

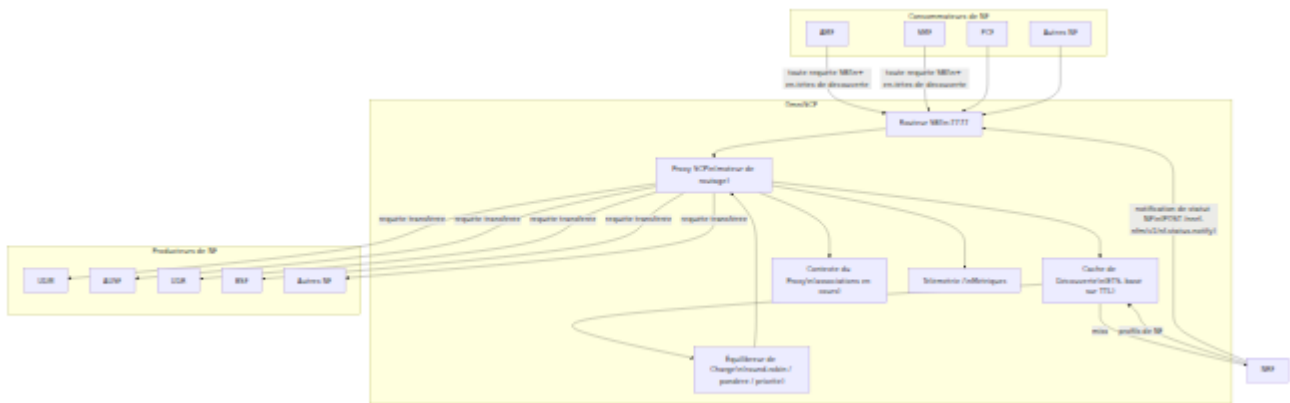
# Guide d'Opérations OmniSCP

## Table des Matières

1. Aperçu du Composant
  2. Rôle 3GPP et Références de Spécifications
  3. Points de Terminaison SBI
  4. Référence de Configuration
  5. Procédures Clés
  6. Observabilité
  7. Limitations Connues
  8. Dépannage
- 

## Aperçu du Composant

OmniSCP implémente la fonction réseau Proxy de Communication de Service (SCP) définie dans 3GPP TS 29.500 et TS 23.501. Le SCP agit comme un proxy HTTP inverse entre les consommateurs de NF et les producteurs de NF dans l'Architecture Basée sur les Services 5G (SBA). Il fournit la découverte NRF déléguée, l'équilibrage de charge entre les instances de producteurs de NF, la réessai en cas d'échec, et la mise en cache des résultats de découverte NRF.



## Modes de Routage

Le SCP prend en charge trois modes de routage, évalués par ordre de priorité sur chaque requête entrante :

1. **Transfert direct** — l'en-tête `3gpp-Sbi-Target-apiRoot` est présent. La requête est transférée directement à l'URI de base spécifiée sans recherche NRF.
2. **Découverte déléguée** — les en-têtes `3gpp-Sbi-Discovery-target-nf-type` et `3gpp-Sbi-Discovery-service-names` sont présents. Le SCP interroge le NRF (ou utilise le cache) et sélectionne une instance via la stratégie d'équilibrage de charge configurée.
3. **Inférence basée sur le chemin** — Aucun en-tête de routage présent. Le SCP infère le type de NF cible à partir du préfixe de chemin (par exemple, `/nudm-` → UDM) et effectue une découverte déléguée.

# Rôle 3GPP et Références de Spécifications

Élément	Référence
Définition NF SCP	3GPP TS 23.501 Section 7.3
Modèle de communication indirect SCP	3GPP TS 29.500 Section 6.10
En-têtes 3gpp-Sbi-Discovery-*	3GPP TS 29.500 Section 6.10.3
En-tête 3gpp-Sbi-Target-apiRoot	3GPP TS 29.500 Section 6.10.3.2
En-tête 3gpp-Sbi-Producer-Id	3GPP TS 29.500 Section 6.10.3.3
Équilibrage de charge SCP	3GPP TS 29.500 Section 6.10.4
Service de découverte NF	3GPP TS 29.510 Section 6.2
Notification de statut NF NRF	3GPP TS 29.510 Section 6.3
Cadre commun SBI	3GPP TS 29.500

---

## Points de Terminaison SBI

OmniSCP fonctionne comme un proxy transparent. Il n'y a qu'un seul point de terminaison géré localement ; tous les autres chemins sont transférés au producteur de NF approprié.

