Guide des opérations OmniHSS

Introduction

OmniHSS est une implémentation de Home Subscriber Server (HSS) conçue pour les réseaux 4G LTE (EPC) et IMS (IP Multimedia Subsystem). En tant que base de données centrale et centre d'authentification pour les réseaux mobiles, OmniHSS gère les identifiants des abonnés, les données de profil et fournit des services d'authentification et d'autorisation pour les services de données et de voix.

Construit sur Elixir et la machine virtuelle Erlang, OmniHSS offre la haute disponibilité, la tolérance aux pannes et l'évolutivité requises pour l'infrastructure moderne des télécommunications.

Qu'est-ce qu'un Home Subscriber Server ?

Le HSS est un composant critique dans les réseaux LTE et IMS qui :

- **Stocke les données des abonnés** - Identifiants, informations de profil et abonnements aux services
- **Effectue l'authentification** - Valide les abonnés tentant d'accéder au réseau
- **Gère l'autorisation** - Contrôle les services auxquels les abonnés peuvent accéder
- **Suit la localisation** - Maintient les informations de localisation actuelles pour le routage
- **Contrôle le roaming** - Applique les politiques de roaming en fonction des réseaux visités
- **Gère l'équipement** - Fonctionne comme un Equipment Identity Register (EIR) pour le contrôle des dispositifs

Fonctionnalités clés

Fonctionnalités opérationnelles

- **Interface S6a** - Authentification et gestion de localisation pour les réseaux LTE/EPC
- **Interface Cx** - Enregistrement et authentification IMS
- **Interface Sh** - Accès aux données de profil IMS et notifications d'abonnement
- **Interface S13** - Vérification de l'identité de l'équipement (OmniHSS

fonctionne comme EIR)
- **Interface Gx** - Contrôle des politiques et de la facturation (OmniHSS fonctionne comme PCRF)
- **Interface Rx** - Contrôle des politiques médias IMS (OmniHSS fonctionne comme PCRF)
- **Contrôle du roaming** - Contrôle granulaire sur le roaming de données et IMS par PLMN
- **Multiples MSISDN** - Support pour plusieurs numéros de téléphone par abonné
- **API RESTful** - API de provisioning complète pour l'intégration (également utilisée par OmniHLR)
- **Panneau de contrôle Web** - Surveillance en temps réel et état du système

Intégration des éléments du réseau

OmniHSS s'interface avec les éléments de réseau suivants :

- **MME** (Mobility Management Entity) - Gestion de la mobilité et des sessions LTE
- **P-GW** (PDN Gateway) - Reçoit des politiques d'OmniHSS (fonction PCRF)
- **P-CSCF** (Proxy Call Session Control Function) - Autorisation des médias IMS
- **I-CSCF** (Interrogating CSCF) - Requêtes de routage IMS
- **S-CSCF** (Serving CSCF) - Enregistrement et authentification IMS
- **AS** (Application Server) - Accès aux données des abonnés IMS
- **OmniHLR** - HLR hérité qui communique avec OmniHSS via API

Structure de la documentation

Ce guide des opérations est organisé en les documents suivants :

Documentation de base

- **Aperçu de l'architecture** - Architecture du système, composants et pile Diameter
- **Guide de configuration** - Référence de configuration complète avec exemples
- **Relations entre entités** - Modèle de données et relations entre entités

Guides opérationnels

- **Panneau de contrôle** - Utilisation de l'interface de surveillance basée sur le web
- **Métriques et surveillance** - Surveillance du système et vérifications de santé
- **Guide de dépannage** - Diagnostic et résolution des problèmes courants
- **Référence API** - Documentation complète des points de terminaison API

- **Webhooks** - Notifications d'événements en temps réel et intégration

Documentation des fonctionnalités

- **Gestion des profils** - Profils EPC, IMS, APN et roaming
- **Contrôle du roaming** - Configuration des politiques de roaming
- **Flux de protocoles** - Procédures de protocole Diameter et flux de messages
- **PCRF** - Fonction de règles de politique et de facturation (interfaces Gx/Rx, QoS, VoLTE)
- **EIR** - Registre d'identité de l'équipement (interface S13, validation IMEI)
- **Fonctionnalités Multi-MSISDN et Multi-IMSI** - Support de plusieurs numéros de téléphone et plusieurs IMSI

Démarrage rapide pour les opérations

Accéder au système

Panneau de contrôle (Interface Web)

```
URL: https://[hostname]:7443
```

Le Panneau de contrôle fournit une surveillance en temps réel des abonnés et des pairs Diameter.

Point de terminaison API

```
URL: https://[hostname]:8443
```

L'API RESTful permet le provisioning et la gestion des abonnés.

Fichiers de configuration clés

- `config/runtime.exs` - Configuration d'exécution (base de données, Diameter, paramètres réseau)
- `priv/cert/` - Certificats TLS pour HTTPS et Diameter

Opérations essentielles

1. **Vérifier l'état du système** - Accéder à la page d'aperçu du Panneau de contrôle
2. **Surveiller les pairs Diameter** - Accéder à la page Diameter du Panneau de contrôle
3. **Interroger un abonné** - Utiliser le point de terminaison API `/api/subscriber/imsi/:imsi`
4. **Voir la base de données** - Se connecter à la base de données SQL à l'hôte configuré

Support et dépannage

Fichiers journaux

Les journaux système sont sortis vers stdout/stderr et peuvent être capturés par votre gestionnaire de processus (systemd, supervisord, etc.).

Vérifications courantes

- **Connectivité Diameter** - Vérifiez la page Diameter pour l'état des pairs
- **Connectivité de la base de données** - Vérifiez la configuration de la base de données dans runtime.exs
- **Échecs d'authentification des abonnés** - Vérifiez l'état des abonnés pour les comptes d'échec

Surveillance de la santé

- **Vérification de la santé de l'API** - `GET /api/status`
- **Panneau de contrôle** - Accéder à n'importe quelle page du Panneau de contrôle
- **Base de données** - Se connecter à la base de données SQL et vérifier l'accès aux tables

Considérations de sécurité

- **TLS requis** - L'API et le Panneau de contrôle utilisent HTTPS
- **Gestion des certificats** - Les certificats dans `priv/cert/` doivent être valides
- **Sécurité de la base de données** - Sécuriser les identifiants de la base de données dans runtime.exs
- **Isolation du réseau** - L'interface Diameter doit être sur le réseau de gestion
- **Authentification API** - Envisagez de mettre en œuvre l'authentification pour un usage en production

Architecture en un coup d'œil

Prochaines étapes

Pour des procédures opérationnelles détaillées, référez-vous aux sections de documentation spécifiques :

- Commencez par **Aperçu de l'architecture** pour comprendre les composants du système
- Consultez le **Guide de configuration** pour personnaliser votre

déploiement
- Explorez le **Panneau de contrôle** pour la surveillance quotidienne
- Consultez la **Référence API** pour l'automatisation du provisioning

---

Version du document : 1.0
Maintenu par : Équipe des opérations Omnitouch

EIR (Registre d'Identité d'Équipement)

Aperçu

Le HSS comprend un EIR (Registre d'Identité d'Équipement) intégré qui fournit une vérification de l'identité des équipements pour les appareils mobiles. L'EIR valide les numéros IMEI (Identité Internationale d'Équipement Mobile) pour déterminer si l'équipement mobile est autorisé, volé ou sous observation avant de permettre l'accès au réseau.

Capacités Clés

- **Interface S13** : Vérification de l'identité de l'équipement via le protocole Diameter
- **Validation IMEI** : Vérifier l'identité de l'équipement en utilisant IMEI/IMEISV
- **Correspondance Flexible** : Correspondance de motifs basée sur des regex pour IMEI, IMEISV et IMSI
- **Classification à Trois Niveaux** : Support pour liste blanche, liste noire et liste grise
- **Politiques Configurables** : Comportement personnalisable pour les équipements inconnus
- **API REST** : Opérations CRUD complètes pour la gestion des règles EIR

Architecture

Interface Diameter

Interface	ID d'Application	Pair	Objectif
S13	16 777 252	MME/SGSN	Vérification de l'identité de l'équipement

Base de Données des Règles d'Équipement

L'EIR utilise un système de correspondance basé sur des règles flexible :

Actions de Règle :

- `whitelist` - Autoriser l'équipement
- `blacklist` - Bloquer l'équipement
- `greylist` - Surveiller l'équipement

Modèles Regex : Correspondre à IMEI, IMEISV ou IMSI

Valeurs de Statut d'Équipement

Statut	Code	Signification	Action Réseau
Liste Blanche	0	Équipement approuvé	Autoriser l'accès au réseau
Liste Noire	1	Équipement volé/bloqué	Refuser l'accès au réseau
Liste Grise	2	Équipement sous observation	Autoriser avec surveillance

Interface S13

Opérations Supportées

Demande de Vérification d'Identité d'Équipement (ECR) / Réponse de Vérification d'Identité d'Équipement (ECA)

Direction : MME/SGSN → HSS (EIR)

Déclencheur : MME vérifie l'identité de l'équipement lors de l'attachement ou de la mise à jour de la zone de suivi

AVPs de Demande :

- Session-Id
- Origin-Host, Origin-Realm
- Destination-Realm
- Auth-Session-State
- Terminal-Information
    - IMEI (15 chiffres)
    - Software-Version (2 chiffres, optionnel)
- User-Name (IMSI, optionnel)
- Vendor-Specific-Application-Id

Actions EIR :

1. Extraire IMEI, Software-Version (si présent), et IMSI (si présent)
2. Si IMSI fourni :
    - Valider que l'abonné existe et est activé
    - Mettre à jour l'état de l'abonné avec les dernières informations vues
3. Tenter la recherche d'équipement dans l'ordre de priorité :
    - **Correspondance IMEISV** (IMEI + Software-Version concaténés)
    - **Correspondance IMEI** (IMEI uniquement)
    - **Correspondance IMSI** (si fourni dans la demande)
    - **Politique d'équipement inconnu** (comportement par défaut configuré)
4. Retourner le statut de l'équipement

AVPs de Réponse :

- Session-Id (répété de la demande)
- Result-Code: 2001 (succès)
- Equipment-Status: 0 (liste blanche) / 1 (liste noire) / 2 (liste grise)

Réponses d'Erreur :

- Experimental-Result: 5422 (équipement/abonné non trouvé)
- Experimental-Result: 5012 (erreur générale)

Logique de Correspondance d'Équipement

Ordre de Priorité

L'EIR utilise une stratégie de recherche en cascade pour maximiser la flexibilité de correspondance :

```
1. IMEISV (IMEI + Software-Version)
   ↓ (si pas de correspondance)
2. IMEI uniquement
   ↓ (si pas de correspondance)
3. IMSI (si fourni dans la demande)
   ↓ (si pas de correspondance)
4. Politique d'Équipement Inconnu
```

Algorithme de Correspondance

Étape 1 : Correspondance IMEISV

- Concaténer IMEI + Software-Version : `"35979139461611" + "08" = "3597913946161108"`
- Tester contre tous les motifs regex des règles EIR
- Retourner l'action ("whitelist", "blacklist", "greylist") de la première règle correspondante

Étape 2 : Correspondance IMEI (repli)

- Utiliser uniquement IMEI : `"35979139461611"`
- Tester contre tous les motifs regex des règles EIR
- Retourner l'action de la première règle correspondante

Étape 3 : Correspondance IMSI (repli si IMSI fourni)

- Utiliser l'IMSI de la demande : `"999999876543210"`
- Tester contre tous les motifs regex des règles EIR
- Retourner l'action de la première règle correspondante
- **Cas d'utilisation** : Bloquer tout équipement pour un abonné spécifique

Étape 4 : Politique d'Équipement Inconnu (dernier recours)

- Paramètre de configuration : `eir_unknown_equipment_behaviour`
- Options :
  - `:whitelist` - Autoriser l'équipement inconnu (permissif)
  - `:blacklist` - Bloquer l'équipement inconnu (restrictif)
  - `:greylist` - Observer l'équipement inconnu (modéré)
  - `:reject_unknown_equipment` - Retourner l'erreur 5422 (strict)

Exemples de Modèles Regex

Modèle	Correspond à	Cas d'utilisation
`"35979139461650"`	IMEI exact	Liste blanche/liste noire d'un seul appareil
`"3597913946165.*"`	Wildcard de préfixe IMEI	Gamme de fabricants/modèles
`"3597913946161108"`	IMEISV exact	Appareil spécifique avec version logicielle
`"999999876543210"`	IMSI	Bloquer tout équipement pour l'abonné
`"359791.*"`	Wildcard TAC	Allocation de type d'appareil entière

Flux de Messages Courants

Flux 1 : Vérification d'Équipement - IMEI connu sur liste blanche

Flux 2 : Vérification d'Équipement - IMEI sur liste noire (Appareil volé)

Flux 3 : Vérification d'Équipement - Équipement Inconnu (Politique de Liste Blanche)

Flux 4 : Vérification d'Équipement - Équipement Inconnu (Politique de Rejet)

Flux 5 : Vérification d'Équipement - Abonné Inconnu

Flux 6 : V��rification d'Équipement - Correspondance IMEISV

Flux 7 : Vérification d'Équipement - Blocage IMSI

API REST

Gestion des Règles EIR

Chemin de base : `/api/eir/rule`

Lister Toutes les Règles EIR

Demande :

```
GET /api/eir/rule
```

Réponse (HTTP 200) :

```
{
  "data": [
    {
      "id": 1,
      "action": "whitelist",
      "regex": "3597913946165.*",
      "inserted_at": "2025-01-15T10:30:00Z",
      "updated_at": "2025-01-15T10:30:00Z"
    },
    {
      "id": 2,
      "action": "blacklist",
      "regex": "35979139461640",
      "inserted_at": "2025-01-16T14:20:00Z",
      "updated_at": "2025-01-16T14:20:00Z"
    }
  ]
}
```

Obtenir une Règle EIR Spécifique

Demande :

```
GET /api/eir/rule/{id}
```

Réponse (HTTP 200) :

```
{
  "data": {
    "id": 1,
    "action": "whitelist",
    "regex": "3597913946165.*"
  }
}
```

Créer une Règle EIR

Demande :

```
POST /api/eir/rule
Content-Type: application/json
```

```
{
  "action": "blacklist",
  "regex": "35979139461640"
}
```

Validation :

- `action` : Requis, doit être "whitelist", "blacklist" ou "greylist"
- `regex` : Requis, doit être un motif regex valide, unique parmi toutes les règles

Réponse (HTTP 201) :

```
{
  "data": {
    "id": 3,
    "action": "blacklist",
    "regex": "35979139461640"
  }
}
```

Réponse d'Erreur (HTTP 400) :

```
{
  "errors": {
    "regex": ["a déjà été pris"]
  }
}
```

Mettre à Jour une Règle EIR (Partielle)

Demande :

```
PATCH /api/eir/rule/{id}
Content-Type: application/json

{
  "action": "greylist"
}
```

Réponse (HTTP 200) :

```
{
  "data": {
    "id": 3,
    "action": "greylist",
    "regex": "35979139461640"
  }
```

```
}
```

Remplacer une Règle EIR

Demande :

```
PUT /api/eir/rule/{id}
Content-Type: application/json

{
  "action": "whitelist",
  "regex": "359791394616.*"
}
```

Réponse (HTTP 200) :

```
{
  "data": {
    "id": 3,
    "action": "whitelist",
    "regex": "359791394616.*"
  }
}
```

Supprimer une Règle EIR

Demande :

```
DELETE /api/eir/rule/{id}
```

Réponse (HTTP 204 No Content)

Configuration

Configuration du Service Diameter

Application S13 (`config/runtime.exs`) :

```
%{
  application_name: :hss_s13,
  application_dictionary: :diameter_gen_3gpp_s13,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_252}
  ]
}
```

Comportement des Équipements Inconnus

Configurer le comportement par défaut pour les équipements ne correspondant à aucune règle dans `config/runtime.exs` :

Exemple :

```
config :hss, :eir,
  unknown_equipment_behaviour: :whitelist
```

Valeurs Valides :

- `:whitelist` - Autoriser les équipements inconnus (par défaut, permissif)
- `:blacklist` - Bloquer les équipements inconnus (restrictif)
- `:greylist` - Surveiller les équipements inconnus (modéré)
- `:reject_unknown_equipment` - Retourner l'erreur Diameter 5422 (strict)

Cas d'Utilisation :

- **Développement/Test** : `:whitelist` - Autoriser tous les appareils
- **Production (permissif)** : `:whitelist` - Bloquer uniquement les appareils connus comme mauvais
- **Production (modéré)** : `:greylist` - Journaliser les appareils inconnus pour révision
- **Production (strict)** : `:reject_unknown_equipment` - Autoriser uniquement les appareils enregistrés

Gestion des Erreurs

Code de Résultat	Type	Signification	Cause
2001	Succès	DIAMETER_SUCCESS	Vérification de l'équipement terminée
5422	Expérimental	DIAMETER_ERROR_EQUIPMENT_UNKNOWN	Abonné non trouvé ou équipement inconnu rejeté
5012	Expérimental	DIAMETER_ERROR_UNKNOWN	Erreur de traitement

Cas d'Utilisation

1. Gestion des Appareils Volés

Scénario : Appareil signalé volé

Action :

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "35979139461640"  # IMEI exact
}
```

Résultat : Appareil refusé l'accès au réseau lors de la prochaine attache

2. Liste Blanche du Fabricant

Scénario : Pré-approuver toute la gamme de modèles d'appareils

Action :

```
POST /api/eir/rule
{
  "action": "whitelist",
  "regex": "359791394.*"  # TAC pour fabricant/modèle
}
```

Résultat : Tous les appareils dans la plage TAC approuvés

3. Verrouillage d'Équipement d'Abonné

Scénario : Bloquer tout équipement pour un abonné spécifique (verrouillage SIM)

Action :

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "999999876543210"  # IMSI
}
```

Résultat : Tout équipement utilisé avec cette SIM est bloqué

4. Liste Grise d'Équipement de Test

Scénario : Surveiller l'équipement de test en production

Action :

```
POST /api/eir/rule
{
  "action": "greylist",
  "regex": "35979139.*"  # Plage TAC d'équipement de test
}
```

Résultat : Équipement autorisé mais signalé pour surveillance

5. Contrôle de Version Logicielle

Scénario : Bloquer une version de firmware vulnérable spécifique

Action :

```
POST /api/eir/rule
{
  "action": "blacklist",
  "regex": "359791394616.*05"  # Plage IMEI + Version Logicielle 05
}
```

Résultat : Seuls les appareils avec la Version Logicielle "05" dans la plage IMEI sont bloqués

Détails de Mise en Œuvre

Composants Internes

La fonctionnalité EIR est mise en œuvre à l'aide de plusieurs modules internes :

- **Gestionnaire de Protocole S13** - Traitement des messages ECR/ECA
- **Moteur de Correspondance d'Équipement** - Correspondance IMEI/IMEISV/IMSI basée sur des regex
- **Base de Données des Règles EIR** - Stockage et recherche de motifs
- **Contrôleur API REST** - Points de terminaison de gestion des règles

Fonction de Recherche de Statut d'Équipement

La recherche de statut d'équipement suit cette logique en cascade :

1. **Correspondance IMEISV** : Vérifier IMEI + Software-Version concaténés
2. **Correspondance IMEI** : Vérifier uniquement IMEI
3. **Correspondance IMSI** : Vérifier IMSI (si fourni)
4. **Équipement Inconnu** : Appliquer la politique par défaut configurée

Résultats Possibles :

- `whitelist` - Équipement autorisé
- `blacklist` - Équipement bloqué
- `greylist` - Équipement sous observation
- `reject_unknown_equipment` - Rejet strict

Considérations de Sécurité

Confidentialité de l'IMEI

Les numéros IMEI sont des identifiants sensibles. L'EIR :

- Ne journalise pas les valeurs IMEI en texte clair par défaut
- Utilise des recherches de base de données hachées (si configuré)
- Restreint l'accès API aux administrateurs authentifiés

Ordre des Règles

Les règles EIR sont évaluées dans l'ordre de la base de données (par ID). Pour les motifs conflictuels :

```
Règle 1 : regex "359791.*" action "whitelist"  (large)
Règle 2 : regex "35979139461640" action "blacklist"  (spécifique)
```

Recommandation : Créer des règles spécifiques avant des jokers larges pour s'assurer que la liste noire a la priorité.

Limitation de Taux

Envisagez de mettre en œuvre une limitation de taux sur :

- Les demandes S13 ECR provenant de pairs non fiables
- Les modifications de règles de l'API REST EIR
- Les requêtes de recherche IMEI pour prévenir les attaques d'énumération

Documentation Connexe

- Protocoles Diameter - Spécification du protocole S13
- Référence API - Documentation complète de l'API
- Architecture - Architecture globale du HSS
- Guide des Opérations - Procédures opérationnelles

Annexe : Structure de l'IMEI

Format IMEI (15 chiffres)

```
35 9791 394616 1
|  |    |      └─ Chiffre de contrôle (algorithme de Luhn)
```

```
│  │    └─ Numéro de série (6 chiffres)
│  └─ FAC (Code d'Assemblage Final, 4 chiffres)
└─ TAC (Code d'Allocation de Type, 8 chiffres au total incluant RBI)
   │  └─ RBI (Identifiant de l'Organe de Rapport, 2 chiffres)
   └─ Fabricant/Modèle (6 chiffres)
```

Format IMEISV (16 chiffres)

```
35 9791 394616 1 08
│  │    │      │ └─ Version Logicielle (2 chiffres)
└─ IMEI (15 chiffres)
```

Exemples de Modèles

IMEI/IMEISV	Modèle	Correspond à
359791394616108	3597913946161.*	Tous les appareils avec TAC+FAC+Numéro de série 359791394616*
359791394616140	35979139461614.	Tous les chiffres de contrôle pour le Numéro de série 359791394616141-9
35979139461640	35979139461640	Correspondance IMEI exacte
3597913946163008	3597913946163008	Correspondance IMEISV exacte (IMEI + SV)

PCRF (Fonction de Règles de Politique et de Facturation)

Vue d'ensemble

Le HSS comprend un PCRF (Fonction de Règles de Politique et de Facturation) intégré qui fournit un contrôle de politique et des règles de facturation pour les sessions de données mobiles. Le PCRF contrôle les politiques de Qualité de Service (QoS), l'allocation de bande passante et les règles de facturation pour les porteuses par défaut et dédiées dans les réseaux LTE.

Capacités clés

- **Interface Gx** : Contrôle de politique pour PGW/PCEF (Passerelle de Données de Paquet / Fonction d'Application de Politique et de Facturation)
- **Interface Rx** : Autorisation et QoS pour les flux multimédias IMS (Système Multimédia IP)
- **Gestion Dynamique des Politiques** : Mises à jour de politique en temps réel via des Requêtes de Ré-Authentification (RAR)
- **Support VoLTE** : Création de porteuses dédiées pour les appels vocaux avec QoS garanti
- **Règles de Facturation** : Définir le comportement de facturation et les profils de vitesse à l'aide de Modèles de Flux de Trafic (TFT)
- **REST API** : Contrôle programmatique de l'application des politiques et de la gestion des règles

Architecture

Interfaces Diameter

Interface	ID d'application	Pair	Objectif
Gx	16,777,238	PGW (PCEF)	Gestion de session PDN, application de QoS, règles de facturation
Rx	16,777,236	P-CSCF (AF)	Autorisation multimédia IMS, réservation de bande passante

Gestion de l'état de session

Le PCRF maintient l'état de session pour les connexions PDN actives et les appels VoLTE :

Interface Gx

Opérations Supportées

1. Requête de Contrôle de Crédit - Initiale (CCR-I)

Déclencheur : PGW crée une nouvelle connexion PDN pour l'abonné

AVPs de Requête :

- Session-Id
- Origin-Host, Origin-Realm
- Subscription-Id (contient IMSI)
- Called-Station-Id (nom APN)
- IP-CAN-Type (type de Réseau d'Accès de Connectivité IP)
- RAT-Type (Technologie d'Accès Radio)
- Framed-IP-Address (adresse IP de l'UE)

Actions PCRF :

1. Rechercher l'abonné par IMSI
2. Récupérer le profil APN et la configuration QoS
3. Créer une entrée de suivi de session
4. Construire les politiques QoS à partir du profil APN

AVPs de Réponse :

- Result-Code: 2001 (DIAMETER_SUCCESS)
- QoS-Information (limites de bande passante agrégées APN)
- Default-EPS-Bearer-QoS (QCI, ARP, priorité)
- Bearer-Control-Mode

2. Requête de Contrôle de Crédit - Mise à Jour (CCR-U)

Déclencheur : PGW signale des changements de session (mise à jour de localisation, changement de RAT, etc.)

Actions PCRF :

1. Localiser la session existante par ID de session
2. Mettre à jour les paramètres de session (type RAT, localisation, etc.)
3. Retourner les politiques mises à jour si nécessaire

Réponse : Result-Code 2001 avec des mises à jour de politique optionnelles

3. Requête de Contrôle de Crédit - Terminer (CCR-T)

Déclencheur : PGW termine la connexion PDN

Actions PCRF :

1. Localiser la session par ID de session
2. Supprimer la session et les enregistrements d'appel associés
3. Confirmer la terminaison

Réponse : Result-Code 2001

4. Requête de Ré-Authentification (RAR)

Direction : PCRF → PGW (HSS initie)

Déclencheur :

- Configuration d'appel IMS (Rx AAR déclenche Gx RAR)
- Terminaison d'appel IMS (Rx STR déclenche Gx RAR)
- Ré-auth manuelle via REST API

AVPs RAR :

- Session-Id (ID de session PGW)
- Auth-Application-Id: 16,777,238
- Re-Auth-Request-Type (0 = Autoriser uniquement)
- Charging-Rule-Install/Remove
- QoS-Information (pour les porteuses dédiées)

Actions PGW : Créer/modifier/supprimer des porteuses dédiées en fonction des règles de facturation

Règles de Facturation et Modèles de Flux de Trafic

Le PCRF prend en charge la définition des règles de facturation avec des Modèles de Flux de Trafic (TFT) pour contrôler :

- **Facturation spécifique au service** - Tarifs différents pour la vidéo, les jeux, les réseaux sociaux, etc.
- **Profils de vitesse** - Limiter ou prioriser le trafic correspondant à des motifs spécifiques
- **Politiques basées sur l'utilisation** - Appliquer diff��rentes QoS en fonction du type de trafic ou de la destination

Les règles de facturation peuvent être :

- Installées dynamiquement via Gx RAR en fonction de la détection

d'application
- Prédéfinies et déclenchées par des conditions spécifiques (heure de la journée, localisation, quota)
- Associées à des TFT à l'aide de règles de filtrage de paquets (5-tuple : protocole, IP source/destination, port source/destination)

Cas d'utilisation courants :

- **Zero-rating** - Accès illimité à des services spécifiques (Spotify, WhatsApp, Facebook) sans consommer de quota de données
- **Accès post-quota** - Autoriser le portail d'auto-assistance et les sites de support même après que l'abonné ait épuisé son allocation de données
- **Vitesse par paliers** - Haute vitesse pour les services premium, limitée pour le contenu standard
- **Politiques basées sur le temps** - Streaming illimité hors pointe, priorisation en période de pointe
- **Politiques de roaming** - Facturation différente pour l'utilisation des données internationales par rapport à l'utilisation nationale
- **SLA d'entreprise** - QoS garantie pour les applications critiques pour les affaires

Structure de la Politique QoS

QoS de la Porteuse par Défaut (à partir du profil APN) :

```
{
  "QoS-Class-Identifier": 9,          // QCI (9 = porteuse par
défaut)
  "APN-Aggregate-Max-Bitrate-UL": 50000,  // kbps
  "APN-Aggregate-Max-Bitrate-DL": 100000, // kbps
  "Allocation-Retention-Priority": {
    "Priority-Level": 8,
    "Pre-emption-Capability": 1,      // Peut préempter
    "Pre-emption-Vulnerability": 1    // Peut être préempté
  }
}
```

QoS de la Porteuse Dédiée (pour VoLTE) :

```
{
  "QoS-Class-Identifier": 1,          // QCI 1 = Voix
Conversationnelle
  "Max-Requested-Bandwidth-UL": 128000,   // bps
  "Max-Requested-Bandwidth-DL": 128000,   // bps
  "Guaranteed-Bitrate-UL": 128000,
  "Guaranteed-Bitrate-DL": 128000
}
```

Interface Rx

Opérations Supportées

1. Requête AA (AAR) / Réponse AA (AAA)

Déclencheur : P-CSCF demande une autorisation pour la session multimédia IMS (configuration d'appel VoLTE)

AVPs de Requête :

- Session-Id (identifiant de session P-CSCF)
- Subscription-Id (IMSI ou URI SIP)
- Media-Component-Description
    - Media-Type (audio, vidéo)
    - Max-Requested-Bandwidth-UL/DL
    - Codec-Data
    - Flow-Description (filtres de paquets 5-tuple)
- AF-Application-Identifier

Actions PCRF :

1. Rechercher l'abonné par IMSI ou URI SIP
2. Trouver la session IMS active
3. Extraire les paramètres multimédias (codec, bande passante, règles de flux)
4. Créer une entrée de suivi d'appel
5. **Déclencher Gx RAR vers PGW** pour créer une porteuse dédiée
6. Attendre la réponse Gx RAA
7. Retourner Rx AAA avec le résultat de l'autorisation

AVPs de Réponse :

- Result-Code: 2001 (succès) ou 5063 (service non autorisé)

2. Requête de Terminaison de Session (STR) / Réponse de Terminaison de Session (STA)

Déclencheur : P-CSCF termine la session IMS (fin d'appel)

Actions PCRF :

1. Localiser la session d'appel par ID de session P-CSCF
2. **Déclencher Gx RAR vers PGW** pour supprimer la porteuse dédiée
3. Supprimer l'entrée de suivi d'appel
4. Retourner la confirmation STA

Réponse : Result-Code 2001

Flux de Messages Communs

Flux 1 : Établissement de Session PDN

Flux 2 : Configuration d'Appel VoLTE (Rx AAR → Gx RAR)

Flux 3 : Terminaison d'Appel VoLTE (Rx STR → Gx RAR)

Flux 4 : Mise à Jour de Session PDN

Flux 5 : Terminaison de Session PDN

Flux 6 : Ré-Auth Manuelle via REST API

REST API

Point de terminaison PCRF Re-Auth

Point de terminaison : `POST /api/operation/pcrf_re_auth`

Objectif : Déclencher manuellement une Requête de Ré-Authentification Gx pour rafraîchir les politiques

Quand l'utiliser : Ce point de terminaison manuel est généralement utilisé pour le dépannage ou pour forcer le rafraîchissement de la politique sur des abonnés spécifiques. Pour les mises à jour de politique de routine (changement de profils QoS APN), le système déclenche automatiquement la ré-auth pour toutes les sessions affectées - aucune action manuelle n'est nécessaire.

Corps de la Requête :

```
{
  "imsi": "999999876543210",
  "apn": "ims"
}
```

Réponse de Succès (HTTP 200) :

```
{
  "data": "Gx Re-Auth Request for 999999876543210 sent to
pgw.epc.mnc999.mcc999.3gppnetwork.org, Result-Code: 2001"
}
```

Réponse d'Erreur (HTTP 400) :

```
{
  "error": "Unable to send Re-Auth Request for 999999876543210 on APN
ims, no active PDN Session found"
}
```

API de Configuration de Politique

Le PCRF récupère les politiques QoS à partir des configurations APN stockées dans la base de données. Ces politiques peuvent être créées et gérées via REST API.

Application Automatique des Politiques : Lorsque vous mettez à jour un profil QoS APN (par exemple, changement des limites de bande passante ou QCI), le système envoie automatiquement des Requêtes de Ré-Authentification Gx (RAR) à tous les PGW avec des sessions PDN actives utilisant cet APN. Cela garantit que les changements de politique sont appliqués immédiatement à tous les abonnés connectés sans intervention manuelle.

Architecture de Politique

Les politiques sont définies à travers une structure à trois niveaux :

```
Identifiant APN → Profil QoS APN → Profil APN
     ↓                  ↓                ↓
  "internet"      QCI, AMBR, ARP    Lien entre les deux
```

1. Créer un Identifiant APN

Définir le nom de l'APN et le support de version IP.

