور على فشل المصادقة:

```
grep "authentication.*fail" /var/log/omnihss/omnihss.log
```

تحقق من أحداث نظير Diameter:

```
grep "Diameter peer" /var/log/omnihss/omnihss.log
```

العثور على أخطاء قاعدة البيانات:

```
grep -i "database.*error" /var/log/omnihss/omnihss.log
```

إرشادات التصعيد

متى يجب التصعيد

قم بالتصعيد إلى دعم الهندسة/البائع عندما:

1. **فشل النظام بالكامل** الذي لا يمكن حله بإجراءات موثقة
2. **تلف البيانات** أو حالة قاعدة بيانات غير متسقة
3. **أخطاء برمجية مشبوهة** أو سلوك غير متوقع
4. **مشاكل الأداء** التي لا يمكن حلها بالتعديل
5. **حوادث أمنية** أو وصول غير مصرح به
6. **أسئلة حول سلوك غير موثق**

المعلومات التي يجب تقديمها

عند التصعيد، قم بتضمين:

1. **الأعراض التفصيلية** - ما الذي يفشل، متى، لمن
2. **الخطوات المتخذة** - ما الذي تم استكشافه بالفعل
3. **السجلات** - مقتطفات السجل ذات الصلة التي تظهر المشكلة
4. **التكوين** - أجزاء ذات صلة من runtime.exs (احذف البيانات الحساسة)
5. **البيئة** - إصدار OmniHSS، إصدار نظام التشغيل، إصدار قاعدة البيانات
6. **الأثر** - عدد المشتركين المتأثرين، الأثر التجاري
7. **أمثلة المشتركين** - IMSIs محددة تظهر المشكلة

القضايا الحرجة مقابل غير الحرجة

القضايا الحرجة (تصعيد فوري):

- النظام معطل تمامًا
- جميع المشتركين غير قادرين على الاتصال
- تلف قاعدة البيانات
- خرق أمني

القضايا غير الحرجة (توثيق وتصعيد خلال ساعات العمل):

- مشاكل مشترك واحد يمكن العمل حولها
- تدهور الأداء الذي يمكن إدارته
- طلبات تحسين
- أسئلة توثيق

مرجع رسائل الخطأ الشائعة

أخطاء المصادقة

رسالة الخطأ	السبب	الحل
"فشل توليد متجهات المصادقة"	مجموعة مفاتيح مفقودة أو غير صالحة	تحقق من تكوين مجموعة المفاتيح
"فشل مزامنة SQN"	SQN خارج التزامن	انتظر لإعادة المزامنة
"المشترك غير موجود"	IMSI غير صالح	تحقق من IMSI، زود المشترك
"المشترك معطل"	enabled=false	تمكين المشترك

أخطاء Diameter

رسالة الخطأ	السبب	الحل
"مهلة اتصال نظير Diameter"	مشكلة في الشبكة	تحقق من الاتصال الشبكي
"فشل تبادل CER/CEA"	عدم تطابق التكوين	تحقق من تكوين Diameter
"التطبيق غير مدعوم"	النظير لا يدعم التطبيق المطلوب	تحقق من تطبيقات النظير
"فشل مصافحة TLS"	مشكلة في الشهادة	تحقق من الشهادات

أخطاء قاعدة البيانات

رسالة الخطأ	السبب	الحل
"تم رفض الاتصال"	قاعدة البيانات معطلة	ابدأ قاعدة البيانات
"فشلت المصادقة"	بيانات اعتماد خاطئة	إصلاح بيانات الاعتماد
"لا توجد اتصالات متاحة"	استنفاد التجمع	زيادة حجم التجمع
"مهلة الاستعلام"	استعلام بطيء	تحسين الاستعلامات

أخطاء API

رسالة الخطأ	السبب	الحل
"key_set_id does not exist"	مفتاح أجنبي غير صالح	إنشاء مجموعة المفاتيح أولاً
"تم أخذ IMSI بالفعل"	IMSI مكرر	استخدم IMSI مختلف أو احذف الموجود
"خطأ في التحقق"	إدخال غير صالح	تحقق من تنسيق الحقل والمتطلبات