Méthode	Chemin	Géré Localement	Description
POST	/nnrf-nfm/v1/nf-status-notify	Oui	Reçoit les notifications de changement de statut NF NRF. Lors des événements <code>NF_DEREGISTERED</code> ou <code>NF_PROFILE_CHANGED</code> , invalide l'ensemble du cache de découverte. Retourne 204 No Content.
*	/* (tous les autres chemins)	Non — transféré	Toute méthode et chemin ne correspondant pas à ce qui précède est transféré au producteur de NF résolu selon le mode de routage actif.

## Réponses d'Erreur du Proxy

Lorsque le SCP ne peut pas compléter une opération de proxy, il retourne un corps `ProblemDetails` par rapport à TS 29.500.

Statut HTTP	Cause	Condition
400 Bad Request	MANDATORY_IE_MISSING	Aucune information de routage disponible : pas de 3gpp-Sbi-Target-apiRoot, pas d'en-têtes de découverte, et le chemin ne peut pas être mappé à un service connu.
502 Bad Gateway	TARGET_NF_NOT_REACHABLE	Toutes les instances de producteurs de NF sélectionnées ont retourné des erreurs 5xx ou des erreurs de connexion après des réessais, ou aucune URI SBI n'a pu être résolue pour une instance découverte.
504 Gateway Timeout	NF_DISCOVERY_FAILURE	La découverte NRF a retourné zéro instance de NF pour le service demandé.
500 Internal Server Error	SYSTEM_FAILURE	Erreur interne inattendue dans le proxy SCP.

# En-têtes 3gpp-Sbi Consommés

En-tête	Description
<code>3gpp-Sbi-Target-apiRoot</code>	Cible de routage directe. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-target-nf-type</code>	Type de NF à découvrir (par exemple, <code>UDM</code> ). Utilisé pour la découverte déléguée. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-service-names</code>	Liste de noms de services séparés par des virgules. La première valeur est utilisée comme principale. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-requester-nf-type</code>	Type de NF demandeur pour la portée de la requête NRF. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-target-plmn-list</code>	Liste de PLMN cible. Transmise à la découverte NRF. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-requester-snssai-list</code>	Liste S-NSSAI demandeur. Transmise à la découverte NRF. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-nf-set-id</code>	Filtre d'ID de set de NF pour la découverte. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-target-nf-instance-id</code>	ID d'instance de NF spécifique à cibler. Supprimé avant le transfert.
<code>3gpp-Sbi-Discovery-requester-nf-instance-id</code>	ID d'instance demandeur. Supprimé avant le transfert.

## En-têtes 3gpp-Sbi Produits

En-tête	Description
<code>3gpp-Sbi-Producer-Id</code>	Ajouté à chaque réponse transférée. Contient l' <code>nfInstanceId</code> du producteur de NF qui a traité la requête, permettant le lien consommateur-producteur par rapport à TS 29.500 Section 6.10.3.3.

## Référence de Configuration

Tous les paramètres sont définis via l'environnement de l'application (typiquement `config/runtime.exs`).

```
config :omniscp,  
  sbi_scheme: "http",  
  sbi_addr: "127.0.0.200",  
  sbi_port: 7777,  
  nrf_uri: "http://127.0.0.10:7777",  
  mcc: "999",  
  mnc: "70",  
  heartbeat_interval: 10_000,  
  discovery_cache_ttl: 60_000,  
  lb_strategy: :round_robin,  
  max_retries: 1,  
  upstream_timeout: 5_000
```

# Tableau des Paramètres

Paramètre	Par Défaut	Type	Descript
sbi_scheme	"http"	chaîne	Schéma de transport pour l'écouteur SBI
sbi_addr	"127.0.0.200"	chaîne	Adresse IP à laquelle le serveur HTTP SBI est accessible. Les consommateurs de NF doivent router le trafic vers cette adresse.
sbi_port	7777	entier	Port TCP sur lequel le serveur HTTP SBI écoute
nrf_uri	"http://127.0.0.10:7777"	chaîne	URI de base de l'interface NRF. Utilisé pour l'enregistrement de NF, le heartbeat, et les requêtes de découverte de NF au nom des consommateurs
mcc	"999"	chaîne	Code de Pay Mobile. Inclus dans le profil SCP enregistré avec le NRF.

