OmniEIR مرجع تكوين

نظرة عامة | دليل العمليات | المقاييس والمراقبة | استكشاف الأخطاء

يمكن تجاوز مجموعة فرعية من تعيش جميع تكوينات OmniEIR تحت مفتاح التطبيق `:omnieir`. المفاتيح بواسطة متغيرات البيئة، ولكن ذلك ساري المفعول فقط في **تكوين وقت تشغيل الإنتاج** (`config/runtime.exs`).

هيكل التكوين

```
config :omnieir,
  # هوية مستمع SBI (إلى المعلن NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.23",
  sbi_port: 7777,

  # تسجيل NRF
  nrf_uri: "http://127.0.0.10:7777",
  heartbeat_interval: 10_000,

  # PLMN (تجاوز لكل نشر) المقدم
  mcc: "999",
  mnc: "70",

  # واجهة برمجة التطبيقات REST لـ OmniHSS التي تحتوي على قواعد EIR
الخاصة بالمشغل
  hss_api_base_url: "https://127.0.0.1:8443",

  # مفتاح واجهة برمجة التطبيقات لـ OmniHSS (دور eir_lookup).
إلزامي، لا يوجد افتراضي.
  hss_api_key: "<مفتاح واجهة برمجة التطبيقات لـ OmniHSS مع دور
eir_lookup>",

  # الحكم الذي يتم إرجاعه عندما لا تتطابق أي قاعدة مع المعدات
المقدمة
  unknown_equipment_status: "WHITELISTED"
```

المعلمات الأساسية

المعلمة	النوع	الافتراضي	
`sbi_scheme`	سلسلة	`"http"`	`EIR_SB`
`sbi_addr`	سلسلة	`"127.0.0.23"`	`EIR_SB`
`sbi_port`	عدد صحيح	`7777`	`EIR_SB`
`nrf_uri`	سلسلة	`"http://127.0.0.10:7777"`	`EIR_NR`
`heartbeat_interval`	عدد صحيح (مللي ثانية)	`10_000`	لا شيء
`mcc`	سلسلة	`"999"`	`EIR_MC`
`mnc`	سلسلة	`"70"`	`EIR_MN`
`hss_api_base_url`	سلسلة	`"https://127.0.0.1:8443"`	`HSS_AP`
`hss_api_key`	سلسلة	لا شيء (مطلوب)	لا شيء

المعلمة	النوع	الافتراضي	
`unknown_equipment_status`	سلسلة	`"WHITELISTED"`	`EIR_UNI`

مما يتطابق مع ،(`verify_none`) في المختبر OmniHSS يتم قبول الشهادة الذاتية التوقيع لـ مستهلكي HSS-REST الآخرين (OmniUDR). قم بإنهاء HSS خلف CA موثوق في الإنتاج.

تستخدم OmniHSS التحكم في الوصول القائم على الدور على واجهة برمجة التطبيقات REST صالح مع `401`. قيمة `x-omnihss-key` الخاصة بها. ترفض الطلب بدون رأس `hss_api_key` بكتابته في السجل. قم بتثبيت هذا الإصدار قبل تمكين التحكم في OmniEIR هي سر. لا تقوم بشكل مفتوح EIR وإلا فإن كل قراءة قاعدة تفشل وتفشل تحقق، OmniHSS الوصول على.

توفير القواعد (OmniHSS)

ليس لدى OmniEIR **واجهة برمجة تطبيقات توفير خاصة به**. يتم إنشاء القواعد ضد OmniHSS، على سبيل المثال، JG لـ S13 4 تمامًا كما هو الحال في واجهة:

```
curl -k -X POST https://<hss>:8443/api/eir/rule \
  -H 'content-type: application/json' \
  -d '{"action":"blacklist","regex":"^35316005"}'
```

- `action` هو واحد من `whitelist`، `blacklist`، `greylist`.
- `regex` يتم مطابقته مع سلسلة هوية المعدات. يتم تقييم القواعد بالترتيب الذي تعيده OmniHSS؛ الفائز هو أول تطابق.