العودة إلى دليل العمليات API → | التالي: مرجع ←

تكامل Webhook مع OmniHSS

← العودة إلى دليل العمليات

جدول المحتويات

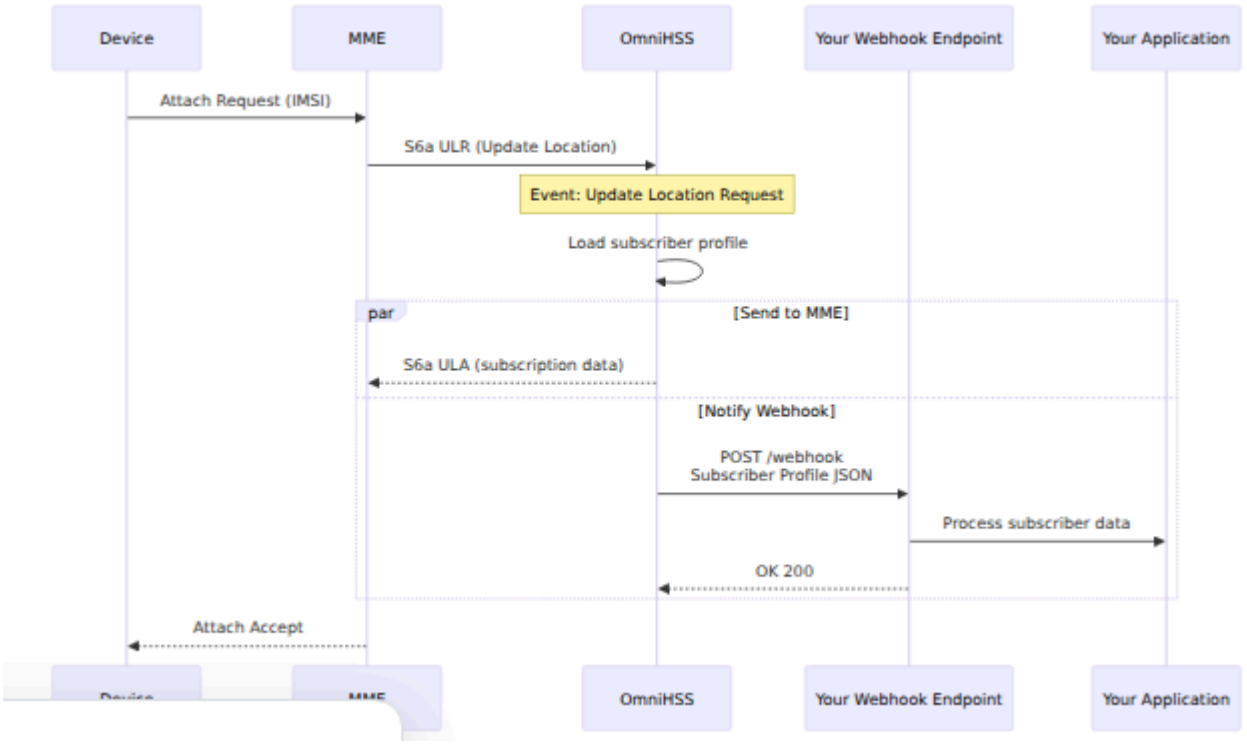
- نظرة عامة
- كيف تعمل Webhooks
- أحداث Webhook
- حمولة Webhook
- التكوين
- حالات الاستخدام
- اعتبارات الأمان
- استكشاف الأخطاء وإصلاحها

نظرة عامة

يدعم OmniHSS **webhooks** لإخطار الأنظمة الخارجية حول أحداث المشتركين في الوقت الحقيقي. عندما تحدث أحداث معينة (مثل تحديثات الموقع، طلبات المصادقة، أو تسجيلات IMS)، يمكن لـ OmniHSS إرسال طلب HTTP POST إلى نقطة النهاية المحددة لـ webhook الخاصة بك مع بيانات ملف تعريف المشترك الكامل.

ما هي Webhooks؟

Webhooks هي ردود HTTP تتيح لـ OmniHSS دفع إشعارات الأحداث إلى تطبيقك أثناء حدوثها، بدلاً من الحاجة إلى تطبيقك لاستعلام واجهة برمجة التطبيقات HSS عن التغييرات.



الفوائد الرئيسية

- **إشعارات في الوقت الحقيقي** - احصل على تحديثات فورية عند حدوث أحداث المشتركين
- **بيانات مشترك كاملة** - يتضمن كل webhook ملف تعريف المشترك الكامل (نفسه كـ `GET /api/subscriber`)
- **أتمتة مدفوعة بالأحداث** - قم بتحفيز سير العمل، التحليلات، أو الت Provisioning بناءً على أحداث الشبكة
- **تقليل الاستعلامات** - لا حاجة للاستعلام المستمر عن واجهة برمجة التطبيقات لتغييرات حالة المشترك
- **مرونة التكامل** - ربط OmniHSS بأنظمة الفوترة، منصات التحليلات، أو التطبيقات المخصصة

كيف تعمل Webhooks

تدفق الأحداث

1. **يحدث الحدث** - يقوم المشترك بإجراء (التوصيل، تحديث الموقع، تسجيل IMS، إلخ)
2. **يعالج الحدث** - يتعامل OmniHSS مع طلب/استجابة Diameter بشكل طبيعي **HSS**

3. **يتم تحفيز Webhook** - إذا تم تسجيل webhook لهذا النوع من الأحداث، يرسل HSS HTTP POST إلى نقطة النهاية الخاصة بك
4. **تتضمن بيانات المشترك** - تحتوي حمولة webhook على ملف تعريف المشترك الكامل كـ JSON
5. **تستجيب تطبيقك** - يجب أن تعيد نقطة النهاية الخاصة بك HTTP 200-299 لتأكيد الاستلام

ضمانات التسليم

- **تسليم بأفضل جهد** - يتم إرسال webhooks بشكل غير متزامن ولا تعيق العمليات الشبكية
- **مهلة** - تنتهي مهلة طلبات webhook بعد 5 ثوانٍ
- **لا إعادة محاولات** - إذا كانت نقطة النهاية الخاصة بك غير متاحة أو تعيد خطأ، فلن يتم إعادة محاولة webhook
- **ترتيب غير مضمون** - قد تصل الأحداث بترتيب غير صحيح تحت حمل عالي

مهم: العمليات الشبكية (المصادقة، تحديثات الموقع، إلخ) **لا** تعتمد على تسليم webhook. إذا كانت نقطة النهاية الخاصة بك معطلة، يستمر خدمة المشترك بشكل طبيعي.

