



Guide des opérations OmniPGW

OmniPGW - Plan de contrôle de la passerelle de paquets (PGW-C)

par *Omnitouch Network Services*

Table des matières

1. [Aperçu](#)
 2. [Architecture](#)
 3. [Interfaces réseau](#)
 4. [Concepts clés](#)
 5. [Prise en main](#)
 6. [Configuration](#)
 7. [Interface Web - Tableau de bord des opérations en temps réel](#)
 8. [Surveillance et métriques](#)
 9. [Documentation détaillée](#)
 10. [Ressources supplémentaires](#)
 11. [Contributions](#)
 12. [Support](#)
-

Aperçu

OmniPGW est une implémentation de haute performance du Plan de contrôle de la passerelle de paquets (PGW-C) pour les réseaux 3GPP LTE Evolved Packet Core (EPC), développée par Omnitouch Network Services. Il gère les fonctions du plan de contrôle pour les sessions de données, y compris :

- **Gestion des sessions** - Création, modification et terminaison des sessions de données UE (Équipement Utilisateur)
- **Attribution d'adresses IP** - Attribution d'adresses IP aux appareils mobiles à partir de pools configurés
- **Contrôle des politiques et de la facturation** - Interface avec PCRF pour l'application des politiques et la facturation
- **Coordination du plan utilisateur** - Contrôle du PGW-U (Plan utilisateur) pour le transfert de paquets

Ce que fait PGW-C

- **Accepte les demandes de session** de SGW-C via l'interface S5/S8 (GTP-C)

- **Alloue des adresses IP UE** à partir de pools de sous-réseaux configurés
 - **Demande des décisions de politique** à PCRF via l'interface Gx (Diameter)
 - **Programme des règles de transfert** dans PGW-U via l'interface Sxb (PFCP)
 - **Gère l'application QoS** à travers des contextes de bearer et des règles QoS
 - **Suit les informations de facturation** pour les systèmes de facturation
-

Architecture

Aperçu des composants

Architecture des processus

PGW-C est construit sur Elixir/OTP et utilise une architecture de processus supervisée :

- **Superviseur d'application** - Superviseur de niveau supérieur gérant tous les composants
- **Courtiers de protocole** - Gèrent les messages de protocole entrants/sortants
- **Processus de session** - Un GenServer par connexion PDN active
- **Registres** - Suivent les ressources allouées (IPs, TEIDs, SEIDs, etc.)
- **Gestionnaire de nœud PFCP** - Maintient les associations PFCP avec les pairs PGW-U

Chaque composant est supervisé et redémarrera automatiquement en cas de défaillance, garantissant la fiabilité du système.

Interfaces réseau

PGW-C implémente trois interfaces 3GPP principales :

Interface S5/S8 (GTP-C v2)

But : Signalisation du plan de contrôle entre SGW-C et PGW-C

Protocole : GTP-C Version 2 sur UDP

Messages clés :

- Demande/Réponse de création de session
- Demande/Réponse de suppression de session

- Demande/Réponse de création de bearer
- Demande/Réponse de suppression de bearer

Configuration : Voir [Configuration S5/S8](#)

Interface Sxb (PFCP)

But : Signalisation du plan de contrôle entre PGW-C et PGW-U

Protocole : PFCP (Protocole de contrôle de transfert de paquets) sur UDP

Messages clés :

- Demande/Réponse de configuration d'association
- Demande/Réponse d'établissement de session
- Demande/Réponse de modification de session
- Demande/Réponse de suppression de session
- Demande/Réponse de heartbeat

Configuration : Voir [Documentation de l'interface PFCP/Sxb](#)

Interface Gx (Diameter)

But : Interface de la fonction de règles de politique et de facturation (PCRF)

Protocole : Diameter (RFC IETF 6733)

Messages clés :

- Demande/Réponse de contrôle de crédit initial (CCR-I/CCA-I)
- Demande/Réponse de contrôle de crédit de terminaison (CCR-T/CCA-T)

Configuration : Voir [Documentation de l'interface Diameter Gx](#)

Concepts clés

Session PDN

Une session PDN (Packet Data Network) représente la connexion de données d'un UE à un réseau externe (comme Internet). Chaque session a :

- **Adresse IP UE** - Allouée à partir d'un pool de sous-réseaux configuré
- **APN** (Nom de point d'accès) - Identifie le réseau externe
- **Contexte de bearer** - Contient des paramètres QoS et des informations de tunnel
- **ID de facturation** - Identifiant unique pour la facturation

- **TEID** (Identifiant de point de terminaison de tunnel) - Identifiant de tunnel de l'interface S5/S8
- **SEID** (Identifiant de point de terminaison de session) - Identifiant de session de l'interface Sxb

Contexte de bearer

Un bearer représente un flux de trafic avec des caractéristiques QoS spécifiques :

