Référence de Configuration OmniNEF

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

Toute la configuration se trouve sous la clé d'application `:omninef`. Les valeurs par défaut à la compilation se trouvent dans `config/config.exs` (miroité par `OmniNef.Config`) ; les déploiements en production remplacent un sous-ensemble via des variables d'environnement dans `config/runtime.exs`.

Table des Matières

- Écouteur SBI
- NRF et PLMN
- Registre AF
- Contrôle de Flux
- Variables d'Environnement

Écouteur SBI

Clé	Type	Par défaut	Description
`sbi_scheme`	chaîne	`"http"`	Schéma annoncé dans le profil NRF. L'écouteur lui-même sert du HTTP simple.
`sbi_addr`	chaîne	`"127.0.0.30"`	Adresse de liaison/annonce SBI.
`sbi_port`	entier	`7777`	Port d'écoute SBI (API montante + statut).

NRF et PLMN

Clé	Type	Par défaut	
`nrf_uri`	chaîne	`"http://127.0.0.10:7777"`	URI de base d découverte.
`mcc`	chaîne	`"999"`	MCC PLMN se d'enregistrem
`mnc`	chaîne	`"70"`	MNC PLMN se
`heartbeat_interval`	entier (ms)	`10_000`	Intervalle de
`nef_fqdn`	chaîne	dérivé	FQDN de ce N `nef.5gc.mnc<`

Registre AF

`af_registry` est une carte indexée par la clé API de l'AF. Chaque valeur définit ce que l'AF peut faire. Elle est vide par défaut : **aucun AF ne peut appeler le NEF tant qu'un n'est pas provisionné**.

```
config :omninef,
  af_registry: %{
    "af-secret-001" => %{
      af_id: "af-acme",             # identifiant écho dans les
journaux
      allowed_apis: :all,           # ou une liste d'atomes API
(voir ci-dessous)
      rate_limit_per_sec: 20        # optionnel ; revient à
default_rate_limit_per_sec
    }
  }
```

`allowed_apis` est soit `:all` soit une liste tirée de :

Atome API	Ressource montante
`:monitoring_event`	`/3gpp-monitoring-event/...`
`:parameter_provision`	`/nnef-pp/...`
`:af_session_with_qos`	`/3gpp-as-session-with-qos/...`
`:traffic_influence`	`/3gpp-traffic-influence/...`

La clé API est présentée par l'AF sous la forme `Authorization: Bearer <key>` ou `X-Api-Key: <key>`.

Contrôle de Flux

Clé	Type	Par défaut	Description
`default_rate_limit_per_sec`	entier	`10`	Plafond par demande AF appliqué lorsqu'une spécification AF omet `rate_limit_per_sec`.

Le contrôle de flux utilise une fenêtre glissante d'une seconde par AF. Un AF à ou au-dessus de son plafond reçoit `429`.

Variables d'Environnement

Définies dans `config/runtime.exs` pour `MIX_ENV=prod`. Les variables non définies reviennent aux valeurs par défaut à la compilation ci-dessus.

Variable	Correspond à	
`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`	dérivé
`NEF_DEFAULT_RATE_LIMIT_PER_SEC`	`default_rate_limit_per_sec`	`10`
`NEF_AF_REGISTRY`	`af_registry` (JSON)	non dé

`NEF_AF_REGISTRY` est un objet JSON de la même forme que la carte `af_registry`, avec `allowed_apis` comme la chaîne `"all"` ou un tableau de chaînes de noms d'API :

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

Un JSON mal formé provoque une erreur au démarrage, de sorte qu'une mauvaise configuration de déploiement échoue rapidement plutôt que de désactiver silencieusement tous les AFs.

Métriques et Surveillance d'OmniNEF

Vue d'ensemble | Guide des opérations | Référence de configuration | Dépannage

État actuel

L'observabilité est fournie par des **journaux d'application structurés** et un journal standard des requêtes. Les opérateurs surveillent OmniNEF à travers ses journaux, qui capturent l'autorisation, le throttling et l'activité de traduction à travers les interfaces nord et sud.

