Referência de Configuração do OmniNEF

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

Toda a configuração reside sob a chave de aplicativo `:omninef`. Os padrões em tempo de compilação estão em `config/config.exs` (espelhado por `OmniNef.Config`); implantações em produção substituem um subconjunto via variáveis de ambiente em `config/runtime.exs`.

Índice

Listener SBI

Chave	Tipo	Padrão	Descrição
`sbi_scheme`	string	`"http"`	Esquema anunciado no perfil NRF. O listener em si serve HTTP simples.
`sbi_addr`	string	`"127.0.0.30"`	Endereço de ligação/anúncio do SBI.
`sbi_port`	integer	`7777`	Porta de escuta do SBI (API norte + status).

NRF e PLMN

Chave	Tipo	Padrão	
`nrf_uri`	string	`"http://127.0.0.10:7777"`	URI base do I
`mcc`	string	`"999"`	MCC PLMN se e no FQDN N
`mnc`	string	`"70"`	MNC PLMN se
`heartbeat_interval`	integer (ms)	`10_000`	Intervalo de I
`nef_fqdn`	string	derivado	Este FQDN d `nef.5gc.mnc`

Registro AF

`af_registry` é um mapa indexado pela chave da API do AF. Cada valor define o que o AF pode fazer. Ele está vazio por padrão: **nenhum AF pode chamar o NEF até que um seja provisionado**.

```
config :omninef,
  af_registry: %{
    "af-secret-001" => %{
      af_id: "af-acme",              # identificador ecoado nos
logs
      allowed_apis: :all,            # ou uma lista de átomos de
API (veja abaixo)
      rate_limit_per_sec: 20         # opcional; recai sobre
default_rate_limit_per_sec
    }
  }
```

`allowed_apis` é `:all` ou uma lista extraída de:

Átomo da API	Recurso Norte
`:monitoring_event`	`/3gpp-monitoring-event/...`
`:parameter_provision`	`/nnef-pp/...`
`:af_session_with_qos`	`/3gpp-as-session-with-qos/...`
`:traffic_influence`	`/3gpp-traffic-influence/...`

A chave da API é apresentada pelo AF como `Authorization: Bearer <key>` ou `X-Api-Key: <key>`.

Controle de Fluxo

Chave	Tipo	Padrão	Descrição
`default_rate_limit_per_sec`	integer	`10`	Teto de requisições por AF aplicado quando uma especificação de AF omite `rate_limit_per_sec`.

O controle de fluxo utiliza uma janela deslizante de um segundo por AF. Um AF que atinge ou ultrapassa seu teto recebe `429`.

Variáveis de Ambiente

Definidas em `config/runtime.exs` para `MIX_ENV=prod`. Variáveis não definidas recuam para os padrões em tempo de compilação acima.

Variável	Mapeia para	
`NEF_SBI_SCHEME`	`sbi_scheme`	`http`
`NEF_SBI_ADDR`	`sbi_addr`	`127.0.`
`NEF_SBI_PORT`	`sbi_port`	`7777`
`NEF_NRF_URI`	`nrf_uri`	`http:/`
`NEF_MCC`	`mcc`	`999`
`NEF_MNC`	`mnc`	`70`
`NEF_FQDN`	`nef_fqdn`	derivad
`NEF_DEFAULT_RATE_LIMIT_PER_SEC`	`default_rate_limit_per_sec`	`10`
`NEF_AF_REGISTRY`	`af_registry` (JSON)	não def

`NEF_AF_REGISTRY` é um objeto JSON da mesma forma que o mapa `af_registry`, com `allowed_apis` como a string `"all"` ou um array de strings de nomes de API:

```
NEF_AF_REGISTRY='{"af-secret-001":{"af_id":"af-
acme","allowed_apis":"all","rate_limit_per_sec":20}}'
```

JSON malformado gera erro na inicialização, de modo que uma configuração de implantação ruim falhe rapidamente em vez de desabilitar silenciosamente todos os AFs.

