Referencia de Configuración de OmniEIR

Descripción general | Guía de Operaciones | Métricas y Monitoreo | Solución de Problemas

Toda la configuración de OmniEIR vive bajo la clave de aplicación `:omnieir`. Un subconjunto de claves puede ser sobrescrito por variables de entorno, pero eso solo tiene efecto en la **configuración de tiempo de ejecución de producción** (`config/runtime.exs`).

Estructura de Configuración

```
config :omnieir,
  # Identidad del oyente SBI (anunciada al NRF)
  sbi_scheme: "http",
  sbi_addr: "127.0.0.23",
  sbi_port: 7777,

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

  # PLMN servido (sobrescribir por implementación)
  mcc: "999",
  mnc: "70",

  # API REST de OmniHSS que contiene las reglas EIR del operador
  hss_api_base_url: "https://127.0.0.1:8443",

  # Clave API de OmniHSS (rol eir_lookup). Obligatoria, sin valor
por defecto.
  hss_api_key: "<Clave API de OmniHSS con rol eir_lookup>",

  # Veredicto devuelto cuando ninguna regla coincide con el equipo
presentado
  unknown_equipment_status: "WHITELISTED"
```

Parámetros Principales

Parámetro	Tipo	Por Defecto	
`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	Ninguno (requerido)	Ningu

Parámetro	Tipo	Por Defecto	
`unknown_equipment_status`	string	`"WHITELISTED"`	`EIR_U`

El certificado TLS autofirmado del laboratorio OmniHSS es aceptado (`verify_none`), coincidiendo con los otros consumidores de HSS-REST (OmniUDR). Termine el HSS detrás de una CA confiable en producción.

OmniHSS utiliza control de acceso basado en roles en su API REST. Rechaza una solicitud sin un encabezado `x-omnihss-key` válido con `401`. El valor de `hss_api_key` es un secreto. OmniEIR no lo escribe en el registro. Instale esta versión antes de habilitar el control de acceso en OmniHSS, de lo contrario, cada lectura de regla fallará y la verificación de EIR fallará abierta.

Aprovisionamiento de las reglas (OmniHSS)

OmniEIR **no tiene una API de aprovisionamiento propia**. Las reglas se crean contra OmniHSS, exactamente como para la interfaz S13 de 4G, por ejemplo:

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

- `action` es uno de `whitelist`, `blacklist`, `greylist`.

- `regex` se compara con la cadena de identidad del equipo. Las reglas se evalúan en el orden en que OmniHSS las devuelve; la primera coincidencia gana.

Configuración del lado de AMF (activando la verificación)

La verificación del equipo es realizada por el **AMF**, y está **desactivada por defecto** para que las implementaciones existentes no se vean afectadas. Actívelo bajo la clave `:omniamf`:

Parámetro	Tipo	Por Defecto	Descripción
`eir_enabled`	boolean	`false`	Cuando es `true`, el AMF consulta el 5G-EIR durante el registro y rechaza los PEIs en la lista negra.
`eir_uri`	string | nil	`nil`	URI SBI estática de 5G-EIR. Cuando es `nil`, el AMF descubre el EIR a través del NRF (NFType `5G_EIR`).

```
config :omniamf,
  eir_enabled: true
  # eir_uri: "http://127.0.0.23:7777"   # opcional; omitir para
usar el descubrimiento de NRF
```

Métricas y Monitoreo de OmniEIR

Descripción general | Referencia de configuración | Guía de operaciones | Solución de problemas

Endpoint de Prometheus

OmniEIR expone un endpoint de recolección de Prometheus a través de `TelemetryMetricsPrometheus` en `prometheus_metrics_port` (por defecto **9572**):

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

Todas las etiquetas son de baja cardinalidad (`status` / `result` / `nf_type`) por lo que el conteo de series se mantiene limitado.

Métricas

Métrica	Tipo	Etiquetas	
`omni_eir_equipment_check_count`	contador	`status`	Chequeos de `EquipmentSt` (`WHITELISTE`
`omni_eir_hss_request_count`	contador	`result`	Lecturas de `/api/eir/ru` (`success`/`fa`
`omni_eir_hss_request_duration_ms`	medidor	`result`	Latencia de regla EIR de
`omni_eir_nrf_registration_status`	medidor	`nf_type`	Estado de re registrado, 0
`beam_*`	medidor	ninguno	Estadísticas (memoria, c tiempo de ac

Eventos de telemetría subyacentes

Evento	Mediciones	Metadatos	Emitido por
`[:omnieir, :equipment_check]`	`count`	`status`	OmniEIR en cada veredicto resuelto
`[:omnieir, :hss, :request]`	`count`, `duration_ms`	`endpoint`, `result`	OmniEIR en cada `GET /api/eir/rule` a OmniHSS
`[:omniamf, :eir, :check]`	`count`	`result` (`:whitelisted` | `:greylisted` | `:blacklisted` | `:unknown` | `:error`)	El AMF en cada chequeo de equipo

El AMF también emite su evento existente `[:omniamf, :registration, :result]` con `result: :rejected` cuando un PEI en la lista negra impide un registro. (La serie `[:omniamf, :eir, :check]` se expone en el endpoint de Prometheus del **AMF**, no en el de OmniEIR.)

