Referência de Configuração do OmniEIR

Visão Geral | Guia de Operações | Métricas e Monitoramento | Solução de Problemas

Toda a configuração do OmniEIR reside sob a chave de aplicação `:omnieir`. Um subconjunto de chaves pode ser substituído por variáveis de ambiente, mas isso só tem efeito na **configuração de tempo de execução de produção** (`config/runtime.exs`).

Estrutura da Configuração

```
config :omnieir,
  # Identidade do ouvinte SBI (anunciada para o NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.23",
  sbi_port: 7777,

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

  # PLMN servido (substituir por implantação)
  mcc: "999",
  mnc: "70",

  # API REST do OmniHSS que contém as regras de EIR do operador
  hss_api_base_url: "https://127.0.0.1:8443",

  # Chave da API do OmniHSS (papel eir_lookup). Obrigatória, sem
padrão.
  hss_api_key: "<Chave da API do OmniHSS com papel eir_lookup>",

  # Veredicto retornado quando nenhuma regra corresponde ao
equipamento apresentado
  unknown_equipment_status: "WHITELISTED"
```

Parâmetros Principais

Parâmetro	Tipo	Padrão	
`sbi_scheme`	string	`"http"`	`EIR_S`
`sbi_addr`	string	`"127.0.0.23"`	`EIR_S`
`sbi_port`	integer	`7777`	`EIR_S`
`nrf_uri`	string	`"http://127.0.0.10:7777"`	`EIR_N`
`heartbeat_interval`	integer (ms)	`10_000`	none
`mcc`	string	`"999"`	`EIR_M`
`mnc`	string	`"70"`	`EIR_M`
`hss_api_base_url`	string	`"https://127.0.0.1:8443"`	`HSS_A`
`hss_api_key`	string	Nenhum (obrigatório)	Nenhu

Parâmetro	Tipo	Padrão	
`unknown_equipment_status`	string	`"WHITELISTED"`	`EIR_U`

O certificado TLS autoassinado do laboratório OmniHSS é aceito (`verify_none`), correspondendo aos outros consumidores HSS-REST (OmniUDR). Termine o HSS atrás de uma CA confiável em produção.

O OmniHSS usa controle de acesso baseado em papéis em sua API REST. Ele rejeita uma solicitação sem um cabeçalho `x-omnihss-key` válido com `401`. O valor de `hss_api_key` é um segredo. O OmniEIR não o registra no log. Instale esta versão antes de habilitar o controle de acesso no OmniHSS, caso contrário, cada leitura de regra falha e a verificação do EIR falha abertamente.

Provisionamento das regras (OmniHSS)

O OmniEIR **não possui uma API de provisionamento própria**. As regras são criadas contra o OmniHSS, exatamente como para a interface S13 do 4G, por exemplo:

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

- `action` é um dos `whitelist`, `blacklist`, `greylist`.

- `regex` é comparado com a string de identidade do equipamento. As regras são avaliadas na ordem em que o OmniHSS as retorna; a primeira correspondência vence.

Configuração do lado do AMF (ativando a verificação)

A verificação do equipamento é realizada pelo **AMF**, e está **desativada por padrão**, portanto, implantações existentes não são afetadas. Habilite-a sob a chave `:omniamf`:

Parâmetro	Tipo	Padrão	Descrição
`eir_enabled`	boolean	`false`	Quando `true`, o AMF consulta o 5G-EIR durante o registro e rejeita PEIs na lista negra.
`eir_uri`	string | nil	`nil`	URI SBI estática do 5G-EIR. Quando `nil`, o AMF descobre o EIR via NRF (NFType `5G_EIR`).

```
config :omniamf,
  eir_enabled: true
  # eir_uri: "http://127.0.0.23:7777"   # opcional; omita para
usar a descoberta do NRF
```

Métricas e Monitoramento do OmniEIR

Visão Geral | Referência de Configuração | Guia de Operações | Solução de Problemas

Endpoint do Prometheus

OmniEIR expõe um endpoint de coleta do Prometheus via `TelemetryMetricsPrometheus` na `prometheus_metrics_port` (padrão **9572**):

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

Todos os rótulos têm baixa cardinalidade (`status` / `result` / `nf_type`), então a contagem de séries permanece limitada.

