OmniNEF □置参考

□述 | 操作指南 | 指标和监控 | 故障排除

所有配置都在 `:omninef` 应用程序键下。编译时的默认值在 `config/config.exs` 中（由 `OmniNef.Config` 镜像）；生产部署通过 `config/runtime.exs` 中的环境变量覆盖一部分。

目录

- SBI 监听器
- NRF 和 PLMN
- AF 注册表
- 限流
- 环境变量

SBI 监听器

键	类型	默认值	描述
`sbi_scheme`	字符串	`"http"`	在 NRF 配置文件中宣传的方案。监听器本身提供普通 HTTP。
`sbi_addr`	字符串	`"127.0.0.30"`	SBI 绑定/宣传地址。
`sbi_port`	整数	`7777`	SBI 监听端口（北向 API + 状态）。

NRF 和 PLMN

键	类型	默认值	
`nrf_uri`	字 ﷺ 串	`"http://127.0.0.10:7777"`	用于注册和发现的 NRF 基
`mcc`	字符串	`"999"`	提供的 PLMN MCC。
`mnc`	字符串	`"70"`	提供的 PLMN MNC
`heartbeat_interval`	整数（毫秒）	`10_000`	NRF 心跳间隔。
`nef_fqdn`	字符串	派生	此 NEF 的 FQDN。 `nef.5gc.mnc<mr`

AF 注册表

`af_registry` 是一个以 AF 的 API 密钥为键的映射。每个值限制 AF 可以执行的操作。默认情况下为空：没有 **AF** 可以调用 **NEF**，直到一个被置。

```
config :omninef,
  af_registry: %{
    "af-secret-001" => %{
      af_id: "af-acme",                # 录在日志中的标识符
      allowed_apis: :all,              # 或 API 原子列表（见下文）
      rate_limit_per_sec: 20           # 可选；回退到
default_rate_limit_per_sec
    }
  }
```

`allowed_apis` 可以是 `:all` 或从以下列表中提取的列表：

API 原子	北向资源
`:monitoring_event`	`/3gpp-monitoring-event/...`
`:parameter_provision`	`/nnef-pp/...`
`:af_session_with_qos`	`/3gpp-as-session-with-qos/...`
`:traffic_influence`	`/3gpp-traffic-influence/...`

API 密钥由 AF ﷺ `Authorization: Bearer <key>` 或 `X-Api-Key: <key>` 的形式提供。

限流

键	类型	默认值	描述
`default_rate_limit_per_sec`	整数	`10`	当 AF 规范省略 `rate_limit_per_sec` 时应用的每个 AF 请求上限。

限流使用每个 AF 的滑动一秒窗口。达到或超过上限的 AF 将收到 `429`。

环境变量

在 `config/runtime.exs` 中为 `MIX_ENV=prod` 设置。未设置的变量回退到上述编译时默认值。

变量	映射到	
`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`	派生
`NEF_DEFAULT_RATE_LIMIT_PER_SEC`	`default_rate_limit_per_sec`	`10`
`NEF_AF_REGISTRY`	`af_registry` (JSON)	未设置（空）

`NEF_AF_REGISTRY` 是一个与 `af_registry` 映射形状相同的 JSON 对象，`allowed_apis` 为字符串 `"all"` 或 API 名称字符串的数组：

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

格式错误的 JSON 在启动时���引发错误，因此不良的部署配置会快速失败，而不是静默地禁用所有 AF。

OmniNEF 指标与监控

□述 | 操作指南 | 配置参考 | 故障排除

当前状态

可观察性通过 结构化应用日志 和标准请求日志提供。操作员通过其日志监控 OmniNEF，这些日志捕获了授权、限流和翻译活动，涵盖了北向和南向接口。

日志中需要关注的内容

应用日志是操作 OmniNEF 的主要信号。

授权与限流

被拒绝的北向请求以 `ProblemDetails` 响应的形式出现。请注意：

- `401 UNAUTHORIZED` 的上升率：一个 AF 提供了缺失或未知的 API 密钥（配置错误的客户端或未配置的 AF）。
- `403 OPERATION_NOT_ALLOWED`：一个已知的 AF 调用其无权访问的 API。检查 AF 的 `allowed_apis`。
- `429 TOO_MANY_REQUESTS`：一个 AF 超过了其请求上限。考虑提高其 `rate_limit_per_sec` 或调查客户端。