Paramètre	Par Défaut	Type	Descript
<code>mnc</code>	<code>"70"</code>	chaîne	Code de Rés Mobile. Inclu dans le profi SCP enregist avec le NRF.
<code>heartbeat_interval</code>	<code>10_000</code>	entier (ms)	Intervalle en les requêtes heartbeat NI
<code>discovery_cache_ttl</code>	<code>60_000</code>	entier (ms)	<p>Durée de vie les entrées c cache de découverte l indexées par <code>{target_nf_ service_nam</code></p> <p>Les entrées expirées son évincées paresseusen lors de la recherche et une tâche de nettoyage en arrière-plan toutes les 30 secondes.</p> <p>Augmentez   des déploier stables ; dim lorsque les p de NF chang fréquemmer</p>

Paramètre	Par Défaut	Type	Descript
lb_strategy	:round_robin	atome	Stratégie d'équilibrage charge pour sélection de producteurs NF. Valeurs valides : :round_robin, :weighted, :priority. section Équilibrage Charge pour sémantiques
max_retries	1	entier	Nombre maximum de tentatives de réessai lorsqu'un producteur retourne des erreurs 5xx ou une erreur de connexion. Une valeur de 1 signifie une tentative ou plus un réessai. Réglez sur 0 pour désactiver les réessais.
upstream_timeout	5_000	entier (ms)	Délai d'attente pour les requêtes HTTP en amont

Paramètre	Par Défaut	Type	Descript
			vers les producteurs (délai de réception). Les requêtes qui dépassent ce délai sont considérées comme des échecs et peuvent déclencher un réessai.

## Stratégies d'Équilibrage de Charge

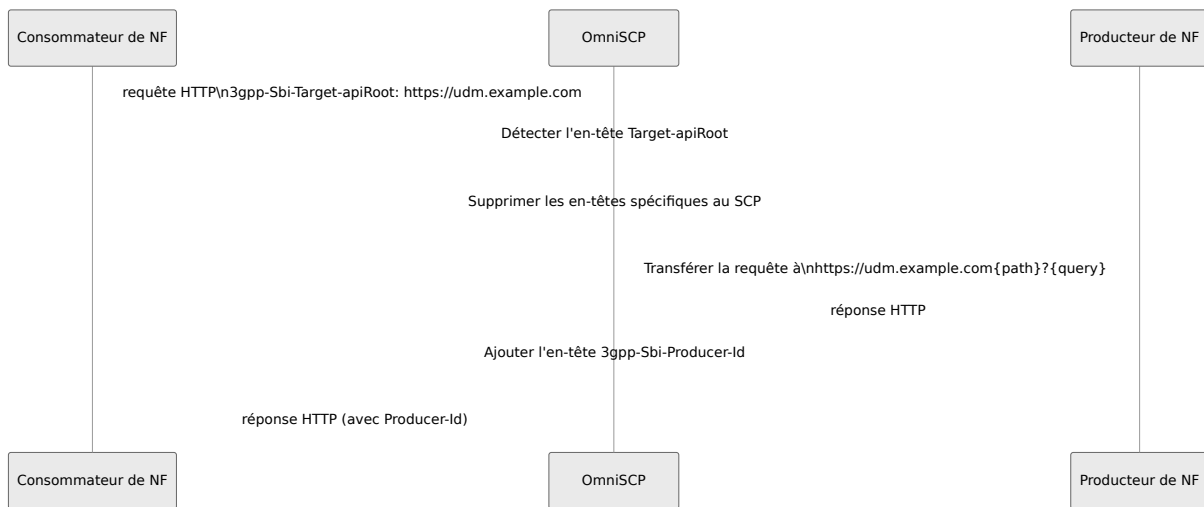
Stratégie	Description
<code>:round_robin</code>	Parcourt les instances saines dans l'ordre. L'état est maintenu par paire <code>{nf_type, service_name}</code> . C'est la stratégie par défaut et recommandée pour des déploiements NF uniformes.
<code>:weighted</code>	Sélectionne l'instance avec le score <code>load - capacity</code> le plus bas. Utilise les champs <code>load</code> et <code>capacity</code> du profil NF NRF. Privilégie les instances avec une haute capacité et une faible charge actuelle.
<code>:priority</code>	Sélectionne l'instance avec la valeur <code>priority</code> la plus basse (priorité la plus élevée). Utile pour des déploiements actif/standby.