Ce qu'il faut surveiller dans les journaux

Les journaux d'application sont le signal principal pour faire fonctionner OmniNEF.

Autorisation et Throttling

Les requêtes nord rejetées apparaissent sous forme de réponses `ProblemDetails`. Surveillez :

- Un taux croissant de `401 UNAUTHORIZED` : un AF présente une clé API manquante ou inconnue (un client mal configuré ou un AF non provisionné).
- `403 OPERATION_NOT_ALLOWED` : un AF connu appelle une API à laquelle il n'est pas autorisé. Vérifiez les `allowed_apis` de l'AF.

- `429 TOO_MANY_REQUESTS` : un AF dépasse son plafond de requêtes. Envisagez d'augmenter son `rate_limit_per_sec` ou d'enquêter sur le client.

Traduction Nord-Sud

Chaque capacité enregistre l'opération qu'elle effectue, y compris l'identifiant UE cible et le NF producteur résolu. Surveillez-les pour confirmer que les abonnements et les sessions atteignent le UDM/PCF/UDR.

- `503 NF_UNAVAILABLE` indique que la découverte NRF n'a trouvé aucune instance UDM/PCF/UDR appropriée.
- `502 TARGET_NF_NOT_REACHABLE` indique que le NF producteur a été découvert mais que l'appel SBI a échoué.
- `400 MANDATORY_IE_INCORRECT` indique un échec de validation de la requête (identifiant UE manquant, QoS, cible de routage, ou un type de surveillance non pris en charge).

Journalisation des requêtes

La journalisation standard des requêtes couvre chaque requête SBI nord traitée par l'auditeur. Utilisez-la pour observer le volume des requêtes, les méthodes et les chemins, et pour corréler l'activité de l'AF avec les événements de traduction.

Vérification de la santé

La santé est mieux évaluée en combinant :

- **Vérification de vivacité :** `GET /nnef/v1/status` retourne `200 {"status":"UP"}` lorsque l'auditeur SBI est opérationnel. Voir le Guide des opérations.
- **Enregistrement NRF :** confirmez qu'OmniNEF apparaît dans le NRF en tant qu'instance NF `NEF` et envoie des signaux de vie. Le comportement d'enregistrement est décrit dans le Guide des opérations.

- **Signaux de journal :** les événements d'autorisation, de throttling et de traduction décrits ci-dessus.

Guide des opérations OmniNEF

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

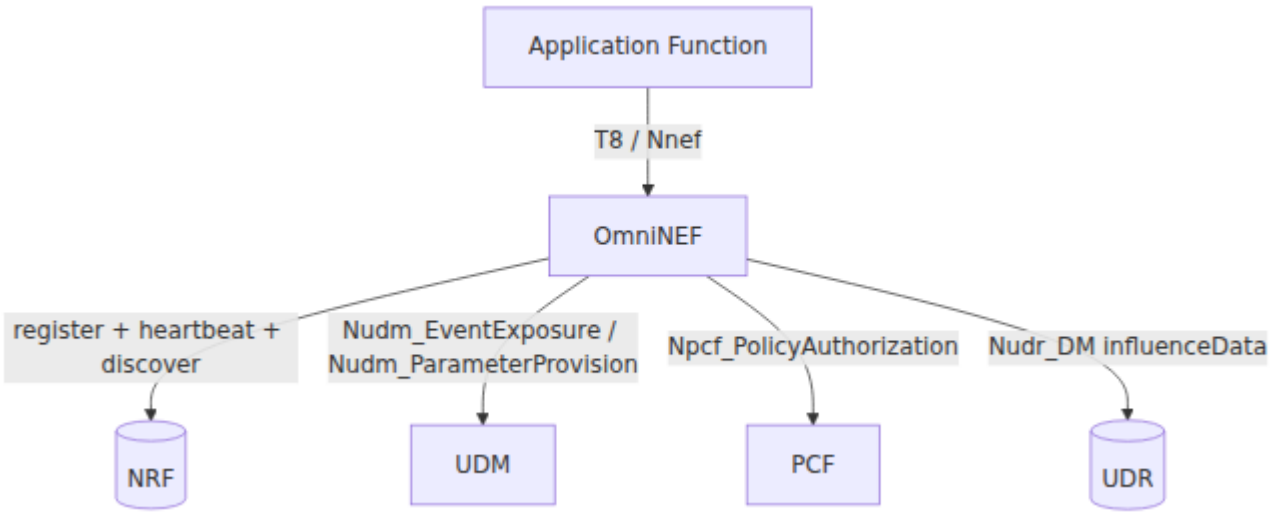
Ce guide décrit comment OmniNEF se comporte en tant que passerelle d'exposition montante du cœur 5G et comment l'opérer. OmniNEF est la fonction d'exposition réseau définie dans 3GPP TS 23.501 §6.2.5, exposant l'API T8 (TS 29.122) / services Nnef (TS 29.522) vers les fonctions d'application.