北向到南向的翻译

每个能力记录其执行的操作，包括目标 UE 标识符和解析的生产者 NF。请关注这些日志以确认订阅和会话是否到达 UDM/PCF/UDR。

- `503 NF_UNAVAILABLE` ��示 NRF 发现没有合适的 UDM/PCF/UDR 实例。
- `502 TARGET_NF_NOT_REACHABLE` 表示生产者 NF 被发现但 SBI 调用失败。
- `400 MANDATORY_IE_INCORRECT` 表示请求验证失败（缺少 UE 标识符、QoS、路由目标或不支持的监控类型）。

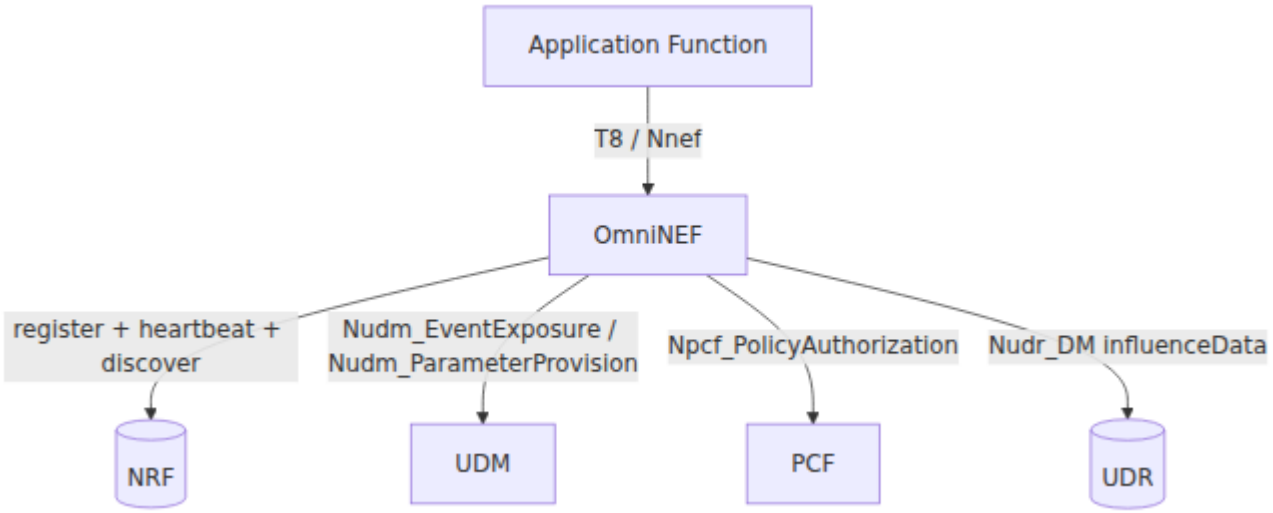
请求日志

标准请求日志涵盖了监听器处理的每个北向 SBI 请求。使用它来观察请求量、方法和路径，并将 AF 活动与翻译事件关联起来。

健康检查

健康状况最好通过结合以下内容来评估：

- 存活性：`GET /nnef/v1/status` 返回 `200 {"status":"UP"}` 当 SBI 监听器正在服务时。请参见操作指南。
- **NRF** 注册：确认 OmniNEF 在 NRF 中作为 `NEF` NF 实例出现并且正在发送心跳。注册行为在 操作指南 中描述。
- 日志信号：上述描述的授权、限流和翻译事件。



OmniNEF 操作指南

□述 | 配置参考 | 指标和监控 | 故障排除

本指南描述了 OmniNEF 作为 5G 核心的北向暴露网关的行为以及如何操作它。OmniNEF 是在 3GPP TS 23.501 §6.2.5 中定义的网络暴露功能，暴露 T8 API (TS 29.122) / Nnef 服务 (TS 29.522) 给应用功能。

目录

- 架构□述
- 请求生命周期
- 授权和限流
- 北向 API
- 南向互通
- SBI 端点
- NRF 注册
- 操作说明

架构概述

OmniNEF 终止面向外部 AF 的北向 API，并将每个请求转换为面向核心生产者 NF 的 SBI 操作。它以 NFType `NEF` 向 NRF 注册，并使用 NRF 发现来解析��务给定请求的 UDM、PCF 或 UDR。