Une instance est marquée comme non saine après 3 échecs consécutifs et se rétablit automatiquement après une période de refroidissement de 30

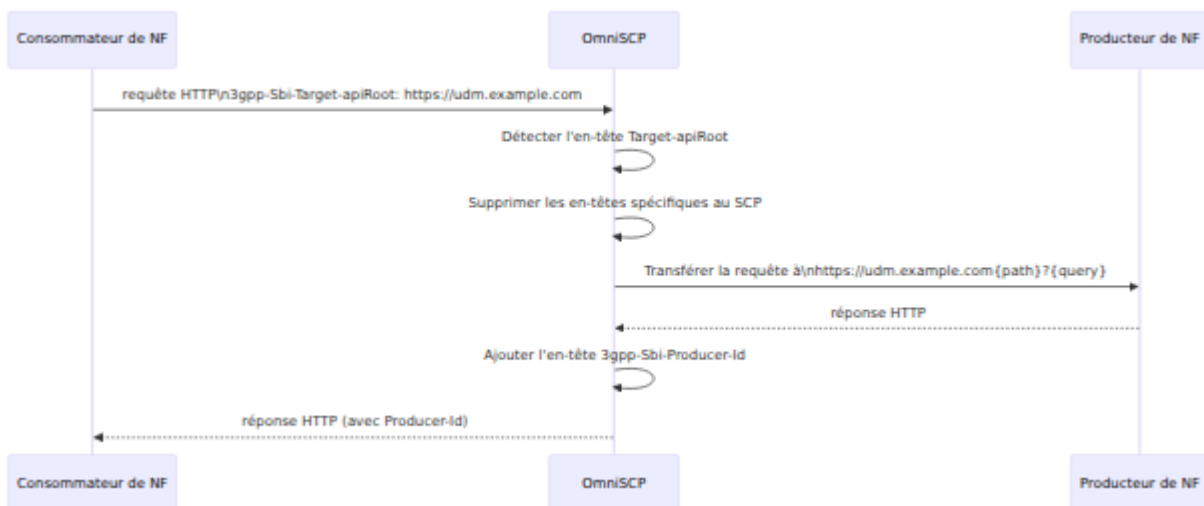
secondes. Lorsque toutes les instances sont non saines, l'équilibreur de charge revient à la liste complète des instances.

# Procédures Clés

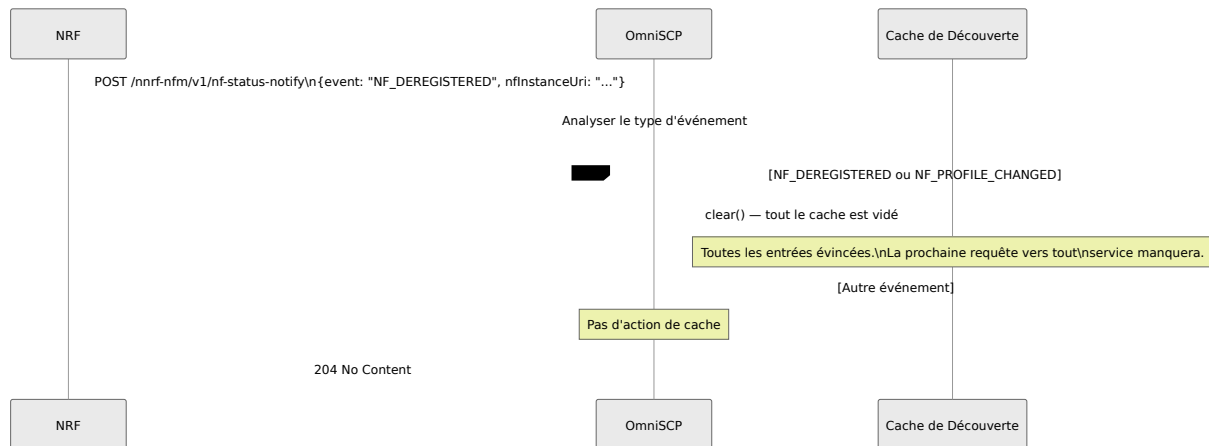
## Transfert Direct (Mode 1)