Point de terminaison : `POST /api/apn/identifier`

Corps de la Requête :

```
{
  "apn_identifier": {
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

Options de Version IP :

- `"ipv4"` - IPv4 uniquement
- `"ipv6"` - IPv6 uniquement
- `"ipv4v6"` - Double pile (IPv4 et IPv6)
- `"ipv4_or_ipv6"` - Le réseau décide (soit IPv4 soit IPv6)

Réponse (HTTP 201) :

```
{
  "data": {
    "id": 1,
    "apn": "internet",
    "ip_version": "ipv4v6"
  }
}
```

Validation :

- `apn` : Requis, 1-254 caractères, unique
- `ip_version` : Requis, doit être l'une des quatre options ci-dessus

Lister les Identifiants APN : `GET /api/apn/identifier`

2. Créer un Profil QoS APN

Définir les paramètres QoS (bande passante, QCI, priorité).

Point de terminaison : `POST /api/apn/qos_profile`

Corps de la Requête :

```
{
  "apn_qos_profile": {
    "name": "Internet à Effort Optimal",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Paramètres QoS :

Champ	Type	Plage	Description
`name`	string	1-254 chars	Nom du profil (unique)
`qci`	integer	1-254	Identifiant de Classe QoS (1-4 = GBR, 5-9 = Non-GBR)
`allocation_retention_priority`	integer	1-15	Niveau ARP (1 = priorité la plus élevée)
`apn_ambr_dl_kbps`	integer	1-4,294,967,293	Débit Maximum

Champ	Type	Plage	Description
			Agrégé APN en Descendant (kbps)
`apn_ambr_ul_kbps`	integer	1-4,294,967,293	Débit Maximum Agrégé APN en Montant (kbps)
`pre_emption_capability`	boolean	true/false	Peut préempter des porteuses de priorité inférieure
`pre_emption_vulnerability`	boolean	true/false	Peut être préempté par des porteuses de priorité supérieure

Valeurs QCI Courantes :

- 1 - Voix Conversationnelle (VoLTE) - GBR, budget de délai de 100 ms
- 2 - Vidéo Conversationnelle - GBR, budget de délai de 150 ms
- 5 - Signalisation IMS - Non-GBR, budget de délai de 100 ms
- 9 - Porteuse par Défaut (Internet) - Non-GBR, budget de délai de 300 ms

Réponse (HTTP 201) :

```
{
  "data": {
    "id": 1,
    "name": "Internet à Effort Optimal",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Lister les Profils QoS : `GET /api/apn/qos_profile`

3. Créer un Profil APN

Lier l'identifiant APN avec un profil QoS.

Point de terminaison : `POST /api/apn/profile`

Corps de la Requête :

```
{
  "apn_profile": {
    "name": "Profil APN Internet",
```

```
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
}
```

Champs :

- `name` : Nom du profil (unique), utilisé pour référence
- `apn_identifier_id` : ID provenant de Créer un Identifiant APN
- `apn_qos_profile_id` : ID provenant de Créer un Profil QoS APN

Réponse (HTTP 201) :

```
{
  "data": {
    "id": 1,
    "name": "Profil APN Internet",
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
}
```

Contraintes :

- `apn_identifier_id` et `apn_qos_profile_id` doivent référencer des enregistrements existants
- Chaque combinaison d'identifiant APN et de profil QoS doit être unique

Lister les Profils APN : `GET /api/apn/profile`

Exemple Complet de Configuration de Politique

Étape 1 : Créer une Politique APN IMS (VoLTE)

```
# 1. Créer un Identifiant APN
curl -X POST https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "ims",
      "ip_version": "ipv4v6"
    }
  }'
# Réponse : {"data": {"id": 2, ...}}

# 2. Créer un Profil QoS (Signalisation IMS)
curl -X POST https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
```

```
  -d '{
    "apn_qos_profile": {
      "name": "QoS Signalisation IMS",
      "qci": 5,
      "allocation_retention_priority": 2,
      "apn_ambr_dl_kbps": 5000,
      "apn_ambr_ul_kbps": 5000,
      "pre_emption_capability": true,
      "pre_emption_vulnerability": false
    }
  }'
# Réponse : {"data": {"id": 2, ...}}

# 3. Créer un Profil APN
curl -X POST https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_profile": {
      "name": "Profil APN IMS",
      "apn_identifier_id": 2,
      "apn_qos_profile_id": 2
    }
  }'
# Réponse : {"data": {"id": 2, ...}}
```

Étape 2 : Assigner à l'Abonné

Une fois créé, le profil APN est assigné aux abonnés via des profils EPC. Voir Référence API pour lier les profils APN aux abonnés.

Mise à Jour et Suppression de Politique

Mettre à Jour le Profil QoS :

```
PATCH /api/apn/qos_profile/{id}
PUT /api/apn/qos_profile/{id}
```

Exemple - Augmenter la Bande Passante pour Tous les Utilisateurs :

```
# Mettre à jour le profil QoS ID 1 pour augmenter la bande passante
curl -X PATCH https://hss.example.com:8443/api/apn/qos_profile/1 \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "apn_ambr_dl_kbps": 150000,
      "apn_ambr_ul_kbps": 75000
    }
  }'
```

Ce qui se Passe Automatiquement :

1. Le profil QoS est mis à jour dans la base de données
2. Le système identifie toutes les sessions PDN actives utilisant les APN liés à ce profil QoS
3. Pour chaque session active, un Gx RAR est envoyé au PGW correspondant
4. Les PGW mettent à jour la QoS de la porteuse pour refléter les nouvelles limites de bande passante
5. Tous les abonnés connectés reçoivent immédiatement la politique mise à jour

Scénario d'Exemple : Si 100 abonnés sont actuellement connectés sur l'APN "internet" utilisant le profil QoS ID 1, tous les 100 verront leurs limites de bande passante mises à jour à 150 Mbps en descendant / 75 Mbps en montant dans les secondes suivant l'achèvement de l'appel API.

Remarque : Lorsque vous mettez à jour un profil QoS APN, le système **déclenche automatiquement une ré-auth** pour toutes les sessions PDN actives utilisant cet APN, appliquant les nouvelles politiques immédiatement aux abonnés attachés. Aucune ré-auth manuelle n'est requise.

Supprimer des Ressources :

```
DELETE /api/apn/identifier/{id}
DELETE /api/apn/qos_profile/{id}
DELETE /api/apn/profile/{id}
```

Contraintes de Suppression :

- Impossible de supprimer des identifiants APN ou des profils QoS référencés par des profils APN
- Impossible de supprimer des profils APN assignés à des abonnés actifs

Modèles de Politique

Internet Haute Vitesse (100 Mbps en descendant / 50 Mbps en montant) :

```
{
  "apn_qos_profile": {
    "name": "Internet Haute Vitesse",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 100000,
    "apn_ambr_ul_kbps": 50000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Internet Premium (500 Mbps en descendant / 100 Mbps en montant) :

```
{
  "apn_qos_profile": {
    "name": "Internet Premium",
    "qci": 8,
    "allocation_retention_priority": 5,
    "apn_ambr_dl_kbps": 500000,
    "apn_ambr_ul_kbps": 100000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

IoT/M2M (Bande Passante Faible) :

```
{
  "apn_qos_profile": {
    "name": "IoT M2M",
    "qci": 9,
    "allocation_retention_priority": 10,
    "apn_ambr_dl_kbps": 1024,
    "apn_ambr_ul_kbps": 512,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Services d'Urgence (Priorité Maximale) :

```
{
  "apn_qos_profile": {
    "name": "Profil APN d'Urgence",
    "qci": 5,
    "allocation_retention_priority": 1,
    "apn_ambr_dl_kbps": 10000,
    "apn_ambr_ul_kbps": 10000,
    "pre_emption_capability": true,
    "pre_emption_vulnerability": false
  }
}
```

Configuration

Configuration du Service Diameter

Application Gx (`config/runtime.exs`) :

```
%{
  application_name: :hss_gx,
  application_dictionary: :diameter_gen_3gpp_gx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_238}
  ]
}
```

Application Rx (`config/runtime.exs`) :

```
%{
  application_name: :hss_rx,
  application_dictionary: :diameter_gen_3gpp_rx,
  vendor_specific_application_ids: [
    %{vendor_id: 10415, auth_application_id: 16_777_236}
  ]
}
```

Paramètres QoS

Les paramètres QoS sont extraits de :

- **Porteuse par Défaut** : Configuration du profil APN dans la base de données
    - `apn_qos_profile.qci` (Identifiant de Classe QoS)
    - `apn_qos_profile.apn_ambr_ul_kbps` (Débit Maximum Agrégé en Montant)
    - `apn_qos_profile.apn_ambr_dl_kbps` (Débit Maximum Agrégé en Descendant)
    - `apn_qos_profile.priority_level` (Priorité de Conservation d'Allocation)
- **Porteuse Dédiée** : Extrait de la Description du Composant Multimédia Rx AAR
    - QCI : 1 (Voix Conversationnelle)
    - Débit Garanti : À partir des AVPs de Bande Passante Demandée Maximale
    - Filtres de Flux : À partir des AVPs de Description de Flux

Gestion des Erreurs

Code de Résultat	Type	Signification	Cause
2001	Succès	DIAMETER_SUCCESS	Requête traitée avec succès
5001	Expérimental	Utilisateur non trouvé	IMSI non présent dans la base de

Code de Résultat	Type	Signification	Cause
			données des abonnés
5002	Expérimental	Session non trouvée	La session PDN n'existe pas pour mise à jour/terminer
5063	Expérimental	Service non autorisé	Autorisation multimédia IMS refusée

Détails de Mise en Œuvre

Gestion de Session

Le PCRF suit :

- **Sessions PDN Actives** - Une par APN, par abonné
- **Appels VoLTE** - Plusieurs appels par session IMS (prend en charge les appels en conférence)
- **Politiques QoS** - Appliquées dynamiquement en fonction de la configuration APN
- **Règles de Facturation** - Modèles de flux de trafic et politiques spécifiques au service

Fonctionnalités Avancées de Politique

Le PCRF prend en charge un contrôle de politique avancé, y compris :

- **Installation/Suppression de règles de facturation** via l'interface Gx
- **Correspondance de Modèle de Flux de Trafic (TFT)** pour la différenciation de service
- **Profils de vitesse dynamiques** en fonction de l'application ou du type de trafic
- **Politiques conscientes du service** déclenchées par des conditions réseau ou le comportement des abonnés

Contactez votre administrateur système pour des informations sur la configuration des règles de facturation avancées et des politiques basées sur les TFT.

Documentation Connexe

- Protocoles Diameter - Spécifications détaillées des protocoles
- Référence API - Documentation complète de l'API
- Architecture - Architecture globale du HSS
- Mapping de Données - Mappages de la base de données aux AVP Diameter

Gestion des erreurs de l'API

← Retour à la référence de l'API

Table des matières

Réponses d'erreur courantes

400 Mauvaise demande

```
{
  "error": "Invalid JSON format"
}
```

Causes :

- JSON mal formé
- Champs requis manquants
- Types de données invalides

404 Non trouvé

```
{
  "error": "Resource not found"
}
```

Causes :

- L'abonné/le profil/l'entité n'existe pas
- ID incorrect dans l'URL

422 Entité non traitable

```
{
  "errors": {
    "imsi": ["has already been taken"],
    "key_set_id": ["does not exist"]
  }
```

```
}
```

Causes :

- Échecs de validation
- Contraintes de base de données violées
- Références de clé étrangère inexistantes

500 Erreur interne du serveur

```
{
  "error": "Internal server error"
}
```

Causes :

- Problèmes de connectivité à la base de données
- Erreurs inattendues de l'application

Flux de gestion des erreurs

← Retour à la référence de l'API

Exemples d'utilisation de l'API

← Retour à la référence API

Table des matières

Provisionnement complet d'un abonné

Cet exemple démontre le flux de travail complet pour le provisionnement d'un nouvel abonné à partir de zéro. Le processus implique la création de tous les profils et composants requis avant de créer l'abonné.

Prérequis : Cet exemple utilise `jq` pour l'analyse JSON. Installez-le avec `apt-get install jq` ou `brew install jq`.

Sections connexes :

- Gestion des ensembles de clés
- Profils APN
- Profils EPC
- Gestion des abonnés

```
# 1. Créer un ensemble de clés
KEY_SET_ID=$(curl -k -X POST https://hss.example.com:8443/api/key_set
\
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }' | jq -r '.data.id')

# 2. Créer un profil QoS APN
APN_QOS_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
qos_profile \
  -H "Content-Type: application/json" \
```

```
  -d '{
    "apn_qos_profile": {
      "name": "Default Internet QoS",
      "qci": 9,
      "allocation_retention_priority": 8,
      "apn_ambr_dl_kbps": 50000,
      "apn_ambr_ul_kbps": 25000
    }
  }' | jq -r '.data.id')

# 3. Créer un identifiant APN
APN_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "internet",
      "ip_version": 2
    }
  }' | jq -r '.data.id')

# 4. Créer un profil APN
APN_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile\": {
      \"name\": \"Internet APN\",
      \"apn_identifier_id\": $APN_ID,
      \"apn_qos_profile_id\": $APN_QOS_ID
    }
  }" | jq -r '.data.id')

# 5. Créer un profil EPC
EPC_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "Standard Data Plan",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    }
  }' | jq -r '.data.id')

# 6. Créer un abonné
SUBSCRIBER_ID=$(curl -k -X POST https://hss.example.com:8443/api/
subscriber \
```

```
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": $KEY_SET_ID,
      \"epc_profile_id\": $EPC_PROFILE_ID
    }
  }" | jq -r '.data.id')

echo "Abonné provisionné avec succès avec l'ID : $SUBSCRIBER_ID"
```

Ce que cela crée :

Ce flux de travail de provisionnement crée un abonné complet avec :

1. **Clés cryptographiques** (Ensemble de clés) - Pour l'authentification
2. **Profil de service de données** (Profil EPC) - Paramètres de bande passante et d'accès au réseau
3. **Configuration APN** (Profil APN) - Point d'accès avec QoS
4. **Enregistrement d'abonné** (Abonné) - L'entité abonné réelle

Prochaines étapes :

- Ajouter des numéros de téléphone : Voir Gestion MSISDN
- Activer les services vocaux : Créer et attribuer un Profil IMS
- Configurer l'itinérance : Créer et attribuer un Profil d'itinérance
- Lier une carte SIM physique : Créer et attribuer une SIM

Voir aussi :

- Documentation Multi-MSISDN - Attribution de plusieurs numéros de téléphone
- Documentation des profils - Configuration avancée des profils

---

Provisionnement complet d'une IP statique

Cet exemple démontre le provisionnement d'un abonné avec une adresse IP statique à partir de zéro.

Scénario : Provisionner un abonné appareil IoT qui a besoin d'une adresse IPv4 statique sur l'APN "internet".

```
# Prérequis : jq doit être installé (apt-get install jq ou brew
install jq)

# 1. Créer un ensemble de clés
KEY_SET_ID=$(curl -k -X POST https://hss.example.com:8443/api/key_set
```

```
\
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }' | jq -r '.data.id')

# 2. Créer un profil QoS APN
APN_QOS_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "name": "IoT Best Effort",
      "qci": 9,
      "allocation_retention_priority": 8,
      "apn_ambr_dl_kbps": 10000,
      "apn_ambr_ul_kbps": 5000
    }
  }' | jq -r '.data.id')

# 3. Créer un identifiant APN
APN_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/
identifier \
  -H "Content-Type: application/json" \
  -d '{
    "apn_identifier": {
      "apn": "internet",
      "ip_version": 0
    }
  }' | jq -r '.data.id')

# 4. Créer un profil APN
APN_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile\": {
      \"name\": \"IoT Internet APN\",
      \"apn_identifier_id\": $APN_ID,
      \"apn_qos_profile_id\": $APN_QOS_ID
    }
  }" | jq -r '.data.id')

# 5. Créer une IP statique pour l'APN
```

```
STATIC_IP_ID=$(curl -k -X POST https://hss.example.com:8443/api/epc/
static_ip \
  -H "Content-Type: application/json" \
  -d "{
    \"static_ip\": {
      \"apn_profile_id\": $APN_PROFILE_ID,
      \"ipv4_static_ip\": \"100.64.1.100\"
    }
  }" | jq -r '.data.id')

# 6. Créer un profil EPC
EPC_PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "IoT Data Plan",
      "ue_ambr_dl_kbps": 10000,
      "ue_ambr_ul_kbps": 5000
    }
  }' | jq -r '.data.id')

# 7. Créer un MSISDN (numéro de téléphone)
MSISDN_ID=$(curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{
    "msisdn": {
      "msisdn": "14155551000"
    }
  }' | jq -r '.data.id')

# 8. Créer un abonné avec IP statique
SUBSCRIBER_ID=$(curl -k -X POST https://hss.example.com:8443/api/
subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001999999999\",
      \"key_set_id\": $KEY_SET_ID,
      \"epc_profile_id\": $EPC_PROFILE_ID,
      \"msisdns\": [$MSISDN_ID],
      \"static_ips\": [$STATIC_IP_ID]
    }
  }" | jq -r '.data.id')

echo "Abonné IoT provisionné avec succès !"
echo "  ID de l'abonné : $SUBSCRIBER_ID"
echo "  IMSI : 001001999999999"
```

```
echo "  MSISDN : 14155551000"
echo "  IPv4 statique : 100.64.1.100 (sur l'APN 'internet')"
```

Ce que cela crée :

Ce flux de travail de provisionnement crée un abonné IoT complet avec :

1. **Clés cryptographiques** (Ensemble de clés) - Pour l'authentification
2. **Configuration APN** (Profil APN) - Point d'accès "internet"
3. **Attribution d'IP statique** (IP statique) - Adresse IPv4 fixe 100.64.1.100
4. **Profil de service de données** (Profil EPC) - Limites de bande passante optimisées pour IoT
5. **Numéro de téléphone** (MSISDN) - Pour l'identification de l'appareil
6. **Enregistrement d'abonné** (Abonné) - L'entité abonné complète

Résultat :

Lorsque cet abonné se connecte au réseau et se connecte à l'APN "internet", il recevra l'adresse IP statique `100.64.1.100` au lieu d'une adresse DHCP dynamique.

Prochaines étapes :

- Ajouter des APN supplémentaires avec des IP statiques : Répétez les étapes 2-5 pour chaque APN
- Activer les services vocaux : Créer et attribuer un Profil IMS
- Configurer l'itinérance : Créer et attribuer un Profil d'itinérance
- Lier une carte SIM physique : Créer et attribuer une SIM

Voir aussi :

- Gestion des IP statiques - Documentation d��taillée sur les IP statiques
- Provisionnement complet d'un abonné - Provisionnement de base sans IP statique
- Documentation Multi-MSISDN - Attribution de plusieurs numéros de téléphone

---

← Retour à la référence API

Référence API OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu de l'API

URL de Base

```
https://[hostname]:8443/api
```

Format de la Demande

- **Content-Type :** `application/json`
- **Protocole :** HTTPS uniquement
- **Port :** 8443 (configurable)

Format de la Réponse

Toutes les réponses sont en JSON avec la structure suivante :

Réponse de Succès :

```
{
  "data": { ... }
}
```

Réponse d'Erreur :

```
{
```

```
  "error": "Description du message d'erreur"
}
```

Codes de Statut HTTP

Code	Signification	Cas d'Utilisation
200	OK	GET, PUT, DELETE réussi
201	Créé	POST réussi
400	Mauvaise Demande	Données d'entrée invalides
404	Non Trouvé	La ressource n'existe pas
422	Entité Non Traitable	Erreur de validation
500	Erreur Interne du Serveur	Erreur côté serveur

Flux de Demande API

Gestion des Abonnés

Lister les Abonnés

Récupérer tous les abonnés ou filtrer par critères.

Point de Terminaison : `GET /api/subscriber`

Paramètres de Requête :

Paramètre	Type	Description
`enabled`	boolean	Filtrer par statut activé
`ims_enabled`	boolean	Filtrer par statut IMS activé

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/subscriber
```

Exemple de Réponse :

```
{
  "data": [
    {
      "id": 1,
      "imsi": "001001123456789",
      "enabled": true,
      "ims_enabled": true,
      "sim_id": 1,
      "key_set_id": 1,
      "epc_profile_id": 1,
      "ims_profile_id": 1,
      "roaming_profile_id": 1,
      "custom_attributes": {},
      "inserted_at": "2025-10-15T10:30:00Z",
```

```
      "updated_at": "2025-10-15T10:30:00Z"
    }
  ]
}
```

Obtenir un Abonné par ID

Récupérer un abonné spécifique par ID de base de données.

Point de Terminaison : `GET /api/subscriber/:id`

Paramètres de Chemin :

Paramètre	Type	Description
`id`	integer	ID de base de données de l'abonné

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/subscriber/1
```

Obtenir un Abonné par IMSI

Récupérer un abonné par son IMSI.

Point de Terminaison : `GET /api/subscriber/imsi/:imsi`

Paramètres de Chemin :

Paramètre	Type	Description	Format
`imsi`	string	Identité d'Abonné Mobile Internationale	14-15 chiffres

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/subscriber/imsi/001001123456789
```

Cas d'Utilisation : Dépannage d'un abonné spécifique par son IMSI.

Obtenir un Abonné par MSISDN

Récupérer un abonné par son numéro de téléphone.

Point de Terminaison : `GET /api/subscriber/msisdn/:msisdn`

Paramètres de Chemin :

Paramètre	Type	Description	Format
`msisdn`	string	Numéro ISDN de Station Mobile	1-15 chiffres (E.164)

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/subscriber/msisdn/14155551234
```

Cas d'Utilisation : Recherche d'informations sur un abonné lorsque vous n'avez que son numéro de téléphone.

Créer un Abonné

Provisionner un nouvel abonné.

Point de Terminaison : `POST /api/subscriber`

Corps de la Demande :

```
{
  "subscriber": {
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "sim_id": 1,
    "key_set_id": 1,
    "epc_profile_id": 1,
    "ims_profile_id": 1,
    "roaming_profile_id": 1,
    "custom_attributes": {
      "note": "Abonné de test"
    }
  }
}
```

Champs Requis :

- `imsi` - Doit être de 14-15 chiffres, unique
- `key_set_id` - Doit référencer un Ensemble de Clés existant
- `epc_profile_id` - Doit référencer un Profil EPC existant

Champs Optionnels :

- `enabled` - Par défaut : true
- `ims_enabled` - Par défaut : true
- `sim_id` - Référence à une carte SIM
- `ims_profile_id` - Référence à un Profil IMS (requis pour les services IMS)
- `roaming_profile_id` - Référence à un Profil de Roaming (requis pour le contrôle du roaming)
- `msisdns` - Tableau d'IDs MSISDN (numéros de téléphone)
- `static_ips` - Tableau d'IDs IP Statique pour les attributions APN
- `custom_attributes` - Paires clé-valeur personnalisées

Voir Aussi :

- Exemple Complet de Provisionnement d'Abonné - Flux de travail de bout en bout
- Documentation Multi-MSISDN - Attribution de numéros de téléphone aux abonnés
- Gestion des IP Statique - Attribution d'IPs statiques aux APNs

Exemple de Demande :

```
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": 1,
      "epc_profile_id": 1
    }
  }'
```

Flux de Provisionnement :

Mettre à Jour un Abonné

Modifier un abonné existant.

Point de Terminaison : `PUT /api/subscriber/:id`

Paramètres de Chemin :

Paramètre	Type	Description
`id`	integer	ID de base de données de l'abonné

Corps de la Demande :

```
{
  "subscriber": {
    "enabled": false,
    "ims_enabled": false,
    "epc_profile_id": 2,
    "custom_attributes": {
      "note": "Désactivé temporairement"
    }
  }
}
```

Champs Modifiables :

- `enabled` - Activer/désactiver tous les services
- `ims_enabled` - Activer/désactiver les services IMS
- `sim_id` - Changer l'attribution de la carte SIM
- `key_set_id` - Changer les clés cryptographiques (soyez prudent !)
- `epc_profile_id` - Changer le profil de service de données
- `ims_profile_id` - Changer le profil de service vocal
- `roaming_profile_id` - Changer la politique de roaming
- `msisdns` - Mettre à jour les numéros de téléphone attribués à l'abonné
- `static_ips` - Mettre à jour les attributions IP statique aux APNs
- `custom_attributes` - Mettre à jour les données personnalisées

Non Modifiables :

- `imsi` - Ne peut pas changer l'IMSI (supprimer et recréer à la place)

Voir Aussi :

- Gestion des Profils - Gestion des profils de service

Exemple de Demande :

```
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "enabled": false
    }
  }'
```

Cas d'Utilisation :

- Désactiver temporairement l'abonné : `{"enabled": false}`
- Désactiver uniquement les services vocaux : `{"ims_enabled": false}`
- Changer le profil de service : `{"epc_profile_id": 2}` (voir Profils EPC)
- Mettre à jour la politique de roaming : `{"roaming_profile_id": 3}` (voir Gestion du Roaming)

Supprimer un Abonné

Supprimer un abonné du système.

Point de Terminaison : `DELETE /api/subscriber/:id`

Paramètres de Chemin :

Paramètre	Type	Description
`id`	integer	ID de base de données de l'abonné

Exemple de Demande :

```
curl -k -X DELETE https://hss.example.com:8443/api/subscriber/1
```

Avertissement : Cela supprime définitivement l'abonné et toutes les données d'état associées (sessions PDN, appels, etc.). L'IMSI peut être réutilisé après la suppression.

Remarque : La suppression d'un abonné ne supprime PAS les éléments associés :

- Ensemble de Clés - Peut être réutilisé pour d'autres abonnés
- SIM - Peut être réattribuée à un nouvel abonné
- Profils - Ressources partagées utilisées par plusieurs abonnés
- MSISDNs - Doit être supprimé séparément si désiré

Annuler la Demande de Localisation (Détachement Forcé)

Envoyer une Demande d'Annulation de Localisation (CLR) pour détacher de force un abonné de son MME actuellement enregistré.

Point de Terminaison : `POST /api/subscriber/cancel_location`

Corps de la Demande :

```
{
  "imsi": "001001123456789"
}
```

Paramètres :

Paramètre	Type	Requis	Description
`imsi`	string	Oui	IMSI de l'abonné à détacher (14-15 chiffres)

Exemple de Demande :

```
curl -k -X POST https://hss.example.com:8443/api/subscriber/cancel_location
\
  -H "Content-Type: application/json" \
  -d '{"imsi": "001001123456789"}'
```

Réponse de Succès (200 OK) :

```
{
  "data": {
    "message": "Demande d'Annulation de Localisation envoyée avec succès",
    "imsi": "001001123456789",
    "destination_host": "mme01.operator.com",
    "destination_realm": "epc.operator.com"
  }
}
```

Réponse d'Erreur (404 Non Trouvé) :

```
{
  "error": "Abonné non trouvé ou non actuellement enregistré à un MME"
}
```

Comportement :

- Envoie un CLR S6a au MME où l'abonné est actuellement enregistré (`subscriber_state.last_seen_mme`)
- Utilise `Cancellation-Type: subscription_withdrawal` (force le détachement complet)
- Définit `CLR-Flags: {s6a_indicator: 1, reattach_required: 1}` (l'UE doit se ré-authentifier)
- Retourne 404 si l'abonné n'a jamais été enregistré ou si `last_seen_mme` est nul
- **Affects all MSISDNs** associés à l'IMSI (même appareil physique/SIM)

Cas d'Utilisation :

- **Prévention de Fraude :** Détacher immédiatement un abonné suspect
- **Résiliation de Souscription :** Forcer la déconnexion lorsque le compte est désactivé

- **Dépannage :** Effacer l'enregistrement MME obsolète pour le débogage
- **Migration :** Forcer la ré-authentification pour appliquer de nouveaux paramètres de profil
- **Sécurité :** Déconnecter immédiatement un abonné compromis

Considérations Multi-IMSI :

Lors de l'utilisation de CLR avec des scénarios multi-MSISDN :

1. **Plusieurs MSISDN, Un Seul IMSI :**

```
// L'abonné a l'IMSI 001001123456789 avec les MSISDNs ["+1234567890",
"+9876543210"]
POST /api/subscriber/cancel_location
{"imsi": "001001123456789"}

// Résultat : Un CLR envoyé, les deux MSISDNs affectés (même appareil)
```

2. **IMSI Différents (Appareils Différents) :**

```
// Deux abonnés avec le même MSISDN mais des IMSIs différents
(scénario de portabilité de numéro)
// Abonné A : IMSI 001001111111111, MSISDN "+1234567890"
// Abonné B : IMSI 001001222222222, MSISDN "+1234567890"

POST /api/subscriber/cancel_location
{"imsi": "001001111111111"}

// Résultat : Seul l'Abonné A est détaché, l'Abonné B n'est pas
affecté
```

Remarques Importantes :

- **Basé sur l'IMSI :** CLR est toujours envoyé par IMSI, pas par MSISDN
- **Asynchrone :** CLR est envoyé de manière asynchrone ; la réponse de succès signifie que le CLR a été envoyé, pas que le MME l'a traité
- **Pas de validation de l'état du MME :** CLR est envoyé même si le MME est injoignable (comportement standard de l'HSS)
- **Idempotent :** Sûr d'appeler plusieurs fois pour le même IMSI

Documentation Connexe :

- Flux de Protocole de Demande d'Annulation de Localisation
- Scénarios Multi-IMSI
- Architecture de l'Interface S6a

Gestion des MSISDN

Les MSISDN (numéros de téléphone) peuvent être attribués aux abonnés pour activer les services vocaux. Voir Documentation Multi-MSISDN pour des détails sur l'attribution de plusieurs numéros à un seul abonné.

Lister les MSISDN

Récupérer tous les numéros de téléphone.

Point de Terminaison : `GET /api/msisdn`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/msisdn
```

Obtenir un MSISDN

Récupérer un numéro de téléphone spécifique.

Point de Terminaison : `GET /api/msisdn/:id`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/msisdn/1
```

Créer un MSISDN

Créer un nouveau numéro de téléphone.

Point de Terminaison : `POST /api/msisdn`

Corps de la Demande :

```
{
  "msisdn": {
    "msisdn": "14155551234"
  }
}
```

Validation :

- Doit être de 1 à 15 chiffres
- Doit être unique
- Doit suivre le format E.164 (format international sans le signe +)

Exemple de Demande :

```
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{
    "msisdn": {
      "msisdn": "14155551234"
    }
  }'
```

Assigner un MSISDN à un Abonné

Pour attribuer un numéro de téléphone à un abonné, vous devez créer un enregistrement de jointure. Cela se fait généralement par le biais de l'endpoint de mise à jour de l'abonné ou via une manipulation directe de la base de données.

Modèle Multi-MSISDN :

Voir Fonctionnalités Multi-MSISDN et Multi-IMSI pour une utilisation détaillée.

Supprimer un MSISDN

Supprimer un numéro de téléphone.

Point de Terminaison : `DELETE /api/msisdn/:id`

Exemple de Demande :

```
curl -k -X DELETE https://hss.example.com:8443/api/msisdn/1
```

Gestion des SIM

Les enregistrements de carte SIM stockent des informations physiques sur la carte SIM, y compris l'ICCID, les détails du fournisseur, les codes PIN/PUK et les clés OTA. Les enregistrements de SIM peuvent être liés à des abonnés.

Voir Aussi :

- Documentation Multi-IMSI - Plusieurs abonnés sur une seule carte SIM physique

Lister les SIM

Récupérer toutes les cartes SIM.

Point de Terminaison : `GET /api/sim`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/sim
```

Obtenir une SIM

Récupérer une carte SIM spécifique.

Point de Terminaison : `GET /api/sim/:id`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/sim/1
```

Créer une SIM

Créer un nouvel enregistrement de carte SIM.

Point de Terminaison : `POST /api/sim`

Corps de la Demande :

```
{
  "sim": {
    "iccid": "8991101200003204510",
    "sim_vendor": "Gemalto",
    "batch_name": "2025-Q1-Batch-01",
    "is_esim": false,
    "pin1": "1234",
    "pin2": "5678",
    "puk1": "12345678",
    "puk2": "87654321",
    "adm1": "admin-code-1",
    "kic": "0123456789ABCDEF0123456789ABCDEF",
    "kid": "FEDCBA9876543210FEDCBA9876543210"
  }
}
```

Champs Requis :

- `iccid` - 19-20 chiffres, unique

Champs Optionnels mais Importants :

- `sim_vendor` - Nom du fabricant
- `batch_name` - Pour le suivi
- `is_esim` - Drapeau booléen pour eSIM
- `pin1`, `pin2` - Codes PIN utilisateur
- `puk1`, `puk2` - Codes de déverrouillage PIN
- `adm1`-`adm10` - Codes administratifs
- `kic`, `kid` - Clés de sécurité OTA (chaîne hexadécimale)

Exemple de Demande :

```
curl -k -X POST https://hss.example.com:8443/api/sim \
  -H "Content-Type: application/json" \
  -d '{
    "sim": {
      "iccid": "8991101200003204510",
      "sim_vendor": "Gemalto"
    }
  }'
```

Mettre à Jour une SIM

Modifier les données de la carte SIM.