请求生命周期

每个北向资源创建请求遵循相同的路径：

1. 授权 调用 AF 的 API 密钥，并检查其是否有权访问请求的 API。
2. 限流 检查 AF 的每秒请求上限。
3. 验证 请求体（目标 UE 标识符、所需 QoS、路由目标等）。
4. 发现 NRF 中的目标 NF（UDM/PCF/UDR），并选择一个负载感知实例。
5. 转换并发送 相应的 SBI 请求到生产者 NF。
6. 存储 创建的资源（拥有 AF、表示、下游拆除 URL），并返回 `201 Created`，带有指向单个资源的 `Location` 头。

`GET` 单个资源返回存储的表示；`DELETE` 在生产者 NF 中拆除资源（尽力而为），并移除 NEF 侧记录。

授权和限流

NEF 是不受信任的第三方 AF 和受信任的核心之间的边界，因此授权是强制性的（TS 23.501 §6.2.5）。

- 身份验证： AF 以 `Authorization: Bearer <key>` 或 `X-Api-Key: <key>` 的形式提供 API 密钥。密钥在 AF 注册表中查找。缺失或未知的密钥返回 `401`。
- 授权：每个 AF 的作用域为 `:all` API 或显式列表。已知的 AF 调用其没有权利访问的 API 返回 `403`。
- 限流：每个 AF 有一个每秒请求上限（其自身或配置的默认值）。超出该限制的 AF 返回 `429`。窗口是滑动的一秒。

有关如何注册 AF 的信息，请参见 配置参考。

北向 API

功能	北向资源	方法
监控事件 (Nnef_EventExposure)	`/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`	POST, GET, DELETE
参数配置 (Nnef_ParameterProvision)	`/nnef-pp/v1/{afId}/provisionings`	POST, GET, DELETE
带 QoS 的 AF 会话 (Nnef_AFsessionWithQoS)	`/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions`	POST, GET, DELETE
流量影响 (Nnef_TrafficInfluence)	`/3gpp-traffic-influence/v1/{afId}/subscriptions`	POST, GET, DELETE

监控事件

AF 订阅由 `externalId` 或 `msisdn` 标识的 UE 的网络事件。支持的 `monitoringType` 值映射到 UDM 事件类型:

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`

外部标识符映射到 UDM GPSI (`extid-<externalId>` 或 `msisdn-<msisdn>`).

参数□置

AF 为 UE (`externalId` / `msisdn`) 或组 (`externalGroupId`) 提供预期的 UE 行为或通信特性参数。接受显式的 `ppData` 对象或认可的顶级配置字段；NEF 通过 `Nudm_ParameterProvision` 应用这些参数，UDM 将其持久化到 UDR。

带 **QoS** 的 **AF** 会话

AF 提供 UE 地址 (`ueIpv4Addr` / `ueIpv6Addr`)、要处理的 IP 流和 `qosReference`（或请求的 QoS）。NEF 在 PCF 创建一个单独的应用会话上下文，并安装相应的策略到 SMF。

流量影响

AF 请求核心将选定流量引导到 DNAI / 应用位置。路由目标取决于范围：

- 单个 **UE**（`gpsi` 或 `supi` 存在）→ 在 **PCF** 中的应用会话。
- 组 / 任何 **UE**（没有单个标识符）→ 存储为 **UDR** 中的 `influenceData` 应用数据，PCF 在构建未来匹配会话的策略时读取。

南向互通

NEF 从 NRF 解析每个生产者 NF（`Nnrf_NFDiscovery`，按服务名称过滤）并选择负载最低的实例。然后发出映射的 SBI 请求：

- `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)

当生产者 NF 返回 `Location` 时，NEF 保留解析的绝对 URL，以便稍后可以删除资源。对于监控事件，NEF 向生产者 NF 注册一个 每个订阅 的通知回调 URL（`…/nnef-eventexposure/v1/notifications/{subId}`）；当生产者向该回调 POST 事件报告时，NEF 将其映射到 T8 `MonitoringNotification` 并转发到 AF 存储的 `notificationDestination`（事件暴露数据路径）。转发是尽力而为。NEF 始终以 `204` 确认生产者回调。NEF 会丢弃未知或过期的订阅的通知。请参见 通知转发故障排除条目。