Métricas e Monitoramento do OmniNEF

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

Status Atual

A observabilidade é fornecida por **logs de aplicação estruturados** e registro padrão de requisições. Os operadores monitoram o OmniNEF através de seus logs, que capturam atividades de autorização, limitação e tradução nas interfaces de norte a sul e de sul a norte.

O que Observar nos Logs

Os logs da aplicação são o sinal primário para operar o OmniNEF.

Autorização e Limitação

Requisições rejeitadas de norte a sul aparecem como respostas `ProblemDetails`. Fique atento a:

- Uma taxa crescente de `401 UNAUTHORIZED`: um AF apresenta uma chave de API ausente ou desconhecida (um cliente mal configurado ou um AF não provisionado).
- `403 OPERATION_NOT_ALLOWED`: um AF conhecido chama uma API à qual não tem direito. Verifique os `allowed_apis` do AF.
- `429 TOO_MANY_REQUESTS`: um AF excede seu teto de requisições. Considere aumentar seu `rate_limit_per_sec` ou investigar o cliente.

Tradução de Norte a Sul

Cada capacidade registra a operação que realiza, incluindo o identificador do UE alvo e o NF produtor resolvido. Fique atento a esses logs para confirmar que assinaturas e sessões estão chegando ao UDM/PCF/UDR.

- `503 NF_UNAVAILABLE` indica que a descoberta do NRF não encontrou uma instância adequada de UDM/PCF/UDR.
- `502 TARGET_NF_NOT_REACHABLE` indica que o NF produtor foi descoberto, mas a chamada do SBI falhou.
- `400 MANDATORY_IE_INCORRECT` indica uma falha na validação da requisição (identificador do UE ausente, QoS, alvo de roteamento ou um tipo de monitoramento não suportado).

Registro de Requisições

O registro padrão de requisições cobre cada requisição SBI de norte a sul tratada pelo listener. Use-o para observar o volume de requisições, métodos e caminhos, e para correlacionar a atividade do AF com eventos de tradução.

Verificação de Saúde

A saúde é melhor avaliada combinando:

- **Vigência:** `GET /nnef/v1/status` retorna `200 {"status":"UP"}` quando o listener do SBI está ativo. Veja o Guia de Operações.
- **Registro no NRF:** confirme que o OmniNEF aparece no NRF como uma instância NF `NEF` e está enviando batimentos cardíacos. O comportamento de registro é descrito no Guia de Operações.
- **Sinais de Log:** os eventos de autorização, limitação e tradução descritos acima.

Guia de Operações do OmniNEF

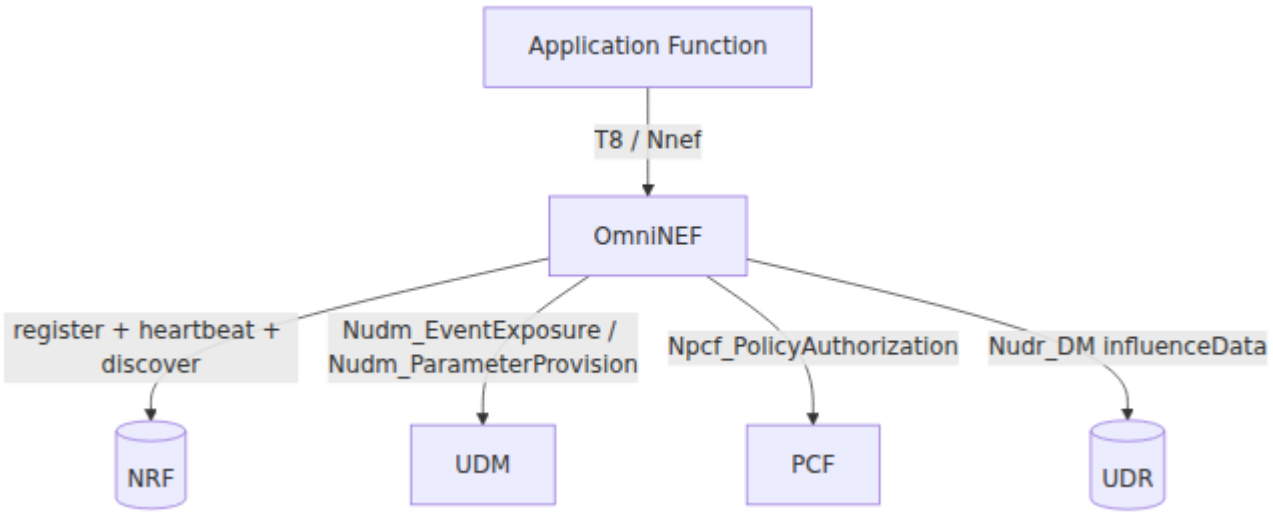
Visão Geral | Referência de Configuração | Métricas e Monitoramento | Solução de Problemas