أحداث Webhook

يمكن لـ OmniHSS تحفيز webhooks للأحداث التالية:

أحداث EPC/LTE

الحدث	الزناد	الوصف
`update_location_request`	S6a ULR	يقوم المشترك بالتوصيل أو إجراء تحديث منطقة التتبع
`authentication_information_request`	S6a AIR	تطلب الشبكة متجهات المصادقة للمشترك
`purge_request`	S6a PUR	يقوم MME بإزالة سياق المشترك (الجهاز مغلق، مفصول)
`cancel_location_answer`	S6a CLA	يعترف MME بإلغاء تسجيل المشترك

أحداث IMS

الحدث	الزناد	الوصف
`ims_registration`	Cx SAR	يسجل المشترك لخدمة IMS/VoLTE
`ims_deregistration`	Cx SAR (de-reg)	يلغي المشترك تسجيله من IMS
`ims_profile_request`	Sh UDR	يطلب خادم التطبيق ملف تعريف IMS للمشترك

أحداث السياسة (PCRF)

الحدث	الزناد	الوصف
`policy_request`	Gx CCR	يطلب P-GW سياسة لجلسة بيانات المشترك
`media_authorization`	Rx AAR	يطلب P-CSCF تفويض الوسائط لمكالمة IMS

أحداث Multi-IMSI

الحدث	الزناد	الوصف
`imsi_switch`	ULR لـ IMSI مختلف على نفس SIM	يقوم الجهاز بالتبديل إلى IMSI مختلف على SIM متعدد IMSI

حمولة Webhook

تنسيق الطلب

عند حدوث حدث، يرسل OmniHSS طلب HTTP POST إلى عنوان URL الخاص بـ webhook الذي قمت بتكوينه:

```
POST /your-webhook-endpoint HTTP/1.1
Host: your-server.com
Content-Type: application/json
X-OmniHSS-Event: update_location_request
X-OmniHSS-Event-ID: 550e8400-e29b-41d4-a716-446655440000
X-OmniHSS-Timestamp: 2025-01-15T14:30:00Z

{
  "event": "update_location_request",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "timestamp": "2025-01-15T14:30:00Z",
  "subscriber": {
    "id": "d290f1ee-6c54-4b01-90e6-d701748f0851",
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "msisdns": [
      {"id": "16fd2706-8baf-433b-82eb-8c7fada847da", "msisdn":
"14155551001"},
      {"id": "27ae3807-9cbf-4a4c-93fc-9d8afdb958eb", "msisdn":
"14155551002"}
    ],
    "sim": {
      "id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
      "iccid": "8991101200003204510",
      "is_esim": false
    },
    "key_set": {
      "id": "6ba7b810-9dad-41d1-80b4-00c04fd430c8",
      "amf": "8000"
    },
    "epc_profile": {
      "id": "e58ed763-928c-4155-bee9-fdbaaadc15f3",
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    },
    "ims_profile": {
      "id": "7c9e6679-7425-40de-944b-e07fc1f90ae7",
      "name": "Standard VoLTE"
    },
    "roaming_profile": {
      "id": "9c858901-8a57-4791-81fe-4c455b099bc9",
```

```
      "name": "International Roaming Allowed"
    },
    "subscriber_state": {
      "mme_host": "mme-01.example.com",
      "mme_realm": "epc.mnc001.mcc001.3gppnetwork.org",
      "visited_plmn": "001001",
      "last_update": "2025-01-15T14:30:00Z"
    },
    "custom_attributes": {
      "account_type": "premium",
      "billing_plan": "unlimited"
    }
  },
  "event_context": {
    "visited_plmn": "310410",
    "mme_host": "mme-roaming.example.com",
    "location_update_type": "initial_attach"
  }
}
```

هيكل الحمولة

الحقل	النوع	الوصف
`event`	string	نوع الحدث (مثل `update_location_request`)
`event_id`	string	UUID فريد لتسليم هذا webhook
`timestamp`	string	طابع زمني ISO 8601 عند حدوث الحدث
`subscriber`	object	**ملف تعريف المشترك الكامل** (نفسه كـ `GET /api/subscriber/:id`)
`event_context`	object	بيانات سياق إضافية خاصة بالحدث

حقول سياق الحدث

يحتوي كائن `event_context` على معلومات خاصة بالحدث:

`update_location_request`:

```
{
  "visited_plmn": "310410",
  "mme_host": "mme-roaming.example.com",
  "mme_realm": "epc.mnc410.mcc310.3gppnetwork.org",
  "location_update_type": "initial_attach"
}
```