SBI 端点

- `GET /nnef/v1/status`：存活探测；返回 `200 {"status":"UP"}`。
- 北向 API 表中的北向资源端点。

不匹配的路径返回 `404`，并带有 3GPP `ProblemDetails` ���体。

NRF 注册

在启动时，OmniNEF 以 NFType `NEF` 向 NRF 注册，宣传四个服务（`nnef-eventexposure`、`nnef-pp`、`nnef-afsessionwithqos`、`nnef-trafficinfluence`）及其 SBI IP 端点，然后在配置的间隔上进行心跳。容量和优先级来自共享的 `Omni5gEx.NRF.Config` 辅助工具。

操作说明

- 普通 **HTTP**：SBI 监听器提供普通 HTTP。对于超出受信网络的任何暴露，请在外部终止 TLS（反向代理或服务网格）。
- 非持久状态：AF 注册表、速率限制器窗口和创建的资源存储在内存中。重新启动时，AF 从配置中重新种子，NEF 会忘记之前创建的北向资源（底层核心 NF 资源在过期或直接删除之前会持续存在）。

- 下游拆除是尽力而为：`DELETE` 总是移除 NEF 侧记录，即使生产者 NF 短暂不可达；该失败会被记录。

OmniNEF 故障排除

目录

- 常见问题

常见问题

每个 AF 请求返回 401

AF 的 API 密钥不在注册表中。注册表默认是空的，因此新部署会拒绝所有请求，直到 AF 被配置。将 AF 添加到 `af_registry`（或 `NEF_AF_REGISTRY`），并确认客户端发送 `Authorization: Bearer <key>` 或 `X-Api-Key: <key>`。请参见 配置参考。

某些 API 返回 403

AF 是已知的，但其 `allowed_apis` 不包括它正在调用的 API。将 `allowed_apis` 设置为 `:all`，或将相关 API 原子添加到列表中。

AF 在负载下返回 429

AF 超出了每秒请求的上限。提高其 `rate_limit_per_sec`（或 `default_rate_limit_per_sec`），或限制客户端。窗口是一个滑动的一秒。

请求失败，返回 503 NF_UNAVAILABLE

NRF 发现没有 UDM/PCF/UDR ���例提供所需服务。确认目标 NF 已在 NRF 注册并且健康，以及 `nrf_uri` 是正确的。

请求失败，返回 502 TARGET_NF_NOT_REACHABLE

生产者 NF 已被发现，但对其的 SBI 调用失败。检查与生产者 NF 的连接性及其日志；NEF 记录了底层错误。

AF 创建了监控事件订阅但从未收到通知

事件通知现在遵循数据路径端到端：在创建时，NEF 在 UDM 注册一个 每个订阅 的回调（`.../nnef-eventexposure/v1/notifications/{subId}`）；当生产者 NF 向该回调 POST 事件报告时，NEF 将其映射到 T8 `MonitoringNotification` 并转发给 AF 的 `notificationDestination`。如果 AF 没有看到任何内容，请按顺序检查：

- 订阅携带了可达的 `notificationDestination`（当缺失时，NEF 记录 `subscription <id> has no notificationDestination`）。
- 生产者 NF 实际上正在发出报告，并且可以到达 NEF 的回调 URL（NEF 广告的 `sbi_base_url` 必须可以从 UDM/AMF 路由）。
- 转发 POST 成功。NEF 将失败的交付记录为 `relay to AF <url> ... failed`。转发是尽力而为：NEF 始终以 `204` 回应生产者回调，因此生产者不会将暂时不可用的 AF 视为永久回调失败。对于未知/过期的订阅，通知会被记录并丢弃（同样是 `204`）。

请求失��，返回 400

请求体缺少该能力的必填字段：UE 标识符（`externalId`/`msisdn`）、AF QoS 会话的 `qosReference`、流量影响的路由目标，或不支持的 `monitoringType`。`ProblemDetails` 的 `detail` 字段命名了具体的验证失败。