Este guia descreve como o OmniNEF se comporta como o gateway de exposição norte do Core 5G e como operá-lo. O OmniNEF é a Função de Exposição de Rede definida em 3GPP TS 23.501 §6.2.5, expondo a API T8 (TS 29.122) / serviços Nnef (TS 29.522) em direção às Funções de Aplicação.

Índice

Visão Geral da Arquitetura

O OmniNEF termina a API norte em direção às AFs externas e traduz cada solicitação em uma operação SBI em direção a um NF produtor do core. Ele se registra no NRF como NFType `NEF` e usa a descoberta do NRF para resolver o UDM, PCF ou UDR que atende a uma solicitação específica.



Ciclo de Vida da Solicitação

Cada solicitação de criação de recurso norte segue o mesmo caminho:

1. **Autorizar** a AF chamadora a partir de sua chave de API e verificar se ela tem direito à API solicitada.
2. **Controlar** o fluxo contra o teto de solicitações por segundo da AF.
3. **Validar** o corpo da solicitação (identificador do UE alvo, QoS requerida, alvo de roteamento, …).
4. **Descobrir** o NF alvo (UDM/PCF/UDR) a partir do NRF e selecionar uma instância ciente da carga.
5. **Traduzir e enviar** a solicitação SBI correspondente para o NF produtor.
6. **Armazenar** o recurso criado (AF proprietário, representação, URL de desmantelamento a jusante) e retornar `201 Created` com um cabeçalho `Location` apontando para o recurso individual.

`GET` no recurso individual retorna a representação armazenada; `DELETE` desmantela o recurso no NF produtor (melhor esforço) e remove o registro do lado do NEF.

Autorização e Controle de Fluxo

O NEF é o limite entre AFs de terceiros não confiáveis e o core confiável, portanto, a autorização é obrigatória (TS 23.501 §6.2.5).

- **Autenticação:** a AF apresenta uma chave de API como `Authorization: Bearer <key>` ou `X-Api-Key: <key>`. As chaves são consultadas no registro da AF. Uma chave ausente ou desconhecida retorna `401`.
- **Direito:** cada AF é limitada a `:all` APIs ou uma lista explícita. Uma AF conhecida chamando uma API à qual não tem direito retorna `403`.
- **Controle de Fluxo:** cada AF tem um teto de solicitações por segundo (o seu próprio ou o padrão configurado). Uma AF que excede isso retorna `429`. A janela é deslizante de um segundo.

Veja a Referência de Configuração para como integrar uma AF.

APIs Norte

Capacidade	Recurso norte	Método
Eventos de Monitoramento (Nnef_EventExposure)	`/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`	POST, G DELETE
Provisionamento de Parâmetros (Nnef_ParameterProvision)	`/nnef-pp/v1/{afId}/provisionings`	POST, G DELETE
Sessão AF com QoS (Nnef_AFsessionWithQoS)	`/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions`	POST, G DELETE
Influência de Tráfego (Nnef_TrafficInfluence)	`/3gpp-traffic-influence/v1/{afId}/subscriptions`	POST, G DELETE

Eventos de Monitoramento

Uma AF se inscreve em eventos de rede para um UE identificado por `externalId` ou `msisdn`. Os valores suportados de `monitoringType` mapeiam para tipos de eventos do UDM:

T8 `monitoringType`	UDM `eventType`
`LOSS_OF_CONNECTIVITY`	`LOSS_OF_CONNECTIVITY`
`UE_REACHABILITY`	`UE_REACHABILITY_FOR_DATA`
`LOCATION_REPORTING`	`LOCATION_REPORTING`
`ROAMING_STATUS`	`ROAMING_STATUS`
`COMMUNICATION_FAILURE`	`COMMUNICATION_FAILURE`
`AVAILABILITY_AFTER_DDN_FAILURE`	`AVAILABILITY_AFTER_DDN_FAILURE`

O identificador externo é mapeado para um GPSI do UDM (`extid-<externalId>` ou `msisdn-<msisdn>`).

Provisionamento de Parâmetros

Uma AF provisiona parâmetros de comportamento esperado do UE ou características de comunicação para um UE (`externalId` / `msisdn`) ou um grupo (`externalGroupId`). Um objeto `ppData` explícito ou os campos de provisionamento de nível superior reconhecidos são aceitos; o NEF os aplica via `Nudm_ParameterProvision`, que o UDM persiste no UDR.

Sessão AF com QoS

Uma AF fornece o endereço do UE (`ueIpv4Addr` / `ueIpv6Addr`), os fluxos IP a serem tratados e uma `qosReference` (ou QoS solicitada). O NEF cria um Contexto de Sessão de Aplicação Individual no PCF, que instala a política correspondente em direção ao SMF.

Influência de Tráfego

Uma AF solicita ao core que direcione o tráfego selecionado para um DNAI / local de aplicação. O alvo de roteamento depende do escopo:

- **UE Individual** (`gpsi` ou `supi` presente) → uma sessão de aplicação no **PCF**.
- **Grupo / qualquer-UE** (sem identificador individual) → armazenado como dados de aplicação `influenceData` no **UDR**, que o PCF lê ao construir a política para sessões correspondentes futuras.

Interoperabilidade Sul

O NEF resolve cada NF produtor a partir do NRF (`Nnrf_NFDiscovery`, filtrado por nome do serviço) e seleciona a instância com menor carga. Em seguida, emite a solicitação SBI mapeada:

- `POST …/nudm-ee/v1/{gpsi}/ee-subscriptions` (UDM)
- `PUT …/nudm-pp/v1/{gpsi}/pp-data` (UDM)
- `POST …/npcf-policyauthorization/v1/app-sessions` (PCF)
- `PUT …/nudr-dr/v1/application-data/influenceData/{id}` (UDR)

Quando um NF produtor retorna um `Location`, o NEF retém a URL absoluta resolvida para que o recurso possa ser excluído posteriormente. Para eventos de monitoramento, o NEF registra um URL de callback de notificação **por assinatura** com o NF produtor (`…/nnef-eventexposure/v1/notifications/{subId}`); quando o produtor POSTa um relatório de evento para esse callback, o NEF o mapeia para uma `MonitoringNotification` T8 e o retransmite para o `notificationDestination` armazenado da AF (o caminho de dados de exposição de eventos). A retransmissão é de melhor esforço. O NEF sempre reconhece o callback do produtor com `204`. O NEF descarta notificações para uma assinatura desconhecida ou expirada. Veja a entrada de solução de problemas de retransmissão de notificações.

Endpoints SBI

- `GET /nnef/v1/status`: verificação de vivacidade; retorna `200 {"status":"UP"}`.
- Os endpoints de recurso norte na tabela APIs Norte.

Caminhos não correspondidos retornam `404` com um corpo `ProblemDetails` da 3GPP.

Registro NRF

Na inicialização, o OmniNEF se registra no NRF como NFType `NEF`, anunciando quatro serviços (`nnef-eventexposure`, `nnef-pp`, `nnef-afsessionwithqos`, `nnef-trafficinfluence`) e seu endpoint IP SBI, em seguida, envia batimentos cardíacos no intervalo configurado. A capacidade e a prioridade vêm dos auxiliares compartilhados `Omni5gEx.NRF.Config`.