تكوين جانب AMF (تفعيل الفحص)

وهو **معطل افتراضيًا** حتى لا تتأثر النشر الحالية. قم، **AMF** يتم تنفيذ فحص المعدات بواسطة بتمكينه تحت مفتاح `:omniamf`:

المعلمة	النوع	الافتراضي	الوصف
`eir_enabled`	بولياني	`false`	عندما يكون `true`، يستعلم AMF 5 عنG-EIR المدرجة في PEIs أثناء التسجيل ويرفض القائمة السوداء.
`eir_uri`	سلسلة | nil	`nil`	URI 5 ثابت لـG-EIR SBI. عندما يكون `nil`، يكتشف AMF EIR عبر NRF (NFType `5G_EIR`).

```
config :omniamf,
  eir_enabled: true
  # eir_uri: "http://127.0.0.23:7777"   # اختياري؛ احذفه لاستخدام اكتشاف NRF
```

OmniEIR مقاييس ومراقبة

نظرة عامة | مرجع التكوين | دليل العمليات | استكشاف الأخطاء وإصلاحها

Prometheus نقطة نهاية

تقوم OmniEIR بتعريض نقطة نهاية سحب Prometheus عبر `TelemetryMetricsPrometheus` على `prometheus_metrics_port` (الافتراضي **9572**):

```
GET http://<eir-host>:9572/metrics
```

بحيث يبقى عدد السلاسل (`nf_type` / `result` / `status`) جميع التسميات ذات كثافة منخفضة محدودًا.

المقاييس

المقياس	النوع	التسميات	
`omni_eir_equipment_check_count`	عداد	`status`	المعدات حسب حالة `EquipmentStatus` (`WHITELISTED`/`BL`
`omni_eir_hss_request_count`	عداد	`result`	قراءات OmniHSS (حسب النتيجة (`succ`
`omni_eir_hss_request_duration_ms`	مقياس	`result`	لأحدث قراءة لقواعد EIR.
`omni_eir_nrf_registration_status`	مقياس	`nf_type`	حالة تسجيل NRF (1
`beam_*`	مقياس	لا شيء	إحصائيات BEAM VM منافذ، وقت التشغيل)

أحداث القياس الأساسية

الحدث	القياسات	البيانات الوصفية	المصدر
`[:omnieir, :equipment_check]`	`count`	`status`	عند كل OmniEIR حكم محلل
`[:omnieir, :hss, :request]`	`count`, `duration_ms`	`endpoint`, `result`	عند كل OmniEIR `GET /api/eir/rule` إلى OmniHSS
`[:omniamf, :eir, :check]`	`count`	`result` (`:whitelisted` | `:greylisted` | `:blacklisted` | `:unknown` | `:error`)	عند كل AMF الـ فحص للمعدات

كما يقوم الـ AMF بإصدار حدثه الحالي `[:omniamf, :registration, :result]` مع `result: :rejected` عندما يمنع PEI المدرج في القائمة السوداء التسجيل. (تسلسل `[:omniamf, :eir, :check]` متاح على **نقطة نهاية** Prometheus الخاصة بـ AMF، وليس OmniEIR.)

ما يجب مراقبته

- زيادة معدل `[:omnieir, :hss, :request]` مع `result: :failure` تعني أن OmniEIR لا يمكنه الوصول إلى OmniHSS. ثم يفشل الـ AMF (كل جهاز في الفتح مسموح). يجب التنبيه على ذلك.
- `[:omniamf, :eir, :check]` مع `result: :blacklisted` يعد عدد الأجهزة المحظورة؛ و `:error` يعد أحداث الفشل المفتوح في الـ AMF.

السجلات

تقوم OmniEIR والـ AMF بتسجيل كل قرار. السطور الملحوظة:

- AMF: `5G-EIR returned BLACKLISTED for PEI <pei> (<supi>); barring registration`
- AMF: `5G-EIR check failed for <supi> (<reason>); failing open`
- OmniEIR: `Could not read EIR rules from HSS: <reason>`

OmniEIR دليل عمليات

نظرة عامة | مرجع التكوين | المقاييس والمراقبة | استكشاف الأخطاء وإصلاحها

الدور

OmniEIR 5 هو سجل هوية معدات 3GPP. أثناء تسجيل UE، يسأل AMF عما إذا كانت PEI (IMEI/IMEISV) للجهاز مسموح بها؛ تعيد OmniEIR `WHITELISTED` أو `BLACKLISTED` أو `GREYLISTED`. يتم حساب الحكم من قواعد المشغل المحتفظ بها في OmniHSS.