Qué observar

- Una tasa creciente de `[:omnieir, :hss, :request]` con `result: :failure` significa que OmniEIR no puede alcanzar a OmniHSS. El AMF entonces falla en abierto (cada dispositivo permitido). Alerta sobre esto.
- `[:omniamf, :eir, :check]` con `result: :blacklisted` cuenta dispositivos bloqueados; `:error` cuenta eventos de falla abierta en el AMF.

Registros

OmniEIR y el AMF registran cada decisión. Líneas 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>`

Guía de Operaciones de OmniEIR

Descripción general | Referencia de Configuración | Métricas y Monitoreo | Solución de Problemas

Rol

OmniEIR es el Registro de Identidad de Equipos 5G. Durante el registro del UE, el AMF le pregunta si el PEI (IMEI/IMEISV) del dispositivo está permitido; OmniEIR devuelve `WHITELISTED`, `BLACKLISTED` o `GREYLISTED`. El veredicto se calcula a partir de las reglas del operador que se encuentran en OmniHSS.

Puntos finales

El oyente SBI expone el servicio N5g-eir_EquipmentIdentityCheck (TS 29.511):

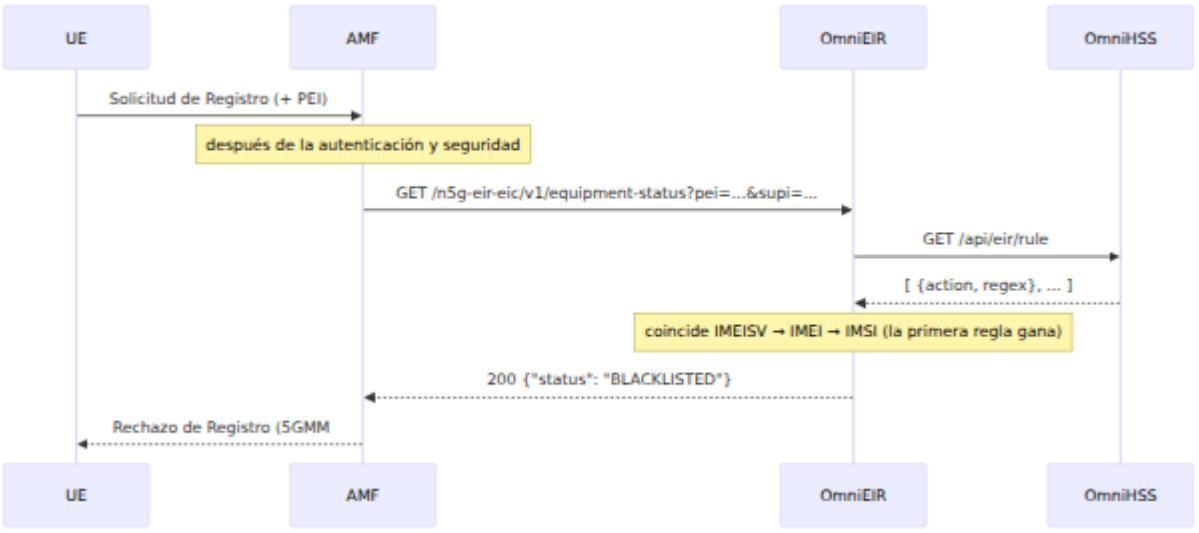
Método	Ruta	Descripción
`GET`	`/n5g-eir-eic/v1/equipment-status?pei={pei}&supi={supi}`	Devuelve `EirResponseData`: `{"status": "<EquipmentStatus>"}`. `pei` es obligatorio; `supi` es opcional.
`GET`	`/n5g-eir-eic/v1/status`	Prueba de disponibilidad (`{"status":"UP"}`).

`pei` es un PEI en forma TS 23.003: `imei-<15 dígitos>` o `imeisv-<16 dígitos>`. `supi` es `imsi-<dígitos>`.

Ejemplo:

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

Flujo de Mensajes



Para un veredicto `WHITELISTED` o `GREYLISTED` (o cualquier error de EIR), el AMF procede con el registro.