Notas Operacionais

- **HTTP Simples:** o listener SBI serve HTTP simples. Termine o TLS externamente (um proxy reverso ou malha de serviços) para qualquer exposição além de uma rede confiável.
- **Estado não persistente:** o registro da AF, janelas do limitador de taxa e armazenamento de recursos criados estão na memória. Na reinicialização, as AFs são re-semeadas a partir da configuração e os recursos norte criados anteriormente são esquecidos pelo NEF (os recursos do NF do core subjacente persistem até expirarem ou serem removidos diretamente).
- **Desmantelamento a jusante é melhor esforço:** um `DELETE` sempre remove o registro do lado do NEF, mesmo que o NF produtor esteja brevemente inacessível; a falha é registrada.

Solução de Problemas do OmniNEF

Visão Geral | Guia de Operações | Referência de Configuração | Métricas e Monitoramento

Índice

Problemas Comuns

Cada solicitação de AF retorna 401

A chave da API do AF não está no registro. O registro está vazio por padrão, então uma nova implantação rejeita tudo até que um AF seja provisionado. Adicione o AF ao `af_registry` (ou `NEF_AF_REGISTRY`) e confirme se o cliente envia `Authorization: Bearer <key>` ou `X-Api-Key: <key>`. Veja a Referência de Configuração.

Um AF recebe 403 em algumas APIs

O AF é conhecido, mas seu `allowed_apis` não inclui a API que está chamando. Defina `allowed_apis` como `:all`, ou adicione o átomo da API relevante à lista.

Um AF recebe 429 sob carga

O AF está excedendo seu teto de solicitações por segundo. Aumente seu `rate_limit_per_sec` (ou `default_rate_limit_per_sec`), ou limite o cliente. A janela é de um segundo deslizante.

Solicitações falham com 503 NF_UNAVAILABLE

A descoberta do NRF não retornou nenhuma instância de UDM/PCF/UDR oferecendo o serviço necessário. Confirme se o NF de destino está registrado no NRF e saudável, e se `nrf_uri` está correto.

Solicitações falham com 502 TARGET_NF_NOT_REACHABLE

O NF produtor foi descoberto, mas a chamada SBI para ele falhou. Verifique a conectividade com o NF produtor e seus logs; o NEF registra o erro subjacente.

Um AF cria uma assinatura de evento de monitoramento, mas nunca recebe notificações

As notificações de eventos agora seguem o caminho de dados de ponta a ponta: ao criar, o NEF registra um callback **por assinatura** com o UDM (`.../nnef-eventexposure/v1/notifications/{subId}`); quando o NF produtor POSTa um relatório de evento para esse callback, o NEF mapeia para um T8 `MonitoringNotification` e o retransmite para o `notificationDestination` do AF. Se o AF não vê nada, verifique, na ordem:

- A assinatura continha um `notificationDestination` acessível (o NEF registra `subscription <id> has no notificationDestination` quando está ausente).
- O NF produtor está realmente emitindo relatórios e pode alcançar a URL de callback do NEF (o `sbi_base_url` anunciado do NEF deve ser roteável a partir do UDM/AMF).
- O POST de retransmissão é bem-sucedido. O NEF registra uma entrega falhada como `relay to AF <url> ... failed`. A retransmissão é feita com o melhor esforço: o NEF sempre responde ao callback do produtor com `204` para que o produtor não trate um AF temporariamente fora do ar como uma falha permanente de callback. Notificações para uma assinatura desconhecida/expirada são registradas e descartadas (também `204`).

Solicitações falham com 400

O corpo da solicitação está faltando um campo obrigatório para essa capacidade: um identificador de UE (`externalId`/`msisdn`), um `qosReference` para uma sessão de QoS do AF, um alvo de roteamento para influência de tráfego, ou um `monitoringType` não suportado. O campo `detail` do `ProblemDetails` nomeia a falha de validação específica.