- **Bearer par défaut** - Créé avec chaque session PDN
- **Bearers dédiés** - Bearers supplémentaires pour des besoins QoS spécifiques
- **EBI** (Identifiant de bearer EPS) - Identifiant unique pour chaque bearer
- **Paramètres QoS** - QCI, ARP, débits (MBR, GBR)

Règles PFCP

Le PGW-C programme le PGW-U avec des règles de traitement des paquets :

- **PDR** (Règle de détection de paquets) - Correspond aux paquets (montant/ descendant)
- **FAR** (Règle d'action de transfert) - Spécifie le comportement de transfert
- **QER** (Règle d'application QoS) - Applique des limites de débit
- **BAR** (Règle d'action de mise en tampon) - Contrôle la mise en tampon des paquets

Voir [Documentation de l'interface PFCP](#) pour plus de détails.

Attribution d'adresses IP

Les adresses IP des UE sont attribuées à partir de pools de sous-réseaux configurés :

- **Sélection basée sur l'APN** - Différents APN peuvent utiliser différents sous-réseaux
- **Attribution dynamique** - Sélection aléatoire d'une IP dans la plage disponible
- **Attribution statique** - Support pour les adresses IP demandées par l'UE
- **Détection de collision** - Assure une attribution d'IP unique

Voir [Attribution de pool IP UE](#) pour la configuration.

Prise en main

Prérequis

- Elixir ~1.16
- Erlang/OTP 26+
- Connectivité réseau vers SGW-C, PGW-U et PCRF
- Compréhension de l'architecture EPC LTE

Démarrer OmniPGW

1. **Configurer les paramètres d'exécution** dans config/runtime.exs
2. **Compiler l'application :**

```
mix deps.get  
mix compile
```

3. **Démarrer l'application :**

```
mix run --no-halt
```

Vérification du fonctionnement

Vérifiez les journaux pour un démarrage réussi :

```
[info] Démarrage d'OmniPGW...  
[info] Démarrage de l'exportateur de métriques sur 127.0.0.42:42069  
[info] Démarrage du courtier S5/S8 sur 127.0.0.10  
[info] Démarrage du courtier Sxb sur 127.0.0.20  
[info] Démarrage du courtier Gx  
[info] Démarrage du gestionnaire de nœud PFCP  
[info] OmniPGW démarré avec succès
```

Accédez aux métriques à <http://127.0.0.42:42069/metrics> (adresse configurée).

Configuration

Toute la configuration d'exécution est définie dans config/runtime.exs. La configuration est structurée en plusieurs sections :

Aperçu de la configuration

Référence rapide de configuration

Section	But	Documentation
metrics	Exportateur de métriques Prometheus	Guide de surveillance
diameter	Interface Gx vers PCRF	Configuration Diameter Gx
s5s8	Interface GTP-C vers SGW-C	Configuration S5/S8
sxb	Interface PFCP vers PGW-U	Configuration PFCP
ue	Pools d'adresses IP UE	Configuration du pool IP
pco	Options de configuration de protocole	Configuration PCO

Voir le [Guide de configuration complet](#) pour des informations détaillées.

Interface Web - Tableau de bord des opérations en temps réel

OmniPGW comprend une **Interface Web** intégrée pour la surveillance et les opérations en temps réel, offrant une visibilité instantanée sur l'état du système sans avoir besoin d'outils en ligne de commande ou de requêtes de métriques.

Accéder à l'Interface Web

`http://<omnipgw-ip>:<web-port>/`

Pages disponibles :

Page	URL	But	Taux de rafraîchissement
Sessions PGW	<code>/pgw_sessions</code>	Voir toutes les sessions PDN actives	2 secondes
Sessions PFCP	<code>/pfcp_sessions</code>	Voir les sessions PFCP avec PGW-U	2 secondes
État UPF	<code>/upf_status</code>	Surveiller les associations de pairs PFCP	2 secondes
Pairs Diameter	<code>/diameter</code>	Surveiller la connectivité PCRF	1 seconde
Journaux	<code>/logs</code>	Diffusion en temps réel des journaux	En direct

Fonctionnalités clés

Mises à jour en temps réel :

- Toutes les pages se rafraîchissent automatiquement (pas de recharge manuel nécessaire)
- Diffusion de données en direct depuis les processus OmniPGW
- Indicateurs de statut codés par couleur (vert/rouge)

Recherche et filtrage :

- Rechercher des sessions par IMSI, IP, MSISDN ou APN
- Filtrage instantané sans recharge de page

Détails extensibles :

- Cliquez sur n'importe quelle ligne pour voir tous les détails
- Inspecter l'état complet de la session
- Voir la configuration et les capacités des pairs

Aucune authentification requise (usage interne) :

- Accès direct depuis le réseau de gestion
- Conçu pour l'utilisation par l'équipe NOC/opérations
- Lier uniquement à l'IP de gestion pour des raisons de sécurité