نقاط النهاية

يقدم مستمع SBI خدمة N5g-eir_EquipmentIdentityCheck (TS 29.511):

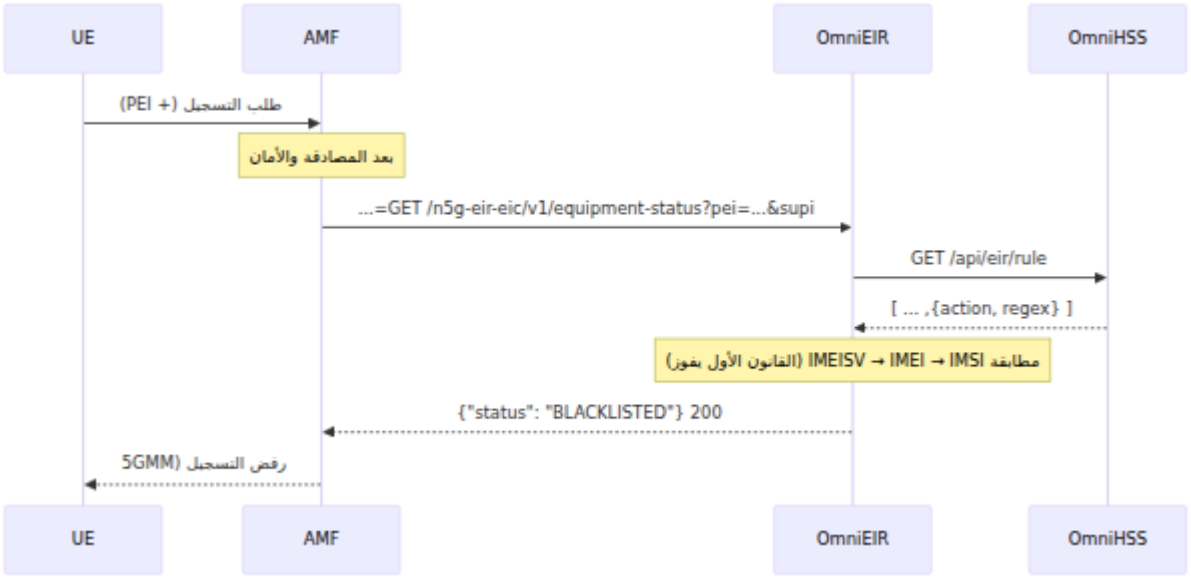
الطريقة	المسار	الوصف
`GET`	`/n5g-eir-eic/v1/equipment-status?pei={pei}&supi={supi}`	يعيد `EirResponseData`: `{"status":"<EquipmentStatus>"}`. `pei` إلزامي؛ `supi` اختياري.
`GET`	`/n5g-eir-eic/v1/status`	اختبار الحضور (`{"status":"UP"}`).

`pei` هو PEI في شكل TS 23.003: `imei-<15 digits>` أو `imeisv-<16 digits>`. `supi` هو `imsi-<digits>`.

مثال:

```
curl 'http://127.0.0.23:7777/n5g-eir-eic/v1/equipment-status?
pei=imei-353160051234567'
# -> {"status":"WHITELISTED"}
```

تدفق الرسائل



التسجيل AMF يواصل، (EIR أو أي خطأ) أو `GREYLISTED` بالنسبة لحكم `WHITELISTED`.

منطق المطابقة

تعكس OmniEIR 4 قرار 3GPP TS 29.513، لذا فإن مجموعة القواعد الواحدة تحكم كل من الراديوهات. بالنظر إلى المعدات المعالجة، تحاول، بالترتيب، وتتوقف عند أول قاعدة تتطابق معها `regex`:

1. سلسلة الأرقام الكاملة **IMEISV** (IMEI + إصدار البرنامج)، ثم
2. **IMEI** فقط، ثم
3. **IMSI** (من SUPI).

إذا لم يتطابق أي شيء، يتم إرجاع `unknown_equipment_status` المكون.

سلوك الفشل المفتوح

فشل مفتوح: إذا كان AMF بوابة جانب EIR مصممة عمداً لتكون غير متاح، أو أعاد خطأ، أو لم يقدم UE أي PEI، فقط حكم `BLACKLISTED` يستمر التسجيل. هذا يمنع EIR الصريح يمنع الجهاز المعطل من عزل كل مشترك. يتطلب النشر الذي يحتاج إلى دلالات الفشل المغلقة تعيين HSS أو OmniEIR على `unknown_equipment_status: "BLACKLISTED"` (لذا يتم حظر الأجهزة غير المتطابقة). لاحظ أن انقطاع EIR الكلي لا يزال يفشل مفتوحًا في AMF حسب التصميم.