Point de Terminaison : `PUT /api/sim/:id`

Exemple de Demande :

```
curl -k -X PUT https://hss.example.com:8443/api/sim/1 \
  -H "Content-Type: application/json" \
  -d '{
    "sim": {
      "batch_name": "Nom de Lot Mis à Jour"
    }
  }'
```

Supprimer une SIM

Supprimer un enregistrement de carte SIM.

Point de Terminaison : `DELETE /api/sim/:id`

Avertissement : Assurez-vous qu'aucun abonné ne référence cette SIM avant de la supprimer.

Gestion des Ensembles de Clés

Les ensembles de clés contiennent le matériel cryptographique (Ki, OPC/OP, AMF, SQN) utilisé pour l'authentification des abonnés via l'algorithme Milenage. Chaque abonné doit référencer un ensemble de clés.

Voir Aussi :

- Flux de Protocole - Procédures d'authentification utilisant des ensembles de clés

Lister les Ensembles de Clés

Récupérer tous les ensembles de clés cryptographiques.

Point de Terminaison : `GET /api/key_set`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/key_set
```

Obtenir un Ensemble de Clés

Récupérer un ensemble de clés spécifique.

Point de Terminaison : `GET /api/key_set/:id`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/key_set/1
```

Exemple de Réponse :

```
{
  "data": {
    "id": 1,
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "op": null,
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenage",
    "ota_counter": 0
  }
}
```

Créer un Ensemble de Clés

Créer un nouvel ensemble de clés cryptographiques.

Point de Terminaison : `POST /api/key_set`

Corps de la Demande :

```
{
  "key_set": {
    "ki": "0123456789ABCDEF0123456789ABCDEF",
    "opc": "FEDCBA9876543210FEDCBA9876543210",
    "amf": "8000",
    "sqn": 0,
    "authentication_algorithm": "milenage"
  }
}
```

Champs Requis :

- `ki` - Clé de 128 bits (32 caractères hexadécimaux)
- Soit `opc` OU `op` (l'OPC peut être dérivé de l'OP)
- `authentication_algorithm` - Actuellement seulement "milenage"

Champs Optionnels :

- `amf` - Par défaut : "8000"
- `sqn` - Par défaut : 0
- `ota_counter` - Par défaut : 0

Format des Clés :

- Toutes les clés sont des chaînes hexadécimales
- Ki, OPC, OP : 32 caractères hexadécimaux (128 bits)
- AMF : 4 caractères hexadécimaux (16 bits)

Exemple de Demande :

```
curl -k -X POST https://hss.example.com:8443/api/key_set \
  -H "Content-Type: application/json" \
  -d '{
    "key_set": {
      "ki": "0123456789ABCDEF0123456789ABCDEF",
      "opc": "FEDCBA9876543210FEDCBA9876543210",
      "authentication_algorithm": "milenage"
    }
  }'
```

Avertissement de Sécurité : Les ensembles de clés contiennent des matériaux cryptographiques hautement sensibles. Protégez l'accès à l'API en conséquence.

Mettre à Jour un Ensemble de Clés

Modifier un ensemble de clés existant.

Point de Terminaison : `PUT /api/key_set/:id`

Avertissement : Changer les clés pour un abonné actif entraînera des échecs d'authentification. Ne mettez à jour les clés que pendant les fenêtres de maintenance ou pour de nouveaux abonnés.

Impact : Les mises à jour affectent immédiatement tous les abonnés utilisant cet ensemble de clés. Les abonnés actifs échoueront à l'authentification lors de la prochaine tentative de connexion.

Supprimer un Ensemble de Clés

Supprimer un ensemble de clés.

Point de Terminaison : `DELETE /api/key_set/:id`

Avertissement : Assurez-vous qu'aucun abonné ne référence cet ensemble de clés avant de le supprimer. Interrogez d'abord les abonnés pour vérifier les références.

Gestion des Profils

Profils EPC

Les profils EPC (Evolved Packet Core) définissent les paramètres de service de données pour les abonnés. Ces profils sont référencés lors de la création des abonnés.

Lister les Profils EPC

Point de Terminaison : `GET /api/epc/profile`

Obtenir un Profil EPC

Point de Terminaison : `GET /api/epc/profile/:id`

Créer un Profil EPC

Point de Terminaison : `POST /api/epc/profile`

Corps de la Demande :

```
{
  "epc_profile": {
    "name": "Plan de Données Standard",
    "ue_ambr_dl_kbps": 100000,
    "ue_ambr_ul_kbps": 50000,
    "network_access_mode": 0,
    "tracking_area_update_interval_seconds": 54
  }
}
```

Champs :

Champ	Description	Unités	Valeurs Typiques
`name`	Nom du profil	Texte	Identifiant unique
`ue_ambr_dl_kbps`	Limite de bande passante de téléchargement	Kbps	10000-1000000
`ue_ambr_ul_kbps`	Limite de bande passante de téléchargement	Kbps	5000-500000
`network_access_mode`	Type d'accès	Enum	0=Packet uniquement, 2=Packet+Réservé
`tracking_area_update_interval_seconds`	Minuteur TAU	Secondes	54 (typique)

Exemple de Demande :

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    }
  }'
```

Voir Aussi :

- Documentation des Profils - Guide de configuration détaillé des profils
- Provisionnement Complet d'Abonné - Utilisation des profils EPC dans le provisionnement

Mettre à Jour un Profil EPC

Point de Terminaison : `PUT /api/epc/profile/:id`

Remarque : Les modifications des profils EPC affectent tous les abonnés utilisant ce profil. Les sessions actives peuvent devoir être rétablies.

Supprimer un Profil EPC

Point de Terminaison : `DELETE /api/epc/profile/:id`

Avertissement : Assurez-vous qu'aucun abonné ne référence ce profil avant de le supprimer.

Profils IMS

Les profils IMS (IP Multimedia Subsystem) définissent les paramètres de service vocal et les Critères de Filtrage Initiaux (IFC) pour les abonnés. Ces profils sont référencés lors de la création des abonnés avec les services IMS activés.

Lister les Profils IMS

Point de Terminaison : `GET /api/ims/profile`

Créer un Profil IMS

Point de Terminaison : `POST /api/ims/profile`

Corps de la Demande :

```
{
  "ims_profile": {
    "name": "VoLTE Standard",
    "ifc_template": "<Modèle-IMS-XML-ici>"
  }
}
```

Voir Aussi :

- Documentation des Profils - Détails et exemples de modèles IFC
- Flux de Protocole - Flux d'enregistrement IMS et d'appels

Profils APN

Les profils APN (Access Point Name) se composent de trois composants qui fonctionnent ensemble :

1. **Identifiant APN** - Définit le nom de l'APN et la version IP
2. **Profil QoS APN** - Définit les paramètres de Qualité de Service
3. **Profil APN** - Combine identifiant et QoS, lié aux Profils EPC

Voir Documentation PCRF pour la configuration détaillée des politiques, la gestion de la QoS et la ré-authentification automatique. Voir aussi Documentation des Profils pour des exemples de configuration APN.

Lister les Identifiants APN

Point de Terminaison : `GET /api/apn/identifier`

Créer un Identifiant APN

Point de Terminaison : `POST /api/apn/identifier`

Corps de la Demande :

```
{
  "apn_identifier": {
    "apn": "internet",
    "ip_version": 2
  }
}
```

Valeurs de Version IP :

- `0` - IPv4 uniquement
- `1` - IPv6 uniquement
- `2` - IPv4v6 (double pile)
- `3` - IPv4 ou IPv6 (choix du réseau)

Lister les Profils QoS APN

Point de Terminaison : `GET /api/apn/qos_profile`

Créer un Profil QoS APN

Point de Terminaison : `POST /api/apn/qos_profile`

Corps de la Demande :

```
{
  "apn_qos_profile": {
    "name": "Internet Meilleur Effort",
    "qci": 9,
    "allocation_retention_priority": 8,
    "apn_ambr_dl_kbps": 50000,
    "apn_ambr_ul_kbps": 25000,
    "pre_emption_capability": false,
    "pre_emption_vulnerability": true
  }
}
```

Lister les Profils APN

Point de Terminaison : `GET /api/apn/profile`

Créer un Profil APN

Point de Terminaison : `POST /api/apn/profile`

Corps de la Demande :

```
{
  "apn_profile": {
    "name": "Profil APN Internet",
    "apn_identifier_id": 1,
    "apn_qos_profile_id": 1
  }
}
```

Champs Requis :

- `apn_identifier_id` - Doit référencer un Identifiant APN existant
- `apn_qos_profile_id` - Doit référencer un Profil QoS APN existant

Voir Aussi :

- Provisionnement Complet d'Abonné - Exemple complet incluant la configuration APN
- Profils EPC - Les profils APN sont liés aux profils EPC

Gestion des IP Statique

Les adresses IP statiques peuvent être attribuées à des APNs spécifiques pour des abonnés individuels. Cela permet aux abonnés de recevoir une adresse IPv4 et/ou IPv6 prédéterminée lors de la connexion à un APN particulier, plutôt que de recevoir une adresse dynamique d'un pool DHCP.

Architecture :

Flux de Données Lors de la Connexion de l'Abonné :

Réponse de Mise à Jour de Localisation - Cartographie des Données de Configuration APN :

Ce diagramme montre exactement d'où provient chaque champ dans l'AVP de Configuration APN de la Réponse de Mise à Jour de Localisation S6a dans la base de données :

Observations Clés :

1. **Identifiant de Contexte** : Index séquentiel (0, 1, 2...) pour chaque APN dans le profil

2. **Sélection de Service** : Provient directement de `apn_identifier.apn` (ex : "internet", "ims")
3. **Type de PDN** : Encodé à partir de `apn_identifier.ip_version` (ipv4=0, ipv6=1, ipv4v6=2, ipv4_or_ipv6=3)
4. **Paramètres QoS** : Tous provenant de la table `apn_qos_profile`
5. **Bande Passante AMBR** : Les valeurs sont multipliées par 1000 (conversion kbps → bps)
6. **Adresse IP de Partie Servie** : Incluse uniquement si une IP statique existe pour cette combinaison abonné+APN
    - Processus de recherche : `subscriber.static_ips` → filtrer par `apn_profile_id` → extraire les IPs
    - La compatibilité de la version IP est vérifiée par rapport à `apn_identifier.ip_version`
7. **VPLMN-Dynamic-Address-Allowed** : Codé en dur à 0 (non autorisé) - force l'utilisation d'une IP statique si fournie

Hiérarchie des Relations :

Concepts Clés :

- **Attribution par APN** : Chaque IP Statique est liée à un Profil APN spécifique
- **Une IP par APN par Abonné** : Un abonné ne peut avoir qu'une seule attribution IP statique par APN
- **Support IPv4 et IPv6** : Les IP statiques peuvent être uniquement IPv4, uniquement IPv6 ou double pile
- **Unicité Globale des IP** : Chaque adresse IP doit être globalement unique à travers **tous** les enregistrements d'IP statique dans le système
    - La même adresse IPv4 ou IPv6 ne peut pas être attribuée à plusieurs abonnés (même sur différents APNs)
    - Cela empêche les conflits de routage et l'ambiguïté des adresses IP
    - Appliqué par des index uniques de base de données sur les champs `ipv4_static_ip` et `ipv6_static_ip`
- **Relation Plusieurs-à-Plusieurs** : Les abonnés et les IP Statique sont liés via une table de jointure

Cas d'Utilisation :

- Adresses IP fixes pour des appareils IoT
- Hébergement de serveurs sur des appareils mobiles (nécessite une IP statique pour les connexions entrantes)
- Applications héritées nécessitant des adresses IP spécifiques
- Routage de politique réseau basé sur l'adresse IP source
- Conformité réglementaire nécessitant le suivi des adresses IP

Lister les IP Statique

Récupérer toutes les attributions IP statiques.

Point de Terminaison : `GET /api/epc/static_ip`

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/epc/static_ip
```

Exemple de Réponse :

```
{
  "data": [
    {
      "id": 1,
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111",
      "apn_profile": {
        "id": 5,
        "name": "Profil APN Internet",
        "apn_identifier": {
          "apn": "internet",
          "ip_version": "ipv4v6"
        }
      },
      "inserted_at": "2025-11-15T10:30:00Z",
      "updated_at": "2025-11-15T10:30:00Z"
    }
  ]
}
```

Obtenir une IP Statique

Récupérer une attribution IP statique spécifique.

Point de Terminaison : `GET /api/epc/static_ip/:id`

Paramètres de Chemin :

Paramètre	Type	Description
`id`	integer	ID de base de données de l'IP statique

Exemple de Demande :

```
curl -k https://hss.example.com:8443/api/epc/static_ip/1
```

Créer une IP Statique

Créer une nouvelle attribution IP statique pour un APN.

Point de Terminaison : `POST /api/epc/static_ip`

Corps de la Demande :

```
{
  "static_ip": {
    "apn_profile_id": 5,
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111"
  }
```

```
}
```

Champs Requis :

- `apn_profile_id` - Doit référencer un Profil APN existant
- Au moins une des `ipv4_static_ip` OU `ipv6_static_ip` doit être spécifiée

Champs Optionnels :

- `ipv4_static_ip` - Adresse IPv4 (notation décimale pointée)
- `ipv6_static_ip` - Adresse IPv6 (notation standard)

Validation du Format IP :

- IPv4 : Format standard décimal pointé (ex : `100.64.1.1`)
- IPv6 : Format standard hexadécimal séparé par des deux-points (ex : `2606:4700:4700::1111`)
- Les adresses IPv4 et IPv6 doivent être **globalement uniques à travers tous les enregistrements d'IP statique**
  - Cela empêche les conflits d'adresses IP dans le réseau
  - La même IP ne peut pas être attribuée à plusieurs abonnés, même sur différents APNs
  - C'est une contrainte au niveau de la base de données appliquée par des index uniques

Options de Configuration :

Configuration	IPv4	IPv6	Exemple
IPv4 Seulement	✓	-	`{"ipv4_static_ip": "100.64.1.1"}`
IPv6 Seulement	-	✓	`{"ipv6_static_ip": "2606:4700:4700::1111"}`
Double Pile	✓	✓	Les deux champs spécifiés

Exemples de Demandes :

IP Statique uniquement IPv4 :

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1"
    }
  }'
```

IP Statique uniquement IPv6 :

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 6,
```

```
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }'
```

IP Statique double pile :

```
curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }'
```

Réponse de Succès (201 Créé) :

```
{
  "data": {
    "id": 1,
    "apn_profile_id": 5,
    "ipv4_static_ip": "100.64.1.1",
    "ipv6_static_ip": "2606:4700:4700::1111",
    "inserted_at": "2025-11-15T10:30:00Z",
    "updated_at": "2025-11-15T10:30:00Z"
  }
}
```

Voir Aussi :

- Attribuer une IP Statique à un Abonné - Comment lier cela à un abonné
- Profils APN - Gestion des configurations APN

Mettre à Jour une IP Statique

Modifier une attribution IP statique existante.

Point de Terminaison : `PUT /api/epc/static_ip/:id`

Paramètres de Chemin :

Paramètre	Type	Description
`id`	integer	ID de base de données de l'IP statique

Corps de la Demande :

```
{
  "static_ip": {
    "ipv4_static_ip": "100.64.1.2",
    "ipv6_static_ip": "2606:4700:4700::1112"
  }
```

```
}
```

Champs Modifiables :

- `ipv4_static_ip` - Changer l'adresse IPv4
- `ipv6_static_ip` - Changer l'adresse IPv6
- `apn_profile_id` - Changer l'attribution APN

Non Modifiables :

- `id` - Clé primaire (lecture seule)

Avertissement : Changer l'adresse IP pour un abonné actif affectera sa prochaine connexion PDN. Les sessions PDN actives continueront à utiliser l'ancienne IP jusqu'à ce qu'elles se déconnectent et se reconnectent.

Exemple de Demande :

```
curl -k -X PUT https://hss.example.com:8443/api/epc/static_ip/1 \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "ipv4_static_ip": "100.64.1.2"
    }
  }'
```

Supprimer une IP Statique

Supprimer une attribution IP statique.

Point de Terminaison : `DELETE /api/epc/static_ip/:id`

Paramètres de Chemin :

Paramètre	Type	Description
`id`	integer	ID de base de données de l'IP statique

Exemple de Demande :

```
curl -k -X DELETE https://hss.example.com:8443/api/epc/static_ip/1
```

Comportement :

- Supprime l'attribution IP statique
- N'affecte PAS le Profil APN (l'APN reste disponible pour d'autres abonnés)
- Les abonnés utilisant cette IP statique recevront des IP dynamiques lors de la prochaine connexion
- L'adresse IP devient disponible pour réutilisation après suppression

Avertissement : Si un abonné utilise activement cette IP statique, la supprimer entraînera la réception d'une IP dynamique lors de sa prochaine connexion PDN. Assurez-vous que les abonnés sont hors ligne ou envoyez une Demande d'Annulation de Localisation avant de supprimer.

Assigner une IP Statique à un Abonné

Pour attribuer une IP statique à un abonn��, vous devez associer l'enregistrement IP statique à l'Abonné lors de la création ou de la mise à jour.

Modèle d'Attribution :

1. **Créer l'IP Statique** (voir Créer une IP Statique)
2. **Attribuer à l'Abonné** en utilisant le champ `static_ips`

Créer un Abonné avec IP Statique :

```
# Étape 1 : Créer une IP statique pour l'APN "internet"
STATIC_IP_ID=$(curl -k -X POST https://hss.example.com:8443/api/epc/
static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1",
      "ipv6_static_ip": "2606:4700:4700::1111"
    }
  }' | jq -r '.data.id')

# Étape 2 : Créer un abonné avec l'IP statique attribuée
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": 1,
      \"epc_profile_id\": 1,
      \"static_ips\": [$STATIC_IP_ID]
    }
  }"
```

Mettre à Jour un Abonné Existant avec IP Statique :

```
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "static_ips": [1, 2]
    }
  }'
```

Plusieurs IP Statique (Différents APNs) :

Un abonné peut avoir plusieurs IP statiques tant que chacune est pour un APN différent :

```
# Créer une IP statique pour l'APN "internet"
INTERNET_IP=$(curl -k -X POST https://hss.example.com:8443/api/epc/
static_ip \
```

```
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 5,
      "ipv4_static_ip": "100.64.1.1"
    }
  }' | jq -r '.data.id')

# Créer une IP statique pour l'APN "ims"
IMS_IP=$(curl -k -X POST https://hss.example.com:8443/api/epc/static_ip \
  -H "Content-Type: application/json" \
  -d '{
    "static_ip": {
      "apn_profile_id": 6,
      "ipv4_static_ip": "100.64.2.1"
    }
  }' | jq -r '.data.id')

# Attribuer les deux à l'abonné
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d "{
    \"subscriber\": {
      \"imsi\": \"001001123456789\",
      \"key_set_id\": 1,
      \"epc_profile_id\": 1,
      \"static_ips\": [$INTERNET_IP, $IMS_IP]
    }
  }"
```

Règles de Validation :

- ✓ **Autorisé** : Plusieurs IP statiques pour différents APNs
- ✗ **Rejeté** : Plusieurs IP statiques pour le même APN

Exemple d'Erreur - APN Dupliqué :

```
# Cela échouera si les deux IP statiques référencent le même APN
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "static_ips": [1, 2]
    }
  }'

# Réponse d'Erreur :
{
  "errors": {
    "static_ips": [
      "les IP statiques par apn par abonné doivent être uniques. par ex un
abonné ne peut pas se voir attribuer l'IP statique 100.64.1.1 pour internet
```

```
et aussi 100.64.1.2 pour internet"
    ]
  }
}
```

Voir Aussi :

- Créer un Abonné - Provisionnement d'abonné
- Mettre à Jour un Abonné - Modification de la configuration de l'abonné
- Exemple Complet de Provisionnement d'IP Statique - Flux de travail de bout en bout

---

Gestion du Roaming

Les profils de roaming contrôlent si les abonnés peuvent accéder aux services de données et IMS sur des réseaux visités. Les profils sont attribués aux abonnés et se composent de règles correspondant aux MCC/MNC.

Lister les Profils de Roaming

Point de Terminaison : `GET /api/roaming/profile`

Créer un Profil de Roaming

Point de Terminaison : `POST /api/roaming/profile`

Corps de la Demande :

```
{
  "roaming_profile": {
    "name": "Transporteurs des États-Unis uniquement",
    "data_action_if_no_rules_match": 1,
    "ims_action_if_no_rules_match": 1
  }
}
```

Valeurs d'Action :

- `0` - Autoriser
- `1` - Refuser

Actions par Défaut :

- `data_action_if_no_rules_match` - Action lorsque aucune règle de roaming ne correspond
- `ims_action_if_no_rules_match` - Action par défaut spécifique à IMS

Lister les Règles de Roaming

Point de Terminaison : `GET /api/roaming/rule`

Créer une Règle de Roaming

Point de Terminaison : `POST /api/roaming/rule`

Corps de la Demande :

```
{
  "roaming_rule": {
    "name": "Autoriser AT&T",
    "mcc": "310",
    "mnc": "410",
    "data_action": 0,
    "ims_action": 0
  }
}
```

Champs :

- `mcc` - Code Pays Mobile (3 chiffres)
- `mnc` - Code Réseau Mobile (2-3 chiffres)
- `data_action` - Autoriser (0) ou Refuser (1) les services de données
- `ims_action` - Autoriser (0) ou Refuser (1) les services IMS/vocaux

Voir Aussi :

- Documentation sur le Roaming - Configuration détaillée et exemples
- Flux de Protocole - Comment fonctionne le contrôle du roaming dans les flux Diameter

---

Gestion de l'EIR

OmniHSS fonctionne comme un Registre d'Identité d'Équipement (EIR) via l'interface Diameter S13. Les règles EIR contrôlent l'accès des appareils en fonction des modèles IMEI.

Voir Documentation EIR pour le contrôle d'identité des équipements détaillé, les flux d'interface S13 et la validation IMEI.

Lister les Règles EIR

Point de Terminaison : `GET /api/eir/rule`

Créer une Règle EIR

Point de Terminaison : `POST /api/eir/rule`

Corps de la Demande :

```
{
  "eir_rule": {
    "name": "Bloquer iPhone 6",
```

```
    "imei_regex": "^35[0-9]{6}0[0-9]{7}$",
    "action": 1
  }
}
```

Champs :

- `name` - Nom descriptif pour la règle
- `imei_regex` - Expression régulière pour correspondre aux numéros IMEI
- `action` - Liste blanche (0), Liste noire (1) ou Liste grise (2)

Valeurs d'Action :

- `0` - Liste blanche (autoriser)
- `1` - Liste noire (refuser)
- `2` - Liste grise (autoriser mais suivre)

Cas d'Utilisation :

- Bloquer les appareils volés (liste noire de numéros IMEI spécifiques)
- Restreindre les types d'appareils (liste noire par modèle TAC)
- Autoriser uniquement les appareils approuvés (modèle de liste blanche avec refus par défaut)

Voir Aussi :

- Flux de Protocole - Flux d'interface S13 et flux de vérification EIR
- Vue d'Ensemble de l'Architecture - Fonction EIR d'OmniHSS

Documentation Supplémentaire

Pour plus d'informations, consultez la documentation suivante :

- **Statut et Santé** - Points de terminaison de vérification de la santé de l'API
- **Gestion des Erreurs** - Erreurs courantes et dépannage
- **Exemples d'Utilisation de l'API** - Flux de travail de provisionnement complet

---

← Retour au Guide des Opérations | Suivant : Panneau de Contrôle →

État et santé de l'API

← Retour à la référence de l'API

État du système

Vérifiez si l'API répond.

Point de terminaison : `GET /api/status`

Exemple de requête :

```
curl -k https://hss.example.com:8443/api/status
```

Exemple de réponse :

```
{
  "status": "ok"
}
```

Cas d'utilisation : Vérification de la santé pour les équilibreurs de charge et les systèmes de surveillance.

← Retour à la référence de l'API

Vue d'ensemble de l'architecture d'OmniHSS

← Retour au guide des opérations

Table des matières

Vue d'ensemble du système

OmniHSS est construit sur Elixir et la plateforme Erlang/OTP, fournissant un système hautement concurrent et tolérant aux pannes, conçu pour les charges de travail de télécommunications. L'architecture suit une approche en couches avec une séparation claire des préoccupations.

Architecture des composants

Composants principaux

Gestionnaires d'application Diameter

Chaque application Diameter (S6a, Cx, Sh, S13, Gx, Rx) est implémentée comme un module gestionnaire DiameterEx qui :

1. **S'inscrit auprès de DiameterEx** - S'abonne à des ID d'application Diameter spécifiques
2. **Valide les demandes** - Extrait les AVP, valide l'état du souscripteur
3. **Traite la logique métier** - Appelle les modules de logique métier appropriés
4. **Construit les réponses** - Construit des messages de réponse Diameter avec des AVP

5. **Gère les erreurs** - Retourne des codes de résultat Diameter appropriés

---

Pile Diameter

Configuration du service Diameter

OmniHSS configure un seul service Diameter avec plusieurs applications prises en charge :

Gestion de la connexion entre pairs

Flux de messages Diameter

Couche d'application

Interface S6a (LTE/EPC)

Gère l'authentification et la gestion de la mobilité pour les réseaux LTE.

Interface Cx (IMS)

Gère l'enregistrement et l'authentification IMS.

Interface Sh (Données de profil IMS)

Fournit aux serveurs d'application IMS un accès aux données de profil des abonnés.

Interface Gx (Contrôle de politique)

Gère le contrôle de politique et de facturation pour les sessions de données. **Voir Documentation PCRF pour plus de détails.**

Interface Rx (Média IMS)

Contrôle la politique média IMS et les porteurs dédiés pour VoLTE. **Voir Documentation PCRF pour plus de détails.**

Interface S13 (EIR)

Valide l'IMEI de l'appareil par rapport aux règles d'identité de l'équipement. **Voir Documentation EIR pour plus de détails.**

Couche de données

Vue d'ensemble du schéma de base de données

Modèle de référentiel Ecto

Stratégie de requête optimisée

Chaque procédure Diameter utilise des requêtes optimisées qui préchargent uniquement les associations nécessaires :

Interfaces externes

Architecture API

Architecture du panneau de contrôle

Architecture de déploiement

Déploiement sur un seul nœud

Exemple de flux de processus : Authentification

Cet exemple montre le flux complet pour une demande d'authentification :

Principes architecturaux clés

1. Tolérance aux pannes

- Les arbres de supervision Erlang/OTP redémarrent automatiquement les processus échoués
- Les gestionnaires Diameter isolés empêchent les pannes en cascade
- Pooling de connexions à la base de données avec reconnexion automatique

2. Concurrence

- Chaque demande Diameter est traitée dans son propre processus
- Pas d'état partagé entre les gestionnaires de demande
- Pooling de connexions à la base de données pour des requêtes parallèles

3. Modularité

- Chaque application Diameter dans un module séparé
- Séparation claire entre l'interface, la logique métier et les couches de données
- Algorithmes d'authentification modulables

4. Performance

- Requêtes de base de données optimisées avec préchargement sélectif
- Transfert de données minimal pour chaque type de procédure
- Pooling de connexions et keepalive

5. Observabilité

- Surveillance en temps réel via le panneau de contrôle
- Journalisation structurée tout au long de l'application
- Suivi de l'état des pairs Diameter
- Suivi de l'état des abonnés avec des horodatages

← Retour au guide des opérations | Suivant : Configuration →

Guide de Configuration OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu du Fichier de Configuration

OmniHSS utilise deux fichiers de configuration principaux :

config/config.exs (Temps de Compilation)

Contient la configuration statique qui ne change pas entre les environnements :

- Configuration de la page du Panneau de Contrôle
- Configuration des points de terminaison de l'API
- Paramètres de télémétrie

config/runtime.exs (Temps d'Exécution)

Contient la configuration spécifique à l'environnement qui change par déploiement :

- Paramètres de connexion à la base de données
- Configuration des pairs Diameter
- Paramètres du PLMN domestique
- Sélection S-CSCF IMS
- Liaisons d'interface réseau

Configuration à l'Exécution

Priorité de Configuration

Modèle de Variable d'Environnement

OmniHSS suit ce modèle pour la configuration :

- Les noms des variables d'environnement sont en MAJUSCULES avec des underscores
- Les valeurs par défaut sont fournies dans runtime.exs
- Les identifiants de base de données doivent utiliser des variables d'environnement en production

---

Configuration de la Base de Données

Configuration de Base de Données de Base

```
# config/runtime.exs

config :hss, Hss.Repo,
  # Paramètres de connexion à la base de données
  username: System.get_env("DATABASE_USERNAME", "root"),
  password: System.get_env("DATABASE_PASSWORD", "password"),
  hostname: System.get_env("DATABASE_HOSTNAME", "localhost"),
  database: System.get_env("DATABASE_NAME", "omnihss"),

  # Paramètres du pool de connexions
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "20")),

  # Délais d'attente (en millisecondes)
  timeout: 15_000,
  connect_timeout: 15_000,

  # Options supplémentaires
  show_sensitive_data_on_connection_error: false
```

Paramètres de Configuration de la Base de Données

Paramètre	Description	Par Défaut	Recommandation
`username`	Nom d'utilisateur de la base de données SQL	`"root"`	Utiliser un utilisateur dédié en production
`password`	Mot de passe de la base de données SQL	`"password"`	Utiliser un mot de passe fort, stocker dans une variable d'environnement
`hostname`	Nom d'hôte du serveur de base de données SQL	`"localhost"`	Utiliser un FQDN ou une IP en production
`database`	Nom de la base de données	`"omnihss"`	Garder par défaut sauf si plusieurs instances
`pool_size`	Taille du pool de	`20`	Ajuster en fonction de la charge

Paramètre	Description	Par Défaut	Recommandation
	connexions		(10-50 typique)

Réglage de la Taille du Pool

Directives :

- Commencer avec 20 connexions
- Surveiller les erreurs de "délai d'attente du pool de connexions"
- Augmenter de 10 si des délais d'attente se produisent sous une charge normale
- Chaque connexion utilise ~4 Mo de mémoire
- Trop de connexions peuvent dégrader les performances de la base de données SQL

Exemple : Configuration de Base de Données de Production

```
# config/runtime.exs - Exemple de production

config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),      # Requis en
production
  password: System.fetch_env!("DATABASE_PASSWORD"),      # Requis en
production
  hostname: System.get_env("DATABASE_HOSTNAME", "db.internal.example.com"),
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT", "3306")),
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/mysql-ca.pem",
    verify: :verify_peer
  ]
```

Configuration de Diameter

Configuration du Service Diameter

```
# config/runtime.exs

diameter_config = %{
  service_name: :omnitouch_hss,

  # Liaison réseau
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port: String.to_integer(System.get_env("DIAMETER_LISTEN_PORT",
"3868")),

  # Identité Diameter
  host: System.get_env("DIAMETER_HOST", "omnihss"),
  realm: System.get_env("DIAMETER_REALM",
"epc.mnc001.mcc001.3gppnetwork.org"),
```

```
  # Identification du produit
  product_name: "OmniHSS",
  vendor_id: 10415,  # 3GPP
  supported_vendor_ids: [5535, 10415],

  # Paramètres de protocole
  request_timeout: 5000,

  # Configuration des pairs
  peers: [
    # Ajouter des configurations de pairs ici
  ]
}

config :hss, :diameter, diameter_config
```

Configuration de l'Identité Diameter

Directives :

- **Hôte :** Nom d'hôte court de l'HSS (par exemple, "omnihss", "hss01")
- **Royaume :** Royaume Diameter correspondant à votre PLMN (par exemple, "epc.mnc001.mcc001.3gppnetwork.org")
- **Identité Complète :** Construit comme `{host}.{realm}`

Ajout de Pairs Diameter

Configuration de Pair Statique (Mode Connect)

```
# config/runtime.exs

peers: [
  # Exemple de Pair MME
  %{
    host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.100",
    port: 3868,
    transport: :sctp,  # ou :tcp
    applications: [:s6a]
  },

  # Exemple de Pair P-GW
  %{
    host: "pgw01.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.101",
    port: 3868,
    transport: :sctp,
    applications: [:gx]
  },
```

```
  # Exemple de Pair I-CSCF
  %{
    host: "icscf01.ims.mnc001.mcc001.3gppnetwork.org",
    realm: "ims.mnc001.mcc001.3gppnetwork.org",
    ip: "10.7.25.102",
    port: 3868,
    transport: :tcp,
    applications: [:cx]
  }
]
```

Mode Écoute Seule

Pour les environnements où les pairs initient des connexions à l'HSS :

```
# config/runtime.exs

diameter_config = %{
  # ... autre configuration ...
  peers: []  # Vide - accepter uniquement les connexions entrantes
}
```

Modes de Connexion des Pairs Diameter

Sélection du Protocole de Transport

Transport	Avantages	Inconvénients	Recommandation
SCTP	Multi-streaming, meilleure détection des pannes	Nécessite un support du noyau, configuration du pare-feu	Préféré pour Diameter
TCP	Support universel, règles de pare-feu plus simples	Flux unique, détection des pannes plus lente	Utiliser si SCTP indisponible

Configuration Réseau

Configuration du PLMN Domestique

Le PLMN domestique identifie votre opérateur de réseau :

```
# config/runtime.exs

config :hss, :home_plmn, %{
  mcc: System.get_env("HOME_PLMN_MCC", "001"),  # Code de Pays Mobile
  mnc: System.get_env("HOME_PLMN_MNC", "001")   # Code de Réseau Mobile
}
```

Format du Code PLMN

Exemples :

- AT&T (USA) : MCC=310, MNC=410
- Verizon (USA) : MCC=311, MNC=480
- Vodafone (UK) : MCC=234, MNC=15
- Réseau de Test : MCC=001, MNC=01

Liaison d'Interface Réseau

```
# config/runtime.exs

# Interface Diameter
listen_ip: System.get_env("DIAMETER_LISTEN_IP", "0.0.0.0"),  # Toutes les
interfaces
# Ou interface spécifique :
# listen_ip: "10.7.25.186",

# Interface API
config :hss, HssWeb.Api.Endpoint,
  http: [
    ip: {0, 0, 0, 0},  # Toutes les interfaces
    port: 8443
  ]

# Interface du Panneau de Contrôle
config :hss, HssWeb.ControlPanel.Endpoint,
  http: [
    ip: {0, 0, 0, 0},  # Toutes les interfaces
    port: 7443
  ]
```

Options de Liaison d'Interface :

Configuration IMS

Configuration de Sélection S-CSCF

```
# config/runtime.exs

config :hss, :ims, %{
  scscf: %{
    # Méthode de sélection : :random_peer ou :round_robin
    selection_method: :random_peer,

    # Liste des pairs S-CSCF disponibles
    peers: [
      %{
        host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060",
        capabilities: []  # Optionnel : correspondance des capacités
      },
      %{
        host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060",
        capabilities: []
```

```
      }
    ]
  }
}
```

Méthodes de Sélection S-CSCF

Méthodes de Sélection :

Méthode	Description	Cas d'Utilisation
`:random_peer`	Sélectionne aléatoirement un S-CSCF	Distribution de charge uniforme
`:round_robin`	Assigne séquentiellement les S-CSCF	Distribution prévisible

Configuration du Royaume IMS

Typiquement, l'IMS utilise un royaume séparé de l'EPC :

```
# Royaume EPC
"epc.mnc001.mcc001.3gppnetwork.org"

# Royaume IMS
"ims.mnc001.mcc001.3gppnetwork.org"
```

Configuration EIR

Voir [Documentation EIR] pour des détails complets sur la vérification de l'identité des équipements.