Flux de travail opérationnels

Dépannage de session :

1. L'utilisateur signale un problème de connexion
2. Ouvrir la page des sessions PGW
3. Rechercher par IMSI ou numéro de téléphone
4. Vérifier que la session existe et a :
 - Adresse IP UE allouée
 - Paramètres QoS de PCRF
 - Points de terminaison de tunnel établis
5. Si aucune session trouvée → Vérifier la page Diameter pour la connectivité PCRF

Vérification de la santé du système :

1. Ouvrir la page État UPF → Vérifier que tous les pairs PGW-U sont "Associés"
2. Ouvrir la page Diameter → Vérifier que tous les pairs PCRF sont "Connectés"
3. Ouvrir les sessions PGW → Vérifier le nombre de sessions actives par rapport à la capacité

Surveillance de la capacité :

- Jeter un coup d'œil au nombre de sessions PGW
- Comparer à la capacité sous licence/attendue

- Identifier les pics d'utilisation
- Surveiller la distribution entre les APN

Interface Web vs. Métriques

Utilisez l'Interface Web pour :

- Détails de session individuels
- État des pairs en temps réel
- Vérifications rapides de la santé
- Dépannage d'utilisateurs spécifiques
- Vérification de la configuration

Utilisez les métriques Prometheus pour :

- Tendances historiques
- Alertes et notifications
- Graphiques de planification de capacité
- Analyse de performance
- Surveillance à long terme

Meilleure pratique : Utilisez les deux ensemble - Interface Web pour les opérations immédiates, Prometheus pour les tendances et les alertes.

Surveillance et métriques

En plus de l'Interface Web, OmniPGW expose des métriques compatibles avec Prometheus pour la surveillance :

Métriques disponibles

- **Métriques de session**
 - teid_registry_count - Sessions S5/S8 actives
 - seid_registry_count - Sessions PFCP actives
 - session_id_registry_count - Sessions Gx actives
 - address_registry_count - Adresses IP UE allouées
 - charging_id_registry_count - IDs de facturation actifs
- **Métriques de message**
 - s5s8_inbound_messages_total - Messages GTP-C reçus
 - sxb_inbound_messages_total - Messages PFCP reçus
 - gx_inbound_messages_total - Messages Diameter reçus
 - Durées de traitement des messages
- **Métriques d'erreur**

- s5s8_inbound_errors_total - Erreurs de protocole S5/S8
- sxb_inbound_errors_total - Erreurs de protocole PFCP
- gx_inbound_errors_total - Erreurs Diameter

Accéder aux métriques

Les métriques sont exposées via HTTP à l'endpoint configuré :

```
curl http://127.0.0.42:42069/metrics
```

Voir [Guide de surveillance et de métriques pour la configuration du tableau de bord et des alertes](#).

Documentation détaillée

Cette section fournit un aperçu complet de toute la documentation OmniPGW. Les documents sont organisés par sujet et cas d'utilisation.

Structure de la documentation

Documentation OmniPGW		
└─ OPERATIONS.md (Ce guide)		
└─ docs/		
└─ Configuration et installation		Référence complète de
└─ configuration.md		
└─ runtime.exe		
└─ ue-ip-allocation.md	Configuration du pool IP	
└─ pco-configuration.md	Paramètres DNS, P-CSCF, MTU	
└─ Interfaces réseau		
└─ pfcp-interface.md	Sxb/PFCP (communication PGW-U)	
└─ diameter-gx.md	Gx (communication PCRF)	
└─ diameter-gy.md	Gy/Ro (communication OCS)	
└─ s5s8-interface.md	S5/S8 (communication SGW-C)	
└─ Opérations		
└─ session-management.md	Cycle de vie de la session PDN	
└─ monitoring.md	Métriques Prometheus et alertes	

Documentation par sujet

◊ Prise en main

Document	Description	But
OPERATIONS.md	Guide principal des opérations (ce	Aperçu et prise en

Document	Description	But
document)		main

❖ Configuration

Document	Description	Lignes
configuration.md	Référence complète de runtime.exs	1,600+
ue-ip-allocation.md	Gestion et allocation du pool IP UE	943
pco-configuration.md	Options de configuration de protocole (DNS, P-CSCF, MTU)	344

❖ Interfaces réseau

Document	Description	Lignes
pfcp-interface.md	Interface PFCP/Sxb vers PGW-U	1,355
diameter-gx.md	Interface Diameter Gx vers PCRF (Contrôle de politique)	941
diameter-gy.md	Interface Diameter Gy/Ro vers OCS (Facturation en ligne)	1,100+
s5s8-interface.md	Interface GTP-C S5/S8 vers SGW-C	456

❖ Opérations et surveillance

Document	Description	Lignes
session-management.md	Cycle de vie et opérations de session PDN	435
monitoring.md	Métriques Prometheus, tableaux de bord Grafana, alertes	807