## Découverte Déléguée et Transfert (Mode 2)



# Notification de Statut NRF (Invalidation du Cache)



## Inférence de Service Basée sur le Chemin (Mode 3)

Lorsque aucun en-tête de routage n'est présent, le SCP extrait le nom du service à partir du préfixe de chemin de la requête et le mappe à un type de NF en utilisant le tableau intégré suivant :

Préfixe de Chemin	Type de NF
nudm-	UDM
nausf-	AUSF
namf-	AMF
nsmf-	SMF
npcf-	PCF
nudr-	UDR
nnssf-	NSSF
nbsf-	BSF
nnrf-	NRF

Remarque : les préfixes `nchf-`, `nnef-`, et `naf-` ne figurent pas dans la carte intégrée (limitation SCP-L1). Les requêtes vers les services CHF, NEF ou AF nécessitent des en-têtes de découverte explicites lors de l'utilisation du mode 3.

---

# Observabilité

## Événements de Télémétrie

Événement	Mesures	Étiquettes	Description
<code>[ :omniscp, :proxy, :requests]</code>	<code>count,</code> <code>duration_ms</code>	<code>target_nf_type,</code> <code>result</code>	Résultat du proxy par requête
<code>[ :omniscp, :proxy, :result]</code>	<code>count,</code> <code>duration_ms</code>	<code>target_nf_type,</code> <code>result</code>	Même événement utilisé pour l'histogramme de distribution
<code>[ :omniscp, :discovery, :cache]</code>	<code>hits,</code> <code>misses</code>	<code>target_nf_type,</code> <code>service_name</code>	Hit/miss de cache par service
<code>[ :omniscp, :cache, :hit]</code>	<code>count</code>	—	Compteur agrégé de hits de cache
<code>[ :omniscp, :cache, :miss]</code>	<code>count</code>	—	Compteur agrégé de misses de cache
<code>[ :omniscp, :associations, :active]</code>	<code>count</code>	—	Mesure : associations de proxy actives
<code>[ :omni5g, :nrf, :registration]</code>	<code>status</code>	<code>nf_type</code>	Statut d'enregistrement NRF (1=registré, 0=non)

Valeurs des étiquettes de résultat : `success` (2xx/3xx), `client_error` (4xx), `server_error` (5xx), `error` (connexion/délai).

## Métriques Prometheus

### Métriques du Proxy SCP

Métrique	Type	Étiquettes
<code>omni_scp.proxy.requests.count</code>	compteur	<code>target_nf_type</code> , <code>result</code>
<code>omni_scp.proxy.requests.duration_ms</code>	résumé	<code>target_nf_type</code>
<code>omni_scp.proxy_requests.total</code>	compteur	<code>target_nf_type</code> , <code>result</code>
<code>omni_scp.proxy_request.duration_ms</code>	distribution	<code>target_nf_type</code>
<code>omni_scp.active_associations.count</code>	jauge	--

### Métriques de Cache

Métrie	Type	Étiquettes	Descr
<code>omni_scp.discovery.cache.hits</code>	compteur	<code>target_nf_type</code> , <code>service_name</code>	Hits de cache service
<code>omni_scp.discovery.cache.misses</code>	compteur	<code>target_nf_type</code> , <code>service_name</code>	Misses cache service
<code>omni_scp.cache_hits.total</code>	compteur	--	Compt agrégé hits de cache
<code>omni_scp.cache_misses.total</code>	compteur	--	Compt agrégé misses cache