Paramètres du Registre d'Identité des Équipements

```
# config/runtime.exs

config :hss, :eir, %{
  # Comportement pour les équipements inconnus (aucune règle correspondante)
  unknown_equipment_behaviour: :whitelist
  # Options :
  #   :whitelist - Autoriser les équipements inconnus
  #   :blacklist - Bloquer les équipements inconnus
  #   :greylist - Suivre mais autoriser les équipements inconnus
  #   :reject_unknown_equipment - Rejeter avec un code de résultat
spécifique
}
```

Comportement des Équipements Inconnus

Options de Comportement :

Option	Résultat	Cas d'Utilisation
`:whitelist`	Autoriser tous les IMEI inconnus	Réseau ouvert, test
`:blacklist`	Bloquer tous les IMEI inconnus	Sécurité modérée

Option	Résultat	Cas d'Utilisation
`:greylist`	Autoriser mais suivre les IMEI inconnus	Mode de surveillance
`:reject_unknown_equipment`	Rejeter avec un code spécifique	Haute sécurité

Recommandation : Commencer avec `:whitelist` pendant les tests, passer à `:greylist` pour la surveillance en production, puis `:blacklist` pour une sécurité stricte.

Configuration de l'API et du Panneau de Contrôle

Configuration du Point de Terminaison de l'API

```
# config/config.exs

config :hss, HssWeb.Api.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(json)],
  pubsub_server: Hss.PubSub,

  # Configuration HTTPS
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: "priv/cert/omnitouch.crt",
    keyfile: "priv/cert/omnitouch.pem"
  ]
```

Configuration du Panneau de Contrôle

```
# config/config.exs

config :hss, HssWeb.ControlPanel.Endpoint,
  url: [host: "localhost"],
  render_errors: [view: HssWeb.ErrorView, accepts: ~w(html json)],
  pubsub_server: Hss.PubSub,
  live_view: [signing_salt: "some-secret"],

  # Configuration HTTPS
  https: [
    port: 7443,
    cipher_suite: :strong,
    certfile: "priv/cert/omnitouch.crt",
    keyfile: "priv/cert/omnitouch.pem"
  ]
```

Configuration du Certificat TLS

Exigences du Certificat :

- Certificat X.509 valide

- Clé privée correspondante
- Inclure les certificats intermédiaires si nécessaire
- CN ou SAN doit correspondre au nom d'hôte

Pour la Production :

```
https: [
  port: 8443,
  cipher_suite: :strong,
  certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss.crt"),
  keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss.key"),
  cacertfile: System.get_env("TLS_CA_FILE", "/etc/ssl/certs/ca-bundle.crt")
]
```

Flux de Travail de Configuration

Configuration de Déploiement Initial

Liste de Vérification de Configuration

Configuration Essentielle

- ☐ Connexion à la base de données (nom d'hôte, identifiants)
- ☐ PLMN domestique (MCC, MNC)
- ☐ Hôte et royaume Diameter
- ☐ IP d'écoute et port Diameter
- ☐ Certificats TLS pour l'API et le Panneau de Contrôle

Intégration des Éléments Réseau

- ☐ Pairs Diameter configurés (si utilisant le mode connect)
- ☐ Règles de pare-feu autorisant le trafic Diameter (port 3868)
- ☐ Règles de pare-feu autorisant le trafic HTTPS (ports 7443, 8443)
- ☐ Résolution DNS pour les identités Diameter

Configuration IMS (si utilisant des fonctionnalités IMS)

- ☐ Liste des pairs S-CSCF configurée
- ☐ Méthode de sélection S-CSCF choisie
- ☐ Royaume IMS configuré

Configuration Optionnelle

- ☐ Comportement EIR configuré
- ☐ Taille du pool de base de données réglée
- ☐ Liaison d'interface réseau restreinte

Vérification de la Configuration

Après avoir modifié la configuration :

1. **Vérification de la Syntaxe :**

   ```
   Vérifiez les journaux pour les erreurs de chargement de configuration
   ```

2. **Accès au Panneau de Contrôle :**

   ```
   Accédez à https://[hostname]:7443
   Vérifiez que la page d'aperçu se charge
   ```

3. **Accès à l'API :**

   ```
   curl -k https://[hostname]:8443/api/status
   ```

4. **Statut Diameter :**

   ```
   Vérifiez la page Diameter du Panneau de Contrôle
   Vérifiez les connexions des pairs
   ```

5. **Connectivité à la Base de Données :**

   ```
   Vérifiez le Panneau de Contrôle pour les données des abonnés
   Ou connectez-vous directement à la base de données SQL
   ```

Exemple Complet de Configuration à l'Exécution

```
# config/runtime.exs - Exemple complet de production

import Config

#
==============================================================================
# CONFIGURATION DE LA BASE DE DONNÉES
#
==============================================================================
config :hss, Hss.Repo,
  username: System.fetch_env!("DATABASE_USERNAME"),
  password: System.fetch_env!("DATABASE_PASSWORD"),
  hostname: System.get_env("DATABASE_HOSTNAME", "db.omnihss.internal"),
  database: System.get_env("DATABASE_NAME", "omnihss"),
  port: String.to_integer(System.get_env("DATABASE_PORT", "3306")),
  pool_size: String.to_integer(System.get_env("DATABASE_POOL_SIZE", "30")),
  timeout: 15_000,
  connect_timeout: 15_000,
  ssl: true,
  ssl_opts: [
    cacertfile: "/etc/ssl/certs/mysql-ca.pem",
    verify: :verify_peer
```

```
  ]

#
# ============================================================================
# CONFIGURATION DU PLMN DOMESTIQUE
#
# ============================================================================
config :hss, :home_plmn, %{
  mcc: System.get_env("HOME_PLMN_MCC", "001"),
  mnc: System.get_env("HOME_PLMN_MNC", "001")
}

#
# ============================================================================
# CONFIGURATION DE DIAMETER
#
# ============================================================================
diameter_config = %{
  service_name: :omnitouch_hss,
  listen_ip: System.get_env("DIAMETER_LISTEN_IP", "10.7.25.186"),
  listen_port: String.to_integer(System.get_env("DIAMETER_LISTEN_PORT",
"3868")),
  host: System.get_env("DIAMETER_HOST", "omnihss01"),
  realm: System.get_env("DIAMETER_REALM",
"epc.mnc001.mcc001.3gppnetwork.org"),
  product_name: "OmniHSS",
  vendor_id: 10415,
  supported_vendor_ids: [5535, 10415],
  request_timeout: 5000,
  peers: [
    %{
      host: "mme01.epc.mnc001.mcc001.3gppnetwork.org",
      realm: "epc.mnc001.mcc001.3gppnetwork.org",
      ip: "10.7.25.100",
      port: 3868,
      transport: :sctp,
      applications: [:s6a]
    }
  ]
}

config :hss, :diameter, diameter_config

#
# ============================================================================
# CONFIGURATION IMS
#
# ============================================================================
config :hss, :ims, %{
  scscf: %{
    selection_method: :random_peer,
    peers: [
      %{host: "sip:scscf01.ims.mnc001.mcc001.3gppnetwork.org:5060"},
```

```
      %{host: "sip:scscf02.ims.mnc001.mcc001.3gppnetwork.org:5060"}
    ]
  }
}

#
================================================================================
# CONFIGURATION EIR
#
================================================================================
config :hss, :eir, %{
  unknown_equipment_behaviour: :whitelist
}

#
================================================================================
# CONFIGURATION DU POINT DE TERMINAISON DE L'API
#
================================================================================
config :hss, HssWeb.Api.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 8443],
  https: [
    port: 8443,
    cipher_suite: :strong,
    certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss.crt"),
    keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss.key")
  ],
  url: [host: System.get_env("API_HOST", "api.omnihss.internal"), port:
8443]

#
================================================================================
# CONFIGURATION DU POINT DE TERMINAISON DU PANNEAU DE CONTRÔLE
#
================================================================================
config :hss, HssWeb.ControlPanel.Endpoint,
  http: [ip: {0, 0, 0, 0}, port: 7443],
  https: [
    port: 7443,
    cipher_suite: :strong,
    certfile: System.get_env("TLS_CERT_FILE", "/etc/ssl/certs/omnihss.crt"),
    keyfile: System.get_env("TLS_KEY_FILE", "/etc/ssl/private/omnihss.key")
  ],
  url: [host: System.get_env("CP_HOST", "hss.omnihss.internal"), port: 7443]
```

← Retour au Guide des Opérations | Suivant : Relations d'Entité →

Guide du Panneau de Contrôle OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu du Panneau de Contrôle

Le Panneau de Contrôle OmniHSS est une interface de surveillance basée sur le web qui fournit une visibilité en temps réel sur l'état du système, l'activité des abonnés et la connectivité Diameter. Construit avec Phoenix LiveView, il se met à jour automatiquement sans nécessiter de rafraîchissements de page.

Caractéristiques Clés

- **Mises à jour en temps réel** - Se rafraîchit automatiquement chaque seconde
- **Surveillance des Abonnés** - Voir les abonnés actifs et leur état actuel
- **État Diameter** - Surveiller les connexions entre pairs en temps réel
- **Ressources Système** - Suivre la performance de l'application
- **Visualiseur de Configuration** - Inspecter la configuration en cours d'exécution

Informations d'Accès

```
URL: https://[hostname]:7443
Protocole: HTTPS uniquement
Port: 7443 (configurable)
Certificat: Configuré dans config/config.exs
```

Accéder au Panneau de Contrôle

Accès Initial

1. Ouvrez un navigateur web
2. Naviguez vers `https://[hostname]:7443`
3. Acceptez le certificat TLS (s'il est auto-signé)
4. Vous serez présenté avec la page d'Aperçu par défaut

Avertissements de Certificat TLS

Si vous utilisez des certificats auto-signés, les navigateurs afficheront des avertissements de sécurité. Cela est attendu pour les déploiements internes.

Pour la Production : Utilisez des certificats signés par une Autorité de Certification de confiance.

Exigences Réseau

- **Le port 7443** doit être accessible depuis votre réseau de gestion
- **HTTPS** est obligatoire - HTTP n'est pas pris en charge
- **Les règles de pare-feu** doivent autoriser le trafic vers le port 7443

Compatibilité des Navigateurs

Le Panneau de Contrôle utilise des technologies web modernes (LiveView, WebSockets) :

- Chrome/Chromium (recommandé)
- Firefox
- Safari
- Edge

Remarque : Internet Explorer n'est pas pris en charge.

Page d'Aperçu

URL : `https://[hostname]:7443/overview`

La page d'Aperçu affiche tous les abonnés et leurs informations d'état en temps réel.

Mise en Page de la Page

Colonnes de la Table

Colonne	Description	Valeurs
ID	ID de la base de données des abonnés	Entier
Enabled	État du service	✓ (activé) / ✗ (désactivé)
IMSI	Identité Internationale d'Abonné Mobile	14-15 chiffres
ICCID	ID de la carte SIM	19-20 chiffres ou "N/A"
EPC Profile	Nom du profil de service de données	Nom ou ID de profil
IMS Profile	Nom du profil de service vocal	Nom de profil, ID, ou "N/A"
Roaming Profile	Nom de la politique d'itinérance	Nom de profil, ID, ou "N/A"

Détails des Lignes Dépliables

Cliquez sur n'importe quelle ligne pour déplier et voir l'état détaillé de l'abonné :

Informations de Localisation

Champs :

- **MCC** - Code Pays Mobile (3 chiffres)
- **MNC** - Code Réseau Mobile (2-3 chiffres)
- **TAC** - Code de Zone de Suivi
- **Cell ID** - Identifiant de la cellule de service
- **eNodeB ID** - Identifiant de la station de base
- **ECI** - Identifiant de Cellule E-UTRAN

Informations Réseau

Champs :

- **Dernière Vue MME** - Nom d'hôte MME de service actuel
- **Dernier Domaine Vu** - Domaine Diameter de MME
- **Type RAT** - Technologie d'Accès Radio (par exemple, "E-UTRAN" pour LTE)
- **Dernière Vue À** - Horodatage du dernier message Diameter

Informations IMS

Champs :

- **S-CSCF Assigné** - URI SIP S-CSCF actuellement assigné
- **Identité Publique IMS** - URI SIP (par exemple,

sip:+14155551234@ims.example.com)
- **Dernière Vue P-CSCF** - Dernier P-CSCF qui a contacté HSS
- **Dernière Vue I-CSCF** - Dernier I-CSCF qui a contacté HSS

Informations de Session

Champs :

- **Sessions PDN** - Nombre de connexions de données actives
- **Appels Actifs** - Nombre d'appels VoLTE actifs

Indicateurs d'État

Comment identifier l'état :

- **Idle :** Pas d'informations de localisation, pas de MME
- **Attached :** Dernière Vue MME présente, informations de localisation disponibles
- **PDN Active :** Nombre de sessions PDN > 0
- **IMS Registered :** S-CSCF assigné présent
- **In Call :** Nombre d'appels actifs > 0

Auto-Rafraîchissement

La page d'Aperçu se rafraîchit automatiquement **toutes les 1 seconde** pour afficher des mises à jour en temps réel.

Indicateurs visuels :

- De nouvelles données apparaissent sans rechargement de page
- Les horodatages se mettent à jour en temps réel
- Aucun rafraîchissement manuel nécessaire

Cas d'Utilisation

1. **Surveiller les Abonnés Actifs**
    - Voir quels abonnés sont actuellement attachés
    - Vérifier le réseau de service actuel (pour l'itinérance)
    - Vérifier l'état d'enregistrement IMS
2. **Dépannage**
    - Vérifier si l'abonné est activé
    - Vérifier l'horodatage de la dernière vue (l'abonné est-il réactif ?)
    - Confirmer les affectations de profil
    - Voir les informations de localisation actuelles

3. **Surveillance de Capacité**
    - Compter le nombre total d'abonnés attachés
    - Surveiller le nombre de sessions PDN
    - Suivre les appels VoLTE actifs

Page Diameter

URL : `https://[hostname]:7443/diameter`

La page Diameter montre l'état en temps réel de toutes les connexions entre pairs Diameter.

Mise en Page de la Page

Colonnes de la Table

Colonne	Description	Valeurs
Hostname	Nom d'hôte du pair Diameter	FQDN
Realm	Domaine Diameter	Nom de domaine
IP:Port	Adresse réseau	Adresse IP et port
Transport	Protocole de transport	TCP ou SCTP
Status	État de la connexion	Connecté / Déconnecté

État de Connexion

Détails des Lignes Dépliables

Cliquez sur n'importe quel pair pour voir des informations supplémentaires :

Informations de Connexion :

- **Type de Connexion** - Initiée par HSS ou pair
- **Nom du Produit** - Identification du produit du pair
- **IDs d'Application** - Applications Diameter prises en charge

Exemples d'ID d'Application :

- 16777251 - S6a (MME)
- 16777238 - Gx (P-GW)
- 16777216 - Cx (I-CSCF, S-CSCF)
- 16777217 - Sh (Serveur d'Application)
- 16777236 - Rx (P-CSCF)
- 16777252 - S13 (client EIR, si externe)

Flux de Connexion entre Pairs

Auto-Rafraîchissement

La page Diameter se rafraîchit automatiquement **toutes les 1 seconde**.

Cas d'Utilisation

1. **Vérifier la Connectivité**
    - Assurez-vous que tous les pairs attendus sont connectés
    - Identifiez immédiatement les pairs déconnectés
    - Surveillez les connexions instables
2. **Dépannage**
    - Vérifiez si le pair est accessible
    - Vérifiez le protocole de transport (TCP vs SCTP)
    - Confirmez que les IDs d'application correspondent aux attentes
    - Identifiez quel côté a initié la connexion
3. **Planification de Capacité**
    - Comptez le nombre total de pairs connectés
    - Surveillez la stabilité des connexions
    - Planifiez une capacité supplémentaire pour les pairs

Problèmes Courants

Le Pair Montre Déconnecté

Causes Possibles :

1. Problème de connectivité réseau
2. Le pair est hors service ou redémarre
3. Pare-feu bloquant le trafic
4. Incompatibilité de configuration Diameter
5. Problème de certificat (si TLS est utilisé)

Étapes de Dépannage :

1. Vérifiez la connectivité réseau : `ping [peer-ip]`
2. Vérifiez si le port est accessible : `telnet [peer-ip] 3868`
3. Vérifiez les règles de pare-feu
4. Consultez les journaux HSS pour les messages d'erreur
5. Vérifiez que la configuration Diameter du pair correspond à celle de HSS

Le Pair Se Connecte et Se Déconnecte Répétitivement

Causes Possibles :

1. Instabilité du réseau
2. Incompatibilité de délai de garde
3. Problèmes de ressources du pair
4. Incompatibilité d'application Diameter

Étapes de Dépannage :

1. Vérifiez la stabilité du réseau
2. Consultez les temporisateurs de garde des deux côtés
3. Vérifiez les ressources système du pair
4. Vérifiez que les IDs d'application correspondent des deux côtés

---

Page Application

URL : `https://[hostname]:7443/application`

La page Application fournit des informations de surveillance au niveau du système et d'utilisation des ressources.

Caractéristiques

- **Informations sur le Processus** - Nombre de processus Erlang VM et mémoire
- **Mémoire Système** - Mémoire totale et utilisée
- **Temps de Fonctionnement de l'Application** - Durée de fonctionnement d'OmniHSS
- **Version de la VM Erlang** - Informations sur la version d'exécution

Métriques Clés

Cas d'Utilisation

1. **Surveillance de la Santé**
    - Vérifiez que l'application fonctionne
    - Vérifiez les fuites de mémoire (augmentation de la mémoire au fil du temps)
    - Surveillez la croissance du nombre de processus
2. **Planification de Capacité**
    - Suivez les tendances d'utilisation de la mémoire

    - Planifiez une extension en fonction du nombre de processus
    - Vérifiez que les ressources système sont adéquates

3. **Dépannage**

    - Identifiez l'épuisement des ressources
    - Vérifiez si un redémarrage est nécessaire
    - Vérifiez la version de la VM Erlang

Page de Configuration

URL : `https://[hostname]:7443/configuration`

La page de Configuration affiche la configuration actuelle en cours d'exécution d'OmniHSS.

Caractéristiques

- **Voir la Configuration** - Inspecter tous les paramètres de configuration
- **Rechercher la Configuration** - Trouver des paramètres spécifiques
- **Variables d'Environnement** - Voir les valeurs résolues

Catégories de Configuration

Cas d'Utilisation

1. **Vérification de la Configuration**

    - Vérifiez que les paramètres runtime.exs sont appliqués
    - Confirmez les paramètres de connexion à la base de données
    - Vérifiez la configuration des pairs Diameter

2. **Dépannage**

    - Identifiez les erreurs de configuration
    - Vérifiez que les variables d'environnement sont correctement définies
    - Comparez la configuration attendue et réelle

3. **Documentation**

    - Exportez la configuration actuelle pour la documentation
    - Partagez la configuration avec l'équipe de support

Remarque de Sécurité : La page de configuration peut afficher des informations sensibles (mots de passe de base de données, clés). Restreignez l'accès de

manière appropriée.

Navigation et Interface

Barre de Navigation Supérieure

La navigation est toujours visible en haut de la page pour un accès rapide.

Raccourcis Clavier

Bien que le Panneau de Contrôle n'implémente pas de raccourcis clavier personnalisés, les raccourcis standard du navigateur fonctionnent :

- **Ctrl+R / F5** - Rafraîchissement manuel de la page (bien que l'auto-rafraîchissement rende cela inutile)
- **Ctrl+F** - Rechercher sur la page
- **Ctrl+T** - Ouvrir un nouvel onglet (pour plusieurs pages)

Surveillance Multi-Onglets

Vous pouvez ouvrir plusieurs pages du Panneau de Contrôle dans des onglets de navigateur séparés pour une surveillance simultanée :

Configuration d'Exemple :

- Onglet 1 : Page d'Aperçu (surveiller les abonnés)
- Onglet 2 : Page Diameter (surveiller la connectivité)
- Onglet 3 : Page Application (surveiller les ressources)

Tous les onglets se mettront à jour indépendamment.

Design Réactif

Le Panneau de Contrôle est optimisé pour les navigateurs de bureau. Les navigateurs mobiles sont pris en charge mais peuvent nécessiter un défilement horizontal pour les tables.

Résolution Recommandée : 1920x1080 ou plus pour un affichage confortable.

Meilleures Pratiques de Surveillance

Opérations Quotidiennes

1. **Début de Shift**

- Ouvrez la page d'Aperçu du Panneau de Contrôle
- Vérifiez que le nombre d'abonnés attendus est attaché
- Vérifiez la page Diameter - tous les pairs connectés

2. **Pendant le Shift**

   - Gardez la page d'Aperçu ouverte pour une surveillance en temps réel
   - Surveillez les changements d'état inhabituels
   - Surveillez les pairs déconnectés sur la page Diameter

3. **Fin de Shift**

   - Vérifiez que le système est stable
   - Vérifiez la page Application pour les tendances d'utilisation des ressources
   - Documentez toute anomalie

Flux de Travail de Dépannage

Seuils d'Alerte

Établissez des seuils de surveillance pour des alertes proactives :

Métrique	Avertissement	Critique
Pairs Diameter Déconnectés	1 pair	2+ pairs ou pair critique
Utilisation de la Mémoire	> 80%	> 90%
Échecs d'Authentification des Abonnés	> 5%	> 10%
Nombre de Processus	> 80% de la limite	> 95% de la limite

← Retour au Guide des Opérations | Suivant : Métriques & Surveillance →

Relations d'Entités OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu des Entités

OmniHSS organise les données des abonnés en entités logiques avec des relations claires. Comprendre ces entités est crucial pour des tâches opérationnelles telles que le provisionnement, le dépannage et la planification de capacité.

Catégories d'Entités

Entités Principales

Abonné

L'**Abonné** est l'entité centrale représentant un utilisateur mobile.

Champs :

Champ	Type	Description	Contraintes
`id`	bigint	Clé primaire	Auto-incrément
`enabled`	boolean	Indicateur de service activé	Par défaut : true
`ims_enabled`	boolean	Services IMS activés	Par défaut : true
`imsi`	string	Identité Internationale de l'Abonné Mobile	14-15 chiffres, unique
`custom_attributes`	map	Données personnalisées clé-valeur	Optionnel

Champ	Type	Description	Contraintes
sim_id	bigint	Clé étrangère vers SIM	Optionnel
key_set_id	bigint	Clé étrangère vers Ensemble de Clés	Requis
epc_profile_id	bigint	Clé étrangère vers Profil EPC	Requis
ims_profile_id	bigint	Clé étrangère vers Profil IMS	Optionnel
roaming_profile_id	bigint	Clé étrangère vers Profil de Roaming	Optionnel
subscriber_state_id	bigint	Clé étrangère vers État de l'Abonné	Auto-créé

Points Clés :

- Chaque abonné doit avoir exactement un IMSI
- L'IMSI doit comporter 14-15 chiffres (pas de lettres ni de caractères spéciaux)
- Un abonné peut avoir plusieurs MSISDN (numéros de téléphone)
- L'état de l'abonné est automatiquement créé lors de la création de l'abonné
- L'indicateur `enabled` contrôle tous les services (données et IMS)
- L'indicateur `ims_enabled` contrôle uniquement les services IMS

SIM

L'entité **SIM** représente une carte SIM physique ou intégrée.

Champs :

Champ	Type	Description	Niveau de Sécurité
iccid	string	Identifiant de la Carte à Circuit Intégré	Public
sim_vendor	string	Fabricant de la SIM	Public
batch_name	string	Lot de fabrication	Public
is_esim	boolean	Indicateur de SIM intégrée	Public
pin1, pin2	string	Codes PIN	Sensible
puk1, puk2	string	Codes PUK	Sensible
adm1 - adm10	string	Codes administratifs	Très Sensible
kic, kid	binary	Clés de sécurité OTA	Très Sensible

Points Clés :

- L'ICCID identifie de manière unique la carte SIM
- Une SIM peut être assignée à un seul abonné à la fois
- Les codes PIN/PUK sont destinés au verrouillage de la SIM par l'utilisateur final
- Les codes ADM sont destinés aux opérations administratives de la SIM
- KIC/KID sont pour les mises à jour OTA (Over-The-Air) de la SIM

Ensemble de Clés

L'**Ensemble de Clés** contient des clés cryptographiques pour l'authentification.

Champs :

Champ	Type	Description	Taille
`ki`	binary	Clé secrète	128 bits (16 octets)
`opc`	binary	Clé de variante opérateur (dérivée)	128 bits
`op`	binary	Clé opérateur (pour dériver OPC)	128 bits
`amf`	binary	Champ de Gestion d'Authentification	16 bits (2 octets)
`sqn`	bigint	Numéro de séquence (anti-replay)	48 bits
`authentication_algorithm`	string	Nom de l'algorithme	Actuellement "milenage"
`ota_counter`	bigint	Compteur d'opération OTA	Entier

Points Clés :

- Plusieurs abonnés peuvent partager le même ensemble de clés
- Ki est le secret maître partagé avec la SIM
- Soit OPC soit OP doit être fourni (OPC peut être dérivé de OP)
- SQN est incrémenté à chaque authentification
- Milenage est actuellement le seul algorithme pris en charge

Algorithme d'Authentification :

MSISDN

Le **MSISDN** représente un numéro de téléphone.

Champs :

Champ	Type	Description	Format
`msisdn`	string	Numéro ISDN de la Station Mobile	1-15 chiffres, format E.164

Points Clés :

- MSISDN est le numéro de téléphone au format international
- Plusieurs MSISDN peuvent être assignés à un seul abonné
- Un MSISDN ne peut pas être partagé entre plusieurs abonnés
- Format : Code pays + Numéro national (par exemple, "14155551234" pour +1 415-555-1234)

Modèle Multi-MSISDN :

Entités de Profil

Profil EPC

Le **Profil EPC** définit les caractéristiques de service de données pour LTE.

Champs :

Champ	Type	Description	Unités
`name`	string	Nom du profil	Texte
`ue_ambr_dl_kbps`	integer	Limite de bande passante de téléchargement	Kbps
`ue_ambr_ul_kbps`	integer	Limite de bande passante d'envoi	Kbps
`network_access_mode`	integer	Restrictions d'accès	Enum
`tracking_area_update_interval_seconds`	integer	Intervalle TAU	Secondes

Modes d'Accès au Réseau :

AMBR (Débit Maximum Agrégé) :

Profil IMS

Le **Profil IMS** définit les caractéristiques des services vocaux/vidéo.

Champs :

Champ	Type	Description	Format
`name`	string	Nom du profil	Texte
`ifc_template`	text	Modèle XML des Critères de Filtrage Initiaux	XML avec variables

Variables du Modèle IFC :

Points Clés :

- IFC (Critères de Filtrage Initiaux) contrôle le routage des appels dans IMS
- Le modèle est rendu lorsque l'abonné s'enregistre
- Les variables sont remplacées par les données réelles de l'abonné
- Envoyé au S-CSCF lors de l'enregistrement IMS

Profil APN

Le **Profil APN** définit les caractéristiques d'un point d'accès de données spécifique.

Entités Associées :

Identifiant APN

Champ	Type	Description	Exemple
`apn`	string	Nom de l'APN	"internet", "ims", "mms"
`ip_version`	integer	Support du protocole IP	Voir ci-dessous

Options de Version IP :

Profil QoS APN

Paramètres QoS :

Paramètre	Description	Plage	Porteur par Défaut
`qci`	Identifiant de Classe QoS	1-9	QCI 9 (Internet)
`allocation_retention_priority`	Priorité ARP	1-15	8 (priorité inférieure)
`apn_ambr_dl_kbps`	Limite de téléchargement APN	0+	Varie
`apn_ambr_ul_kbps`	Limite d'envoi APN	0+	Varie
`pre_emption_capability`	Peut préempter d'autres	true/ false	false
`pre_emption_vulnerability`	Peut être préempté	true/ false	true

Valeurs QCI :

Profil de Roaming

Le **Profil de Roaming** contrôle l'accès lorsque l'abonné visite d'autres réseaux.

Règle de Roaming :

Évaluation des Règles :

Entités d'État

État de l'Abonné

L'**État de l'Abonné** suit le statut en temps réel de l'abonné.

Champs Clés :

Informations de Localisation :

- `last_seen_mcc`, `last_seen_mnc` - Réseau visité
- `last_seen_tac` - Code de Zone de Suivi
- `last_seen_cell_id` - ID de Cellule
- `last_seen_enodeb_id` - ID de eNodeB
- `last_seen_eci` - Identifiant de Cellule E-UTRAN

Éléments Réseau :

- `last_seen_mme` - MME actuel servant l'abonné
- `last_seen_realm` - Domaine Diameter de MME
- `last_seen_rat_type` - Technologie d'Accès Radio (LTE, 5G, etc.)