Fonctionnalités de la documentation

❖ Diagrammes Mermaid

Tous les documents incluent des **diagrammes Mermaid** pour une compréhension visuelle :

- Diagrammes d'architecture
- Diagrammes de séquence (flux de messages)
- Machines d'état
- Topologie réseau

❖ Exemples pratiques

Chaque document comprend :

- Exemples de configuration du monde réel
- Configurations prêtes à copier-coller
- Cas d'utilisation courants

◊ Dépannage

Chaque document d'interface comprend :

- Problèmes courants et solutions
- Commandes de débogage
- Métriques pour le diagnostic

◊ Renvois croisés

Les documents sont largement interconnectés pour une navigation facile.

Chemins de lecture

Pour les opérateurs réseau

1. [OPERATIONS.md](#) - Aperçu (ce document)
2. [configuration.md](#) - Installation
3. [monitoring.md](#) - Surveillance
4. [session-management.md](#) - Opérations quotidiennes

Pour les ingénieurs réseau

1. [OPERATIONS.md](#) - Aperçu de l'architecture (ce document)
2. [pfcp-interface.md](#) - Contrôle du plan utilisateur
3. [diameter-gx.md](#) - Contrôle de politique
4. [diameter-gy.md](#) - Facturation en ligne
5. [s5s8-interface.md](#) - Gestion des sessions
6. [ue-ip-allocation.md](#) - Gestion des IP

Pour la configuration et le déploiement

1. [configuration.md](#) - Référence complète
2. [ue-ip-allocation.md](#) - Pools IP
3. [pco-configuration.md](#) - Paramètres réseau
4. [monitoring.md](#) - Configuration de la surveillance

Statistiques du document

- **Documents totaux :** 10
- **Lignes totales :** ~7,300+
- **Taille totale :** ~180 Ko
- **Diagrammes Mermaid :** 65+

- **Exemples de code : 120+**

Concepts clés couverts

Architecture

- ♦ Séparation du plan de contrôle/plan utilisateur
- ♦ Architecture OTP/Elixir
- ♦ Supervision des processus
- ♦ Sessions basées sur GenServer

Protocoles

- ♦ PFCP (Protocole de contrôle de transfert de paquets)
- ♦ GTP-C v2 (Protocole de tunneling GPRS)
- ♦ Diameter (RFC 6733)

Interfaces 3GPP

- ♦ Sxb (PGW-C ↔ PGW-U)
- ♦ Gx (PGW-C ↔ PCRF)
- ♦ Gy/Ro (PGW-C ↔ OCS)
- ♦ S5/S8 (SGW-C ↔ PGW-C)

Opérations

- ♦ Gestion des sessions
- ♦ Stratégies d'attribution d'IP
- ♦ Application de QoS
- ♦ Intégration de la facturation
- ♦ Surveillance et alertes

Ressources supplémentaires

Spécifications 3GPP

Spécification	Titre
TS 29.274	GTP-C v2 (interface S5/S8)
TS 29.244	PFCP (interface Sxb)
TS 29.212	Interface Diameter Gx (Contrôle de politique)
TS 32.299	Applications de facturation Diameter (Gy/Ro)
TS 32.251	Facturation du domaine de paquets
TS 23.401	Architecture EPC

Documentation connexe

- README du projet : [README.md](#)
 - Fichier de configuration : [config/runtime.exs](#)
-

Contributions

Pour mettre à jour la documentation :

1. Modifier les fichiers Markdown dans `docs/`
 2. Inclure des diagrammes Mermaid pour les concepts visuels
 3. Ajouter des exemples pratiques
 4. Renvois croisés vers les documents connexes
 5. Mettre à jour OPERATIONS.md si de nouveaux documents sont ajoutés
-

Liens rapides

- [Dépôt GitHub](#)
 - [README du projet](#)
 - [Fichier de configuration](#)
-

Support

Pour des questions ou des problèmes avec OmniPGW :

- Consultez la documentation de ce guide
 - Vérifiez les exemples de configuration
 - Consultez les sections de dépannage dans les documents d'interface
 - Référez-vous au dépôt du projet pour les contributions
-

OmniPGW - *Plan de contrôle de la passerelle de paquets LTE de niveau opérateur*

Développ◆◆ par Omnitouch Network Services

Version de la documentation : 1.0 Dernière mise à jour : 2025-10-29



Guide de Configuration d'OmniPGW

Référence Complète pour la Configuration de runtime.exs

par Omnitouch Network Services

Table des Matières

1. [Aperçu](#)
 2. [Structure du Fichier de Configuration](#)
 3. [Configuration des Métriques](#)
 4. [Configuration de Diameter/Gx](#)
 5. [Configuration de S5/S8](#)
 6. [Configuration de Sxb/PFCP](#)
 - [Stratégies de Sélection de UPF](#)
 - [Équilibrage de Charge avec des Pools de UPF](#)
 - [Sélection Basée sur DNS](#)
 - [Mode de Simulation](#)
 7. [Configuration du Pool IP UE](#)
 8. [Configuration de PCO](#)
 9. [Configuration de l'Interface Web](#)
 10. [Exemple Complet](#)
 11. [Validation de la Configuration](#)
-

Aperçu

OmniPGW utilise une **configuration runtime** définie dans config/runtime.exs. Ce fichier est évalué au **démarrage de l'application** et permet une configuration dynamique basée sur des variables d'environnement ou des sources externes.