### Métries NRF

Métrie	Type	Étiquettes	Description
<code>omni_scp.nrf.registration.status</code>	jauge	<code>nf_type</code>	Statut d'enregistreme NRF (1=registr 0=non)

### Métries BEAM VM

Métrique	Type	Description
<code>beam.memory.total</code>	jauge	Mémoire totale BEAM en octets
<code>beam.memory.processes</code>	jauge	Mémoire utilisée par les processus Erlang
<code>beam.memory.processes_used</code>	jauge	Mémoire réellement utilisée par les processus
<code>beam.memory.system</code>	jauge	Mémoire système
<code>beam.memory.atom</code>	jauge	Mémoire totale des atomes
<code>beam.memory.atom_used</code>	jauge	Mémoire des atomes utilisée
<code>beam.memory.binary</code>	jauge	Mémoire binaire
<code>beam.memory.code</code>	jauge	Mémoire de code
<code>beam.memory.ets</code>	jauge	Mémoire de table ETS
<code>beam.processes.count</code>	jauge	Nombre de processus Erlang
<code>beam.ports.count</code>	jauge	Nombre de ports Erlang
<code>beam.atom.count</code>	jauge	Nombre d'atomes
<code>beam.vm.uptime</code>	jauge	Temps de fonctionnement de la VM en secondes

# Modèles de Journal

Niveau	Modèle	Signification
info	Notification de statut NRF reçue	Notification de statut NF reçue
info	Notification NRF : événement=<E> nf=<URI>	Événement de notification analysé
debug	Transfert direct SCP : <METHOD> <URL>	Transfert du mode 1
debug	Transfert délégué SCP : <METHOD> <URL> (tentative <N>)	Tentative de transfert des modes 2/3
warning	SCP réessaie après <STATUS> de <ID>...	Réessai déclenché par 5xx
warning	SCP réessaie après erreur de <ID>...	Réessai déclenché par une erreur de connexion
warning	SCP ne peut pas déterminer la cible pour <METHOD> <PATH>	Chemin du mode 3 non dans la carte de service
warning	La découverte NRF n'a retourné aucune instance pour <NF>/<SVC>	La découverte a retourné une liste vide
warning	Toutes les instances de NF sont non saines, retour à la liste complète	Recul de la santé LB
error	Échec de la découverte NRF : ...	Erreur de requête NRF

Niveau	Modèle	Signification
error	Erreur de proxy SCP : ...	Échec de proxy inattendu
info	Instance NF <ID> récupérée après refroidissement	Santé de l'instance restaurée

---

# Limitations Connues

ID	Sévérité	Description
SCP-H4	Élevée	<del>La dé-concealement ECIES SUCI n'est pas implémentée.</del> <b>RÉSOLU.</b> La dé-concealement du Profil A ECIES (X25519) et du Profil B (secp256r1) est maintenant implémentée dans <code>Omni5gEx.Crypto.SUPI</code> selon l'Annexe C de TS 33.501. OmniUDM effectue la dé-concealement avant la recherche UDR en utilisant les clés privées du réseau domestique configurées via <code>hnet_key_dir</code> . Le SCP n'a pas besoin de dé-concealement des SUCI dans le modèle de communication directe standard.
SCP-M1	Moyenne	Le contrôle de surcharge n'est pas implémenté. L'en-tête <code>3gpp-Sbi-0ci</code> (Informations de Contrôle de Surcharge) n'est pas généré ou consommé. Dans les scénarios de surcharge, le SCP continuera à transférer les requêtes sans réduire la charge ou exercer une pression sur les consommateurs.
SCP-M2	Moyenne	L'indication de contrôle de charge n'est pas implémentée. L'en-tête <code>3gpp-Sbi-Lci</code> (Informations de Contrôle de Charge) n'est pas généré. Les consommateurs ne peuvent pas utiliser OmniSCP pour obtenir des indices de charge de NF pour leurs propres décisions de contrôle de charge.