Table des matières

- Vue d'ensemble de l'architecture
- Cycle de vie de la demande
- Autorisation et limitation
- APIs montantes
- Interconnexion descendante
- Points de terminaison SBI
- Enregistrement NRF
- Remarques opérationnelles

Vue d'ensemble de l'architecture

OmniNEF termine l'API montante vers les AF externes et traduit chaque demande en une opération SBI vers un NF producteur central. Il s'enregistre auprès du NRF en tant que NFType `NEF` et utilise la découverte NRF pour résoudre le UDM, PCF ou UDR qui sert une demande donnée.



Cycle de vie de la demande

Chaque demande de création de ressource montante suit le même chemin :

1. **Autoriser** l'AF appelant à partir de sa clé API et vérifier qu'il est habilité à utiliser l'API demandée.
2. **Limiter** par rapport au plafond de demandes par seconde de l'AF.
3. **Valider** le corps de la demande (identifiant UE cible, QoS requise, cible de routage, …).
4. **Découvrir** le NF cible (UDM/PCF/UDR) à partir du NRF et sélectionner une instance consciente de la charge.
5. **Traduire et envoyer** la demande SBI correspondante au NF producteur.
6. **Stocker** la ressource créée (AF propriétaire, représentation, URL de d��mantèlement en aval) et retourner `201 Created` avec un en-tête `Location` pointant vers la ressource individuelle.

`GET` sur la ressource individuelle retourne la représentation stockée ; `DELETE` démantèle la ressource dans le NF producteur (meilleur effort) et supprime l'enregistrement côté NEF.

Autorisation et limitation

Le NEF est la frontière entre les AF tiers non fiables et le cœur de confiance, donc l'autorisation est obligatoire (TS 23.501 §6.2.5).

- **Authentification :** l'AF présente une clé API sous la forme `Authorization: Bearer <key>` ou `X-Api-Key: <key>`. Les clés sont recherchées dans le registre AF. Une clé manquante ou inconnue retourne `401`.
- **Droit d'accès :** chaque AF est limité à `:all` APIs ou une liste explicite. Un AF connu appelant une API à laquelle il n'est pas habilité retourne `403`.
- **Limitation :** chaque AF a un plafond de demandes par seconde (le sien ou le défaut configuré). Un AF le dépassant retourne `429`. La fenêtre est glissante d'une seconde.

Voir la Référence de configuration pour savoir comment intégrer un AF.