`imsi_switch`:

```
{
  "previous_imsi": "001001111111111",
  "new_imsi": "310410222222222",
  "sim_id": "3f2504e0-4f89-41d3-9a0c-0305e82c3301",
  "previous_mme_host": "mme-home.example.com",
  "new_mme_host": "mme-roaming.example.com"
}
```

`ims_registration`:

```
{
  "scscf_host": "scscf-01.ims.example.com",
  "public_identities": [
    "sip:001001123456789@ims.mnc001.mcc001.3gppnetwork.org",
    "sip:+14155551001@ims.example.com",
    "tel:+14155551001"
  ]
}
```

رؤوس HTTP

الرأس	الوصف	المثال
`Content-Type`	دائمًا `application/json`	`application/json`
`X-OmniHSS-Event`	نوع الحدث	`update_location_request`
`X-OmniHSS-Event-ID`	معرف الحدث الفريد	UUID
`X-OmniHSS-Timestamp`	طابع زمني للحدث	تنسيق ISO 8601
`User-Agent`	إصدار OmniHSS	`OmniHSS/1.0`

التكوين

تسجيل Webhooks

يتم تكوين webhooks عبر واجهة برمجة التطبيقات OmniHSS.

تسجيل Webhook

```
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": [
        "update_location_request",
        "ims_registration",
        "imsi_switch"
      ],
      "enabled": true,
      "description": "Webhook لـنظام الـفوترة الإنـتاجي"
    }
  }'
```

الاستجابة:

```
{
  "data": {
    "id": "4e5d6c7b-8a9f-4b0c-8d1e-2f3a4b5c6d7e",
    "url": "https://your-server.com/omnihss-webhook",
    "events": [
      "update_location_request",
      "ims_registration",
      "imsi_switch"
    ],
    "enabled": true,
    "description": "Webhook لـنظام الـفوترة الإنـتاجي",
    "created_at": "2025-01-15T14:00:00Z"
  }
}
```

قائمة Webhooks

```
curl -k https://hss.example.com:8443/api/webhook
```

تحديث Webhook

```
curl -k -X PUT https://hss.example.com:8443/api/webhook/4e5d6c7b-
8a9f-4b0c-8d1e-2f3a4b5c6d7e \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "enabled": false
    }
  }'
```

حذف Webhook

```
curl -k -X DELETE
https://hss.example.com:8443/api/webhook/4e5d6c7b-8a9f-4b0c-8d1e-
2f3a4b5c6d7e
```

متطلبات نقطة نهاية Webhook

يجب أن تكون نقطة نهاية webhook الخاصة بك:

1. **تقبل طلبات POST** مع `Content-Type: application/json`
2. **تستجيب بسرعة** - إعادة HTTP 200-299 خلال 5 ثوانٍ
3. **تكون idempotent** - التعامل مع التسليمات المكررة بشكل جيد
4. **تستخدم HTTPS** - استخدم نقاط نهاية TLS/SSL (موصى به) لأمان،
5. **التحقق من الحمولة** - تحقق من أن الطلب من OmniHSS (انظر قسم الأمان)

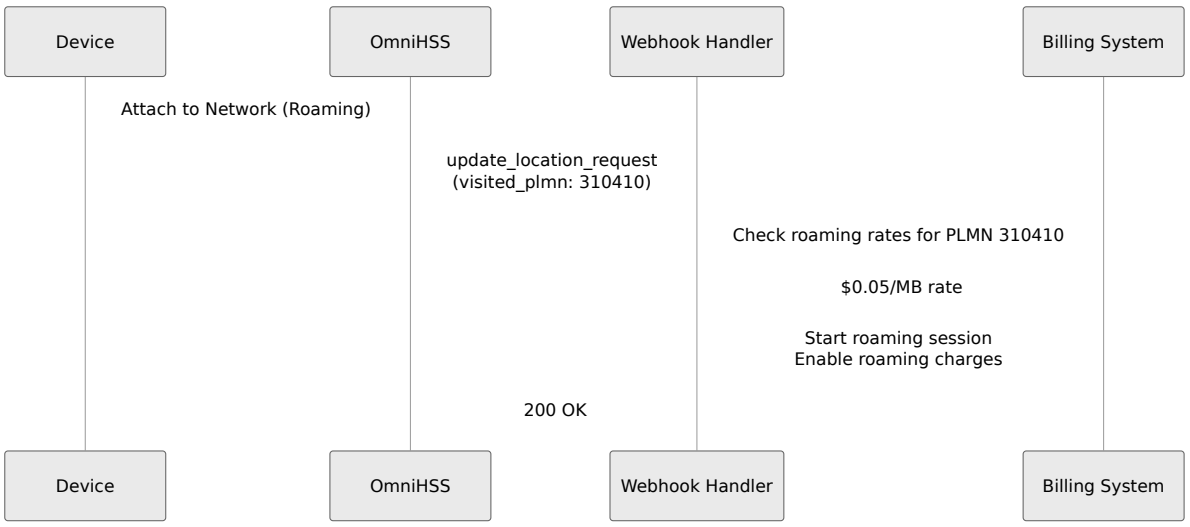
مثال على معالج Webhook (Node.js/Express):

```
const express = require('express');
const app = express();

app.post('/omnihss-webhook', express.json(), (req, res) => {
  const { event, subscriber, event_context } = req.body;

  console.log(`Received event: ${event}`);
  console.log(`Subscriber IMSI: ${subscriber.imsi}`);

  // معالجة بيانات المشترك
  // ... منطق العمل الخاص بك هنا ...

  // الرد فورًا لتأكيد الاستلام
  res.status(200).json({ received: true });

  // التعامل مع المعالجة غير المتزامنة بعد الرد
  processWebhook(req.body).catch(console.error);
});

async function processWebhook(payload) {
  // منطق المعالجة غير المتزامنة الخاص بك
  // مثل تحديث نظام الفوترة، تحفيز التحليلات، إلخ.
}

app.listen(3000);
```