ID	Sévérité	Description
SCP-L1	Faible	La carte d'inférence de service basée sur le chemin (Mode 3) manque d'entrées de préfixe <code>nchf-</code> (CHF), <code>nnef-</code> (NEF), et <code>naf-</code> (AF). Les requêtes vers ces services sans en-têtes de découverte explicites recevront un 400 Bad Request avec la cause <code>MANDATORY_IE_MISSING</code> . Contournement : configurez les consommateurs pour envoyer des en-têtes <code>3gpp-Sbi-Discovery-*</code> pour ces services.
SCP-L3	Faible	Les notifications de statut NRF avec l'événement <code>NF_DEREGISTERED</code> ou <code>NF_PROFILE_CHANGED</code> effacent l'ensemble du cache de découverte plutôt que seulement l'entrée <code>{nf_type, service_name}</code> affectée. Dans les déploiements avec des changements fréquents de profil de NF, cela provoque une série de requêtes de redécouverte NRF.

## Dépannage

### 400 Bad Request — MANDATORY\_IE\_MISSING

Le SCP n'a pas pu déterminer une cible de routage. Vérifiez :

1. Le consommateur envoie-t-il `3gpp-Sbi-Target-apiRoot` ou à la fois `3gpp-Sbi-Discovery-target-nf-type` et `3gpp-Sbi-Discovery-service-names` ?
2. Si vous vous fiez à l'inférence basée sur le chemin (Mode 3), le préfixe de chemin apparaît-il dans la carte de service intégrée ? Notez que `nchf-`, `nnef-`, et `naf-` sont absents (SCP-L1). Ajoutez des en-têtes explicites pour ces services.

## 504 Gateway Timeout — NF\_DISCOVERY\_FAILURE

Le NRF n'a retourné aucune instance de NF. Vérifiez :

1. Le NRF est-il accessible depuis OmniSCP ? Vérifiez `nrf_uri` et la connectivité réseau.
2. Le type de NF cible est-il enregistré dans le NRF ? Interrogez directement le NRF : `GET {nrf_uri}/nnrf-disc/v1/nf-instances?target-nf-type=<TYPE>`.
3. Vérifiez si une notification de statut NRF vient de vider le cache (événement `NF_DEREGISTERED`) et que le NF ne s'est pas réenregistré.

## 502 Bad Gateway — TARGET\_NF\_NOT\_REACHABLE

Toutes les instances de producteurs de NF ont échoué. Vérifiez :

1. Les producteurs de NF fonctionnent-ils et sont-ils accessibles sur les adresses SBI rapportées dans leurs profils NRF ?
2. Vérifiez `upstream_timeout`. Si les producteurs de NF sont lents à répondre, augmentez cette valeur.
3. Vérifiez `max_retries`. S'il est réglé sur `0`, un seul échec devient un 502 immédiat.
4. Vérifiez l'état de santé de l'équilibreur de charge dans les journaux : recherchez `Instance NF <ID> marquée comme non saine après N échecs`.

## Cache de découverte causant un routage obsolète

Si les producteurs de NF changent d'adresses ou redémarrent sans une désinscription NRF appropriée, le cache peut contenir des URI SBI obsolètes jusqu'à ce que le TTL expire. Options :

1. Réduisez `discovery_cache_ttl` pour limiter la fenêtre d'obsolescence.

2. Assurez-vous que les producteurs de NF se désinscrivent du NRF lors de l'arrêt ; cela déclenche une notification de statut NRF qui vide le cache d'OmniSCP.
3. Un redémarrage du processus OmniSCP vide tout l'état du cache.

## Latence élevée du proxy

1. Vérifiez l'histogramme `omni_scp.proxy_request.duration_ms` pour la distribution de latence.
2. Comparez le taux de hits de cache (`omni_scp.cache_hits.total` contre `omni_scp.cache_misses.total`). Un taux de miss élevé signifie des requêtes NRF fréquentes. Augmentez `discovery_cache_ttl`.
3. Vérifiez `upstream_timeout` — les requêtes qui expirent ajoutent la durée complète du délai d'attente à la latence avant de déclencher un réessai.

## Enregistrement NRF non maintenu

Vérifiez la métrique `omni_scp.nrf.registration.status`. Si elle indique 0 :

1. Vérifiez que `nrf_uri` est correct et que le NRF est accessible.
2. Vérifiez que `mcc` et `mnc` correspondent à la configuration PLMN du NRF.
3. Recherchez des erreurs d'enregistrement NRF dans les journaux d'application au démarrage.