Philosophie de Configuration

Principes Clés :

- **Source Unique de Vérité** - Toute la configuration dans un seul fichier
 - **Sécurité de Type** - Configuration validée au démarrage
 - **Flexibilité Environnementale** - Support pour dev, test, production
 - **Defaults Clairs** - Defaults sensés avec des remplacements explicites
-

Structure du Fichier de Configuration

Emplacement du Fichier

```
pgw_c/
  └── config/
      ├── config.exs          # Configuration de base (importe
      │   runtime.exs)
      ├── dev.exs              # Configuration spécifique au développement
      ├── prod.exs             # Configuration spécifique à la production
      └── runtime.exs          # ← Fichier de configuration principal
```

Structure de Niveau Supérieur

```
# config/runtime.exs
import Config

config :logger, level: :info

config :pgw_c,
  metrics: %{...},
  diameter: %{...},
  s5s8: %{...},
  sxb: %{...},
  ue: %{...},
  pco: %{...}
```

Sections de Configuration

Configuration des Métriques

Objectif

Configurer l'exportateur de métriques Prometheus pour le suivi d'OmniPGW.

Bloc de Configuration

```
config :pgw_c,
  metrics: %{
    # Activer/désactiver l'exportateur de métriques
    enabled: true,

    # Adresse IP pour lier le serveur HTTP
    ip_address: "0.0.0.0",
```

```

# Port pour le point de terminaison des métriques
port: 9090,

# Fréquence de sondage des registres (millisecondes)
registry_poll_period_ms: 10_000
}

```

Paramètres

Paramètre	Type	Par Défaut	Description
enabled	Booléen	true	Activer l'exportateur de métriques
ip_address	Chaîne (IP)	"0.0.0.0"	Adresse de liaison (0.0.0.0 = toutes les interfaces)
port	Entier	9090	Port HTTP pour le point de terminaison /metrics
registry_poll_period_ms	Entier	10_000	Intervalle de sondage pour les comptes de registre

Exemples

Production - Lier à une IP spécifique :

```

metrics: %{
  enabled: true,
  ip_address: "10.0.0.20", # Réseau de gestion
  port: 9090,
  registry_poll_period_ms: 5_000 # Sondage toutes les 5 secondes
}

```

Développement - Localhost uniquement :

```

metrics: %{
  enabled: true,
  ip_address: "127.0.0.1",
  port: 42069, # Port non standard
  registry_poll_period_ms: 10_000
}

```

Désactiver les métriques :

```

metrics: %{
  enabled: false
}

```

Accéder aux Métriques

```
# Point de terminaison par défaut
```

```
curl http://<ip_address>:<port>/metrics  
# Exemple  
curl http://10.0.0.20:9090/metrics
```

Voir : [Guide de Surveillance & Métriques](#) pour la documentation détaillée des métriques.

Configuration de Diameter/Gx

Objectif

Configurer le protocole Diameter pour l'interface Gx (communication PCRF).

Bloc de Configuration

```
config :pgw_c,  
diameter: %{  
    # Adresse IP pour écouter les connexions Diameter  
    listen_ip: "0.0.0.0",  
  
    # Identité Diameter d'OmniPGW (Origin-Host)  
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",  
  
    # Domaine Diameter d'OmniPGW (Origin-Realm)  
    realm: "epc.mnc001.mcc001.3gppnetwork.org",  
  
    # Liste des pairs PCRF  
    peer_list: [  
        %{  
            # Identité Diameter PCRF  
            host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",  
  
            # Domaine PCRF  
            realm: "epc.mnc001.mcc001.3gppnetwork.org",  
  
            # Adresse IP PCRF  
            ip: "10.0.0.30",  
  
            # Initier la connexion au PCRF  
            initiate_connection: true  
        }  
    ]  
}
```

Paramètres

Paramètre	Type	Requis	Description
listen_ip	Chaîne (IP)	Oui	Adresse d'écoute Diameter
host	Chaîne (FQDN)	Oui	Origin-Host d'OmniPGW (doit être FQDN)
realm	Chaîne (Domaine)	Oui	Origin-Realm d'OmniPGW
peer_list	Liste	Oui	Configurations des pairs PCRF