Informations IMS :

- `assigned_scscf` - S-CSCF actuel servant l'abonné
- `ims_public_identity` - URI SIP (par exemple, sip:+14155551234@ims.example.com)
- `sh_repository_data` - Données de profil IMS personnalisées

Horodatages :

- `last_seen_at` - Dernier message Diameter reçu
- Divers horodatages `last_*_at` pour différentes procédures

Session PDN

La **Session PDN** représente une connexion de données active.

Cycle de Vie de la Session PDN :

Appel LTE

L'**Appel LTE** représente un appel vocal/vidéo VoLTE actif.

Types d'Appels :

Flux d'Appel VoLTE :

Diagrammes de Relations d'Entités

Relations Complètes d'Entités

Relations de Provisionnement

Ce diagramme montre ce qui doit exister avant de créer un abonné :

Relations d'État de Session

Cycle de Vie des Entités

Cycle de Vie du Provisionnement de l'Abonné

Cycle de Vie de la Session

Modèles de Flux de Données

Flux d'Authentification

Flux de Mise à Jour de Localisation

Flux d'Enregistrement IMS

Flux d'Établissement de Session

Modèles d'Optimisation de Requêtes

OmniHSS optimise les requêtes de base de données en préchargeant sélectivement uniquement les associations nécessaires pour chaque opération :

Requête Minimale (Authentification)

Cas d'Utilisation : S6a AIR - Nécessite uniquement des clés cryptographiques et des règles de roaming

Requête Modérée (Mise à Jour de Localisation)

Cas d'Utilisation : S6a ULR - Nécessite des données complètes du profil EPC

Requête Complète (Enregistrement IMS)

Cas d'Utilisation : Cx SAR - Nécessite le profil IMS et tous les numéros de téléphone

---

← Retour au Guide des Opérations | Suivant : Référence API →

Mappage des Données de Réponse Diameter

← Retour à l'Index de Documentation

Ce document fournit des diagrammes mermaid détaillés montrant d'où provient chaque champ dans les réponses du protocole Diameter dans le système OmniHSS.

Table des Matières

Réponse de Mise à Jour de Localisation (S6a ULA)

La Réponse de Mise à Jour de Localisation est envoyée par le HSS au MME lors des procédures d'attachement LTE. Ce diagramme montre le flux de données complet des tables de base de données aux AVP Diameter.

Mappage des Sources de Données

Mappage Détail des Champs

Source de Base de Données	Champ	AVP Diameter	Transformation
subscriber.enabled	`true/false`	Subscriber-Status	`true → 0 (actif)`, `false → 1 (interdit)`
msisdn.msisdn	`'14155551234'`	MSISDN	Premier MSISDN, encodé TBCD
epc_profile.ue_ambr_ul_kbps	`50000`	Max-Requested-Bandwidth-UL	Multiplier par 1000 (kbps → bps)
epc_profile.ue_ambr_dl_kbps	`100000`	Max-Requested-Bandwidth-DL	Multiplier par 1000 (kbps → bps)
epc_profile.network_access_mode	`0`	Network-Access-Mode	Mappage direct
apn_identifier.apn	`'internet'`	Service-Selection	Chaîne directe
apn_identifier.ip_version	`2`	PDN-Type	`0=IPv4, 1=IPv6, 2=IPv4v6,`

Source de Base de Données	Champ	AVP Diameter	Transformation
			`3=IPv4_or_IPv6`
apn_qos_profile.qci	`9`	QoS-Class-Identifier	Valeur directe
apn_qos_profile.allocation_retention_priority	`8`	Priority-Level	Valeur directe
apn_qos_profile.pre_emption_capability	`false`	Pre-emption-Capability	`false → 0`, `true → 1`
apn_qos_profile.pre_emption_vulnerability	`true`	Pre-emption-Vulnerability	`false → 0`, `true → 1`
apn_qos_profile.apn_ambr_ul_kbps	`25000`	APN AMBR UL	Multiplier par 1000 (kbps → bps)
apn_qos_profile.apn_ambr_dl_kbps	`50000`	APN AMBR DL	Multiplier par 1000 (kbps → bps)
static_ip.ipv4_static_ip	`'100.64.1.1'`	Served-Party-IP-Address (IPv4)	Seulement si attribué à l'abonné
static_ip.ipv6_static_ip	`'2606:4700::1111'`	Served-Party-IP-Address (IPv6)	Seulement si attribué à l'abonné

Transformations Clés:

1. **Bande passante AMBR**: La base de données stocke en kbps, Diameter attend en bps (multiplier par 1000)
2. **Encodage de la Version IP**: `0=IPv4, 1=IPv6, 2=IPv4v6, 3=IPv4_or_IPv6`
3. **Statut de l'Abonné**: `enabled: true → 0 (SERVICE_GRANTED)`, `enabled: false → 1 (OPERATOR_DETERMINED_BARRING)`
4. **Identifiant de Contexte**: Numérotation séquentielle (0, 1, 2...) pour chaque APN dans le profil
5. **IP Statique**: Inclus uniquement si attribué via `static_ips` relation plusieurs-à-plusieurs

Validation de la Logique Métier:

- Vérification de Roaming: Correspondre le PLMN visité contre `roaming_profile.roaming_rules`
- Vérification de l'abonné activé: `subscriber.enabled == true`
- Filtrer les APNs: Peut exclure les APNs IMS si la politique de roaming refuse IMS

Réponse d'Information d'Authentification (S6a AIA)

La Réponse d'Information d'Authentification fournit des vecteurs d'authentification pour les abonnés LTE/EPC.

Mappage des Sources de Données

Composants Clés:

1. **Clés Cryptographiques**: Toutes les clés stockées sous forme de chaînes hexadécimales dans

la table `key_set`
2. **Gestion du SQN**: Numéro de séquence incrémenté après chaque génération de vecteur d'authentification (prévention des attaques par rejeu)
3. **Algorithme Milenage**: 3GPP TS 35.206 - génère des vecteurs d'authentification
4. **Dérivation de KASME**: Clé dérivée de CK||IK utilisant KDF par TS 33.401

Fonctionnalités de Sécurité:

- SQN stocké par abonné (pas global)
- Ki/OPc ne quittent jamais le HSS (seules les valeurs dérivées sont transmises)
- AUTN inclut le numéro de séquence (SQN) et AMF pour l'authentification réseau
- L'algorithme Milenage fournit une authentification mutuelle entre l'UE et le réseau

---

Réponse d'Attribution de Serveur (Cx SAA)

La Réponse d'Attribution de Serveur est envoyée par le HSS au S-CSCF lors de l'enregistrement IMS.

Mappage des Sources de Données

Fonctionnalités Clés:

1. **Modèle IFC**: Modèle XML stocké dans `ims_profile.ifc_template`
2. **Substitution Dynamique**: Remplace `{{msisdn}}`, `{{imsi}}`, `{{impu}}` à l'exécution
3. **Attribution S-CSCF**: Stocke le S-CSCF attribué dans `subscriber_state.assigned_scscf`
4. **Identité Publique IMS**: Format: `sip:+{msisdn}@{ims_domain}` ou `tel:+{msisdn}`

Paramètres du Modèle IFC:

- `{{msisdn}}` - Premier MSISDN de l'abonné
- `{{imsi}}` - IMSI de l'abonné
- `{{impu}}` - Identité Publique Utilisateur IMS (à partir de subscriber_state)
- `{{impi}}` - Identité Privée Utilisateur IMS (typiquement IMSI@realm)

Réponse de Contrôle de Crédit (Gx CCA)

La Réponse de Contrôle de Crédit est envoyée par la fonction PCRF au PGW lors de l'établissement du bearer.

Mappage des Sources de Données

Fonctionnalités Clés:

1. **Suivi de Session**: Crée/met à jour l'enregistrement `pdn_session` pour chaque bearer
2. **Application de QoS**: Fournit QCI et limites de bande passante à partir du profil QoS APN
3. **Règles de Facturation**: Retourne les règles de facturation par défaut pour l'intégration de facturation
4. **CC-Request-Type**: Gère INITIAL (1), UPDATE (2), TERMINATION (3)

Gestion de l'État de Session:

- `INITIAL_REQUEST`: Crée un nouvel enregistrement de session PDN
- `UPDATE_REQUEST`: Met à jour la session PDN existante
- `TERMINATION_REQUEST`: Supprime l'enregistrement de session PDN

Réponse de Données Utilisateur (Sh UDA)

La Réponse de Données Utilisateur est envoyée par le HSS au AS (Serveur d'Application) via l'interface Sh.

Mappage des Sources de Données

Fonctionnalités Clés:

1. **Données de Référentiel**: Peut stocker des XML personnalisés dans `subscriber_state.sh_repository_data`
2. **Indication de Service**: Filtre les données par service demandé (par exemple, présence, messagerie)
3. **Identités Publiques**: Retourne toutes les identités publiques IMS pour l'abonné
4. **Référence vs Transparent**: Prend en charge les modes de données de référence et transparent

---

Réponse de Vérification d'Identité ME (S13 ECA)

La Réponse de Vérification d'Identité ME est envoyée par la fonction EIR au MME pour la validation de l'IMEI.

Mappage des Sources de Données

Fonctionnalités Clés:

1. **Correspondance Regex IMEI**: Les règles utilisent des expressions régulières pour une correspondance flexible
2. **Règles Basées sur le TAC**: Peut correspondre au Code d'Attribution de Type (premiers 8 chiffres)
3. **Comportement par Défaut**: Configurable pour les IMEI inconnus (accepter ou rejeter)
4. **Valeurs de Statut de l'Équipement**:
    - `0` = LISTE BLANCHE (explicitement autorisé)
    - `1` = LISTE NOIRE (volé/bloqué)
    - `2` = LISTE GRIS (autorisé mais surveillé)
    - `5` = INCONNU (aucune règle correspondante)

Cas d'Utilisation:

- Bloquer les appareils volés par IMEI exact
- Bloquer les modèles d'appareils par motif TAC
- Liste blanche uniquement des appareils approuvés
- Suivre les appareils du marché gris

Éléments de Réponse Communs

Toutes les réponses Diameter partagent ces AVP communs :

Exemple de Configuration:

```
config :diameter_ex,
  diameter_host: "hss",
  diameter_realm: "example.com",
  diameter_service_name: "OmniHSS"
```

Résumé du Flux de Données

Pipeline de Traitement des Demandes

Optimisation des Requêtes de Base de Données

OmniHSS utilise **préchargement contextuel** pour minimiser les requêtes de base de données :

```
# Exemple : ULR précharge tout ce qui est nécessaire pour les données d'abonnement
def get_subscriber_data(:update_location_request, imsi) do
  from(s in Subscriber, where: s.imsi == ^imsi)
  |> join(:left, [s], epc in assoc(s, :epc_profile))
  |> join(:left, [s, epc], apn in assoc(epc, :apn_profiles))
  |> join(:left, [s, epc, apn], qos in assoc(apn, :apn_qos_profile))
  |> join(:left, [s], msisdn in assoc(s, :msisdns))
  |> join(:left, [s], sip in assoc(s, :static_ips))
  |> preload([s, epc, apn, qos, msisdn, sip], [
    epc_profile: {epc, apn_profiles: {apn, apn_qos_profile: qos}},
    msisdns: msisdn,
    static_ips: sip
  ])
  |> Repo.one()
end

# Résultat : Requête unique avec tous les jointures - pas de problème N+1
```

Notes d'Implémentation

Gestionnaires de Protocole

Le système implémente des gestionnaires pour les protocoles Diameter suivants :

- **S6a** - Interface LTE/MME pour l'authentification et les mises à jour de localisation
- **Cx** - Interface IMS/CSCF pour l'enregistrement IMS et l'attribution de serveur
- **Sh** - Interface IMS/AS pour la récupération des données d'abonné
- **Gx** - Interface PCRF pour le contrôle de politique et de facturation
- **Rx** - Interface IMS/AF pour l'autorisation de médias
- **S13** - Interface EIR pour la validation de l'IMEI
- **SWx** - Interface WiFi/IMS pour l'authentification d'accès non-3GPP

Modèles de Données

Le schéma de base de données comprend les entités centrales suivantes :

- **Abonné** - Enregistrement d'abonné principal avec IMSI
- **Ensemble de Clés** - Clés cryptographiques pour l'authentification
- **Profil EPC** - Configuration de service LTE
- **Profil APN** - Configuration de point d'accès
- **Profil IMS** - Configuration de service IMS avec modèles IFC
- **Profil de Roaming** - Règles et restrictions de roaming
- **État de l'Abonné** - Suivi dynamique de session et d'état
- **Session PDN** - Suivi de session de bearer actif
- **IP Statique** - Attributions d'adresses IP statiques
- **Règle EIR** - Règles de validation IMEI

← Retour à l'Index de Documentation | Référence API → | Flux de Protocole →

Guide de Surveillance et de Métriques d'OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu de la Surveillance

OmniHSS fournit plusieurs mécanismes pour surveiller la santé du système, la performance et l'activité des abonnés. Le personnel des opérations doit utiliser une combinaison de ces outils pour une visibilité complète.

Couches de Surveillance

Surveillance du Panneau de Contrôle

Le Panneau de Contrôle fournit l'interface principale de surveillance en temps réel.

Surveillance de la Page d'Aperçu

URL : `https://[hostname]:7443/overview`

Métriques Clés Disponibles

États des Abonnés Surveillés

État	Indicateur	Ce que Cela Signifie
Inactif	Pas d'informations de localisation	Abonné éteint ou hors couverture
Attaché	MME présent	Abonné enregistré sur le réseau
PDN Actif	Nombre de sessions PDN > 0	Connexion de données active
Enregistré IMS	S-CSCF assigné	Services vocaux prêts
En Appel	Nombre d'appels actifs > 0	Appel VoLTE en cours

Extraction des Métriques de l'Aperçu

Bien que le Panneau de Contrôle n'exporte pas directement les métriques, vous pouvez :

1. **Compter les lignes visibles** pour le total des abonnés
2. **Scanner les coches vertes** pour compter les abonnés activés
3. **Examiner les détails développés** pour les informations d'état
4. **Noter les horodatages de dernière vue** pour la réactivité

Surveillance de la Page Diameter

URL : `https://[hostname]:7443/diameter`

Métriques Clés

Surveillance des Pairs Critiques

Identifiez les pairs critiques et surveillez leur statut :

Type de Pair	Criticité	Impact si Hors Service
MME	Élevée	Pas de nouvelles connexions LTE
P-GW	Élevée	Pas de sessions de données
S-CSCF	Élevée	Pas d'enregistrements IMS
P-CSCF	Élevée	Pas d'appels VoLTE
I-CSCF	Moyenne	Problèmes de routage IMS
AS	Faible-Moyenne	Service spécifique indisponible

Surveillance de la Page Application

URL : `https://[hostname]:7443/application`

Métriques Clés

Métrique	Description	Plage Normale	Seuil d'Action
Nombre de Processus	Processus Erlang actifs	Varie selon la charge	> 90% de la limite
Utilisation de la Mémoire	Mémoire totale consommée	< 80%	> 90%
Temps de Fonctionnement	Temps depuis le dernier redémarrage	N/A	Suivre pour la stabilité

Surveillance de la Base de Données

Requêtes Directes à la Base de Données

Connectez-vous à la Base de Données SQL pour extraire des métriques détaillées :

Comptes d'Abonnés

Interrogez la base de données pour récupérer :

- Nombre total de tous les abonnés
- Nombre d'abonnés activés
- Nombre d'abonnés activés IMS

Statistiques de Session

Interrogez la base de données pour récupérer :

- Nombre de sessions PDN actives
- Nombre d'appels VoLTE actifs
- Répartition des sessions PDN par profil APN

Statistiques de Localisation

Interrogez la base de données pour récupérer :

- Nombre d'abonnés regroupés par réseau visité (combinaison MCC-MNC)
- Nombre d'abonnés actuellement en roaming (pas sur le PLMN domicile 001-001)
- Répartition des abonnés à travers différents réseaux visités

Activité Récente

Interrogez la base de données pour récupérer :

- Nombre d'abonnés vus dans la dernière heure
- Répartition des abonnés par MME de service
- Analyse des horodatages de la dernière activité des abonnés

Surveillance de la Santé de la Base de Données

Surveillez la santé de la base de données en interrogeant :

- Taille totale de la base de données et tendances de croissance
- Tailles des tables individuelles et comptes de lignes
- Nombre actuel de connexions à la base de données
- Performance des requêtes et utilisation des ressources

Surveillance des Journaux

Sortie des Journaux

OmniHSS sort les journaux vers **stdout/stderr**, qui doivent être capturés par votre gestionnaire de processus.

Niveaux de Journaux

Modèles de Journaux Clés à Surveiller

Événements des Pairs Diameter :

```
[info] Pair Diameter connecté : mme01.epc.example.com
[warn] Pair Diameter déconnecté : pgw01.epc.example.com
[error] Échec de connexion au pair Diameter : délai d'attente
```

Événements de Base de Données :

```
[info] Connexion à la base de données établie
[error] Connexion à la base de données perdue : délai d'attente
[error] Échec de la requête de base de donn��es : blocage détecté
```

Événements d'Authentification :

```
[info] Authentification réussie : IMSI 001001123456789
[warn] Échec d'authentification : IMSI 001001123456789, vecteur
invalide
[error] Roaming refusé : IMSI 001001123456789, MCC 310 MNC 410
```

Agrégation des Journaux

Pour les déploiements en production, mettez en œuvre l'agrégation des journaux :

Intégration de la Surveillance Externe

Point de Vérification de Santé

Vérification de Santé de l'API : `GET /api/status`

```
curl -k https://hss.example.com:8443/api/status
```

Réponse Attendue :

```
{"status": "ok"}
```

Statut HTTP : 200 OK

Intégration des Outils de Surveillance

Exemple Nagios/Icinga

```
#!/bin/bash
# check_omnihss.sh

API_URL="https://hss.example.com:8443/api/status"

response=$(curl -k -s -o /dev/null -w "%{http_code}" "$API_URL" --
max-time 5)

if [ "$response" = "200" ]; then
    echo "OK - API OmniHSS répond"
    exit 0
else
    echo "CRITIQUE - API OmniHSS ne répond pas (HTTP $response)"
    exit 2
fi
```

Intégration Prometheus

Des exportateurs personnalisés peuvent être créés pour exporter les métriques d'OmniHSS vers Prometheus en interrogeant l'API et la base de données.

Intégration SNMP

Pour la surveillance basée sur SNMP, des scripts d'extension SNMP personnalisés peuvent interroger la base de données ou l'API pour des métriques et retourner des valeurs via des OID SNMP.

Indicateurs Clés de Performance

KPI Opérationnels

Seuils de KPI Recommandés

KPI	Cible	Avertissement	Critique
Temps de Fonctionnement du Système	99.99%	< 99.95%	< 99.9%
Temps de Fonctionnement des Pairs Diameter	99.9%	< 99.5%	< 99%
Taux de Réussite d'Authentification	> 99%	< 99%	< 95%
Temps de Réponse Diameter	< 100ms	> 200ms	> 500ms
Temps de Requête de Base de Données	< 50ms	> 100ms	> 500ms
Taux d'Erreur	< 0.1%	> 0.5%	> 1%

KPI de Capacité

Métrique	Surveiller	Plan d'Action À
Total des Abonnés	Compte actuel	80% de la capacité attendue
Sessions PDN Concurrentes	Sessions actives	70% du maximum attendu
Taille de la Base de Données	Mo utilisés	80% du stockage alloué
Connexions à la Base de Données	Connexions actives	80% de la taille du pool

Stratégies d'Alerte

Priorités d'Alerte

Définitions des Alertes

Alertes Critiques (P1)

Système Indisponible :

- Échec de la vérification de santé de l'API
- Panneau de contrôle inaccessible
- Échec de connexion à la base de données
- Action : Enquête immédiate et escalade

Tous les Pairs Diameter Déconnectés :

- Zéro pair connecté

- Action : Vérifier le réseau, redémarrer si nécessaire

Base de Données Hors Service :

- Impossible de se connecter à la Base de Données SQL
- Action : Enquêter sur le serveur de base de données, redémarrer si nécessaire

Alertes de Haute Priorité (P2)

Pair Diameter Critique Hors Service :

- MME principal déconnecté
- P-GW principal déconnecté
- S-CSCF principal déconnecté
- Action : Enquêter sur la connectivité des pairs dans les 15 minutes

Utilisation Élevée de la Mémoire :

- Mémoire > 95%
- Action : Enquêter sur une fuite de mémoire, planifier un redémarrage

Taux d'Échec d'Authentification Élevé :

- 10% des requêtes d'authentification échouent

- Action : Vérifier le provisionnement des abonnés, enquêter sur la cause

Alertes de Moyenne Priorité (P3)

Pair Non Critique Hors Service :

- Pair secondaire déconnecté
- Serveur d'application déconnecté
- Action : Enquêter dans l'heure

Utilisation Élevée de la Mémoire :

- Mémoire > 85%
- Action : Surveiller la tendance, planifier une mise à niveau de capacité

Taux d'Erreur Élevé :

- Taux d'erreur > 1%
- Action : Examiner les journaux, identifier la cause profonde

Alertes de Faible Priorité (P4)

Avertissement de Capacité :

- Abonnés > 80% de la capacité
- Base de données > 80% du stockage alloué
- Action : Planifier une expansion de capacité

Dégradation de Performance :

- Temps de réponse élevés mais acceptables
- Action : Surveiller et optimiser les requêtes

Canaux de Notification d'Alerte

Liste de Vérification de Surveillance

Vérifications Quotidiennes

- ☐ Examiner l'Aperçu du Panneau de Contrôle - comptes d'abonnés normaux
- ☐ Examiner la page Diameter - tous les pairs critiques connectés
- ☐ Examiner la page Application - mémoire et processus dans les limites
- ☐ Vérifier les journaux d'erreurs - pas d'erreurs critiques dans les dernières 24 heures
- ☐ Vérifier que la sauvegarde s'est terminée avec succès

Vérifications Hebdomadaires

- ☐ Examiner les tendances de capacité - croissance des abonnés
- ☐ Examiner les tendances de performance - temps de réponse
- ☐ Examiner la taille de la base de données - taux de croissance acceptable
- ☐ Examiner les taux d'erreur - identifier les modèles
- ☐ Tester les notifications d'alerte - s'assurer qu'elles fonctionnent

Vérifications Mensuelles

- ☐ Revue de planification de capacité - projet à 6 mois d'avance
- ☐ Revue d'optimisation de performance - identifier les requêtes lentes
- ☐ Revue de sécurité - expiration des certificats, vulnérabilités
- ☐ Revue de documentation - mettre à jour les runbooks
- ☐ Test de récupération après sinistre - vérifier que les sauvegardes se restaurent correctement

← Retour au Guide des Opérations | Suivant : Multi-Features →

Fonctionnalités Multi-MSISDN et Multi-IMSI d'OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu

OmniHSS prend en charge des capacités de provisionnement avancées qui permettent des configurations de service flexibles :

Support Multi-MSISDN

Un IMSI → Plusieurs Numéros de Téléphone

Un seul abonné (identifié par un IMSI) peut avoir plusieurs MSISDN (numéros de téléphone) assignés. Tous les numéros sonnent sur le même appareil et partagent les mêmes profils de service.

Support SIM Multi-IMSI

Une SIM → Plusieurs IMSIs

Une seule carte SIM physique peut contenir plusieurs IMSIs, permettant à l'appareil de se connecter à différents réseaux en utilisant différentes identités réseau. Cela est utile pour l'itinérance internationale et les scénarios MVNO.

Multi-MSISDN : Plusieurs Numéros de Téléphone

Comment Ça Fonctionne

Un enregistrement d'abonné dans le HSS a plusieurs MSISDN liés via une table de jointure. Lorsque l'abonné s'enregistre à l'IMS, tous les MSISDN sont inclus dans le

profil IMS, permettant aux appels entrants vers n'importe quel numéro d'atteindre l'appareil.

Caractéristiques Clés

- **Un IMSI** - L'abonné a un seul IMSI lié à sa carte SIM
- **Plusieurs MSISDN** - L'abonné peut avoir plusieurs numéros de téléphone
- **Intégration IMS** - Tous les MSISDN sont enregistrés dans l'IMS
- **Service Partagé** - Tous les numéros partagent les mêmes profils de service (EPC, IMS, Itinérance)

Modèle de Données

Important : Un MSISDN ne peut être assigné qu'à UN seul abonné à la fois. Cependant, un abonné peut avoir de NOMBREUX MSISDN.

Cas d'Utilisation

1. Lignes Professionnelles et Personnelles

Un abonné a à la fois des numéros de téléphone professionnels et personnels sur le même appareil :

2. Numéros Internationaux

Un abonné qui voyage fréquemment a des numéros dans plusieurs pays :

3. Forfaits Familiaux

Un parent gère plusieurs numéros de membres de la famille :

Remarque : Dans OmniHSS, cela nécessiterait plusieurs abonnés (un par SIM/IMSI), chacun ayant potentiellement plusieurs MSISDN.

4. Portage de Ligne Héritée

Lorsqu'un abonné change de numéro mais souhaite garder l'ancien numéro actif pendant la transition :

Configuration

Création de MSISDN

Les MSISDN doivent être créés avant d'être assignés aux abonnés.

```
# Créer le premier MSISDN
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{"msisdn": {"msisdn": "14155551001"}}'

# Créer le deuxième MSISDN
```

```
curl -k -X POST https://hss.example.com:8443/api/msisdn \
  -H "Content-Type: application/json" \
  -d '{"msisdn": {"msisdn": "14155551002"}}'
```

Assignation de MSISDN aux Abonnés

L'assignation se fait via la table de jointure dans la base de données.

Méthode de Base de Données :

1. Interroger la base de données pour obtenir l'ID de l'abonné pour l'IMSI cible
2. Interroger la base de données pour obtenir les ID de MSISDN pour les numéros de téléphone
3. Insérer des enregistrements dans la table de jointure liant subscriber_id à chaque msisdn_id

Cela crée la relation plusieurs-à-plusieurs entre l'abonné et ses numéros de téléphone.

Flux de Provisionnement

Vérification de l'Assignation

Interroger la base de données pour récupérer l'abonné avec tous les MSISDN liés en :

- Joignant la table des abonnés avec la table de jointure
- Joignant la table de jointure avec la table msisdn
- Groupant les résultats par abonné pour voir tous les numéros de téléphone ensemble

Cela montrera l'ID de l'abonné, l'IMSI et une liste de tous les MSISDN assignés.

Intégration IMS

Enregistrement IMS

Lorsque l'abonné s'enregistre à l'IMS, **tous les MSISDN assignés sont inclus** dans le profil IMS envoyé au S-CSCF.

Rendu du Modèle IFC

Le modèle IFC IMS peut référencer tous les MSISDN en utilisant la variable `{{msisdns}}`.

Exemple de Modèle IFC :

```
<ServiceProfile>
  <PublicIdentity>

<Identity>sip:{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <!-- Répéter pour chaque MSISDN -->
```

```
  <PublicIdentity>
    <Identity>sip:+14155551001@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551001</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>sip:+14155551002@ims.example.com</Identity>
  </PublicIdentity>
  <PublicIdentity>
    <Identity>tel:+14155551002</Identity>
  </PublicIdentity>
  <!-- ... -->
</ServiceProfile>
```

Variable de Modèle :

- `{{msisdns}}` - Liste de tous les MSISDN assignés à l'abonné

Identités Publiques

Chaque MSISDN donne généralement lieu à deux identités publiques IMS :

Routage des Appels Entrants

Lorsque quelqu'un appelle l'un des numéros de l'abonné, le réseau IMS route vers le bon URI SIP :

Présentation de l'Appel Sortant

Le téléphone peut choisir quel numéro présenter comme ID de l'appelant pour les appels sortants.

Exemple SIP INVITE :

```
INVITE sip:+15105551234@ims.example.com SIP/2.0
From: "+14155551002" <sip:+14155551002@ims.example.com>;tag=123
To: <sip:+15105551234@ims.example.com>
P-Asserted-Identity: <sip:+14155551002@ims.example.com>
```

Les en-têtes `From` et `P-Asserted-Identity` indiquent lequel des numéros de l'abonné est utilisé.

Dépannage Multi-MSISDN

Problème : MSISDN N'apparaît Pas dans l'Enregistrement IMS

Symptômes :

- S-CSCF montre seulement une identité publique
- Les appels au deuxième numéro échouent

Étapes de Dépannage :

1. **Vérifier l'Assignation MSISDN dans la Base de Données :**
    - Interroger la base de données pour récupérer tous les MSISDN liés à l'IMSI de l'abonné
    - Vérifier la table de jointure pour s'assurer que les relations existent
2. **Vérifier le Modèle de Profil IMS :**
    - Vérifier que le modèle inclut la variable `{{msisdns}}`
    - Confirmer que la syntaxe du modèle est un XML valide
3. **Revoir les Journaux HSS :**
    - Rechercher des messages d'enregistrement IMS (Cx SAR)
    - Vérifier que tous les MSISDN sont inclus dans la réponse
4. **Tester l'Enregistrement IMS :**
    - Déclencher une nouvelle inscription sur le téléphone
    - Vérifier les journaux S-CSCF pour les identités publiques enregistrées

Problème : Impossible d'Assigner un MSISDN à un Abonné

Symptômes :

- L'insertion dans la base de données échoue
- Erreur : "Entrée dupliquée" ou "Contrainte de clé étrangère"

Causes Possibles :

1. **MSISDN Déjà Assigné :**
    - Interroger la base de données pour vérifier si le MSISDN est déjà lié à un autre abonné
    - **Solution :** Supprimer d'abord l'assignation existante, puis créer la nouvelle assignation
2. **MSISDN N'existe Pas :**
    - Interroger la base de données pour vérifier que l'enregistrement MSISDN existe
    - **Solution :** Créer d'abord l'enregistrement MSISDN via l'API ou l'insertion dans la base de données

Problème : Les Appels à Un Numéro Fonctionnent, L'Autre Ne Fonctionne Pas

Symptômes :

- Les appels au numéro principal fonctionnent
- Les appels au numéro secondaire échouent ou sont mal routés

Étapes de Dépannage :

1. **Vérifier les Deux Numéros dans l'Enregistrement IMS :**
    - Vérifier les identités publiques enregistrées par S-CSCF
    - Confirmer que les deux URI SIP sont présents
2. **Vérifier les Règles de Routage IMS :**
    - Vérifier que les règles de routage du modèle IFC s'appliquent à toutes les identités
    - Vérifier si un numéro spécifique nécessite un routage spécial
3. **Tester les Deux Numéros :**

```
# Tester depuis un client SIP
sip:+14155551001@ims.example.com  # Devrait fonctionner
sip:+14155551002@ims.example.com  # Devrait également fonctionner
```

Problème : La Recherche API par MSISDN Renvoie le Mauvais Abonné

Symptômes :

- La requête API `/api/subscriber/msisdn/:msisdn` renvoie un abonné inattendu

Vérification :

Interroger la base de données pour trouver quel abonné le MSISDN est assigné. Cela devrait renvoyer exactement un abonné. S'il renvoie plusieurs ou le mauvais abonné, la table de jointure a des données incorrectes qui doivent être corrigées.

Meilleures Pratiques

Ordre de Provisionnement

1. Créer tous les MSISDN d'abord
2. Créer l'abonné
3. Assigner les MSISDN à l'abonné
4. Vérifier l'assignation avant l'activation

Gestion des MSISDN

- **Documenter les numéros principaux vs secondaires** dans les custom_attributes de l'abonné
- **Porter les numéros séquentiellement** lors du portage pour éviter les interruptions de service
- **Tester tous les numéros** après le provisionnement avant de les donner au client

Configuration IMS

- S'assurer que le modèle IFC gère correctement plusieurs identités publiques

- Tester le routage entrant vers tous les numéros
- Vérifier la présentation de l'ID de l'appelant pour les appels sortants

Migration

Lors de la migration d'un MSISDN unique à multi-MSISDN :

Support SIM Multi-IMSI : Plusieurs Identités Réseau

Comment Ça Fonctionne

Une SIM multi-IMSI contient plusieurs profils d'abonné complets, chacun avec son propre IMSI, clés et identifiants. L'appareil peut basculer entre les IMSIs pour se connecter à différents réseaux, souvent automatiquement en fonction de la localisation ou de la disponibilité du réseau.