APIs montantes

Capacité	Ressource montante	Méthod
Év��nements de surveillance (Nnef_EventExposure)	`/3gpp-monitoring-event/v1/{scsAsId}/subscriptions`	POST, G DELETE
Provisionnement de paramètres (Nnef_ParameterProvision)	`/nnef-pp/v1/{afId}/provisionings`	POST, G DELETE
Session AF avec QoS (Nnef_AFsessionWithQoS)	`/3gpp-as-session-with-qos/v1/{scsAsId}/subscriptions`	POST, G DELETE
Influence du trafic (Nnef_TrafficInfluence)	`/3gpp-traffic-influence/v1/{afId}/subscriptions`	POST, G DELETE

Événements de surveillance

Un AF s'abonne aux événements réseau pour un UE identifié par `externalId` ou `msisdn`. Les valeurs `monitoringType` prises en charge correspondent aux types d'événements 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`

L'identifiant externe est mappé à un GPSI UDM (`extid-<externalId>` ou `msisdn-<msisdn>`).

Provisionnement de paramètres

Un AF provisionne des paramètres de comportement attendu de l'UE ou de caractéristiques de communication pour un UE (`externalId` / `msisdn`) ou un groupe (`externalGroupId`). Soit un objet `ppData` explicite soit les champs de provisionnement de niveau supérieur reconnus sont acceptés ; le NEF les applique via `Nudm_ParameterProvision`, que l'UDM persiste dans l'UDR.

Session AF avec QoS

Un AF fournit l'adresse de l'UE (`ueIpv4Addr` / `ueIpv6Addr`), les flux IP à traiter, et une `qosReference` (ou QoS demandée). Le NEF crée un contexte de session d'application individuelle au PCF, qui installe la politique correspondante vers le SMF.

Influence du trafic

Un AF demande au cœur de diriger le trafic sélectionné vers un emplacement DNAI / application. La cible de routage dépend de la portée :

- **UE individuel** (`gpsi` ou `supi` présent) → une session d'application au **PCF**.
- **Groupe / tout-UE** (pas d'identifiant individuel) → stocké en tant que données d'application `influenceData` dans le **UDR**, que le PCF lit lors de la construction de la politique pour les sessions de correspondance futures.

Interconnexion descendante

Le NEF résout chaque NF producteur à partir du NRF (`Nnrf_NFDiscovery`, filtré par nom de service) et sélectionne l'instance à charge la plus faible. Il émet ensuite la demande SBI mappée :

- `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)

Lorsqu'un NF producteur retourne un `Location`, le NEF conserve l'URL absolue résolue afin que la ressource puisse être supprimée plus tard. Pour les événements de surveillance, le NEF enregistre une URL de rappel de notification **par abonnement** avec le NF producteur (`…/nnef-eventexposure/v1/notifications/{subId}`) ; lorsque le producteur POSTe un rapport d'événement à ce rappel, le NEF le mappe à une `MonitoringNotification` T8 et le relaye à la `notificationDestination` stockée de l'AF (le chemin de données d'exposition d'événements). Le relais est un meilleur effort. Le NEF accuse toujours réception du rappel du producteur avec `204`. Le NEF ignore les notifications pour un abonnement inconnu ou expiré. Voir l'entrée de dépannage sur le relais de notification.

Points de terminaison SBI

- `GET /nnef/v1/status`: sonde de vivacité ; retourne `200 {"status":"UP"}`.
- Les points de terminaison de ressources montantes dans le tableau APIs montantes.

Les chemins non appariés retournent `404` avec un corps `ProblemDetails` 3GPP.

Enregistrement NRF

Au démarrage, OmniNEF s'enregistre auprès du NRF en tant que NFType `NEF`, annonçant quatre services (`nnef-eventexposure`, `nnef-pp`, `nnef-afsessionwithqos`, `nnef-trafficinfluence`) et son point de terminaison IP SBI, puis envoie des signaux de vie à l'intervalle configuré. La capacité et la priorité proviennent des helpers partagés `Omni5gEx.NRF.Config`.