حالات الاستخدام

1. الفوترة وتتبع الاستخدام في الوقت الحقيقي

تتبع استخدام الشبكة للمشتركين وتحفيز أحداث الفوترة في الوقت الحقيقي.



الفوائد:

- اكتشاف فوري عندما يتجول المشتركون دوليًا
- تطبيق رسوم التجوال المناسبة في الوقت الحقيقي
- تتبع أوقات بدء/إنهاء الجلسة بدقة
- توليد تنبيهات الاستخدام عند الوصول إلى العتبات

2. التحليلات والمراقبة

تغذية بيانات نشاط المشتركين إلى منصات التحليلات من أجل لوحات المعلومات والتقارير في الوقت الحقيقي.

حالة الاستخدام: تتبع المشتركين النشطين حسب المنطقة

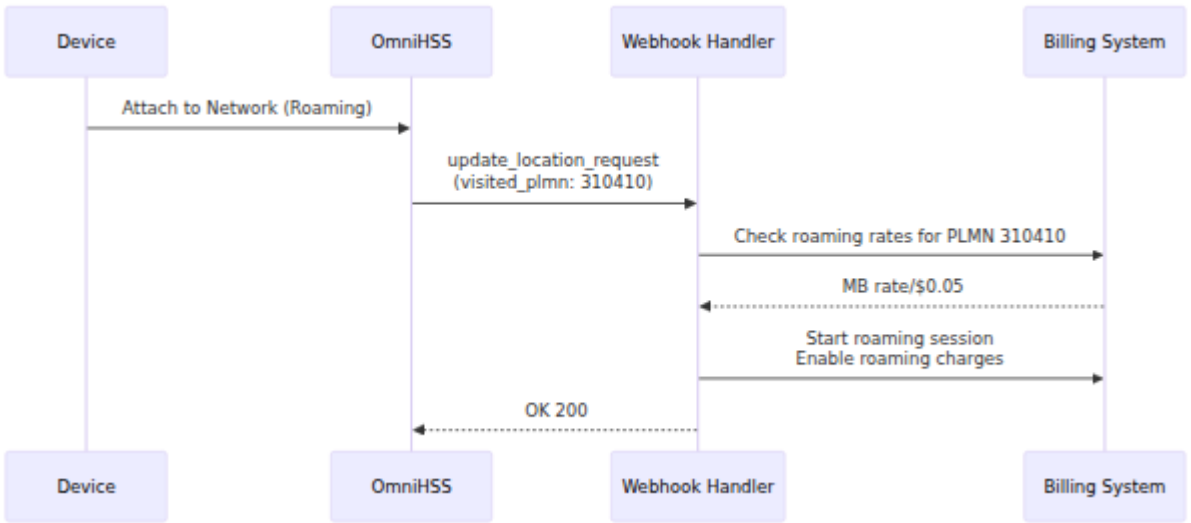
```
// معالج Webhook يغذي البيانات إلى منصة التحليلات
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'update_location_request') {
    await analytics.track({
      event: 'subscriber_location_update',
      imsi: subscriber.imsi,
      visited_plmn: event_context.visited_plmn,
      timestamp: req.body.timestamp,
      profile: subscriber.epc_profile.name
    });
  }

  res.status(200).send();
});
```

لوحة تحكم التحليلات:

- المشتركين النشطين لكل MME
- المشتركين المتجولين حسب الدولة
- توزيع مستوى الخدمة
- معدلات نجاح تسجيل IMS

3. اكتشاف الاحتيال والأمان

اكتشاف أنماط النشاط المشبوهة في الوقت الحقيقي وتحفيز الاستجابات التلقائية.