Configuration des Pairs :

Paramètre	Type	Requis	Description
host	Chaîne (FQDN)	Oui	Identité Diameter PCRF
realm	Chaîne (Domaine)	Oui	Domaine PCRF
ip	Chaîne (IP)	Oui	Adresse IP PCRF
initiate_connection	Booléen	Oui	Indique si OmniPGW se connecte au PCRF

Format FQDN

Les identités Diameter DOIVENT être des FQDN :

```
# CORRECT
host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org"
```

```
# INCORRECT
host: "omnipgw"          # Pas un FQDN
host: "10.0.0.20"        # IP non autorisée
```

Format 3GPP :

```
<hostname>.epc.mnc<MNC>.mcc<MCC>.3gppnetwork.org
```

Exemples :

- omnipgw.epc.mnc001.mcc001.3gppnetwork.org (MCC=001, MNC=001)
- pgw-c.epc.mnc260.mcc310.3gppnetwork.org (MCC=310, MNC=260 - T-Mobile US)

Exemples

Un seul PCRF :

```
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
  realm: "epc.mnc001.mcc001.3gppnetwork.org",
```

```

peer_list: [
    %{
        host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",
        realm: "epc.mnc001.mcc001.3gppnetwork.org",
        ip: "10.0.0.30",
        initiate_connection: true
    }
]
}

```

Plusieurs PCRFs (Redondance) :

```

diameter: %{
    listen_ip: "0.0.0.0",
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    peer_list: [
        %{
            host: "pcrf-primary.epc.mnc001.mcc001.3gppnetwork.org",
            realm: "epc.mnc001.mcc001.3gppnetwork.org",
            ip: "10.0.1.30",
            initiate_connection: true
        },
        %{
            host: "pcrf-backup.epc.mnc001.mcc001.3gppnetwork.org",
            realm: "epc.mnc001.mcc001.3gppnetwork.org",
            ip: "10.0.2.30",
            initiate_connection: true
        }
    ]
}

```

Connexion Initiée par le PCRF :

```

diameter: %{
    listen_ip: "0.0.0.0",
    host: "omnipgw.epc.mnc001.mcc001.3gppnetwork.org",
    realm: "epc.mnc001.mcc001.3gppnetwork.org",
    peer_list: [
        %{
            host: "pcrf.epc.mnc001.mcc001.3gppnetwork.org",
            realm: "epc.mnc001.mcc001.3gppnetwork.org",
            ip: "10.0.0.30",
            initiate_connection: false # Attendre que le PCRF se connecte
        }
    ]
}

```

Voir : [Documentation de l'Interface Diameter Gx](#)

Configuration de S5/S8

Objectif

Configurer l'interface GTP-C pour la communication avec SGW-C.

Bloc de Configuration

```
config :pgw_c,
s5s8: %{
    # Adresse IPv4 locale pour l'interface S5/S8
    local_ipv4_address: "10.0.0.20",

    # Optionnel : Adresse IPv6 locale
    local_ipv6_address: nil,

    # Optionnel : Remplacer le port GTP-C par défaut (2123)
    local_port: 2123
}
```

Paramètres

Paramètre	Type	Par Défaut	Description
local_ipv4_address	Chaîne (IPv4)	Requis	Adresse IPv4 de l'interface S5/S8
local_ipv6_address	Chaîne (IPv6)	nil	Adresse IPv6 de l'interface S5/S8 (optionnel)
local_port	Entier	2123	Port UDP pour GTP-C (port standard 2123)

Détails du Protocole

- **Protocole :** GTP-C Version 2
- **Transport :** UDP
- **Port Standard :** 2123
- **Direction :** Reçoit de SGW-C

Exemples

IPv4 Seulement (Commun) :

```
s5s8: %{
    local_ipv4_address: "10.0.0.20"
}
```

IPv4 + IPv6 Dual-Stack :

```
s5s8: %{
    local_ipv4_address: "10.0.0.20",
    local_ipv6_address: "2001:db8::20"
}
```

Port Personnalisé (Non-Standard) :

```
s5s8: %{
    local_ipv4_address: "10.0.0.20",
    local_port: 2124 # Port personnalisé
}
```

Planification Réseau

Sélection d'Adresse IP :

- Utilisez un réseau de gestion/signalisation dédié
- Assurez-vous de la connectivité depuis tous les nœuds SGW-C
- Considérez la redondance (VRRP/HSRP) pour la haute disponibilité

Règles de Pare-feu :

```
# Autoriser GTP-C depuis SGW-C
iptables -A INPUT -p udp --dport 2123 -s <sgw_c_network> -j ACCEPT
```

Configuration de Sxb/PFCP

Objectif

Configurer l'interface PFCP pour la communication avec PGW-U (Plan Utilisateur).