Remarques opérationnelles

- **HTTP simple :** l'écouteur SBI sert du HTTP simple. Terminez TLS à l'extérieur (un proxy inverse ou une maillage de services) pour toute exposition au-delà d'un réseau de confiance.
- **État non persistant :** le registre AF, les fenêtres de limitation de taux et le stockage de ressources créées sont en mémoire. Au redémarrage, les AF sont resemencés à partir de la configuration et les ressources montantes précédemment créées sont oubliées par le NEF (les ressources NF centrales sous-jacentes persistent jusqu'à ce qu'elles expirent ou soient supprimées directement).
- **Le démantèlement en aval est un meilleur effort :** un `DELETE` supprime toujours l'enregistrement côté NEF même si le NF producteur est brièvement inaccessible ; l'échec est enregistré.

Dépannage d'OmniNEF

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

Table des matières

- Problèmes courants

Problèmes courants

Chaque requête AF renvoie 401

La clé API de l'AF n'est pas dans le registre. Le registre est vide par défaut, donc un déploiement frais rejette tout jusqu'à ce qu'un AF soit provisionné. Ajoutez l'AF à `af_registry` (ou `NEF_AF_REGISTRY`) et confirmez que le client envoie `Authorization: Bearer <key>` ou `X-Api-Key: <key>`. Voir la Référence de configuration.

Un AF reçoit 403 sur certaines API

L'AF est connu mais ses `allowed_apis` n'incluent pas l'API qu'il appelle. Définissez `allowed_apis` sur `:all`, ou ajoutez l'atome API pertinent à la liste.

Un AF reçoit 429 sous charge

L'AF dépasse son plafond de requêtes par seconde. Augmentez son `rate_limit_per_sec` (ou `default_rate_limit_per_sec`), ou limitez le client. La fenêtre est glissante d'une seconde.

Les requêtes échouent avec 503 NF_UNAVAILABLE

La découverte NRF n'a retourné aucune instance UDM/PCF/UDR offrant le service requis. Confirmez que le NF cible est enregistré auprès du NRF et en bonne santé, et que `nrf_uri` est correct.

Les requêtes échouent avec 502 TARGET_NF_NOT_REACHABLE

Le NF producteur a été découvert mais l'appel SBI vers celui-ci a échoué. Vérifiez la connectivité avec le NF producteur et ses journaux ; le NEF enregistre l'erreur sous-jacente.

Un AF crée une souscription d'événement de surveillance mais ne reçoit jamais de notifications

Les notifications d'événements suivent désormais le chemin des données de bout en bout : lors de la création, le NEF enregistre un **callback par souscription** avec l'UDM (`.../nnef-eventexposure/v1/notifications/{subId}`) ; lorsque le NF producteur POSTe un rapport d'événement à ce callback, le NEF le mappe à un T8 `MonitoringNotification` et le relaye à la `notificationDestination` de l'AF. Si l'AF ne voit rien, vérifiez, dans l'ordre :

- La souscription contenait une `notificationDestination` accessible (le NEF enregistre `subscription <id> has no notificationDestination` lorsqu'elle est absente).
- Le NF producteur émet effectivement des rapports et peut atteindre l'URL de callback du NEF (le `sbi_base_url` annoncé du NEF doit être routable depuis l'UDM/AMF).
- Le POST de relais réussit. Le NEF enregistre une livraison échouée comme `relay to AF <url> ... failed`. Le relais est fait au mieux : le NEF répond toujours au callback du producteur avec `204` afin que le producteur ne considère pas un AF temporairement hors service comme un échec de

callback permanent. Les notifications pour une souscription inconnue/expirée sont enregistrées et supprimées (également `204`).

Les requêtes échouent avec 400

Le corps de la requête manque d'un champ obligatoire pour cette capacité : un identifiant UE (`externalId`/`msisdn`), un `qosReference` pour une session QoS AF, une cible de routage pour l'influence du trafic, ou un `monitoringType` non pris en charge. Le champ `detail` des `ProblemDetails` nomme la défaillance de validation spécifique.