Important : Un **seul IMSI peut être actif à tout moment**. Lorsqu'un appareil passe à un IMSI différent sur la même carte SIM, le HSS désenregistre automatiquement l'IMSI précédemment actif.

Mise en Œuvre d'OmniHSS

Dans OmniHSS, chaque IMSI sur une SIM multi-IMSI est provisionné comme un **enregistrement d'abonné séparé**, mais tous font référence à la **même carte SIM** :

Cas d'Utilisation

1. Optimisation de l'Itinérance Internationale

- IMSI d'origine : 001-001 (tarifs du réseau d'origine)
- IMSI d'itinérance US : 310-410 (tarifs locaux US)
- IMSI d'itinérance EU : 234-015 (tarifs locaux EU)
- L'appareil change d'IMSI en fonction de la localisation

2. Service MVNO

- IMSI principal : réseau MVNO (revendeur)
- IMSI de secours : réseau hôte (opérateur parent)
- Basculement automatique si la couverture MVNO n'est pas disponible

3. IoT/M2M Multi-Réseau

- IMSI 1 : opérateur principal
- IMSI 2 : opérateur de secours pour redondance
- IMSI 3 : secours d'urgence/coût faible
- Les dispositifs critiques maintiennent la connectivité

4. Conformité Réglementaire

- Différents IMSIs pour différentes zones réglementaires

- Se conformer aux exigences locales de résidence des données
- Utiliser une identité réseau locale par juridiction

Fonctionnalités Multi-IMSI

Authentification Indépendante

- Chaque IMSI a son propre Ki, OPC et ensemble de clés
- Vecteurs d'authentification séparés par IMSI
- Différents identifiants de sécurité par réseau

Profils de Service Séparés

- Différents profils EPC (bande passante, APNs)
- Différents profils IMS (services vocaux)
- Différentes règles d'itinérance par IMSI

Identité Physique Partagée

- Tous les IMSIs font référence à la même SIM (via sim_id)
- Même ICCID à travers tous les enregistrements d'abonné
- Regroupement logique via la carte SIM

Sélection de Réseau

- L'appareil ou la carte SIM décide quel IMSI utiliser
- Basé sur les réseaux disponibles, la localisation, la politique
- Le HSS authentifie quel que soit l'IMSI que l'appareil présente

Configuration

```
# 1. Créer la carte SIM (capable multi-IMSI)
SIM_ID=$(curl -k -X POST https://hss.example.com:8443/api/sim \
  -d '{"sim": {"iccid": "89911012000003204510", "is_esim": false}}' \
  | jq -r '.data.id')

# 2. Créer l'ensemble de clés pour l'IMSI 1 (réseau d'origine)
KEYSET1=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
  -d '{"key_set": {"ki": "0123456789ABCDEF...", "opc": "FEDCBA9876..."}}' \
  | jq -r '.data.id')

# 3. Créer l'abonné 1 (IMSI d'origine)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d "{\"subscriber\": {
    \"imsi\": \"001001111111111\",
    \"sim_id\": $SIM_ID,
    \"key_set_id\": $KEYSET1,
    \"epc_profile_id\": 1
  }}"

# 4. Créer l'ensemble de clés pour l'IMSI 2 (partenaire d'itinérance)
KEYSET2=$(curl -k -X POST https://hss.example.com:8443/api/key_set \
```

```
  -d '{"key_set": {"ki": "1111111111111111...", "opc": "2222222222..."}}' \
  | jq -r '.data.id')

# 5. Créer l'abonné 2 (IMSI d'itinérance)
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -d "{\"subscriber\": {
    \"imsi\": \"310410222222222\",
    \"sim_id\": $SIM_ID,
    \"key_set_id\": $KEYSET2,
    \"epc_profile_id\": 2
  }}"

# 6. Répéter pour d'autres IMSIs sur la SIM...
```

Flux d'Authentification

Lorsqu'un dispositif multi-IMSI se connecte :

Le HSS n'a pas besoin de savoir qu'il s'agit d'une SIM multi-IMSI—il authentifie simplement quel que soit l'IMSI que l'appareil présente.

Changement d'IMSI et Désenregistrement Automatique

Lorsqu'une SIM multi-IMSI passe d'un IMSI à un autre, un seul IMSI peut être enregistré à la fois sur le réseau. OmniHSS gère cela automatiquement en envoyant une **Demande d'Annulation de Localisation (CLR)** pour désenregistrer l'IMSI précédemment actif lorsqu'un nouvel IMSI de la même carte SIM s'enregistre.

Règle de l'IMSI Actif Unique

Concept Clé : Un seul abonné (IMSI) par carte SIM peut être actif à tout moment.

- Si un abonné est enregistré sur un MME en utilisant **IMSI X**
- Et que le HSS reçoit une Demande de Mise à Jour de Localisation pour **IMSI Y** (sur la même SIM que l'IMSI X)
- Le HSS envoie automatiquement une **Demande d'Annulation de Localisation** pour désenregistrer **IMSI X**

Cela garantit un passage propre entre les IMSIs et empêche les conflits dans le réseau.

Flux de Changement d'IMSI

Pourquoi Cela Est Important

Intégrité du Réseau :

- Empêche les enregistrements dupliqués de la même SIM physique
- Assure que les ressources réseau sont correctement libérées
- Maintient des données de localisation d'abonné précises

Exactitude de la Facturation :

- Un seul IMSI est facturé pour l'accès au réseau à la fois
- Limites de session claires entre les changements d'IMSI
- Génération précise de CDR (Call Detail Record)

Gestion des Ressources :

- Les ressources MME pour l'ancien IMSI sont libérées
- Les contextes PDP et les porteurs sont nettoyés
- Le suivi de localisation reste précis

Déclencheurs de Changement d'IMSI

Le dispositif/SIM décide quand changer d'IMSI en fonction de :

1. **Disponibilité du Réseau**
    - Réseau d'origine IMSI non disponible
    - Passer à l'IMSI du partenaire d'itinérance
2. **Sélection Manuelle**
    - L'utilisateur sélectionne manuellement le réseau
    - La SIM passe à l'IMSI correspondant
3. **Basé sur la Politique**
    - La carte SIM a des règles internes (par exemple, préférer l'IMSI local dans certains pays)
    - Changement automatique basé sur MCC/MNC
4. **Optimisation des Coûts**
    - Passer à l'IMSI avec des tarifs d'itinérance plus bas
    - Utiliser l'IMSI local pour éviter les frais d'itinérance

Considérations IMS

Le même comportement de Demande d'Annulation de Localisation s'applique à l'enregistrement IMS :

Impact Opérationnel

Pour le Personnel Opérationnel :

1. **L'abonné apparaît hors ligne :** Lorsque l'IMSI change, l'ancien IMSI apparaîtra comme "désenregistré" dans le HSS. C'est un comportement normal.
2. **Deux enregistrements d'abonné pour une seule SIM :** Les SIM multi-IMSI auront plusieurs enregistrements d'abonné partageant le même `sim_id`. Un seul sera dans l'état "enregistré" à la fois.
3. **Suivi de localisation :** La table `subscriber_state` suit avec quel MME/SGSN

chaque IMSI est enregistré. Lorsque l'IMSI change, l'ancienne localisation est effacée.

4. **Dépannage :** Si un dispositif ne peut pas être atteint :
    - Vérifier quel IMSI est actuellement enregistré
    - Vérifier que le bon IMSI est utilisé pour le réseau actuel
    - Confirmer qu'un seul IMSI par SIM est dans l'état enregistré

Scénarios Combinés

Multi-IMSI + Multi-MSISDN

Vous pouvez combiner les deux fonctionnalités : plusieurs IMSIs sur une SIM, chacune avec plusieurs MSISDNs.

Exemple de Cas d'Utilisation :

- **Réseau d'origine (IMSI 1) :**
    - Numéro personnel : +1-415-555-1001
    - Numéro professionnel : +1-415-555-1002
- **Réseau d'itinérance US (IMSI 2) :**
    - Numéro personnel : +1-212-555-2001
    - Numéro professionnel : +1-212-555-2002

Lorsque l'appareil est dans le territoire d'origine, il utilise l'IMSI 1 avec ses MSISDNs. Lorsqu'il est en itinérance aux États-Unis, il passe à l'IMSI 2 avec différents MSISDNs optimisés pour le réseau américain.

Procédures Opérationnelles

Gestion des Abonnés Multi-MSISDN

Voir tous les MSISDNs pour un abonné :

```
Interroger via API : GET /api/subscriber/imsi/:imsi
```

La réponse inclut tous les MSISDNs liés.

Dépannage Multi-IMSI

Dispositif ne s'attachant pas avec le deuxième IMSI :

1. Vérifier que l'enregistrement d'abonné secondaire existe pour cet IMSI
2. Vérifier que l'ensemble de clés est configuré correctement pour cet IMSI

3. Vérifier que le profil EPC est assigné
4. Confirmer que les règles d'itinérance permettent l'attachement

Dispositif changeant d'IMSI de manière inattendue :

- Cela est contrôlé par la logique de l'appareil/SIM, pas par le HSS
- Le HSS authentifie quel que soit l'IMSI présenté
- Vérifier les paramètres de sélection d'IMSI de l'appareil

Dépannage Multi-MSISDN

Deuxième numéro ne sonne pas :

1. Vérifier que le MSISDN est lié dans la table de jointure
2. Vérifier que le modèle de profil IMS inclut la variable `{{msisdns}}`
3. Confirmer que l'enregistrement IMS inclut toutes les identités publiques
4. Revoir les journaux S-CSCF pour les identités enregistrées

Les appels sortants n'affichent qu'un seul numéro :

- L'appareil sélectionne quel numéro présenter comme ID de l'appelant
- Cela est une configuration de l'appareil, pas du HSS
- Le HSS fournit toutes les identités ; l'appareil choisit

Résumé des Avantages

Avantages Multi-MSISDN

✓ Une SIM, plusieurs numéros de téléphone
✓ Lignes professionnelles et personnelles séparées
✓ Présence locale internationale
✓ Gestion simplifiée des dispositifs
✓ Tous les numéros partagent le même service de données
✓ Facturation centralisée par IMSI

Avantages SIM Multi-IMSI

✓ Coûts d'itinérance optimisés
✓ Sélection automatique du réseau
✓ Redondance et basculement
✓ Identité réseau locale
✓ Conformité réglementaire
✓ Continuité de service à travers les réseaux

Avantages Combinés

✓ Flexibilité maximale
✓ Différents ensembles de numéros par réseau
✓ Optimisé pour chaque cas d'utilisation
✓ Scénarios commerciaux complexes

✓ Optimisation internationale et locale

← Retour au Guide des Opérations

Gestion des Profils OmniHSS

← Retour au Guide des Opérations

Vue d'ensemble

OmniHSS utilise des **profils** pour définir les caractéristiques de service pour les abonnés. Les profils vous permettent de créer des modèles de service réutilisables qui peuvent être attribués à plusieurs abonnés, simplifiant ainsi le provisionnement et garantissant la cohérence.

Types de Profils

Profils EPC

Les Profils EPC (Evolved Packet Core) définissent les caractéristiques de service de données pour les abonnés LTE.

Paramètres Clés

Paramètre	Description	Valeurs Typiques
`ue_ambr_dl_kbps`	Limite de vitesse de téléchargement	10,000 - 1,000,000 Kbps
`ue_ambr_ul_kbps`	Limite de vitesse d'envoi	5,000 - 500,000 Kbps
`network_access_mode`	Type de service	0 (Seulement paquet), 2 (Paquet+CS)
`tracking_area_update_interval_seconds`	Minuteur TAU	54 secondes (typique)

Création de Profils EPC

```
curl -k -X POST https://hss.example.com:8443/api/epc/profile \
  -H "Content-Type: application/json" \
  -d '{
    "epc_profile": {
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000,
      "network_access_mode": 0
    }
  }'
```

Modèles de Profils EPC Courants

Internet de Base :

- Téléchargement : 10 Mbps (10,000 Kbps)
- Envoi : 5 Mbps (5,000 Kbps)

Standard :

- Téléchargement : 50 Mbps (50,000 Kbps)
- Envoi : 25 Mbps (25,000 Kbps)

Premium :

- Téléchargement : 100 Mbps (100,000 Kbps)
- Envoi : 50 Mbps (50,000 Kbps)

Illimité :

- Téléchargement : 1 Gbps (1,000,000 Kbps)
- Envoi : 500 Mbps (500,000 Kbps)

Profils IMS

Les Profils IMS définissent les caractéristiques de service vocal, principalement à travers des modèles IFC (Initial Filter Criteria).

Modèles IFC

Les modèles IFC sont des documents XML qui définissent les règles de routage des appels pour le S-CSCF.

Variables de Modèle :

- `{{imsi}}` - IMSI de l'abonné
- `{{msisdns}}` - Liste des numéros de téléphone
- `{{mcc}}` - Code du pays d'origine
- `{{mnc}}` - Code du réseau d'origine

Création de Profils IMS

```
curl -k -X POST https://hss.example.com:8443/api/ims/profile \
  -H "Content-Type: application/json" \
  -d '{
    "ims_profile": {
      "name": "Standard VoLTE",
      "ifc_template": "<InitialFilterCriteria>...</InitialFilterCriteria>"
    }
  }'
```

Exemple de Modèle IFC

```
<ServiceProfile>
  <PublicIdentity>

<Identity>sip:{{imsi}}@ims.mnc{{mnc}}.mcc{{mcc}}.3gppnetwork.org</Identity>
  </PublicIdentity>
  <InitialFilterCriteria>
    <Priority>0</Priority>
    <TriggerPoint>
      <ConditionTypeCNF>0</ConditionTypeCNF>
      <SPT>
        <ConditionNegated>0</ConditionNegated>
        <Group>0</Group>
        <Method>INVITE</Method>
      </SPT>
    </TriggerPoint>
    <ApplicationServer>
      <ServerName>sip:as.ims.example.com</ServerName>
      <DefaultHandling>0</DefaultHandling>
    </ApplicationServer>
  </InitialFilterCriteria>
</ServiceProfile>
```

Profils APN

Les Profils APN (Access Point Name) définissent les points d'accès réseau pour les connexions de données.

Composants APN

Identifiant APN

Définit le nom APN et le support du protocole IP.

APNs Courants :

- `internet` - Accès général à Internet
- `ims` - Signalisation IMS/VoLTE
- `mms` - Messagerie multimédia
- `vzwadmin` - Spécifique à l'opérateur

Options de Version IP :

- 0 : IPv4 uniquement
- 1 : IPv6 uniquement
- 2 : IPv4v6 (pile duale)
- 3 : IPv4 ou IPv6 (choix du réseau)

Profil QoS APN

Définit les paramètres de qualité de service.

Valeurs QCI (Identifiant de Classe QoS) :

QCI	Type	Cas d'utilisation	Priorité
1	GBR	Voix conversationnelle	Plus élevé
2	GBR	Vidéo conversationnelle	Élevé
4	GBR	Streaming vidéo	Élevé
5	Non-GBR	Signalisation IMS	Moyen
9	Non-GBR	Internet (par défaut)	Le plus bas

Création d'une Configuration APN Complète

```
# 1. Créer l'Identifiant APN
APN_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/identifier \
  -H "Content-Type: application/json" \
  -d '{"apn_identifier": {"apn": "internet", "ip_version": 2}}' \
  | jq -r '.data.id')

# 2. Créer le Profil QoS APN
QOS_ID=$(curl -k -X POST https://hss.example.com:8443/api/apn/qos_profile \
  -H "Content-Type: application/json" \
  -d '{
    "apn_qos_profile": {
      "name": "Meilleur Effort",
      "qci": 9,
      "allocation_retention_priority": 8,
      "apn_ambr_dl_kbps": 50000,
      "apn_ambr_ul_kbps": 25000,
      "pre_emption_capability": false,
      "pre_emption_vulnerability": true
    }
  }' | jq -r '.data.id')

# 3. Créer le Profil APN
curl -k -X POST https://hss.example.com:8443/api/apn/profile \
  -H "Content-Type: application/json" \
  -d "{
    \"apn_profile\": {
      \"name\": \"Profil APN Internet\",
      \"apn_identifier_id\": $APN_ID,
      \"apn_qos_profile_id\": $QOS_ID
    }
  }"
```

Attribution des APNs au Profil EPC

Les APNs sont liés aux Profils EPC via la table `join_epc_profile_to_apn_profile`.

Insérez des enregistrements dans la table de jointure pour lier les identifiants de profil APN à l'identifiant de profil EPC. Plusieurs profils APN peuvent être attribués à un seul profil EPC.

Profils de Roaming

Voir la documentation détaillée dans le Guide de Contrôle de Roaming.

Attribution de Profils

Relations de Profils d'Abonnés

Attribution des Profils aux Abonnés

```
# Attribuer les profils EPC et IMS lors de la création de l'abonné
curl -k -X POST https://hss.example.com:8443/api/subscriber \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "imsi": "001001123456789",
      "key_set_id": 1,
      "epc_profile_id": 1,
      "ims_profile_id": 1,
      "roaming_profile_id": 1
    }
  }'

# Mettre à jour le profil de l'abonné
curl -k -X PUT https://hss.example.com:8443/api/subscriber/1 \
  -H "Content-Type: application/json" \
  -d '{
    "subscriber": {
      "epc_profile_id": 2
    }
  }'
```

Meilleures Pratiques de Gestion des Profils

Principes de Conception

1. **Créer des Profils Standards** - Définir des niveaux de service communs (Basique, Standard, Premium)
2. **Réutiliser les Profils** - Attribuer le même profil à plusieurs abonnés
3. **Documenter les Changements** - Suivre les modifications de profil
4. **Tester Avant Production** - Vérifier que le profil fonctionne d'abord avec un abonné de test

Convention de Nommage des Profils

```
[Niveau de Service]-[Vitesse]-[Fonctionnalités]

Exemples :
- "Basique-10Mbps-Internet"
- "Premium-100Mbps-VoLTE"
- "Entreprise-1Gbps-MultiAPN"
```

Migration de Profils

Lors du changement de profil d'un abonné :

Important : Les changements de profil prennent effet lors de la prochaine :

- Mise à Jour de Zone de Suivi (TAU)
- Attache
- Enregistrement IMS (pour les changements de profil IMS)

Dépannage des Problèmes de Profils

L'abonné ne reçoit pas la vitesse attendue :

1. Vérifiez les valeurs AMBR du profil EPC attribué
2. Vérifiez les valeurs AMBR du profil QoS APN
3. Vérifiez que le MME/P-GW applique correctement le QoS
4. Vérifiez la congestion du réseau

L'enregistrement IMS échoue :

1. Vérifiez le profil IMS attribué
2. Vérifiez la validité du XML du modèle IFC
3. Consultez les journaux S-CSCF pour les erreurs de traitement IFC
4. Confirmez la configuration de sélection S-CSCF

APN non disponible :

1. Vérifiez que le profil APN est lié au profil EPC
2. Vérifiez que l'identifiant APN correspond à la demande du réseau
3. Consultez la demande de connectivité PDN de l'UE

← Retour au Guide des Opérations | Suivant : Contrôle de Roaming →

Flux de Protocole OmniHSS

← Retour au Guide des Opérations

Vue d'ensemble

Ce document détaille les flux de messages du protocole Diameter pris en charge par OmniHSS. Comprendre ces flux est essentiel pour le dépannage et les opérations.

Interface S6a (LTE/EPC)

Demande d'Information d'Authentification (AIR/AIA)

Le MME demande des vecteurs d'authentification pour l'abonné.

AVPs Clés :

- Demande : User-Name (IMSI), Visited-PLMN-Id, Nombre de Vecteurs Demandés
- Réponse : Authentication-Info (RAND, AUTN, XRES, KASME)

Demande de Mise à Jour de Localisation (ULR/ULA)

Le MME notifie l'HSS de la localisation de l'abonné et récupère les données d'abonnement.

AVPs Clés :

- Demande : User-Name (IMSI), RAT-Type, ULR-Flags, Visited-PLMN-Id, UE-SRVCC-Capability
- Réponse : Subscription-Data (AMBR, APN-Configuration, Network-Access-Mode)

Demande de Purge UE (PUR/PUA)

Le MME notifie l'HSS lorsque le contexte de l'abonné est supprimé.

Demande de Notification (NOR/NOA)

Le MME informe l'HSS de divers événements.

Demande d'Annulation de Localisation (CLR/CLA)

L'HSS initie l'annulation de localisation pour informer le MME que l'abonné doit être détaché. OmniHSS prend en charge l'envoi de CLR automatique et programmatique.

CLR Automatique (Transfert MME)

Lorsqu'un abonné effectue une Demande de Mise à Jour de Localisation depuis un nouveau MME, OmniHSS envoie automatiquement un CLR au MME précédent pour nettoyer les enregistrements obsolètes.

AVPs Clés (CLR Automatique) :

- User-Name: IMSI de l'abonné
- Destination-Host: Nom d'hôte du MME précédent
- Destination-Realm: Domaine du MME précédent
- Cancellation-Type: 0 (Procédure de Mise à Jour MME)
- CLR-Flags: 0
- Subscription-Data: Profil d'abonnement complet

Implémentation : `lib/hss/control/diameter/s6a.ex:216-256`

CLR Programmatique (Déclenché par API)

Les administrateurs peuvent déclencher CLR via l'API programmatique pour détacher de force les abonnés (par exemple, pour un retrait d'abonnement, prévention de fraude ou actions administratives).

AVPs Clés (CLR Programmatique) :

- User-Name: IMSI de l'abonné
- Destination-Host: Nom d'hôte du dernier MME vu
- Destination-Realm: Domaine du dernier MME vu
- Cancellation-Type: `:subscription_withdrawal` (codé comme entier selon 3GPP TS 29.272)
- CLR-Flags:
  - s6a_indicator: 1 (indique l'interface S6a)
  - reattach_required: 1 (l'UE doit se ré-authentifier pour se rattacher)

Implémentation :

- Fonction API : `lib/hss/control/common.ex:557-583`
- Constructeur de Message : `lib/hss/control/diameter/s6a.ex:542-578`

Types d'Annulation

OmniHSS prend en charge plusieurs types d'annulation selon 3GPP TS 29.272 :

Type	Valeur	Description	Cas d'utilisation
Procédure de Mise à Jour MME	0	Changement normal de MME	Automatique lors de ULR depuis un nouveau MME
Procédure de Mise à Jour SGSN	1	Transfert SGSN	Scénarios de transfert 3G/2G
Retrait d'Abonnement	2	Résiliation administrative	Détachement manuel via API
Procédure de Mise à Jour IWF	3	Mise à jour de la fonction d'interconnexion	Interopérabilité avec le réseau hérité
Procédure de Rattachement Initial	4	Enregistrement frais	Forcer la ré-authentification

CLR-Flags

L'AVP CLR-Flags est un masque de bits avec les champs suivants :

Drapeau	Bit	Description
Indicateur S6a/S6d	0	1 = Interface S6a utilisée
Rattachement Requis	1	1 = L'UE doit effectuer un nouveau rattachement

Configuration Exemple des CLR-Flags :

```
clr_flags: %{
  s6a_indicator: 1,        # Utilisation de l'interface S6a
  reattach_required: 1     # Forcer la ré-authentification
}
```

Scénarios Multi-IMSI

OmniHSS suit l'enregistrement MME **par abonné (IMSI)**, et non par MSISDN. Cela est crucial pour comprendre le comportement de CLR dans des scénarios multi-IMSI :

Scénario 1 : Plusieurs MSISDN, Un Seul IMSI

```
Abonné A :
  - IMSI : 999000123456789
  - MSISDNs : ["+1234567890", "+9876543210"]
  - last_seen_mme : "mme01.operator.com"
```

Lorsque cet abonné se déplace vers un nouveau MME :

- **Un CLR envoyé** à "mme01.operator.com" avec IMSI 999000123456789
- Les deux MSISDNs sont affectés (même abonné, même SIM)
- L'AVP User-Name contient l'IMSI, pas les MSISDNs

Scénario 2 : Plusieurs Abonnés (IMSI Différents), Même MSISDN

OmniHSS impose une **contrainte de MSISDN unique** (un MSISDN ne peut pas appartenir à plusieurs abonnés simultanément). Cependant, lors du portage/ migration :

```
Abonné A :
  - IMSI : 999000111111111
  - MSISDN : "+1234567890"
  - last_seen_mme : "mme01.operator.com"

Abonné B (après portage) :
  - IMSI : 999000222222222
  - MSISDN : "+1234567890"  # Même MSISDN, SIM/IMSI différente
  - last_seen_mme : "mme02.operator.com"
```

Lorsque l'Abonné B s'enregistre :

- **Aucun CLR envoyé** (IMSI différent = abonné différent)
- L'Abonné A reste enregistré à mme01
- L'Abonné B s'enregistre à mme02
- Les deux peuvent être actifs simultanément (différents appareils physiques)

Scénario 3 : CLR Programmatique pour Abonné Multi-MSISDN

```
# Appel API pour détacher l'abonné
Hss.Control.Common.send_cancel_location_request(:imsi,
"999000123456789")
```

Résultat :

- **Un CLR envoyé** au dernier_mme_vu de l'abonné
- **Tous les MSISDNs** associés à cet IMSI sont effectivement détachés
- L'IMSI est la clé primaire pour suivre l'enregistrement MME

Notes Importantes

1. **L'IMSI est la Clé :** Les opérations CLR sont toujours **par IMSI**, jamais par MSISDN. La table `subscriber_state` suit `last_seen_mme` par abonné (IMSI).

2. **Opération Atomique :** Chaque abonné ne peut être enregistré qu'à un MME à la fois. Le CLR automatique garantit cela en nettoyant l'ancien enregistrement.

3. **Pas de CLR si Pas de MME Précédent :** Si `last_seen_mme` est `nil` (l'abonné n'a jamais été enregistré), aucun CLR n'est envoyé lors de l'ULR.

4. **Données d'Abonnement Incluses :** Le CLR automatique (durant l'ULR) inclut l'AVP complet `Subscription-Data` pour aider l'ancien MME à nettoyer correctement le contexte.

5. **Asynchrone :** Le CLR est envoyé de manière asynchrone (fire-and-forget). La réponse ULA au nouveau MME n'attend pas de CLA de l'ancien MME.

6. **Gestion des CLA :** OmniHSS reçoit les réponses CLA mais les ignore actuellement (`:discard` à la ligne 398). Cela empêche les boucles de messages et est un comportement standard de l'HSS.

Interface Cx (IMS)

Demande d'Autorisation d'Utilisateur (UAR/UAA)

L'I-CSCF interroge si l'utilisateur est autorisé à s'enregistrer.

Demande d'Attribution de Serveur (SAR/SAA)

Le S-CSCF enregistre/désenregistre l'utilisateur et récupère le profil IMS.

Rendu du Modèle IFC :

- `{{imsi}}` → IMSI réel
- `{{msisdns}}` → Liste des numéros de téléphone
- `{{mcc}}, {{mnc}}` → Codes PLMN d'origine

Demande d'Authentification Multimédia (MAR/MAA)

Le S-CSCF demande des vecteurs d'authentification pour l'enregistrement IMS.

Demande d'Information de Localisation (LIR/LIA)

L'I-CSCF interroge quel S-CSCF sert l'utilisateur.

Interface Sh (Données de Profil IMS)

Demande de Données Utilisateur (UDR/UDA)

Le Serveur d'Application demande des données de profil d'abonné.

Demande de Mise à Jour de Profil (PUR/PUA)

Le Serveur d'Application met à jour les données de profil d'abonné.

Demande de Notifications d'Abonnement (SNR/SNA)

Le Serveur d'Application s'abonne aux changements de profil.

Interface Gx (Contrôle de Politique)

OmniHSS fonctionne comme le PCRF (Fonction de Règles de Politique et de Facturation) via l'interface Gx.

Voir Documentation PCRF pour l'architecture détaillée, la configuration de politique et la gestion de QoS.

Demande de Contrôle de Crédit - Initiale (CCR-I/CCA-I)

Le P-GW demande des règles de politique lorsque la session PDN est établie.

AVPs Clés :

- Demande : Subscription-Id (IMSI), Called-Station-Id (APN), RAT-Type, IP-CAN-Type
- Réponse : QoS-Information (QCI, ARP, AMBR), Charging-Rule-Install

Demande de Contrôle de Crédit - Mise à Jour (CCR-U/CCA-U)

Le P-GW notifie des changements de session.

Demande de Contrôle de Crédit - Terminer (CCR-T/CCA-T)

Le P-GW notifie lorsque la session PDN se termine.

Demande de Ré-Authentification (RAR/RAA)

OmniHSS (PCRF) initie une mise à jour de politique au P-GW.

Interface Rx (Politique Média IMS)

OmniHSS fonctionne comme le PCRF via l'interface Rx pour l'autorisation média IMS.

Voir Documentation PCRF pour les flux d'appels VoLTE détaillés et

l'autorisation média.

Demande AA (AAR/AAA)

Le P-CSCF demande une autorisation média pour la session IMS.

Informations Clés :

- Analyser le SDP pour déterminer le codec et la bande passante
- Calculer la bande passante requise (UL/DL)
- Créer des filtres SDF pour les flux médias
- Déclencher le porteur dédié via Gx RAR

Demande de Terminaison de Session (STR/STA)

Le P-CSCF notifie lorsque la session IMS se termine.

Interface S13 (EIR)

OmniHSS fonctionne comme l'EIR (Registre d'Identité d'Équipement) via l'interface S13.

Voir Documentation EIR pour le contrôle d'identité d'équipement détaillé, la validation IMEI et la gestion de liste noire.

Demande de Vérification d'Identité ME (ECR/ECA)

Un client EIR externe (ou MME) demande la validation de l'équipement.

Valeurs d'État de l'Équipement :

- **Équipement Inconnu (0)** - Appareil autorisé (liste blanche)
- **Équipement Sur Liste Noire (1)** - Appareil bloqué
- **Équipement Sur Liste Grise (2)** - Appareil autorisé mais suivi

---

Flux d'Appel Complet : Appel VoLTE

Configuration d'appel VoLTE de bout en bout montrant plusieurs interfaces.

Dépannage des Problèmes de Protocole

Échecs d'Authentification (S6a AIR)

Vérifiez :

1. Ensemble de clés configuré correctement (Ki, OPC, AMF)
2. Synchronisation SQN (en cas d'échecs répétés)
3. Règles de roaming autorisent le réseau visité

Échecs de Mise à Jour de Localisation (S6a ULR)

Vérifiez :

1. Profil EPC existe et a des APNs configurés
2. Roaming autorisé pour les services de données
3. Format d'identité MME correct

Échecs d'Enregistrement IMS (Cx SAR)

Vérifiez :

1. Profil IMS attribué à l'abonné
2. Modèle IFC XML valide
3. Sélection S-CSCF configurée
4. MSISDNs attribués s'ils sont utilisés dans le modèle

Échecs de Connexion PDN (Gx CCR-I)

Vérifiez :

1. APN existe dans la liste APN du profil EPC
2. Profil QoS APN configuré
3. Table de session PDN pas pleine (si des limites existent)

← Retour au Guide des Opérations

Contrôle de Roaming OmniHSS

← Retour au Guide des Opérations

Vue d'ensemble

OmniHSS fournit un contrôle de roaming granulaire, vous permettant de définir quels réseaux les abonnés peuvent accéder pour les services de données et IMS lors du roaming.

Flux de Contrôle de Roaming

Structure du Profil de Roaming

Composants

Règle de Roaming

Chaque règle spécifie une action pour un réseau spécifique (combinaison MCC/MNC).

Champs :

- `name` - Nom descriptif
- `mcc` - Code de Pays Mobile (3 chiffres)
- `mnc` - Code de Réseau Mobile (2-3 chiffres)
- `data_action` - 0 (Autoriser) ou 1 (Refuser)
- `ims_action` - 0 (Autoriser) ou 1 (Refuser)

Profil de Roaming

Définit le comportement par défaut et lie aux règles.