سيناريوهات اكتشاف الاحتيال:

1. **تغييرات سريعة في الموقع**
    - يتصل المشترك في الدولة A
    - بعد 30 دقيقة، يتصل في الدولة B (غير ممكن جسديًا)
    - الإجراء: وضع علامة على الحساب، إرسال تنبيه إلى فريق الأمان
2. **إساءة استخدام تبديل IMSI**
    - تبديلات IMSI سريعة متعددة على نفس SIM
    - احتمال استنساخ SIM أو استخدام متعدد IMSI غير مصرح به
    - الإجراء: تعطيل جميع IMSIs على SIM، إخطار فريق الاحتيال
3. **التجوال غير المصرح به**
    - يتجول المشترك إلى دولة محظورة (عقوبات، خطر احتيال)
    - الإجراء: تعطيل المشترك تلقائيًا، حظر الوصول إلى الشبكة

تنفيذ المثال:

```
@app.route('/omnihss-webhook', methods=['POST'])
def webhook_handler():
    data = request.json
    subscriber = data['subscriber']
    event_context = data.get('event_context', {})

    if data['event'] == 'update_location_request':
        visited_plmn = event_context.get('visited_plmn')

        # التحقق من البلدان المحظورة
        if visited_plmn in BLOCKED_PLMNS:
            disable_subscriber(subscriber['imsi'])
            alert_security_team(subscriber, 'Roaming to blocked
PLMN')

        # التحقق من السفر المستحيل
        if is_impossible_travel(subscriber['imsi'], visited_plmn):
            flag_for_review(subscriber['imsi'])
            alert_fraud_team(subscriber, 'Impossible travel
detected')

    return jsonify({'status': 'ok'}), 200
```

4. أتمتة الت Provisioning

توفير أو تحديث خدمات المشتركين تلقائيًا بناءً على أحداث الشبكة.

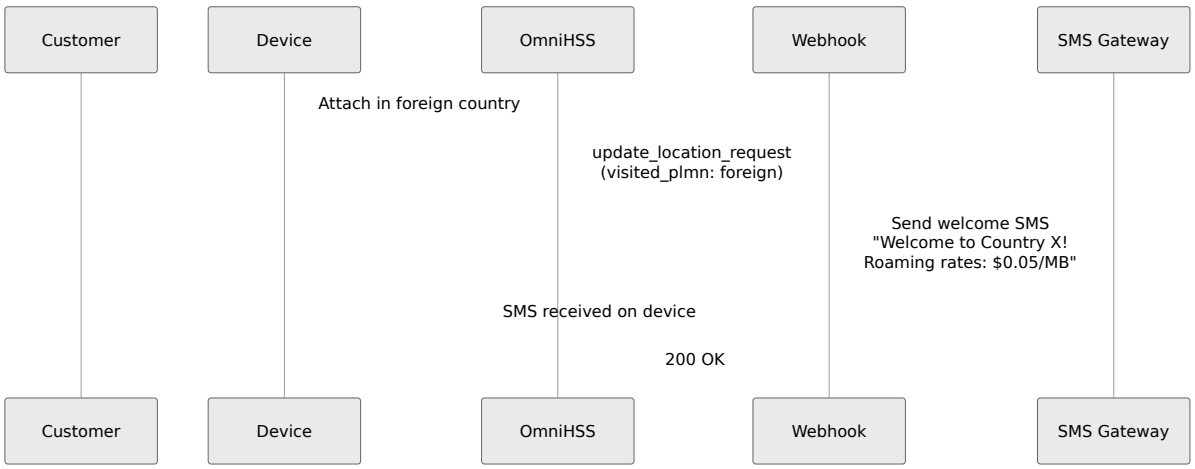
تمكين **حالة الاستخدام:** IMS تلقائيًا عندما يستخدم المشترك VoLTE لأول مرة

```
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber } = req.body;

  if (event === 'ims_registration' && !subscriber.ims_enabled) {
    // تمكين IMS لأول مرة - بشكل دائم IMS مستخدم
    await omnihss.updateSubscriber(subscriber.id, {
      ims_enabled: true,
      custom_attributes: {
        ...subscriber.custom_attributes,
        volte_activated_at: new Date().toISOString()
      }
    });

    // تحديث CRM
    await crm.updateCustomer(subscriber.imsi, {
      features: ['volte']
    });
  }

  res.status(200).send();
});
```

5. إشعارات العملاء

إرسال إشعارات في الوقت الحقيقي للعملاء حول خدمتهم.

حالة الاستخدام: رسالة ترحيبية عند التجوال دوليًا



إشعارات المثال:

- "مرحبًا بك في [البلد]! تنطبق رسوم التجوال."
- "لقد استخدمت 80% من حد بياناتك"
- "الآن على جهازك VoLTE تم تفعيل خدمة"
- "تم ترقية حسابك إلى Premium"

6. إدارة SIM متعددة IMSI

تتبع وإدارة المشتركين الذين لديهم SIM متعددة IMSI، وتلقي الإشعارات عند تبديلهم IMSIs.

```
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'imsi_switch') {
    const { previous_imsi, new_imsi, sim_id } = event_context;

    // تسجيل تبديل IMSI للتحليلات
    await db.logImsiSwitch({
      sim_id,
      from_imsi: previous_imsi,
      to_imsi: new_imsi,
      timestamp: req.body.timestamp
    });

    // تحديث نظام الفوترة
    await billing.endSession(previous_imsi);
    await billing.startSession(new_imsi);

    // تنبيه إذا كان التبديل مفرطًا (احتمال الاحتيال)
    const switchCount = await db.getSwitchCount(sim_id, '24h');
    if (switchCount > 10) {
      await alertFraudTeam(`Excessive IMSI switching: SIM
${sim_id}`);
    }
  }

  res.status(200).send();
});
```

7. التكامل مع الأنظمة الخارجية

ربط OmniHSS بالأنظمة الخارجية دون الحاجة للاستعلام.