Bloc de Configuration

```
config :pgw_c,
sxb: %{
    # Adresse IP locale pour la communication PFCP
    local_ip_address: "10.0.0.20",

    # Optionnel : Remplacer le port PFCP par défaut (8805)
    local_port: 8805
}
```

Paramètres

Paramètre	Type	Par Défaut	Description
local_ip_address	Chaîne (IP)	Requis	Adresse d'écoute PFCP
local_port	Entier	8805	Port UDP PFCP

Important :

- **Tous les pairs UPF sont automatiquement enregistrés** à partir de la configuration `upf_selection` (règles + pool de secours) au démarrage
- Les UPF enregistrés automatiquement utilisent des valeurs par défaut sensées :
 - Nom généré automatiquement : "UPF-<ip>:<port>"
 - Association PFCP passive (attendre que l'UPF initie)
 - Intervalle de battement de 5 secondes
- Les règles et pools de sélection de UPF sont configurés dans la section séparée `upf_selection`. Voir [Stratégies de Sélection de UPF](#) ci-dessous.
- L'enregistrement dynamique de UPF est pris en charge pour les UPF découverts par DNS qui ne sont pas dans la configuration

Exemples

Configuration Minimale :

```
sxb: %{
    local_ip_address: "10.0.0.20"
}

# Tous les UPFs dans upf_selection seront automatiquement enregistrés
# avec :
# - Nom généré automatiquement : "UPF-10.0.0.21:8805"
# - Association PFCP passive (attendre que l'UPF se connecte)
# - Intervalle de battement de 5 secondes
```

Port PFCP Personnalisé :

```
sxb: %{
    local_ip_address: "10.0.0.20",
    local_port: 8806 # Port PFCP non standard
}
```

Exemple Complet avec Sélection de UPF :

```
sxb: %{
    local_ip_address: "10.0.0.20"
},
```

```

upf_selection: %{
  rules: [
    %{
      name: "Pool IMS",
      priority: 10,
      match_field: :apn,
      match_regex: ~r/^ims$/,
      upf_pool: [
        %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight: 100},
        %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 100}
      ]
    }
  ],
  fallback_pool: [
    %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight: 100}
  ]
}
# Tous les 3 UPFs (10.0.1.21, 10.0.1.22, 10.0.2.21) sont automatiquement enregistrés

```

Sélection Basée sur DNS (Enregistrement Dynamique) :

```

sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  dns_enabled: true,
  dns_query_priority: [:ecgi, :tai],
  dns_suffix: "epc.3gppnetwork.org",
  fallback_pool: [
    %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight: 100}
  ]
}
# Les UPFs découverts par DNS seront enregistrés dynamiquement lors de la première utilisation

```

Stratégies de Sélection de UPF

Important : La configuration de sélection de UPF a été simplifiée. Tous les pairs UPF sont automatiquement enregistrés à partir de la configuration `upf_selection`.

Structure de Configuration

La sélection de UPF est configurée dans la section `upf_selection` qui définit :

- Règles Statistiques** - Routage basé sur des motifs avec des pools d'équilibrage de charge
- Paramètres DNS** - Découverte dynamique de UPF basée sur la localisation
- Pool de Secours** - Pool par défaut lorsque aucune règle ne correspond et que DNS échoue

Ordre de Priorité de Sélection

- Règles Statistiques** (Priorité Élevée) - Routage basé sur des motifs avec des pools d'équilibrage de charge
- Sélection Basée sur DNS** (Priorité Inférieure) - Découverte dynamique de UPF basée sur la localisation
- Pool de Secours** (Priorité la Plus Basse) - Pool par défaut lorsque aucune règle ne correspond et que DNS échoue

Flux de Décision de Sélection de UPF

Champs de Correspondance Disponibles

Les règles statiques peuvent correspondre à n'importe lequel de ces attributs de session :

Champ de Correspondance	Description	Exemple de Motif
:imsi	Identité Internationale de l'Abonné Mobile	^313380.* (opérateur US)
:apn	Nom de Point d'Accès / DNN	^internet\.. ou ^ims\.
:serving_network_plmn_id	Identifiant du réseau de service	^313380\$
:sgw_ip_address	Adresse IP SGW	^10\.100\...*
:uli_tai_plmn_id	ID PLMN de la Zone de Suivi	^313.*
:uli_ecgi_plmn_id	ID PLMN de la Cellule E-UTRAN	^313.*

Comparaison des Méthodes de Sélection

Méthode	Quand Utiliser	Avantages	Inconvénients
Pools UPF	Déploiements de production	Équilibrage de charge, HA, poids flexibles	Nécessite plusieurs UPFs
Basé sur APN	Différenciation de service	Routage IMS/Internet séparément	Configuration statique
Basé sur IMSI	Scénarios de Roaming	Routage géographique	Complexité des regex
Basé sur DNS	MEC/Edge computing	Dynamique, conscient de la localisation	Nécessite une infrastructure DNS
Pool de Secours	Filet de sécurité	Toujours avoir un UPF	Peut ne pas être optimal