Champs :

- `name` - Nom du profil
- `data_action_if_no_rules_match` - 0 (Autoriser) ou 1 (Refuser)
- `ims_action_if_no_rules_match` - 0 (Autoriser) ou 1 (Refuser)

Exemples de Configuration

Autoriser Tous les Roamings

```
# Créer un profil qui autorise tout
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Autoriser Tout",
      "data_action_if_no_rules_match": 0,
      "ims_action_if_no_rules_match": 0
    }
  }'
```

Refuser Tous les Roamings

```
# Créer un profil qui bloque tout
curl -k -X POST https://hss.example.com:8443/api/roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Pas de Roaming",
      "data_action_if_no_rules_match": 1,
      "ims_action_if_no_rules_match": 1
    }
  }'
```

Autoriser des Réseaux Spécifiques (Liste Blanche)

```
# Créer un profil avec refus par défaut
PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
roaming/profile \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Uniquement les Opérateurs Américains",
      "data_action_if_no_rules_match": 1,
      "ims_action_if_no_rules_match": 1
    }
  }' | jq -r '.data.id')

# Autoriser AT&T
RULE1=$(curl -k -X POST https://hss.example.com:8443/api/roaming/rule
\
  -H "Content-Type: application/json" \
  -d '{
```

```
    "roaming_rule": {
      "name": "Autoriser AT&T",
      "mcc": "310",
      "mnc": "410",
      "data_action": 0,
      "ims_action": 0
    }
  }' | jq -r '.data.id')

# Autoriser Verizon
RULE2=$(curl -k -X POST https://hss.example.com:8443/api/roaming/rule
\
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Autoriser Verizon",
      "mcc": "311",
      "mnc": "480",
      "data_action": 0,
      "ims_action": 0
    }
  }' | jq -r '.data.id')

# Lier les règles au profil (via la base de données)
# Insérer des enregistrements dans la table
join_roaming_profile_to_roaming_rule
# pour lier chaque ID de règle à l'ID de profil de roaming
```

Autoriser les Données, Bloquer la Voix

```
# Créer une règle qui autorise les données mais bloque IMS
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Données Uniquement - T-Mobile",
      "mcc": "310",
      "mnc": "260",
      "data_action": 0,
      "ims_action": 1
    }
  }'
```

Bloquer des Réseaux Spécifiques (Liste Noire)

```
# Créer un profil avec autorisation par défaut
PROFILE_ID=$(curl -k -X POST https://hss.example.com:8443/api/
roaming/profile \
```

```
  -H "Content-Type: application/json" \
  -d '{
    "roaming_profile": {
      "name": "Bloquer les Réseaux Coûteux",
      "data_action_if_no_rules_match": 0,
      "ims_action_if_no_rules_match": 0
    }
  }' | jq -r '.data.id')

# Bloquer un réseau coûteux spécifique
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Bloquer le Réseau Coûteux",
      "mcc": "206",
      "mnc": "01",
      "data_action": 1,
      "ims_action": 1
    }
  }'
```

Scénarios de Roaming Courants

Scénario 1 : Roaming Domestique Seulement

L'abonné peut roamer dans son pays d'origine mais pas à l'international.

Configuration :

- Par défaut : Refuser tout
- Règles : Autoriser tous les codes MCC des USA (310, 311, 312, 313, 314, 315, 316)

Scénario 2 : Partenaires de Roaming Seulement

L'abonné ne peut roamer que sur des réseaux ayant des accords commerciaux.

Configuration :

- Par défaut : Refuser tout
- Règles : Autoriser chaque réseau partenaire explicitement (par MCC/MNC)

Scénario 3 : Roaming de Données, Pas de Roaming Vocal

L'abonné peut utiliser des données à l'étranger mais doit utiliser le WiFi pour les

appels vocaux.

Configuration :

- Règles : `data_action: 0` (autoriser), `ims_action: 1` (refuser)

Scénario 4 : Accès aux Services d'Urgence

Toujours autoriser les services d'urgence, même si le roaming est bloqué.

Remarque : La gestion des services d'urgence est généralement effectuée au niveau du MME/réseau. Les règles de roaming d'OmniHSS s'appliquent aux services normaux.

Référence MCC/MNC

Codes de Pays Courants (MCC)

MCC	Pays	Réseaux
310-316	USA	AT&T, Verizon, T-Mobile, etc.
302	Canada	Rogers, Bell, Telus
234-235	Royaume-Uni	Vodafone, O2, EE
262	Allemagne	Deutsche Telekom, Vodafone
208	France	Orange, SFR, Bouygues
222	Italie	TIM, Vodafone, Wind
214	Espagne	Movistar, Vodafone

Opérateurs Américains Courants (MCC 310-316)

MCC	MNC	Opérateur
310	410	AT&T
311	480	Verizon
310	260	T-Mobile
310	120	Sprint
313	380	(Réseau de test exemple)

Listes Complètes : Voir ITU-T E.212 ou bases de données MCC/MNC

Points d'Application du Roaming

Interface S6a (Données)

Lorsque l'abonné se connecte au réseau visité :

Interface Cx (IMS)

Lorsque l'abonné s'enregistre à IMS dans le réseau visité :

Dépannage des Problèmes de Roaming

L'Abonné Ne Peut Pas Se Connecter au Réseau Visité

Vérifiez l'attribution du profil de roaming :

- Interrogez la base de données pour voir le profil de roaming attribué à l'abonné
- Vérifiez le nom du profil et les paramètres d'action par défaut

Vérifiez si une règle existe pour le réseau visité :

- Interrogez la base de données pour les règles de roaming correspondant au MCC/MNC du réseau visité
- Vérifiez si une règle existe pour le profil de roaming de l'abonné
- Vérifiez la valeur de `data_action` pour ce réseau spécifique

L'Abonné Peut Se Connecter Mais Pas S'enregistrer à IMS

Vérifiez l'action IMS séparément :

- Interrogez les règles de roaming pour le réseau visité
- Vérifiez les valeurs de `data_action` et `ims_action`
- Recherchez des cas où les données sont autorisées mais IMS est refusé

Comportement de Roaming Inattendu

Examinez les journaux pour les vérifications de roaming :

```
[info] Vérification de roaming : IMSI 001001123456789, PLMN Visité
310-410
[info] Règle de roaming correspondante : "Autoriser AT&T"
[info] Action de données : autoriser, action IMS : autoriser
```

Meilleures Pratiques

Conception de Profil

1. **Commencer restrictif** - Refus par d��faut, autoriser explicitement les partenaires

2. **Tester minutieusement** - Vérifiez les règles en laboratoire avant la production
3. **Documenter les règles** - Maintenir une liste des réseaux autorisés et pourquoi
4. **Réviser régulièrement** - Mettre à jour au fur et à mesure que les accords de roaming changent

Gestion des Règles

1. **Utiliser des noms descriptifs** - "Autoriser-ATT-Données-Uniquement" pas "Règle1"
2. **Vérifier MCC/MNC** - Vérifiez les codes par rapport aux bases de données officielles
3. **Considérer les deux services** - Pensez aux données et à IMS séparément
4. **Surveiller l'utilisation** - Suivre quels réseaux les abonnés visitent réellement

Procédures Opérationnelles

1. **Changements d'Urgence** - Avoir une procédure pour activer/désactiver rapidement le roaming
2. **Mises à Jour en Masse** - Planifier la mise à jour des profils de roaming de plusieurs abonnés
3. **Rapports** - Suivre l'utilisation du roaming et les tentatives refusées
4. **Communication avec les Clients** - Informer les clients des changements de politique de roaming

---

← Retour au Guide des Opérations | Suivant : Flux de Protocoles →

Guide de Dépannage OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu du Dépannage

Approche Générale de Dépannage

Informations à Collecter

Avant de dépanner un problème, collectez :

1. **Informations sur l'Abonné** (si spécifique à l'abonné)
    - IMSI
    - MSISDN (numéro de téléphone)
    - Dernier état connu
    - Messages d'erreur du dispositif
2. **Informations de Timing**
    - Quand le problème a-t-il commencé ?
    - Est-il intermittent ou constant ?
    - Heure de la dernière opération réussie

3. **Portée de l'Impact**
    - Abonné unique ou plusieurs ?
    - Réseau spécifique ou tous les réseaux ?
    - Service spécifique (données/voix) ou les deux ?
4. **État du Système**
    - Vérifiez le Panneau de Contrôle pour l'état du système
    - Examinez l'état des pairs Diameter
    - Vérifiez la connectivité à la base de données

Échecs d'Authentification

Symptômes

- L'abonné ne peut pas se connecter au réseau
- Erreurs "Authentification rejetée"
- Tentatives d'authentification répétées

Causes et Solutions Courantes

Cause 1 : Ensemble de Clés Incorrect

Symptômes :

- Échec d'authentification constant pour un abonné spécifique
- Fonctionne pour d'autres abonnés avec le même profil

Étapes de Diagnostic :

1. Interroger l'abonné pour vérifier key_set_id :

   ```
   curl -k https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
   ```

2. Vérifier que l'ensemble de clés existe et a les bonnes valeurs :

   ```
   curl -k https://hss.example.com:8443/api/key_set/[KEY_SET_ID]
   ```

3. Comparer les valeurs Ki et OPC avec la documentation de la carte SIM

Solution :

- Mettre à jour l'abonné avec le bon ensemble de clés
- Si les clés sont correctes, la carte SIM peut être défectueuse

Cause 2 : SQN Hors Synchronisation

Symptômes :

- L'authentification échoue après avoir fonctionné précédemment
- Erreur : "Échec de synchronisation SQN"
- Fonctionne de manière intermittente

Étapes de Diagnostic :

1. Vérifier l'état de l'abonné pour la valeur SQN dans la base de données
2. Rechercher des erreurs liées au SQN dans les journaux
3. Vérifier la valeur SQN de l'ensemble de clés de l'abonné

Solution :

- Le SQN se resynchronisera automatiquement après que l'abonné envoie AUTS
- Si persistant, réinitialiser le SQN à 0 dans l'ensemble de clés (nécessite une nouvelle connexion de l'abonné)

Avertissement : La réinitialisation du SQN peut causer des problèmes de sécurité. Ne le faites que pendant la maintenance.

Cause 3 : Abonné Désactivé

Symptômes :

- Authentification rejetée immédiatement
- Aucun vecteur d'authentification généré

Étapes de Diagnostic :

1. Vérifier le statut d'activation de l'abonné :

   ```
   curl -k https://hss.example.com:8443/api/subscriber/imsi/[IMSI]
   ```

2. Vérifier que le champ `enabled` est `true`

Solution :

- Activer l'abonné :

  ```
  curl -k -X PUT https://hss.example.com:8443/api/subscriber/[ID]
  \
    -H "Content-Type: application/json" \
    -d '{"subscriber": {"enabled": true}}'
  ```

Cause 4 : Profil EPC Manquant

Symptômes :

- La recherche d'abonné réussit mais l'authentification échoue
- Erreur : "Aucun profil EPC assigné"

Étapes de Diagnostic :

1. Vérifier le champ `epc_profile_id` de l'abonné
2. Vérifier que le profil EPC existe :

```
curl -k https://hss.example.com:8443/api/epc/
profile/[PROFILE_ID]
```

Solution :

- Assigner un profil EPC valide à l'abonné

Organigramme de Dépannage de l'Authentification

Problèmes de Connectivité Diameter

Symptômes

- Les pairs Diameter apparaissent comme déconnectés dans le Panneau de Contrôle
- Erreurs "Aucun itinéraire vers l'hôte"
- Services échouant pour tous les abonnés

Causes et Solutions Courantes

Cause 1 : Connectivité Réseau

Symptômes :

- Le pair ne se connecte jamais
- Erreurs de délai d'attente de connexion
- Ping échoue vers le pair

Étapes de Diagnostic :

1. Vérifier la connectivité réseau de OmniHSS vers le pair :

```
ping [PEER_IP]
```

2. Vérifier si le port Diameter est accessible :

   ```
   telnet [PEER_IP] 3868
   ```

3. Vérifier que les règles de pare-feu autorisent le trafic Diameter (port 3868)

Solution :

- Corriger le routage réseau
- Mettre à jour les règles de pare-feu
- Vérifier que le pair fonctionne et écoute

Cause 2 : Configuration Diameter Incorrecte

Symptômes :

- Les tentatives de connexion échouent
- L'échange CER/CEA échoue
- Le pair rejette la connexion

Étapes de Diagnostic :

1. Examiner la configuration Diameter dans runtime.exs :
   - Vérifier que origin_host du pair correspond à la valeur attendue
   - Vérifier la configuration origin_realm
   - Vérifier que l'adresse IP du pair est correcte
2. Vérifier les journaux pour des erreurs CER/CEA
3. Vérifier que la configuration du pair attend origin_host de OmniHSS

Solution :

- Mettre à jour runtime.exs avec la configuration Diameter correcte
- Redémarrer OmniHSS après modification de la configuration
- Coordonner avec l'administrateur du pair pour vérifier les paramètres

Cause 3 : Problèmes de Certificat (TLS Diameter)

Symptômes :

- La connexion échoue lors de la poignée de main TLS
- Erreurs de validation de certificat
- Erreurs "Certificat expiré" ou "Certificat invalide"

Étapes de Diagnostic :

1. Vérifier que les fichiers de certificat existent dans `priv/cert/`
2. Vérifier l'expiration du certificat :

   ```
   openssl x509 -in priv/cert/diameter.crt -noout -dates
   ```

3. Vérifier que la chaîne de certificats est complète
4. Vérifier le certificat du pair si TLS mutuel

Solution :

- Renouveler les certificats expirés
- Installer la chaîne de certificats correcte
- Mettre à jour les fichiers de certificats et redémarrer OmniHSS

Cause 4 : Mismatch de Support d'Application du Pair

Symptômes :

- Le pair se connecte mais ne prend pas en charge les applications requises
- L'échange de capacités réussit mais les opérations échouent
- Erreurs "Application non supportée"

Étapes de Diagnostic :

1. Vérifier la page Diameter du Panneau de Contrôle pour les applications du pair
2. Vérifier que le pair prend en charge l'application requise (S6a, Cx, Sh, etc.)
3. Examiner l'échange CER/CEA dans les journaux

Solution :

- Vérifier que la configuration du pair inclut les applications Diameter requises
- Vérifier que le type de pair correspond à la fonctionnalité attendue :
  - MME doit prendre en charge S6a (16777251)
  - S-CSCF doit prendre en charge Cx (16777216)
  - P-GW doit prendre en charge Gx (16777238)

Organigramme de Dépannage Diameter

Problèmes de Base de Données

Symptômes

- L'API renvoie des erreurs 500
- Le Panneau de Contrôle ne se charge pas
- Erreurs "Échec de la connexion à la base de données"
- Performance de requête lente

Causes et Solutions Courantes

Cause 1 : Serveur de Base de Données Hors Service

Symptômes :

- Tous les appels API échouent
- Le Panneau de Contrôle affiche une erreur
- Erreurs "Connexion refusée"

Étapes de Diagnostic :

1. Tester la connectivité à la base de données :

   ```
   # Si vous utilisez PostgreSQL
   psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME]

   # Si vous utilisez MySQL
   mysql -h [DB_HOST] -u [DB_USER] -p [DB_NAME]
   ```

2. Vérifier l'état du service de base de données sur le serveur de base de données

3. Vérifier la connectivité réseau vers le serveur de base de données

Solution :

- Démarrer le service de base de données
- Corriger les problèmes du serveur de base de données
- Vérifier le routage réseau vers le serveur de base de données

Cause 2 : Identifiants de Base de Données Incorrects

Symptômes :

- Erreurs "Échec de l'authentification"
- OmniHSS ne peut pas se connecter au démarrage

Étapes de Diagnostic :

1. Examiner la configuration de la base de données dans runtime.exs
2. Tester les identifiants manuellement avec un client de base de données
3. Vérifier les autorisations de l'utilisateur de la base de données

Solution :

- Mettre à jour la configuration de la base de données dans runtime.exs
- Accorder les bonnes autorisations à l'utilisateur de la base de données
- Redémarrer OmniHSS après modification de la configuration

Cause 3 : Pool de Connexion Épuisé

Symptômes :

- Erreurs 500 intermittentes
- Erreurs "Aucune connexion disponible"
- Les périodes de forte charge déclenchent des échecs

Étapes de Diagnostic :

1. Vérifier le nombre de connexions actuelles dans la base de données
2. Examiner la taille du pool de base de données dans runtime.exs
3. Surveiller l'utilisation des connexions pendant les pics de charge

Solution :

- Augmenter la taille du pool dans la configuration runtime.exs
- Enquêter sur les fuites de connexions si le pool s'épuise de manière répétée
- Envisager l'évolutivité de la base de données si la charge est constamment élevée

Cause 4 : Requêtes Lentes

Symptômes :

- Réponses API très lentes
- Délai d'attente sur les recherches d'abonnés
- CPU de la base de données élevé

Étapes de Diagnostic :

1. Interroger la base de données pour le journal des requêtes lentes
2. Identifier les requêtes lentes spécifiques
3. Vérifier les index manquants
4. Vérifier le nombre d'abonnés et la taille des tables

Solution :

- Optimiser les requêtes lentes
- Ajouter des index manquants
- Envisager l'optimisation des performances de la base de données
- Planifier l'évolutivité de la base de données si nécessaire

Organigramme de Dépannage de la Base de Données

Échecs d'Enregistrement EPC

Symptômes

- L'abonné ne peut pas se connecter au réseau LTE
- LMME rejette l'attachement
- Aucune session PDN établie

Causes et Solutions Courantes

Cause 1 : Roaming Refusé

Symptômes :

- L'abonné fonctionne sur le réseau domestique mais échoue en roaming
- Erreurs "Roaming non autorisé"
- Fonctionne pour certains réseaux mais pas d'autres

Étapes de Diagnostic :

1. Vérifier le champ roaming_profile_id de l'abonné
2. Interroger le profil de roaming et les règles
3. Vérifier le MCC/MNC du réseau visité
4. Vérifier si une règle de roaming existe pour ce réseau

Solution :

- Ajouter une règle de roaming pour le MCC/MNC du réseau visité
- Ou mettre à jour l'action par défaut du profil de roaming pour autoriser
- Voir la Documentation sur le Roaming pour la configuration

Cause 2 : Configuration APN Manquante

Symptômes :

- L'attachement réussit mais la session PDN échoue
- Erreurs "APN inconnu" du MME

- L'abonné ne peut pas obtenir de connexion de données

Étapes de Diagnostic :

1. Vérifier que le profil EPC a des profils APN liés
2. Vérifier que l'identifiant APN correspond à ce que le dispositif demande
3. Interroger la configuration du profil APN

Solution :

- Lier les profils APN au profil EPC de l'abonné
- S'assurer que le nom de l'APN correspond à la configuration du dispositif
- Vérifier que le profil QoS de l'APN existe

Cause 3 : MME Non Connecté

Symptômes :

- Tous les abonnés échouent à se connecter
- Aucune communication avec le MME
- Pair Diameter hors service

Étapes de Diagnostic :

1. Vérifier la page Diameter du Panneau de Contrôle
2. Vérifier que l'état du pair MME est "Connecté"
3. Vérifier que le MME prend en charge l'application S6a

Solution :

- Dépanner la connectivité Diameter
- Vérifier la configuration du MME
- Contacter l'administrateur du MME

Cause 4 : Corruption de l'État de l'Abonné

Symptômes :

- L'abonné apparaît comme attaché mais ne peut pas se rattacher
- L'état ne correspond pas à la réalité
- La déconnexion et la reconnexion échouent

Étapes de Diagnostic :

1. Interroger l'état de l'abonné dans la base de données
2. Vérifier les affectations MME obsolètes
3. Vérifier l'horodatage de la dernière mise à jour

Solution :

- Effacer l'état de l'abonné (procédure de déconnexion)
- Réinitialiser le MME de service dans l'état de l'abonné
- Peut nécessiter un cycle d'alimentation de l'abonné

Organigramme de Dépannage de l'Enregistrement EPC

Échecs d'Enregistrement IMS

Symptômes

- L'abonné ne peut pas s'enregistrer pour VoLTE
- "Échec de l'enregistrement IMS" sur le dispositif
- Les données fonctionnent mais pas la voix

Causes et Solutions Courantes

Cause 1 : IMS Désactivé pour l'Abonné

Symptômes :

- L'abonné a des données mais pas d'IMS
- L'enregistrement est rejeté immédiatement

Étapes de Diagnostic :

1. Interroger l'abonné et vérifier le champ `ims_enabled`
2. Vérifier que l'abonné a un `ims_profile_id` assigné

Solution :

- Activer l'IMS pour l'abonné
- Assigner un profil IMS

Cause 2 : S-CSCF Non Connecté

Symptômes :

- Tous les enregistrements IMS échouent
- Aucun trafic Diameter lié à l'IMS

Étapes de Diagnostic :

1. Vérifier la page Diameter du Panneau de Contrôle
2. Vérifier que le pair S-CSCF est connecté

3. Vérifier que le S-CSCF prend en charge l'application Cx

Solution :

- Corriger la connectivité Diameter vers le S-CSCF
- Vérifier la configuration du S-CSCF

Cause 3 : Modèle IFC Manquant ou Invalide

Symptômes :

- L'enregistrement échoue pendant la Réponse d'Autorisation de l'Utilisateur
- Erreurs liées à l'IFC dans les journaux

Étapes de Diagnostic :

1. Interroger le profil IMS de l'abonné
2. Vérifier que le modèle IFC est présent
3. Vérifier la syntaxe XML de l'IFC

Solution :

- Mettre à jour le profil IMS avec un modèle IFC valide
- Voir la Documentation des Profils pour des exemples d'IFC

Cause 4 : Roaming Refusé pour l'IMS

Symptômes :

- L'IMS fonctionne sur le réseau domestique
- Échoue en roaming
- Le roaming de données fonctionne mais pas l'IMS

Étapes de Diagnostic :

1. Vérifier l'action IMS du profil de roaming
2. Vérifier que les règles de roaming ont le bon `ims_action`

Solution :

- Mettre à jour les règles de roaming pour autoriser l'IMS
- Ou mettre à jour l'action IMS par défaut du profil de roaming

Organigramme de Dépannage de l'Enregistrement IMS

Échecs d'Appels VoLTE

Symptômes

- L'enregistrement IMS réussit mais les appels échouent
- Audio unidirectionnel
- L'appel se coupe immédiatement
- Erreur "Appel échoué" sur le dispositif

Causes et Solutions Courantes

Cause 1 : P-CSCF Non Connecté

Symptômes :

- L'enregistrement fonctionne mais les appels échouent
- L'autorisation des médias échoue

Étapes de Diagnostic :

1. Vérifier la page Diameter du Panneau de Contrôle
2. Vérifier que le pair P-CSCF est connecté
3. Vérifier que le P-CSCF prend en charge l'application Rx (fonction PCRF de OmniHSS)

Solution :

- Corriger la connectivité Diameter vers le P-CSCF
- Vérifier que la configuration du P-CSCF pointe vers OmniHSS pour Rx

Cause 2 : Autorisation des Médias Manquante

Symptômes :

- La configuration de l'appel commence mais échoue
- L'échange AAR/AAA échoue
- Erreurs sur l'interface Rx

Étapes de Diagnostic :

1. Vérifier les journaux pour les messages Diameter Rx
2. Vérifier que AAR (AA-Request) a été reçu
3. Vérifier la réponse AAA (AA-Answer)

Solution :

- Vérifier que le P-CSCF envoie AAR pour l'autorisation des médias

- Vérifier la configuration de l'application Rx de OmniHSS
- Vérifier que l'abonné a un enregistrement IMS actif

Cause 3 : Problèmes de QoS/Bearer

Symptômes :

- L'appel se connecte mais pas d'audio
- Audio unidirectionnel
- Problèmes de qualité

Étapes de Diagnostic :

1. Vérifier le profil QoS de l'APN pour l'APN voix
2. Vérifier que le QCI est correctement défini (généralement QCI 1 pour la voix)
3. Vérifier que le P-GW est connecté pour Gx (fonction PCRF)

Solution :

- Vérifier le profil QoS de l'APN pour l'APN IMS
- S'assurer que le QCI 1 est configuré pour le bearer voix
- Corriger la connectivité Diameter vers le P-GW si nécessaire

Organigramme de Dépannage des Appels VoLTE

Problèmes de Roaming

Symptômes

- L'abonné fonctionne à domicile mais pas en roaming
- Certains réseaux de roaming fonctionnent, d'autres non
- Le roaming de données fonctionne mais pas la voix (ou vice versa)

Causes et Solutions Courantes

Cause 1 : Aucun Profil de Roaming Assigné

Symptômes :

- Le roaming échoue pour l'abonné
- D'autres abonnés roament avec succès

Étapes de Diagnostic :

1. Interroger le champ `roaming_profile_id` de l'abonné

2. Vérifier si le champ est nul

Solution :

- Assigner un profil de roaming à l'abonné

Cause 2 : Roaming Refusé par Politique

Symptômes :

- Le roaming échoue systématiquement sur un réseau spécifique
- L'erreur indique un rejet de politique

Étapes de Diagnostic :

1. Identifier le MCC/MNC du réseau visité à partir du dispositif de l'abonné ou du MME
2. Interroger le profil de roaming de l'abonné
3. Vérifier les règles de roaming pour le MCC/MNC correspondant
4. Vérifier l'action par défaut du profil

Solution :

- Ajouter une règle de roaming pour autoriser le réseau visité :

```
curl -k -X POST https://hss.example.com:8443/api/roaming/rule \
  -H "Content-Type: application/json" \
  -d '{
    "roaming_rule": {
      "name": "Autoriser le Réseau Visité",
      "mcc": "310",
      "mnc": "410",
      "data_action": 0,
      "ims_action": 0
    }
  }'
```

Cause 3 : Données Autorisées mais IMS Refusé

Symptômes :

- Le roaming de données fonctionne
- Le roaming voix/IMS échoue
- Disponibilité de service divisée

Étapes de Diagnostic :

1. Interroger les règles de roaming pour le réseau visité

2. Vérifier les valeurs `data_action` vs `ims_action`
3. Vérifier les actions par défaut du profil de roaming

Solution :

- Mettre à jour la règle de roaming pour autoriser l'IMS :
  - Définir `ims_action: 0` pour autoriser
- Ou mettre à jour `ims_action_if_no_rules_match` du profil

Voir la Documentation sur le Roaming pour la configuration détaillée.

Problèmes EIR

Symptômes

- Appareils bloqués de manière inattendue
- Appareils volés non bloqués
- Vérification EIR échouée

Causes et Solutions Courantes

Cause 1 : Regex IMEI Incorrect

Symptômes :

- Mauvais appareils bloqués/autorisés
- La règle correspond incorrectement

Étapes de Diagnostic :

1. Interroger les règles EIR
2. Identifier quelle règle correspond
3. Tester le modèle regex contre l'IMEI réel
4. Vérifier la priorité/l'ordre de la règle

Solution :

- Mettre à jour la règle EIR avec le regex correct
- Tester le regex soigneusement avant de l'appliquer
- Considérer l'ordre des règles (première correspondance gagnante)

Cause 2 : MME Ne Pas Envoyer de Requêtes S13

Symptômes :

- La vérification EIR ne se produit jamais

- Tous les appareils sont autorisés indépendamment des règles

Étapes de Diagnostic :

1. Vérifier si le MME est configuré pour utiliser l'interface S13
2. Vérifier que le pair Diameter du MME est connecté
3. Vérifier le support de l'application S13
4. Examiner la configuration du MME

Solution :

- Configurer le MME pour effectuer des vérifications EIR via S13
- Vérifier que le pair Diameter prend en charge l'application S13 (16777252)
- Contacter l'administrateur du MME si nécessaire

Cause 3 : Pas de Règle par Défaut

Symptômes :

- Les appareils ne correspondant à aucune règle ont un comportement inattendu

Étapes de Diagnostic :

1. Interroger toutes les règles EIR
2. Vérifier si une règle de rattrapage existe
3. Vérifier l'ordre des règles

Solution :

- Ajouter une règle par défaut avec regex `.*` pour correspondre à tous les IMEIs
- Définir l'action appropriée (liste blanche ou liste noire)
- S'assurer que des règles spécifiques sont vérifiées avant la règle de rattrapage

---

Problèmes de Performance

Symptômes

- Réponses API lentes
- Délais d'attente des requêtes Diameter
- Utilisation élevée du CPU ou de la mémoire
- Panneau de Contrôle lent à charger

Causes et Solutions Courantes

Cause 1 : Charge Élevée de la Base de Données

Symptômes :

- Toutes les opérations sont lentes
- CPU de la base de données élevé
- Délais d'attente sur les requêtes

Étapes de Diagnostic :

1. Vérifier l'utilisation des ressources du serveur de base de données
2. Identifier les requêtes lentes
3. Vérifier les index manquants
4. Surveiller les modèles de requêtes

Solution :

- Optimiser les requêtes lentes
- Ajouter des index à la base de données
- Augmenter les ressources de la base de données
- Envisager l'évolutivité de la base de données
- Voir les Problèmes de Base de Données

Cause 2 : Nombre Élevé d'Abonnés

Symptômes :

- Performance dégradée au fil du temps
- La lenteur est corrélée à la croissance des abonnés
- Les opérations de liste sont particulièrement lentes

Étapes de Diagnostic :

1. Interroger le nombre total d'abonnés
2. Vérifier la taille des tables
3. Examiner les plans d'exécution des requêtes
4. Surveiller les tendances d'utilisation des ressources

Solution :

- Planifier une mise à niveau de capacité
- Optimiser les requêtes pour les grands ensembles de données
- Envisager la pagination pour les grands résultats
- Implémenter un cache si nécessaire

Cause 3 : Problèmes de Pair Diameter

Symptômes :

- Les opérations Diameter sont lentes
- Délais d'attente sur un pair spécifique
- Certains pairs rapides, d'autres lents

Étapes de Diagnostic :

1. Vérifier la page Diameter du Panneau de Contrôle
2. Identifier le pair lent
3. Tester la latence réseau vers le pair
4. Vérifier l'utilisation des ressources du pair

Solution :

- Enquêter sur les problèmes de performance du pair
- Vérifier le chemin réseau pour la congestion
- Envisager d'ajouter des pairs redondants
- Augmenter le délai d'attente Diameter si nécessaire

Cause 4 : Problèmes de Mémoire

Symptômes :

- Utilisation de la mémoire de OmniHSS élevée
- Erreurs de mémoire insuffisante
- La performance se dégrade au fil du temps

Étapes de Diagnostic :

1. Vérifier l'utilisation de la mémoire de OmniHSS sur la page Application
2. Surveiller la tendance de la mémoire
3. Vérifier les fuites de mémoire
4. Examiner les paramètres de la VM Erlang

Solution :

- Redémarrer OmniHSS pour effacer la condition temporaire
- Enquêter sur les fuites de mémoire si l'utilisation augmente continuellement
- Ajuster les paramètres de mémoire de la VM Erlang dans runtime.exs
- Planifier une mise à niveau matérielle si l'utilisation est constamment élevée

---

Problèmes d'État des Abonnés

Symptômes

- L'abonné apparaît comme attaché mais ne l'est pas
- Informations d'état obsolètes
- Informations de localisation incorrectes
- Impossible de détacher l'abonné

Causes et Solutions Courantes

Cause 1 : Crash/Redémarrage du MME

Symptômes :

- L'abonné montre un MME de service qui ne sert plus
- L'abonné ne peut pas se connecter après le redémarrage du MME
- L'état est obsolète

Étapes de Diagnostic :

1. Vérifier l'état de l'abonné pour le MME de service
2. Vérifier si le MME a redémarré
3. Vérifier l'heure de la dernière connexion du MME

Solution :

- Attendre que l'abonné se reconnecte (l'état sera mis à jour)
- Ou effacer manuellement l'état de l'abonné
- Le MME doit envoyer Cancel-Location lors du redémarrage

Cause 2 : Détachement Réseau Non Reçu

Symptômes :

- L'abonné éteint mais apparaît comme attaché
- Les sessions PDN restent dans la base de données
- La localisation n'est pas effacée

Étapes de Diagnostic :

1. Vérifier l'horodatage last_seen de l'abonné
2. Vérifier si l'état est ancien (heures ou jours)
3. Vérifier si le dispositif de l'abonné est accessible

Solution :

- L'état sera effacé lorsque l'abonné se reconnectera
- Ou attendre le délai d'expiration de l'état (si implémenté)
- Un nettoyage manuel peut être nécessaire pour un état très obsolète

Cause 3 : Corruption de la Base de Données

Symptômes :

- État incohérent à travers les tables
- Violations de clé étrangère
- L'état n'a pas de sens

Étapes de Diagnostic :

1. Interroger l'état de l'abonné directement depuis la base de données
2. Vérifier les enregistrements orphelins
3. Vérifier l'intégrité référentielle

Solution :

- Identifier et corriger les données incohérentes
- Peut nécessiter un nettoyage manuel de la base de données
- Contacter le support si la corruption est généralisée

Problèmes d'API

Symptômes

- L'API renvoie des erreurs
- Réponses API lentes
- Impossible de créer/mettre à jour des entités
- Erreurs 500

Causes et Solutions Courantes

Cause 1 : Données de Requête Invalides

Symptômes :

- Erreurs 400 ou 422
- Messages d'erreur de validation
- Champ rejeté

Étapes de Diagnostic :

1. Examiner la réponse d'erreur pour des erreurs de champ spécifiques

2. Vérifier le format de la requête API
3. Vérifier que les champs requis sont présents
4. Vérifier les types de données

Solution :

- Corriger les données de la requête pour correspondre à la référence API
- S'assurer que tous les champs requis sont inclus
- Vérifier que les références de clé étrangère existent (ID de profil, etc.)