التكاملات المثال:

- **أنظمة CRM** - تحديث سجلات العملاء باستخدام الخدمة
- **مراقبة الشبكة** - تغذية بيانات المشتركين إلى منصات تحليلات الشبكة
- **أنظمة الفوترة** - تحفيز الرسوم بناءً على أحداث الشبكة
- **أنظمة التذاكر** - إنشاء تذاكر تلقائيًا لفشل المصادقة
- **مخازن البيانات** - تدفق أحداث المشتركين للتحليل الكبير

اعتبارات الأمان

Webhook سر/توقيع

للتحقق من أن webhooks تأتي من OmniHSS، نفذ التحقق من التوقيع:

```
# تكوين webhook مع السر
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": ["update_location_request"],
      "secret": "your-secret-key-here"
    }
  }'
```

ستتضمن OmniHSS رأس `X-OmniHSS-Signature`:

```
X-OmniHSS-Signature:
sha256=5d7a8f9b2c1e3a4d6f7e8b9c0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a
```

تحقق من التوقيع:

```
const crypto = require('crypto');

function verifyWebhook(req) {
  const signature = req.headers['x-omnihss-signature'];
  const secret = process.env.WEBHOOK_SECRET;
  const payload = JSON.stringify(req.body);

  const expectedSignature = 'sha256=' +
    crypto.createHmac('sha256', secret)
      .update(payload)
      .digest('hex');

  return crypto.timingSafeEqual(
    Buffer.from(signature),
    Buffer.from(expectedSignature)
  );
}

app.post('/omnihss-webhook', (req, res) => {
  if (!verifyWebhook(req)) {
    return res.status(401).json({ error: 'Invalid signature' });
  }

  // معالجة webhook...
  res.status(200).send();
});
```

أفضل الممارسات

1. **استخدم HTTPS** - استخدم دائمًا TLS لنقاط نهاية webhook
2. **تحقق من التوقيعات** - تحقق من توقيعات webhook لمنع التزوير
3. **تحديد معدل** - نفذ تحديد معدل على نقاط نهاية webhook
4. **قائمة السماح IP** - قيد وصول webhook إلى عناوين IP الخاصة بـ OmniHSS
5. **مراقبة الفشل** - تتبع فشل تسليم webhook والأخطاء
6. **تنظيف البيانات** - تحقق من صحة وتنظيف حمولة webhook قبل المعالجة
7. **تأمين بيانات الاعتماد** - تخزين أسرار webhook في تكوين آمن (متغيرات البيئة، مدير الأسرار)

خصوصية البيانات

تحتوي حمولة webhook **معلومات حساسة عن المشتركين** على:

- IMSI (هوية المشترك)
- MSISDNs (أرقام الهواتف)
- بيانات الموقع (PLMN الذي تمت زيارته، MME)
- معلومات ملف تعريف الخدمة

متطلبات الامتثال:

- **GDPR** - تأكد من معالجة بيانات webhook وفقًا لـ GDPR
- **احتفاظ البيانات** - تنفيذ سياسات احتفاظ البيانات المناسبة
- **التحكم في الوصول** webhook - قيد وصول نقطة نهاية
- **التشفير** TLS لنقل webhook - استخدم
- **تسجيل التدقيق** webhook للامتثال - سجل جميع تسليمات

استكشاف الأخطاء وإصلاحها

لم يتم استلام Webhook

الأعراض:

- webhook تحدث الأحداث ولكن لم يتم تحفيز
- أي طلبات webhook لم تتلق نقطة نهاية

خطوات استكشاف الأخطاء:

1. **تحقق من تمكين webhook:**

   ```
   curl -k https://hss.example.com:8443/api/webhook
   # تحقق من "enabled": true
   ```

2. **تحقق من تكوين أحداث webhook:**

- تأكد من تضمين نوع الحدث في قائمة `events` الخاصة بـ webhook
- تحقق من أنها في `ims_registration`، مثال: إذا كنت تريد أحداث مصفوفة الأحداث

3. **مراجعة سجلات HSS:**
   - تحقق من أخطاء تسليم webhook
   - ابحث عن مشاكل الاتصال بالشبكة
   - تحقق من عدم وجود فشل في حل DNS
4. **اختبار وصول نقطة النهاية:**

```
curl -X POST https://your-server.com/omnihss-webhook \
  -H "Content-Type: application/json" \
  -d '{"test": true}'
```

انتهاء مهلة webhook

الأعراض:

- أخطاء انتهاء مهلة webhook تظهر سجلات HSS
- تعتبره فاشلاً HSS الطلب ولكن webhook تتلقى نقطة نهاية

الحل:

1. **الرد فوراً:**
   - أعد HTTP 200 في غضون 5 ثوانٍ
   - معالجة البيانات بشكل غير متزامن بعد الرد
2. **تحسين أداء نقطة النهاية:**

```
// سيء - معالجة متزامنة بطيئة
app.post('/webhook', (req, res) => {
  processData(req.body); // يحجب لمدة 10 ثوانٍ
  res.status(200).send();
});

// جيد - معالجة غير متزامنة بعد الرد
app.post('/webhook', (req, res) => {
  res.status(200).send(); // الرد فوراً
  processData(req.body); // معالجة غير متزامنة
});
```

webhooks المكررة

الأعراض:

- يتم تسليم نفس الحدث عدة مرات
- `event_id` هو نفسه للتسليمات المكررة

السبب:

- لا تعيد المحاولة، قد تعيد البنية التحتية OmniHSS على الرغم من أن) محاولات الشبكة للشبكة المحاولة)
- تم تسجيل عدة webhooks لنفس الحدث

الحل:

تنفيذ عدم التكرار باستخدام `event_id`:

```
const processedEvents = new Set();

app.post('/omnihss-webhook', (req, res) => {
  const eventId = req.body.event_id;

  if (processedEvents.has(eventId)) {
    // تمت معالجته بالفعل، تخطي
    return res.status(200).json({ status: 'duplicate' });
  }

  processedEvents.add(eventId);

  // معالجة webhook...
  processWebhook(req.body);

  res.status(200).json({ status: 'processed' });
});
```

webhook يعيد خطأ

الأعراض:

- نقطة النهاية تعيد HTTP 4xx أو 5xx
- سجلات HSS تفشل في تسليم webhook

الأخطاء الشائعة:

1. **401 غير م��رح** - فشل التحقق من التوقيع
   - تحقق من أن سر webhook يتطابق مع التكوين
   - تحقق من خوارزمية حساب التوقيع
2. **400 طلب غير صالح** - حمولة غير صالحة
   - تحقق من تحليل حمولة webhook
   - تأكد من معالجة رأس Content-Type
3. **500 خطأ داخلي في الخادم** - تعطل نقطة النهاية
   - مراجعة سجلات خطأ نقطة النهاية

- إضافة معالجة الأخطاء والتسجيل

الحل:

إضافة معالجة أخطاء شاملة:

```
app.post('/omnihss-webhook', async (req, res) => {
  try {
    // تحقق من التوقيع
    if (!verifyWebhook(req)) {
      return res.status(401).json({ error: 'Invalid signature' });
    }

    // تحقق من الحمولة
    if (!req.body.event || !req.body.subscriber) {
      return res.status(400).json({ error: 'Invalid payload' });
    }

    // معالجة webhook
    await processWebhook(req.body);

    res.status(200).json({ status: 'ok' });

  } catch (error) {
    console.error('خطأ في معالجة webhook:', error);
    // أعد 200 لمنع إعادة المحاولة، سجل الخطأ للتحقيق
    res.status(200).json({ status: 'error', message: error.message
});
  }
});
```

بيانات المشترك المفقودة

الأعراض:

- تم استلام webhook ولكن كائن المشترك غير مكتمل
- الحقول المتوقعة فارغة أو مفقودة

الأسباب المحتملة:

1. **لم يتم تجهيز المشترك بالكامل** (IMS، التجوال) - قد تكون بعض الملفات الشخصية اختيارية
2. **حالة سباق البيانات** webhook - تم تحديث المشترك بين حدث التشغيل وإرسال

الحل:

التعامل مع الحقول الاختيارية بشكل لطيف:

```
const { subscriber } = req.body;

// تحقق من الحقول الاختيارية
const imsProfile = subscriber.ims_profile || { name: 'No IMS' };
const roamingProfile = subscriber.roaming_profile || { name: 'No
Roaming' };

// التعامل مع MSISDNs المفقودة
const msisdns = subscriber.msisdns || [];
```

المراقبة والرؤية

مقاييس webhook

تتبع أداء webhook وموثوقيته:

المقاييس التي يجب مراقبتها:

- معدل تسليم webhook (ناجح مقابل فاشل)
- زمن استجابة webhook (الوقت من الحدث إلى استجابة نقطة النهاية)
- أوقا�ة استجابة نقطة النهاية
- معدلات الأخطاء حسب نقطة النهاية
- الأحداث في الثانية

استعلام لوحة المعلومات (Prometheus/Grafana):

```
# معدل نجاح webhook
rate(omnihss_webhook_success_total[5m]) /
rate(omnihss_webhook_attempts_total[5m])

# زمن استجابة webhook
histogram_quantile(0.95, omnihss_webhook_duration_seconds)
```

سجلات webhook

تمكين تسجيل webhook التفصيلي لأغراض استكشاف الأخطاء وإصلاحها:

تنسيق السجل:

```
{
  "timestamp": "2025-01-15T14:30:00Z",
  "level": "info",
  "component": "webhook",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "webhook_id": "4e5d6c7b-8a9f-4b0c-8d1e-2f3a4b5c6d7e",
  "event_type": "update_location_request",
  "subscriber_imsi": "001001123456789",
  "endpoint": "https://your-server.com/omnihss-webhook",
  "http_status": 200,
  "duration_ms": 145,
  "error": null
}
```

العودة إلى دليل العمليات API → | التالي: مرجع ←