Référence de Configuration OmniEIR

Vue d'ensemble | Guide des Opérations | Métriques et Surveillance | Dépannage

Toute la configuration d'OmniEIR se trouve sous la clé d'application `:omnieir`. Un sous-ensemble de clés peut être remplacé par des variables d'environnement, mais cela ne prend effet que dans la **configuration d'exécution en production** (`config/runtime.exs`).

Structure de Configuration

```
config :omnieir,
  # Identité de l'écouteur SBI (annoncée au NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.23",
  sbi_port: 7777,

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

  # PLMN servi (remplacer par déploiement)
  mcc: "999",
  mnc: "70",

  # API REST OmniHSS contenant les règles EIR de l'opérateur
  hss_api_base_url: "https://127.0.0.1:8443",

  # Clé API OmniHSS (rôle eir_lookup). Obligatoire, pas de valeur
par défaut.
  hss_api_key: "<Clé API OmniHSS avec rôle eir_lookup>",

  # Verdict retourné lorsque aucune règle ne correspond à
l'équipement présenté
  unknown_equipment_status: "WHITELISTED"
```

Paramètres Principaux

Paramètre	Type	Par défaut	
`sbi_scheme`	chaîne	`"http"`	`EIR_SB`
`sbi_addr`	chaîne	`"127.0.0.23"`	`EIR_SB`
`sbi_port`	entier	`7777`	`EIR_SB`
`nrf_uri`	chaîne	`"http://127.0.0.10:7777"`	`EIR_NR`
`heartbeat_interval`	entier (ms)	`10_000`	aucun
`mcc`	chaîne	`"999"`	`EIR_MC`
`mnc`	chaîne	`"70"`	`EIR_MN`
`hss_api_base_url`	chaîne	`"https://127.0.0.1:8443"`	`HSS_AP`
`hss_api_key`	chaîne	Aucun (obligatoire)	Aucun

Paramètre	Type	Par défaut	
`unknown_equipment_status`	chaîne	`"WHITELISTED"`	`EIR_UN`

Le certificat TLS auto-signé du laboratoire OmniHSS est accepté (`verify_none`), correspondant aux autres consommateurs HSS-REST (OmniUDR). Terminez l'HSS derrière une CA de confiance en production.

OmniHSS utilise le contrôle d'accès basé sur les rôles sur son API REST. Il rejette une requête sans un en-tête `x-omnihss-key` valide avec `401`. La valeur de `hss_api_key` est un secret. OmniEIR ne l'écrit pas dans le journal. Installez cette version avant d'activer le contrôle d'accès sur OmniHSS, sinon chaque lecture de règle échoue et la vérification EIR échoue ouvertement.

Provisionnement des règles (OmniHSS)

OmniEIR **n'a pas d'API de provisionnement propre**. Les règles sont créées contre OmniHSS, exactement comme pour l'interface S13 4G, par exemple :

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

- `action` est l'un de `whitelist`, `blacklist`, `greylist`.
- `regex` est comparé à la chaîne d'identité de l'équipement. Les règles sont évaluées dans l'ordre dans lequel OmniHSS les retourne ; le premier match

l'emporte.

Configuration côté AMF (activation de la vérification)

La vérification de l'équipement est effectuée par l'**AMF**, et est **désactivée par défaut** afin que les déploiements existants ne soient pas affectés. Activez-la sous la clé `:omniamf` :

Paramètre	Type	Par défaut	Description
`eir_enabled`	booléen	`false`	Lorsque `true`, l'AMF interroge le 5G-EIR lors de l'enregistrement et rejette les PEI sur liste noire.
`eir_uri`	chaîne | nil	`nil`	URI SBI 5G-EIR statique. Lorsque `nil`, l'AMF découvre l'EIR via le NRF (NFType `5G_EIR`).

```
config :omniamf,
  eir_enabled: true
  # eir_uri: "http://127.0.0.23:7777"   # optionnel ; omettre pour
utiliser la découverte NRF
```

Métriques et Surveillance d'OmniEIR

Vue d'ensemble | Référence de Configuration | Guide des Opérations | Dépannage

Point de terminaison Prometheus

OmniEIR expose un point de terminaison de scraping Prometheus via `TelemetryMetricsPrometheus` sur `prometheus_metrics_port` (par défaut **9572**):

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

Tous les labels ont une faible cardinalité (`status` / `result` / `nf_type`) afin que le nombre de séries reste limité.