Cause 2 : Contrainte de Clé Étrangère

Symptômes :

- Impossible de créer un abonné
- Erreur : "key_set_id n'existe pas"
- Entité référencée introuvable

Étapes de Diagnostic :

1. Identifier quelle clé étrangère échoue
2. Vérifier que l'entité référencée existe :
    - key_set_id → ensembles de clés
    - epc_profile_id → profils EPC
    - ims_profile_id → profils IMS

Solution :

- Créer d'abord l'entité référencée
- Ou utiliser l'ID d'une entité existante
- Suivre le flux de travail de provisionnement complet

Cause 3 : Connectivité à la Base de Données

Symptômes :

- Erreurs 500
- Tous les appels API échouent
- Erreurs de connexion à la base de données

Solution :

- Voir les Problèmes de Base de Données

Outils et Commandes de Diagnostic

Vérifications Rapides du Panneau de Contrôle

1. **Aperçu du Système**
    - URL : `https://[hostname]:7443/overview`
    - Vérifier : Comptes d'abonnés, sessions actives, état du système
2. **État Diameter**
    - URL : `https://[hostname]:7443/diameter`
    - Vérifier : Tous les pairs critiques connectés
3. **Santé de l'Application**
    - URL : `https://[hostname]:7443/application`
    - Vérifier : Utilisation de la mémoire, nombre de processus, temps de fonctionnement

Commandes de Diagnostic API

Vérifier la Santé du Système :

```
curl -k https://hss.example.com:8443/api/status
```

Interroger un Abonné :

```
# Par IMSI
curl -k https://hss.example.com:8443/api/subscriber/imsi/
001001123456789

# Par MSISDN
curl -k https://hss.example.com:8443/api/subscriber/msisdn/
14155551234

# Par ID
curl -k https://hss.example.com:8443/api/subscriber/1
```

Lister Tous les Abonnés :

```
curl -k https://hss.example.com:8443/api/subscriber
```

Vérifier la Configuration du Profil :

```
# Profil EPC
curl -k https://hss.example.com:8443/api/epc/profile/1
```

```
# Profil IMS
curl -k https://hss.example.com:8443/api/ims/profile/1

# Profil de Roaming
curl -k https://hss.example.com:8443/api/roaming/profile/1
```

Commandes de Diagnostic Réseau

Tester la Connectivité du Port Diameter :

```
telnet [PEER_IP] 3868
```

Vérifier le Certificat TLS :

```
openssl s_client -connect [hostname]:8443 -showcerts
```

Tester la Connectivité à la Base de Données :

```
# PostgreSQL
psql -h [DB_HOST] -U [DB_USER] -d [DB_NAME] -c "SELECT COUNT(*) FROM
subscriber;"

# MySQL
mysql -h [DB_HOST] -u [DB_USER] -p -e "SELECT COUNT(*) FROM
subscriber;" [DB_NAME]
```

Analyse des Journaux

Rechercher des Journaux pour un IMSI Spécifique :

```
grep "001001123456789" /var/log/omnihss/omnihss.log
```

Trouver des Échecs d'Authentification :

```
grep "authentication.*fail" /var/log/omnihss/omnihss.log
```

Vérifier les Événements des Pairs Diameter :

```
grep "Diameter peer" /var/log/omnihss/omnihss.log
```

Trouver des Erreurs de Base de Données :

```
grep -i "database.*error" /var/log/omnihss/omnihss.log
```

Directives d'Escalade

Quand Escalader

Escalader au support technique/ingénierie lorsque :

1. **Pannes à l'échelle du système** qui ne peuvent pas être résolues avec des procédures documentées
2. **Corruption de données** ou état incohérent de la base de données
3. **Bugs logiciels suspectés** ou comportement inattendu
4. **Problèmes de performance** qui ne peuvent pas être résolus par l'optimisation
5. **Incidents de sécurité** ou accès non autorisé
6. **Questions sur un comportement non documenté**

Informations à Fournir

Lors de l'escalade, inclure :

1. **Symptômes détaillés** - Ce qui échoue, quand, pour qui
2. **Étapes prises** - Ce que vous avez déjà fait pour le dépannage
3. **Journaux** - Extraits de journaux pertinents montrant le problème
4. **Configuration** - Portions pertinentes de runtime.exs (masquer les données sensibles)
5. **Environnement** - Version de OmniHSS, version de la base de données, version du système d'exploitation
6. **Impact** - Combien d'abonnés sont affectés, impact commercial
7. **Exemples d'abonnés** - IMSIs spécifiques montrant le problème

Critique vs Non-Critique

Problèmes Critiques (Escalader Immédiatement) :

- Système complètement hors service
- Tous les abonnés incapables de se connecter
- Corruption de la base de données
- Violation de sécurité

Problèmes Non-Critiques (Documenter et Escalader Pendant les Heures de Bureau) :

- Problèmes d'abonnés uniques qui peuvent être contournés
- Dégradation de la performance qui est gérable
- Demandes d'amélioration
- Questions de documentation

Référence des Messages d'Erreur Courants

Erreurs d'Authentification

Message d'Erreur	Cause	Solution
"Échec de la génération des vecteurs d'authentification"	Ensemble de clés manquant ou invalide	Vérifier la configuration de l'ensemble de clés
"Échec de synchronisation SQN"	SQN hors synchronisation	Attendre la resynchronisation
"Abonné non trouvé"	IMSI invalide	Vérifier l'IMSI, provisionner l'abonné
"Abonné désactivé"	enabled=false	Activer l'abonné

Erreurs Diameter

Message d'Erreur	Cause	Solution
"Délai d'attente de connexion du pair Diameter"	Problème réseau	Vérifier la connectivité réseau
"Échange CER/CEA échoué"	Mismatch de configuration	Vérifier la configuration Diameter
"Application non supportée"	Le pair ne prend pas en charge l'application requise	Vérifier les applications du pair
"Échec de la poignée de main TLS"	Problème de certificat	Vérifier les certificats

Erreurs de Base de Données

Message d'Erreur	Cause	Solution
"Connexion refusée"	Base de données hors service	Démarrer la base de données
"Échec de l'authentification"	Mauvaises identifiants	Corriger les identifiants
"Aucune connexion disponible"	Pool épuisé	Augmenter la taille du pool
"Délai d'attente de requête"	Requête lente	Optimiser les requêtes

Erreurs d'API

Message d'Erreur	Cause	Solution
"key_set_id n'existe pas"	Clé étrangère invalide	Créer l'ensemble de clés d'abord
"L'IMSI a déjà été pris"	IMSI dupliqué	Utiliser un IMSI différent ou supprimer l'existant
"Erreur de	Entrée invalide	Vérifier le format et les exigences des

Message d'Erreur	Cause	Solution
validation"	champs	

← Retour au Guide des Opérations | Suivant : Référence API →

Intégration Webhook OmniHSS

← Retour au Guide des Opérations

Table des Matières

Aperçu

OmniHSS prend en charge les **webhooks** pour notifier les systèmes externes des événements des abonnés en temps réel. Lorsque des événements spécifiques se produisent (tels que des mises à jour de localisation, des demandes d'authentification ou des enregistrements IMS), OmniHSS peut envoyer une requête HTTP POST à votre point de terminaison webhook configuré avec les données complètes du profil de l'abonné.

Qu'est-ce que les Webhooks ?

Les webhooks sont des rappels HTTP qui permettent à OmniHSS de pousser des notifications d'événements vers votre application au fur et à mesure qu'elles se produisent, plutôt que de nécessiter que votre application interroge l'API HSS pour des changements.

Avantages Clés

- **Notifications en temps réel** - Recevez des mises à jour instantanées lorsque des événements d'abonnés se produisent
- **Données complètes de l'abonné** - Chaque webhook inclut le profil complet de l'abonné (identique à `GET /api/subscriber`)
- **Automatisation pilotée par les événements** - Déclenchez des flux de travail, des analyses ou des provisionnements basés sur des événements réseau
- **Réduction des interrogations** - Pas besoin d'interroger en continu l'API

pour les changements de statut de l'abonné
- **Flexibilité d'intégration** - Connectez OmniHSS à des systèmes de facturation, des plateformes d'analytique ou des applications personnalisées

---

Comment Fonctionnent les Webhooks

Flux d'Événements

1. **Un événement se produit** - Un abonné effectue une action (attachement, mise à jour de localisation, enregistrement IMS, etc.)
2. **HSS traite l'événement** - OmniHSS gère la demande/réponse Diameter normalement
3. **Webhook déclenché** - Si un webhook est enregistré pour ce type d'événement, HSS envoie un POST HTTP à votre point de terminaison
4. **Données de l'abonné incluses** - La charge utile du webhook contient le profil complet de l'abonné au format JSON
5. **Votre application répond** - Votre point de terminaison doit renvoyer HTTP 200-299 pour accuser réception

Garanties de Livraison

- **Livraison en meilleur effort** - Les webhooks sont envoyés de manière asynchrone et ne bloquent pas les opérations réseau
- **Délai d'attente** - Les requêtes webhook expirent après 5 secondes
- **Pas de nouvelles tentatives** - Si votre point de terminaison est indisponible ou renvoie une erreur, le webhook n'est pas réessayé
- **Ordre non garanti** - Les événements peuvent arriver dans le désordre sous forte charge

Important : Les opérations réseau (authentification, mises à jour de localisation, etc.) **ne dépendent pas** de la livraison des webhooks. Si votre point de terminaison webhook est hors ligne, le service des abonnés continue normalement.

Événements Webhook

OmniHSS peut déclencher des webhooks pour les événements suivants :

Événements EPC/LTE

Événement	Déclencheur	Description
`update_location_request`	S6a ULR	L'abonné s'attache ou effectue une Mise à Jour de Zone de Suivi
`authentication_information_request`	S6a AIR	Le réseau demande des vecteurs d'authentification

Événement	Déclencheur	Description
		pour l'abonné
`purge_request`	S6a PUR	MME supprime le contexte de l'abonné (appareil éteint, détaché)
`cancel_location_answer`	S6a CLA	MME accuse réception de la désinscription de l'abonné

Événements IMS

Événement	Déclencheur	Description
`ims_registration`	Cx SAR	L'abonné s'enregistre pour le service IMS/ VoLTE
`ims_deregistration`	Cx SAR (désinscription)	L'abonné se désinscrit de l'IMS
`ims_profile_request`	Sh UDR	Le Serveur d'Application demande le profil IMS de l'abonné

Événements de Politique (PCRF)

Événement	Déclencheur	Description
`policy_request`	Gx CCR	P-GW demande une politique pour la session de données de l'abonné
`media_authorization`	Rx AAR	P-CSCF demande une autorisation média pour un appel IMS

Événements Multi-IMSI

Événement	Déclencheur	Description
`imsi_switch`	ULR pour un IMSI différent sur la même SIM	L'appareil passe à un IMSI différent sur une SIM multi-IMSI

Charge Utile Webhook

Format de Requête

Lorsqu'un événement se produit, OmniHSS envoie une requête HTTP POST à votre URL webhook configurée :

```
POST /your-webhook-endpoint HTTP/1.1
Host: your-server.com
Content-Type: application/json
X-OmniHSS-Event: update_location_request
X-OmniHSS-Event-ID: 550e8400-e29b-41d4-a716-446655440000
X-OmniHSS-Timestamp: 2025-01-15T14:30:00Z
```

```
{
  "event": "update_location_request",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "timestamp": "2025-01-15T14:30:00Z",
  "subscriber": {
    "id": 1234,
    "imsi": "001001123456789",
    "enabled": true,
    "ims_enabled": true,
    "msisdns": [
      {"id": 1, "msisdn": "14155551001"},
      {"id": 2, "msisdn": "14155551002"}
    ],
    "sim": {
      "id": 5678,
      "iccid": "89911012000003204510",
      "is_esim": false
    },
    "key_set": {
      "id": 100,
      "amf": "8000"
    },
    "epc_profile": {
      "id": 1,
      "name": "Premium 100Mbps",
      "ue_ambr_dl_kbps": 100000,
      "ue_ambr_ul_kbps": 50000
    },
    "ims_profile": {
      "id": 1,
      "name": "Standard VoLTE"
    },
    "roaming_profile": {
      "id": 1,
      "name": "Roaming International Autorisé"
    },
    "subscriber_state": {
      "mme_host": "mme-01.example.com",
      "mme_realm": "epc.mnc001.mcc001.3gppnetwork.org",
      "visited_plmn": "001001",
      "last_update": "2025-01-15T14:30:00Z"
    },
    "custom_attributes": {
      "account_type": "premium",
      "billing_plan": "unlimited"
    }
  },
  "event_context": {
    "visited_plmn": "310410",
```

```
    "mme_host": "mme-roaming.example.com",
    "location_update_type": "initial_attach"
  }
}
```

Structure de la Charge Utile

Champ	Type	Description
`event`	string	Type d'événement (ex. `update_location_request`)
`event_id`	string	UUID unique pour cette livraison de webhook
`timestamp`	string	Horodatage ISO 8601 lorsque l'événement s'est produit
`subscriber`	object	**Profil complet de l'abonné** (identique à `GET /api/subscriber/:id`)
`event_context`	object	Données contextuelles supplémentaires spécifiques à l'événement

Champs de Contexte d'Événement

L'objet `event_context` contient des informations spécifiques à l'événement :

Pour `update_location_request`:

```
{
  "visited_plmn": "310410",
  "mme_host": "mme-roaming.example.com",
  "mme_realm": "epc.mnc410.mcc310.3gppnetwork.org",
  "location_update_type": "initial_attach"
}
```

Pour `imsi_switch`:

```
{
  "previous_imsi": "001001111111111",
  "new_imsi": "310410222222222",
  "sim_id": 5678,
  "previous_mme_host": "mme-home.example.com",
  "new_mme_host": "mme-roaming.example.com"
}
```

Pour `ims_registration`:

```
{
  "scscf_host": "scscf-01.ims.example.com",
  "public_identities": [
    "sip:001001123456789@ims.mnc001.mcc001.3gppnetwork.org",
    "sip:+14155551001@ims.example.com",
    "tel:+14155551001"
  ]
```

```
}
```

En-têtes HTTP

En-tête	Description	Exemple
`Content-Type`	Toujours `application/json`	`application/json`
`X-OmniHSS-Event`	Type d'événement	`update_location_request`
`X-OmniHSS-Event-ID`	Identifiant unique de l'événement	UUID
`X-OmniHSS-Timestamp`	Horodatage de l'événement	Format ISO 8601
`User-Agent`	Version d'OmniHSS	`OmniHSS/1.0`

Configuration

Enregistrement des Webhooks

Les webhooks sont configurés via l'API OmniHSS.

Enregistrer un Webhook

```
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": [
        "update_location_request",
        "ims_registration",
        "imsi_switch"
      ],
      "enabled": true,
      "description": "Webhook du système de facturation de production"
    }
  }'
```

Réponse :

```
{
  "data": {
    "id": 1,
    "url": "https://your-server.com/omnihss-webhook",
    "events": [
      "update_location_request",
      "ims_registration",
      "imsi_switch"
    ],
```

```
    "enabled": true,
    "description": "Webhook du système de facturation de production",
    "created_at": "2025-01-15T14:00:00Z"
  }
}
```

Lister les Webhooks

```
curl -k https://hss.example.com:8443/api/webhook
```

Mettre à Jour un Webhook

```
curl -k -X PUT https://hss.example.com:8443/api/webhook/1 \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "enabled": false
    }
  }'
```

Supprimer un Webhook

```
curl -k -X DELETE https://hss.example.com:8443/api/webhook/1
```

Exigences du Point de Terminaison Webhook

Votre point de terminaison webhook doit :

1. **Accepter les requêtes POST** avec `Content-Type: application/json`
2. **Répondre rapidement** - Renvoyer HTTP 200-299 dans les 5 secondes
3. **Être idempotent** - Gérer les livraisons en double avec grâce
4. **Utiliser HTTPS** - Pour la sécurité, utilisez des points de terminaison TLS/SSL (recommandé)
5. **Valider les charges utiles** - Vérifiez que la requête provient d'OmniHSS (voir section Sécurité)

Exemple de Gestionnaire de Webhook (Node.js/Express) :

```
const express = require('express');
const app = express();

app.post('/omnihss-webhook', express.json(), (req, res) => {
  const { event, subscriber, event_context } = req.body;

  console.log(`Événement reçu : ${event}`);
  console.log(`IMSI de l'abonné : ${subscriber.imsi}`);

  // Traiter les données de l'abonné
```

```
  // ... votre logique métier ici ...

  // Répondre immédiatement pour accuser réception
  res.status(200).json({ received: true });

  // Gérer le traitement asynchrone après la réponse
  processWebhook(req.body).catch(console.error);
});

async function processWebhook(payload) {
  // Votre logique de traitement asynchrone
  // ex. : mise à jour du système de facturation, déclenchement
d'analyses, etc.
}

app.listen(3000);
```

Cas d'Utilisation

1. Suivi de Facturation et d'Utilisation en Temps Réel

Suivez l'utilisation du réseau par les abonnés et déclenchez des événements de facturation en temps réel.

Avantages :

- Détectez instantanément lorsque les abonnés se déplacent à l'international
- Appliquez des frais de roaming appropriés en temps réel
- Suivez avec précision les heures de début/fin de session
- Générez des alertes d'utilisation lorsque des seuils sont atteints

2. Analytique et Surveillance

Alimentez les données d'activité des abonnés dans des plateformes d'analytique pour des tableaux de bord et des rapports en temps réel.

Cas d'Utilisation : Suivre les abonnés actifs par région

```
// Gestionnaire de webhook alimentant des données à la plateforme
d'analytique
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'update_location_request') {
    await analytics.track({
      event: 'subscriber_location_update',
      imsi: subscriber.imsi,
```

```
      visited_plmn: event_context.visited_plmn,
      timestamp: req.body.timestamp,
      profile: subscriber.epc_profile.name
    });
  }

  res.status(200).send();
});
```

Tableau de Bord d'Analytique :

- Abonnés actifs par MME
- Abonnés en roaming par pays
- Distribution des niveaux de service
- Taux de réussite d'enregistrement IMS

3. Détection de Fraude et Sécurité

Détectez des modèles d'activité suspects en temps réel et déclenchez des réponses automatisées.

Scénarios de Détection de Fraude :

1. **Changements de Localisation Rapides**
    - L'abonné s'attache dans le Pays A
    - 30 minutes plus tard, s'attache dans le Pays B (physiquement impossible)
    - Action : Marquer le compte, envoyer une alerte à l'équipe de sécurité
2. **Abus de Changement d'IMSI**
    - Multiples changements rapides d'IMSI sur la même SIM
    - Possibilité de clonage de SIM ou d'utilisation non autorisée de multi-IMSI
    - Action : Désactiver tous les IMSI sur la SIM, notifier l'équipe de fraude
3. **Roaming Non Autorisé**
    - L'abonné se déplace vers un pays bloqué (sanctions, risque de fraude)
    - Action : Désactiver automatiquement l'abonné, bloquer l'accès au réseau

Exemple de Mise en Œuvre :

```
@app.route('/omnihss-webhook', methods=['POST'])
def webhook_handler():
    data = request.json
    subscriber = data['subscriber']
```

```
    event_context = data.get('event_context', {})

    if data['event'] == 'update_location_request':
        visited_plmn = event_context.get('visited_plmn')

        # Vérifier les pays bloqués
        if visited_plmn in BLOCKED_PLMNS:
            disable_subscriber(subscriber['imsi'])
            alert_security_team(subscriber, 'Roaming vers PLMN bloqué')

        # Vérifier les voyages impossibles
        if is_impossible_travel(subscriber['imsi'], visited_plmn):
            flag_for_review(subscriber['imsi'])
            alert_fraud_team(subscriber, 'Voyage impossible détecté')

    return jsonify({'status': 'ok'}), 200
```

4. Automatisation de Provisionnement

Provisionnez ou mettez à jour automatiquement les services des abonnés en fonction des événements réseau.

Cas d'Utilisation : Activer automatiquement IMS lorsque l'abonné utilise VoLTE pour la première fois

```
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber } = req.body;

  if (event === 'ims_registration' && !subscriber.ims_enabled) {
    // Premier utilisateur IMS - activer IMS de manière permanente
    await omnihss.updateSubscriber(subscriber.id, {
      ims_enabled: true,
      custom_attributes: {
        ...subscriber.custom_attributes,
        volte_activated_at: new Date().toISOString()
      }
    });

    // Mettre à jour le CRM
    await crm.updateCustomer(subscriber.imsi, {
      features: ['volte']
    });
  }

  res.status(200).send();
});
```

5. Notifications aux Clients

Envoyez des notifications en temps réel aux clients concernant leur service.

Cas d'Utilisation : Message de bienvenue lors du roaming à l'international

Exemples de Notifications :

- "Bienvenue à [Pays] ! Des frais de roaming s'appliquent."
- "Vous avez utilisé 80 % de votre allocation de données"
- "Le service VoLTE est maintenant actif sur votre appareil"
- "Votre compte a été mis à niveau vers Premium"

6. Gestion de SIM Multi-IMSI

Suivez et gérez les abonnés avec des SIM multi-IMSI, recevant des notifications lorsqu'ils changent d'IMSI.

```
app.post('/omnihss-webhook', async (req, res) => {
  const { event, subscriber, event_context } = req.body;

  if (event === 'imsi_switch') {
    const { previous_imsi, new_imsi, sim_id } = event_context;

    // Enregistrer le changement d'IMSI pour l'analytique
    await db.logImsiSwitch({
      sim_id,
      from_imsi: previous_imsi,
      to_imsi: new_imsi,
      timestamp: req.body.timestamp
    });

    // Mettre à jour le système de facturation
    await billing.endSession(previous_imsi);
    await billing.startSession(new_imsi);

    // Alerter si changement excessif (risque de fraude)
    const switchCount = await db.getSwitchCount(sim_id, '24h');
    if (switchCount > 10) {
      await alertFraudTeam(`Changement excessif d'IMSI : SIM
${sim_id}`);
    }
  }

  res.status(200).send();
});
```

7. Intégration avec des Systèmes Externes

Connectez OmniHSS à des systèmes tiers sans interroger.

Exemples d'Intégrations :

- **Systèmes CRM** - Mettre à jour les dossiers clients avec l'utilisation des services
- **Surveillance du Réseau** - Alimenter les données des abonnés dans des plateformes d'analytique réseau
- **Systèmes de Facturation** - Déclencher des frais basés sur des événements réseau
- **Systèmes de Billetterie** - Créer automatiquement des tickets pour des authentifications échouées
- **Entrepôts de Données** - Diffuser des événements d'abonnés pour une analyse de big data

---

Considérations de Sécurité

Secret/Signature de Webhook

Pour vérifier que les webhooks proviennent d'OmniHSS, implémentez la vérification de signature :

```
# Configurer le webhook avec un secret
curl -k -X POST https://hss.example.com:8443/api/webhook \
  -H "Content-Type: application/json" \
  -d '{
    "webhook": {
      "url": "https://your-server.com/omnihss-webhook",
      "events": ["update_location_request"],
      "secret": "your-secret-key-here"
    }
  }'
```

OmniHSS inclura un en-tête `X-OmniHSS-Signature` :

```
X-OmniHSS-Signature:
sha256=5d7a8f9b2c1e3a4d6f7e8b9c0a1b2c3d4e5f6a7b8c9d0e1f2a3b4c5d6e7f8a9b
```

Vérifiez la signature :

```
const crypto = require('crypto');

function verifyWebhook(req) {
  const signature = req.headers['x-omnihss-signature'];
  const secret = process.env.WEBHOOK_SECRET;
```

```
  const payload = JSON.stringify(req.body);

  const expectedSignature = 'sha256=' +
    crypto.createHmac('sha256', secret)
      .update(payload)
      .digest('hex');

  return crypto.timingSafeEqual(
    Buffer.from(signature),
    Buffer.from(expectedSignature)
  );
}

app.post('/omnihss-webhook', (req, res) => {
  if (!verifyWebhook(req)) {
    return res.status(401).json({ error: 'Signature invalide' });
  }

  // Traiter le webhook...
  res.status(200).send();
});
```

Meilleures Pratiques

1. **Utilisez HTTPS** - Utilisez toujours TLS pour les points de terminaison webhook
2. **Validez les signatures** - Vérifiez les signatures des webhooks pour éviter le spoofing
3. **Limitation de taux** - Implémentez une limitation de taux sur les points de terminaison webhook
4. **Liste blanche d'IP** - Restreignez l'accès au webhook aux adresses IP d'OmniHSS
5. **Surveillez les échecs** - Suivez les échecs de livraison et les erreurs des webhooks
6. **Assainissez les données** - Validez et assainissez les charges utiles des webhooks avant traitement
7. **Sécurisez les identifiants** - Stockez les secrets de webhook dans une configuration sécurisée (variables d'environnement, gestionnaire de secrets)

Confidentialité des Données

Les charges utiles des webhooks contiennent des **informations sensibles sur les abonnés** :

- IMSI (identité de l'abonné)
- MSISDNs (numéros de téléphone)
- Données de localisation (PLMN visité, MME)
- Informations sur le profil de service

Exigences de Conformité :

- **RGPD** - Assurez-vous que les données des webhooks sont traitées conformément au RGPD
- **Conservation des données** - Mettez en œuvre des politiques de conservation des données appropriées
- **Contrôle d'accès** - Restreignez l'accès au point de terminaison webhook
- **Chiffrement** - Utilisez TLS pour le transport des webhooks
- **Journalisation d'audit** - Journalisez toutes les livraisons de webhooks pour la conformité

Dépannage

Webhook Non Reçu

Symptômes :

- Des événements se produisent mais le webhook n'est pas déclenché
- Le point de terminaison webhook ne reçoit jamais de requêtes

Étapes de Dépannage :

1. **V��rifiez que le webhook est activé :**

   ```
   curl -k https://hss.example.com:8443/api/webhook
   # Vérifiez "enabled": true
   ```

2. **Vérifiez la configuration des événements du webhook :**

   - Assurez-vous que le type d'événement est inclus dans la liste des `events` du webhook
   - Exemple : Si vous souhaitez des événements `ims_registration`, vérifiez qu'il est dans le tableau des événements

3. **Examinez les journaux HSS :**

   - Vérifiez les erreurs de livraison des webhooks
   - Recherchez des problèmes de connectivité réseau
   - Vérifiez qu'il n'y a pas d'échecs de résolution DNS

4. **Testez l'accessibilité du point de terminaison :**

   ```
   curl -X POST https://your-server.com/omnihss-webhook \
     -H "Content-Type: application/json" \
     -d '{"test": true}'
   ```

Délai d'Attente du Webhook

Symptômes :

- Les journaux HSS montrent des erreurs de délai d'attente du webhook
- Le point de terminaison webhook reçoit la requête mais HSS la marque comme échouée

Solution :

1. **Répondez immédiatement :**
    - Renvoyez HTTP 200 dans les 5 secondes
    - Traitez les données de manière asynchrone après avoir répondu
2. **Optimisez les performances du point de terminaison :**

```
// MAUVAIS - Traitement synchrone lent
app.post('/webhook', (req, res) => {
  processData(req.body); // Bloque pendant 10 secondes
  res.status(200).send();
});

// BON - Traitement asynchrone après réponse
app.post('/webhook', (req, res) => {
  res.status(200).send(); // Répondre immédiatement
  processData(req.body); // Traiter asynchrone
});
```

Webhooks Dupliqués

Symptômes :

- Même événement livré plusieurs fois
- `event_id` est identique pour les livraisons dupliquées

Cause :

- Réessais réseau (bien qu'OmniHSS ne réessaie pas, l'infrastructure réseau pourrait)
- Plusieurs webhooks enregistrés pour le même événement

Solution :

Implémentez l'idempotence en utilisant `event_id` :

```
const processedEvents = new Set();

app.post('/omnihss-webhook', (req, res) => {
```

```
  const eventId = req.body.event_id;

  if (processedEvents.has(eventId)) {
    // Déjà traité, sauter
    return res.status(200).json({ status: 'duplicate' });
  }

  processedEvents.add(eventId);

  // Traiter le webhook...
  processWebhook(req.body);

  res.status(200).json({ status: 'processed' });
});
```

Erreur de Retour du Webhook

Symptômes :

- Le point de terminaison renvoie HTTP 4xx ou 5xx
- Les journaux HSS montrent un échec de livraison du webhook

Erreurs Courantes :

1. **401 Non Autorisé** - Échec de la vérification de la signature
    - Vérifiez que le secret du webhook correspond à la configuration
    - Vérifiez l'algorithme de calcul de la signature
2. **400 Mauvaise Requête** - Charge utile invalide
    - Vérifiez le traitement de la charge utile du webhook
    - Assurez-vous que l'en-tête Content-Type est géré
3. **500 Erreur Interne du Serveur** - Le point de terminaison a échoué
    - Examinez les journaux d'erreur du point de terminaison
    - Ajoutez une gestion des erreurs et des journaux

Solution :

Ajoutez une gestion des erreurs complète :

```
app.post('/omnihss-webhook', async (req, res) => {
  try {
    // Vérifiez la signature
    if (!verifyWebhook(req)) {
      return res.status(401).json({ error: 'Signature invalide' });
    }
```

```
    // Validez la charge utile
    if (!req.body.event || !req.body.subscriber) {
      return res.status(400).json({ error: 'Charge utile invalide' });
    }

    // Traitez le webhook
    await processWebhook(req.body);

    res.status(200).json({ status: 'ok' });

  } catch (error) {
    console.error('Erreur de traitement du webhook :', error);
    // Renvoyer 200 pour éviter le réessai, journaliser l'erreur pour
enquête
    res.status(200).json({ status: 'error', message: error.message });
  }
});
```

Données d'Abonné Manquantes

Symptômes :

- Webhook reçu mais l'objet abonné est incomplet
- Les champs attendus sont nuls ou manquants

Causes Possibles :

1. **Abonné pas complètement provisionné** - Certains profils peuvent être optionnels (IMS, roaming)
2. **Condition de course de données** - Abonné mis à jour entre le déclenchement de l'événement et l'envoi du webhook

Solution :

Gérez les champs optionnels avec grâce :

```
const { subscriber } = req.body;

// Vérifiez les champs optionnels
const imsProfile = subscriber.ims_profile || { name: 'Pas d\'IMS' };
const roamingProfile = subscriber.roaming_profile || { name: 'Pas de
Roaming' };

// Gérer les MSISDNs manquants
const msisdns = subscriber.msisdns || [];
```

Surveillance et Observabilité

Métriques de Webhook

Suivez les performances et la fiabilité des webhooks :

Métriques à Surveiller :

- Taux de livraison des webhooks (réussite vs. échec)
- Latence des webhooks (temps entre l'événement et la réponse du point de terminaison)
- Temps de réponse du point de terminaison
- Taux d'erreur par point de terminaison
- Événements par seconde

Exemple de Requête de Tableau de Bord (Prometheus/Grafana) :

```
# Taux de réussite des webhooks
rate(omnihss_webhook_success_total[5m]) /
rate(omnihss_webhook_attempts_total[5m])

# Latence des webhooks
histogram_quantile(0.95, omnihss_webhook_duration_seconds)
```

Journaux de Webhook

Activez la journalisation détaillée des webhooks pour le dépannage :

Format de Journal :

```
{
  "timestamp": "2025-01-15T14:30:00Z",
  "level": "info",
  "component": "webhook",
  "event_id": "550e8400-e29b-41d4-a716-446655440000",
  "webhook_id": 1,
  "event_type": "update_location_request",
  "subscriber_imsi": "001001123456789",
  "endpoint": "https://your-server.com/omnihss-webhook",
  "http_status": 200,
  "duration_ms": 145,
  "error": null
}
```

← Retour au Guide des Opérations | Suivant : Référence API →