Lógica de Coincidencia

OmniEIR refleja la decisión S13 de 4G, por lo que un solo conjunto de reglas gobierna ambas radios. Dado el equipo analizado, intenta, en orden, y se detiene en la primera regla cuyo `regex` coincide:

1. la cadena de dígitos completa **IMEISV** (IMEI + versión de software), luego
2. el **IMEI** solo, luego
3. el **IMSI** (del SUPI).

Si nada coincide, se devuelve el `unknown_equipment_status` configurado.

Comportamiento de fallo abierto

El acceso del lado AMF es deliberadamente **fail-open**: si el EIR es inalcanzable, devuelve un error, o el UE no presentó ningún PEI, el registro continúa. Solo un veredicto explícito de `BLACKLISTED` impide que un dispositivo se registre. Esto evita que un EIR o HSS roto deje a cada suscriptor varado. Un despliegue que requiere semántica de fallo cerrado establece `unknown_equipment_status: "BLACKLISTED"` en OmniEIR (por lo que los dispositivos no coincidentes son bloqueados). Tenga en cuenta que una interrupción total del EIR aún falla abierto en el AMF por diseño.

Habilitación en un despliegue

1. Proveer reglas en OmniHSS (`POST /api/eir/rule`).
2. Iniciar OmniEIR; confirmar que se registra con el NRF como `5G_EIR`.
3. Establecer `config :omniamf, eir_enabled: true` y reiniciar el AMF.
4. Verificar con un reinicio del teléfono / re-adjunción del UE y observar los registros del AMF para la línea de decisión `5G-EIR`.

Solución de problemas de OmniEIR

Descripción general | Referencia de configuración | Guía de operaciones | Métricas y monitoreo

Problemas comunes

Cada dispositivo está permitido aunque he provisionado una regla de lista negra

Verifique, en orden:

1. **¿Está habilitada la verificación del AMF?** La puerta está apagada por defecto. Establezca `config :omniamf, eir_enabled: true` y reinicie el AMF. Sin esto, el AMF nunca consulta a OmniEIR.
2. **¿Puede OmniEIR alcanzar a OmniHSS?** Un fallo al leer `GET /api/eir/rule` falla **abierto** (dispositivo permitido). Esté atento a `Could not read EIR rules from HSS` en los registros de OmniEIR y `[:omnieir, :hss, :request]` telemetría con `result: :failure`. Confirme `hss_api_base_url`. Confirme que `hss_api_key` esté configurado y tenga el rol de OmniHSS `eir_lookup`. Un `401` de HSS significa que la clave falta o no es conocida por OmniHSS. Un `403` significa que la clave no tiene el rol `eir_lookup`.
3. **¿Coincide la expresión regular con el PEI que presenta el UE?** La expresión regular de la regla se compara con la cadena de dígitos. Una regla escrita para un IMEI de 14 dígitos no coincidirá con un PEI `imei-` de 15 dígitos a menos que la expresión regular esté anclada para permitirlo. Pruebe la expresión regular contra los dígitos exactos del PEI.
4. **¿Recibió realmente el AMF un PEI?** Si el UE no presentó ningún PEI, los registros del AMF indican `EIR enabled but UE ... presented no PEI; allowing` y procede.

El AMF rechaza un dispositivo que no pretendía bloquear

- La `regex` de una regla es más amplia de lo previsto (por ejemplo, `^3531` coincide con todo un rango TAC). Redúzcala.
- `unknown_equipment_status` está configurado como `BLACKLISTED` (cerrado por fallo) y el dispositivo no coincide con ninguna regla. Agregue una regla de `whitelist` para ello o vuelva a la configuración predeterminada `WHITELISTED`.

`400 MANDATORY_QUERY_PARAM_INCORRECT`

El parámetro de consulta `pei` faltaba en la solicitud a `/n5g-eir-eic/v1/equipment-status`. Es obligatorio (TS 29.511).

`500 SYSTEM_FAILURE` de OmniEIR

OmniEIR no pudo leer el conjunto de reglas de OmniHSS. Este es un problema de upstream (HSS); el AMF trata un no-2xx como fallo-abierto. Verifique la salud de OmniHSS y `hss_api_base_url`.

Notas de arquitectura

OmniEIR no tiene una API de aprovisionamiento propia: las reglas de permitir/bloquear/gris de IMEI residen en OmniHSS (un conjunto de reglas compartido con la interfaz S13 de 4G), y OmniEIR las lee a través de la API REST de HSS y aplica la misma lógica de coincidencia. La puerta del AMF está diseñada para fallar-abierto (ver Operaciones), y el servicio N5g-eir es un único Get de estado de equipo por TS 29.511. Termine TLS en un proxy externo frente al oyente SBI.