Métriques

Métrique	Type	Labels	
`omni_eir_equipment_check_count`	compteur	`status`	Vérifications d `EquipmentSta` (`WHITELISTED`
`omni_eir_hss_request_count`	compteur	`result`	Lectures Omn par résultat (`s`
`omni_eir_hss_request_duration_ms`	jauge	`result`	Latence de la OmniHSS la p
`omni_eir_nrf_registration_status`	jauge	`nf_type`	Statut d'enreg enregistré, 0 =
`beam_*`	jauge	aucun	Statistiques st (mémoire, cor temps de fonc

Événements de télémétrie sous-jacents

Événement	Mesures	Métadonnées	Émis par
`[:omnieir, :equipment_check]`	`count`	`status`	OmniEIR à chaque verdict résolu
`[:omnieir, :hss, :request]`	`count`, `duration_ms`	`endpoint`, `result`	OmniEIR à chaque `GET /api/eir/rule` vers OmniHSS
`[:omniamf, :eir, :check]`	`count`	`result` (`:whitelisted` | `:greylisted` | `:blacklisted` | `:unknown` | `:error`)	L'AMF à chaque vérification d'équipement

L'AMF émet également son événement existant `[:omniamf, :registration, :result]` avec `result: :rejected` lorsqu'un PEI blacklisté empêche un enregistrement. (La série `[:omniamf, :eir, :check]` est exposée sur le point de terminaison Prometheus de l'**AMF**, pas celui d'OmniEIR.)

Ce qu'il faut surveiller

- Un taux croissant de `[:omnieir, :hss, :request]` avec `result: :failure` signifie qu'OmniEIR ne peut pas atteindre OmniHSS. L'AMF échoue alors en mode ouvert (chaque appareil est autorisé). Alertez à ce sujet.
- `[:omniamf, :eir, :check]` avec `result: :blacklisted` compte les appareils interdits ; `:error` compte les événements de fail-open à l'AMF.

Journaux

OmniEIR et l'AMF enregistrent chaque décision. Lignes notables :

- 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>`

Guide des opérations OmniEIR

Vue d'ensemble | Référence de configuration | Métriques et surveillance | Dépannage

Rôle

OmniEIR est le Registre d'Identité d'Équipement 5G. Lors de l'enregistrement de l'UE, l'AMF lui demande si le PEI (IMEI/IMEISV) de l'appareil est autorisé ; OmniEIR renvoie `WHITELISTED`, `BLACKLISTED` ou `GREYLISTED`. Le verdict est calculé à partir des règles de l'opérateur conservées dans OmniHSS.

Points de terminaison

L'écouteur SBI expose le service N5g-eir_EquipmentIdentityCheck (TS 29.511) :

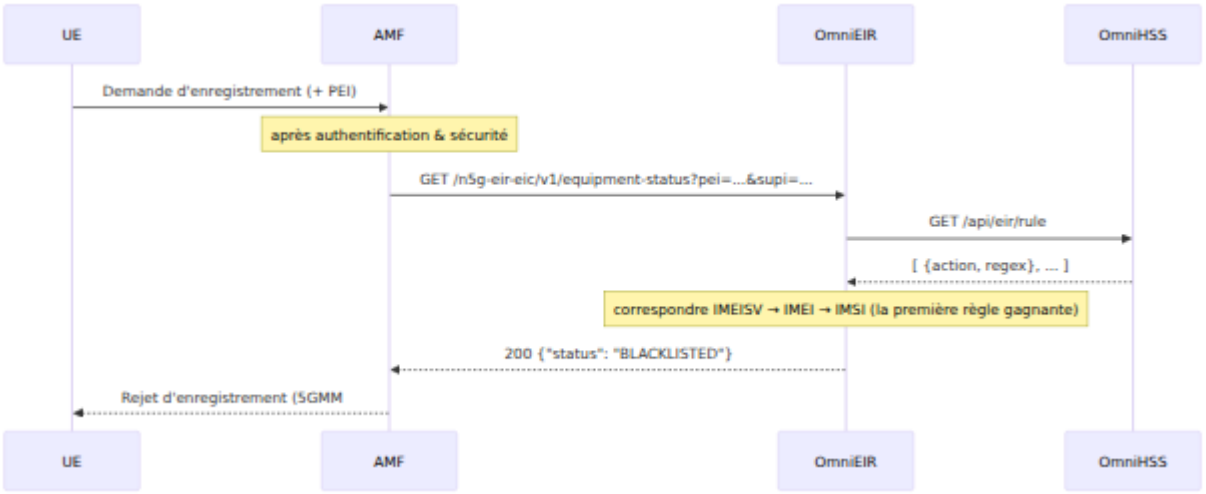
Méthode	Chemin	Description
`GET`	`/n5g-eir-eic/v1/equipment-status?pei={pei}&supi={supi}`	Renvoie `EirResponseData`: `{"status": "<EquipmentStatus>"}`. `pei` est obligatoire ; `supi` est optionnel.
`GET`	`/n5g-eir-eic/v1/status`	Sonde de vivacité (`{"status":"UP"}`).

`pei` est un PEI au format TS 23.003 : `imei-<15 chiffres>` ou `imeisv-<16 chiffres>`. `supi` est `imsi-<chiffres>`.

Exemple :

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

Flux de messages



Pour un verdict `WHITELISTED` ou `GREYLISTED` (ou toute erreur EIR), l'AMF poursuit l'enregistrement.