Métricas

Métrica	Tipo	Rótulos	
`omni_eir_equipment_check_count`	contador	`status`	Verificações de `EquipmentStat` (`WHITELISTED`/
`omni_eir_hss_request_count`	contador	`result`	Leituras do Om por resultado (
`omni_eir_hss_request_duration_ms`	gauge	`result`	Latência da lei EIR do OmniHS
`omni_eir_nrf_registration_status`	gauge	`nf_type`	Status de regis registrado, 0 =
`beam_*`	gauge	nenhum	Estatísticas pa (memória, con processos/port

Eventos de telemetria subjacentes

Evento	Medidas	Metadados	Emitido por
`[:omnieir, :equipment_check]`	`count`	`status`	OmniEIR em cada veredicto resolvido
`[:omnieir, :hss, :request]`	`count`, `duration_ms`	`endpoint`, `result`	OmniEIR em cada `GET /api/eir/rule` para o OmniHSS
`[:omniamf, :eir, :check]`	`count`	`result` (`:whitelisted` | `:greylisted` | `:blacklisted` | `:unknown` | `:error`)	O AMF em cada verificação de equipamento

O AMF também emite seu evento existente `[:omniamf, :registration, :result]` com `result: :rejected` quando um PEI na lista negra impede um registro. (A série `[:omniamf, :eir, :check]` é exposta no endpoint do Prometheus do **AMF**, não no do OmniEIR.)

O que observar

- Uma taxa crescente de `[:omnieir, :hss, :request]` com `result: :failure` significa que o OmniEIR não consegue alcançar o OmniHSS. O AMF então falha em aberto (todos os dispositivos permitidos). Alerta sobre isso.
- `[:omniamf, :eir, :check]` com `result: :blacklisted` conta dispositivos barrados; `:error` conta eventos de falha em aberto no AMF.

Logs

OmniEIR e o AMF registram cada decisão. Linhas notáveis:

- AMF: `5G-EIR retornou BLACKLISTED para PEI <pei> (<supi>); barrando registro`
- AMF: `5G-EIR verificação falhou para <supi> (<reason>); falhando em aberto`
- OmniEIR: `Não foi possível ler as regras EIR do HSS: <reason>`

Guia de Operações do OmniEIR

Visão Geral | Referência de Configuração | Métricas e Monitoramento | Solução de Problemas

Papel

OmniEIR é o Registro de Identidade de Equipamento 5G. Durante o registro do UE, o AMF pergunta se o PEI (IMEI/IMEISV) do dispositivo é permitido; o OmniEIR retorna `WHITELISTED`, `BLACKLISTED` ou `GREYLISTED`. O veredicto é calculado a partir das regras do operador mantidas no OmniHSS.

Endpoints

O ouvinte SBI expõe o serviço N5g-eir_EquipmentIdentityCheck (TS 29.511):

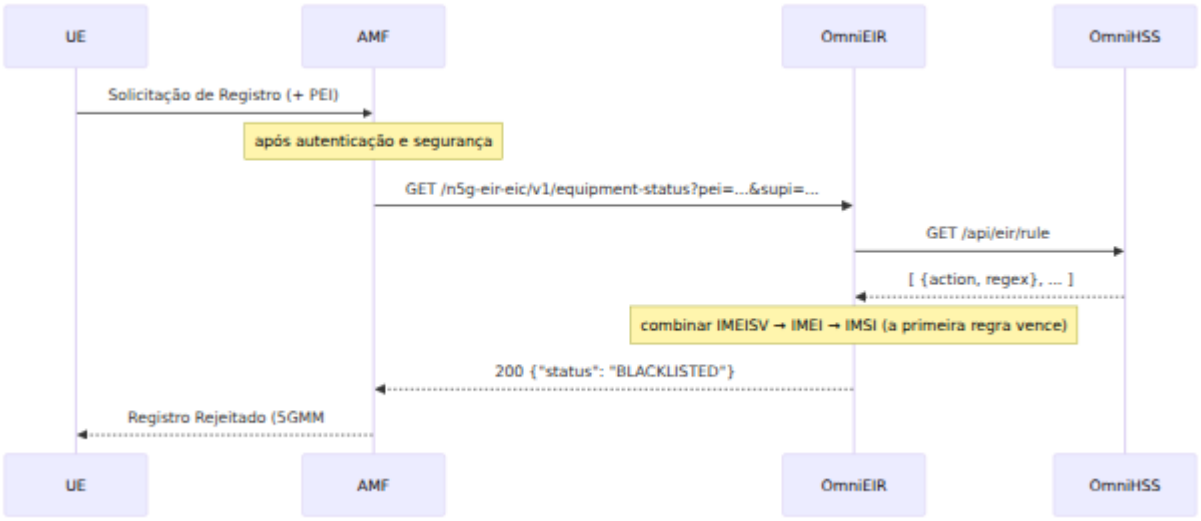
Método	Caminho	Descrição
`GET`	`/n5g-eir-eic/v1/equipment-status?pei={pei}&supi={supi}`	Retorna `EirResponseData`: `{"status": "<EquipmentStatus>"}`. `pei` é obrigatório; `supi` é opcional.
`GET`	`/n5g-eir-eic/v1/status`	Verificação de vivacidade (`{"status":"UP"}`).

`pei` é um PEI no formato TS 23.003: `imei-<15 dígitos>` ou `imeisv-<16 dígitos>`. `supi` é `imsi-<dígitos>`.