التمكين في النشر

1. توفير القواعد في OmniHSS (`POST /api/eir/rule`).
2. بدء OmniEIR مع تأكد من أنه يسجل مع NRF كـ `5G_EIR` ؛ `5`.
3. تعيين `config :omniamf, eir_enabled: true` وإعادة تشغيل AMF.
4. لخط قرار AMF ومراقبة سجلات UE تحقق من خلال إعادة تشغيل الهاتف / إعادة إرفاق `5G-EIR`.

استكشاف أخطاء OmniEIR

نظرة عامة | مرجع التكوين | دليل العمليات | المقاييس والمراقبة

المشكلات الشائعة

يتم السماح لكل جهاز على الرغم من أنني قمت بتوفير قاعدة قائمة سوداء

تحقق، بالترتيب:

1. **هل تم تمكين فحص AMF؟** البوابة مغلقة بشكل افتراضي. قم بتعيين `config :omniamf, eir_enabled: true` وأعد تشغيل AMF. بدون ذلك، لا يستعلم AMF عن OmniEIR.
2. **هل يمكن لـ OmniEIR الوصول إلى OmniHSS؟** الفشل في قراءة `GET /api/eir/rule` يفشل **مفتوحًا** (الجهاز مسموح به). راقب `Could not read EIR rules from HSS` في سجلات OmniEIR و `[:omnieir, :hss, :request]` telemetry مع `result: :failure`. تأكد من `hss_api_base_url`. تع��ي `eir_lookup` تم تعيينه وله دور OmniHSS. تأكد من أن `hss_api_key` أن المفتاح مفقود أو غير معروف لـ HSS `401` تعني أن المفتاح لا OmniHSS. يمتلك الدور `eir_lookup`.
3. **هل يتطابق التعبير العادي مع PEI الذي يقدمه UE؟** يتم مطابقة تعبير القاعدة مكون من 14 رقمًا مع IMEI العادي مع سلسلة الأرقام. لن يتطابق قاعدة مكتوبة لـ PEI مكون من 15 رقمًا ما لم يكن التعبير العادي مثبتًا للسماح بذلك. اختبر التعبير `imei-` العادي ضد الأرقام الدقيقة PEI.
4. **هل استقبل AMF فعلاً PEI؟** إذا لم يقدم UE أي PEI، فإن سجلات AMF `EIR enabled but UE ... presented no PEI; allowing` وتستمر.

جهازًا لم أكن أنوي حظره AMF يرفض

- على سبيل المثال، `3531^` يتطابق مع نطاق) القاعدة أوسع مما هو مقصود `regex` ضيقها. (كامل TAC).
- تم تعيين `unknown_equipment_status` إلى `BLACKLISTED` (فشل مغلق) والجهاز له أو العودة إلى الحالة `whitelist` لا يتطابق مع أي قاعدة. إما إضافة قاعدة

الافتراضية `WHITELISTED`.

`400 MANDATORY_QUERY_PARAM_INCORRECT`

كان معلم الاستعلا`pei` مفقودًا من الطلب إلى `/n5g-eir-eic/v1/equipment-status`. إنه إلزامي (TS 29.511).

`500 SYSTEM_FAILURE` من OmniEIR

لم تتمكن OmniEIR من قراءة مجموعة القواعد من OmniHSS. هذه مشكلة من المصدر (HSS)؛ يتعامل AMF 2 معxx غير كفشل مفتوح. تحقق من صحة OmniHSS و `hss_api_base_url`.

ملاحظات المعمارية

لا تحتوي OmniEIR على واجهة برمجة تطبيقات توفير خاصة بها: تعيش قواعد السماح/الحظر/الرمادي IMEI في OmniHSS (مجموعة قواعد واحدة مشاركة مع واجهة S13 4G)، وتقرأ وتطبق المنطق المطابق المماثل. بوابة HSS REST منها عبر واجهة برمجة تطبيقات OmniEIR هي عملية واحدة للحصول على N5g-eir مفتوحة بالفشل عن تصميم (انظر عمليات)، وخدمة AMF عند وكيل خارجي أمام مستمع TLS قم بإنهاء .TS 29.511 حالة المعدات لكل SBI.