Logique de correspondance

OmniEIR reflète la décision S13 4G, donc un seul ensemble de règles régit les deux radios. Étant donné l'équipement analysé, il essaie, dans l'ordre, et s'arrête à la première règle dont le `regex` correspond :

1. la chaîne de chiffres **IMEISV** complète (IMEI + version logicielle), puis
2. l'**IMEI** seul, puis
3. l'**IMSI** (à partir du SUPI).

Si rien ne correspond, le `unknown_equipment_status` configuré est renvoyé.

Comportement fail-open

Le portail côté AMF est délibérément **fail-open** : si l'EIR est inaccessible, renvoie une erreur, ou si l'UE ne présente aucun PEI, l'enregistrement se poursuit. Seul un verdict explicite `BLACKLISTED` empêche un appareil. Cela empêche un EIR ou un HSS défectueux de laisser chaque abonné à l'abandon. Un déploiement qui nécessite des sémantiques fail-closed définit `unknown_equipment_status: "BLACKLISTED"` sur OmniEIR (donc les appareils non correspondants sont interdits). Notez qu'une panne totale de l'EIR échoue toujours ouvertement au niveau de l'AMF par conception.

Activation dans un déploiement

1. Provisionner des règles dans OmniHSS (`POST /api/eir/rule`).
2. Démarrer OmniEIR ; confirmer qu'il s'enregistre avec le NRF en tant que `5G_EIR`.
3. Définir `config :omniamf, eir_enabled: true` et redémarrer l'AMF.
4. Vérifier avec un redémarrage de téléphone / ré-attachement de l'UE et surveiller les journaux de l'AMF pour la ligne de décision `5G-EIR`.

Dépannage d'OmniEIR

Vue d'ensemble | Référence de configuration | Guide des opérations | Métriques et surveillance

Problèmes courants

Chaque appareil est autorisé même si j'ai provisionné une règle de liste noire

Vérifiez, dans l'ordre :

1. **La vérification AMF est-elle activée ?** La porte est désactivée par défaut. Définissez `config :omniamf, eir_enabled: true` et redémarrez l'AMF. Sans cela, l'AMF ne consulte jamais OmniEIR.
2. **OmniEIR peut-il atteindre OmniHSS ?** Un échec de lecture de `GET /api/eir/rule` échoue **ouvert** (appareil autorisé). Surveillez `Could not read EIR rules from HSS` dans les journaux d'OmniEIR et `[:omnieir, :hss, :request]` télémétrie avec `result: :failure`. Confirmez `hss_api_base_url`. Confirmez que `hss_api_key` est défini et a le rôle OmniHSS `eir_lookup`. Un HSS `401` signifie que la clé est manquante ou inconnue d'OmniHSS. Un `403` signifie que la clé n'a pas le rôle `eir_lookup`.
3. **L'expression régulière correspond-elle au PEI que l'UE présente ?** L'expression régulière de la règle est comparée à la chaîne de chiffres. Une règle écrite pour un IMEI de 14 chiffres ne correspondra pas à un PEI `imei-` de 15 chiffres à moins que l'expression régulière soit ancrée pour le permettre. Testez l'expression régulière contre les chiffres PEI exacts.
4. **L'AMF a-t-il réellement reçu un PEI ?** Si l'UE n'a présenté aucun PEI, les journaux de l'AMF indiquent `EIR enabled but UE ... presented no PEI; allowing` et continue.

L'AMF rejette un appareil que je n'avais pas l'intention de bloquer

- L'`regex` d'une règle est plus large que prévu (par exemple, `^3531` correspond à toute une plage TAC). Réduisez-la.
- `unknown_equipment_status` est défini sur `BLACKLISTED` (échec fermé) et l'appareil ne correspond à aucune règle. Ajoutez soit une règle de `whitelist` pour cela, soit revenez à la valeur par défaut `WHITELISTED`.

`400 MANDATORY_QUERY_PARAM_INCORRECT`

Le paramètre de requête `pei` était manquant dans la demande à `/n5g-eir-eic/v1/equipment-status`. Il est obligatoire (TS 29.511).

`500 SYSTEM_FAILURE` d'OmniEIR

OmniEIR n'a pas pu lire l'ensemble de règles d'OmniHSS. C'est un problème en amont (HSS) ; l'AMF traite un non-2xx comme un échec ouvert. Vérifiez la santé d'OmniHSS et `hss_api_base_url`.

Notes d'architecture

OmniEIR n'a pas d'API de provisionnement propre : les règles d'autorisation/de blocage/de grisage IMEI vivent dans OmniHSS (un ensemble de règles partagé avec l'interface 4G S13), et OmniEIR les lit via l'API REST HSS et applique la même logique de correspondance. La porte AMF est conçue pour être ouverte par défaut (voir Opérations), et le service N5g-eir est une seule demande d'état d'équipement par TS 29.511. Terminez TLS à un proxy externe devant l'auditeur SBI.