Exemplo:

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

Fluxo de Mensagens



Para um veredicto `WHITELISTED` ou `GREYLISTED` (ou qualquer erro do EIR), o AMF prossegue com o registro.

Lógica de Correspondência

OmniEIR espelha a decisão S13 do 4G, de modo que um único conjunto de regras governa ambas as radios. Dado o equipamento analisado, ele tenta, em ordem, e para na primeira regra cujo `regex` corresponda:

1. a string de dígitos completa **IMEISV** (IMEI + versão de software), depois
2. o **IMEI** sozinho, depois
3. o **IMSI** (do SUPI).

Se nada corresponder, o `unknown_equipment_status` configurado é retornado.

Comportamento de Falha Aberta

O portão do lado do AMF é deliberadamente **falha aberta**: se o EIR não estiver acessível, retornar um erro, ou o UE não apresentar nenhum PEI, o registro prossegue. Apenas um veredicto explícito `BLACKLISTED` impede um dispositivo. Isso evita que um EIR ou HSS quebrado deixe todos os assinantes sem serviço. Uma implantação que requer semântica de falha fechada define `unknown_equipment_status: "BLACKLISTED"` no OmniEIR (para que dispositivos não correspondidos sejam barrados). Note que uma interrupção total do EIR ainda falha aberta no AMF por design.

Habilitando em uma implantação

1. Provisione regras no OmniHSS (`POST /api/eir/rule`).
2. Inicie o OmniEIR; confirme que ele se registra no NRF como `5G_EIR`.
3. Defina `config :omniamf, eir_enabled: true` e reinicie o AMF.
4. Verifique com uma reinicialização do telefone / reanexação do UE e observe os logs do AMF para a linha de decisão `5G-EIR`.

Solução de Problemas do OmniEIR

Problemas Comuns

Todo dispositivo é permitido, mesmo que eu tenha provisionado uma regra de blacklist

Verifique, na ordem:

1. **A verificação do AMF está habilitada?** O gate está desligado por padrão. Defina `config :omniamf, eir_enabled: true` e reinicie o AMF. Sem isso, o AMF nunca consulta o OmniEIR.
2. **O OmniEIR pode alcançar o OmniHSS?** Uma falha ao ler `GET /api/eir/rule` falha **aberto** (dispositivo permitido). Fique atento a `Could not read EIR rules from HSS` nos logs do OmniEIR e `[:omnieir, :hss, :request]` telemetria com `result: :failure`. Confirme `hss_api_base_url`. Confirme que `hss_api_key` está definido e tem o papel `eir_lookup` do OmniHSS. Um `401` do HSS significa que a chave está faltando ou não é conhecida pelo OmniHSS. Um `403` significa que a chave não tem o papel `eir_lookup`.
3. **A regex corresponde ao PEI que o UE apresenta?** A regex da regra é comparada com a string de dígitos. Uma regra escrita para um IMEI de 14 dígitos não corresponderá a um PEI `imei-` de 15 dígitos, a menos que a regex esteja ancorada para permitir isso. Teste a regex contra os dígitos exatos do PEI.
4. **O AMF realmente recebeu um PEI?** Se o UE não apresentou nenhum PEI, os logs do AMF `EIR enabled but UE ... presented no PEI; allowing` e prossegue.

O AMF rejeita um dispositivo que eu não pretendia barrar

- A `regex` de uma regra é mais ampla do que o pretendido (por exemplo, `^3531` corresponde a toda uma faixa de TAC). Restringa-a.
- `unknown_equipment_status` está definido como `BLACKLISTED` (fail-closed) e o dispositivo não corresponde a nenhuma regra. Adicione uma regra de `whitelist` para ele ou reverta para o padrão `WHITELISTED`.

`400 MANDATORY_QUERY_PARAM_INCORRECT`

O parâmetro de consulta `pei` estava faltando na solicitação para `/n5g-eir-eic/v1/equipment-status`. É obrigatório (TS 29.511).

`500 SYSTEM_FAILURE` do OmniEIR

O OmniEIR não conseguiu ler o conjunto de regras do OmniHSS. Este é um problema upstream (HSS); o AMF trata um não-2xx como fail-open. Verifique a saúde do OmniHSS e `hss_api_base_url`.

Notas de Arquitetura

O OmniEIR não possui uma API de provisionamento própria: as regras de permitir/bloquear/cinza do IMEI vivem no OmniHSS (um conjunto de regras compartilhado com a interface S13 4G), e o OmniEIR as lê pela API REST do HSS e aplica a mesma lógica de correspondência. O gate do AMF é fail-open por design (veja Operações), e o serviço N5g-eir é um único Get de status de equipamento por TS 29.511. Termine o TLS em um proxy externo na frente do ouvinte SBI.