Méthode	Quand Utiliser	Avantages	Inconvénients
Mode de Simulation	Tester les configs	Test sûr	Pas de trafic réel

Flux Complet d'Établissement de Session

Ce diagramme montre le flux complet de bout en bout de l'établissement de session, y compris la sélection de UPF et la population de PCO :

Points de Décision Clés :

1. Priorité de Sélection de UPF :

- Règles Statistiques (Correspondance de Motif) → Découverte DNS → Pool de Secours
- Filtrage de santé appliqué à toutes les étapes
- Logique Actif/Standby pour haute disponibilité
- **Voir : [Interface PFCP](#)** pour les détails de communication UPF

2. Priorité de Population de PCO :

- Remplacement PCO de Règle → Découverte DNS P-CSCF → Configuration PCO Globale
- Fusion par champ (les règles remplacent des champs spécifiques, le global fournit des valeurs par défaut)
- **Voir : [Configuration PCO](#)** pour les paramètres PCO détaillés

3. Priorité de Découverte P-CSCF :

- FQDN par Règle → Découverte DNS Globale → PCO Statique par Règle → PCO Statique Globale
- **Voir : [Surveillance P-CSCE](#)** pour les métriques de découverte et le suivi de la santé

4. Intégration de Facturation :

- PCRF détermine si la facturation en ligne est requise (Groupe de Notation + Online=1)
- OCS accorde le quota avant l'établissement de session
- PGW-C suit le quota et demande plus via CCR-Update
- **Voir : [Interface Diameter Gx](#) et [Interface Diameter Gy](#)** pour les détails de facturation

Exemple Complet de Configuration

Voici un exemple complet montrant la sélection de UPF multi-pool avec enregistrement automatique des pairs :

```

config :pgw_c,
    # Interface PFCP - Tous les UPFs sont auto-enregistrés à partir de
upf_selection
    sxb: %{
        local_ip_address: "127.0.0.20"
    },

    # Logique de Sélection de UPF - Tous les UPFs définis ici sont
automatiquement enregistrés
    upf_selection: %{
        # Paramètres de sélection basée sur DNS
        dns_enabled: false,
        dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
        dns_suffix: "epc.3gppnetwork.org",
        dns_timeout_ms: 5000,

        # Règles de sélection statiques (évaluées par ordre de priorité)
        rules: [
            # Règle 1 : Trafic IMS - Priorité la Plus Élevée
            %{
                name: "Trafic IMS",
                priority: 20,
                match_field: :apn,
                match_regex: "^ims",
                upf_pool: [
                    %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 80},
                    %{remote_ip_address: "10.100.2.22", remote_port: 8805,
weight: 20}
                ]
            },
            # Règle 2 : APN Entreprise
            %{
                name: "Trafic Entreprise",
                priority: 15,
                match_field: :apn,
                match_regex: "^(enterprise|corporate)\.apn",
                upf_pool: [
                    %{remote_ip_address: "10.100.3.21", remote_port: 8805,
weight: 100}
                ]
            },
            # Règle 3 : Trafic Internet - Équilibré
            %{
                name: "Trafic Internet",
                priority: 5,
                match_field: :apn,
            }
        ]
    }
}

```

```

        match_regex: "^internet",
        upf_pool: [
            %{remote_ip_address: "10.100.1.21", remote_port: 8805,
weight: 33},
            %{remote_ip_address: "10.100.1.22", remote_port: 8805,
weight: 33},
            %{remote_ip_address: "10.100.1.23", remote_port: 8805,
weight: 34}
        ]
    },
],
# Pool de secours - Utilisé lorsque aucune règle ne correspond et
que DNS échoue
fallback_pool: [
    %{remote_ip_address: "127.0.0.21", remote_port: 8805, weight:
100}
]
}

```

Fonctionnalités Clés

Format Actuel :

- ❖ **Enregistrement Automatique** : Tous les UPFs de `upf_selection` sont automatiquement enregistrés au démarrage
- ❖ **Configuration Centralisée** : Toute la sélection de UPF et la configuration des pairs dans une seule section
- ❖ **Pools Requis** : Toutes les règles utilisent le format `upf_pool` (même pour un seul UPF)
- ❖ **Fallback Structuré** : Pool de secours dédié avec distribution pondérée
- ❖ **Intégration DNS** : Paramètres DNS aux côtés des règles de sélection
- ❖ **Enregistrement Dynamique** : Les UPFs découverts par DNS sont automatiquement enregistrés lors de la première utilisation
- ❖ **Suivi de Santé** : Tous les UPFs configurés sont surveillés avec des battements de 5 secondes

Migration depuis le Format Précédent :

- Supprimé : champ `sxb.peer_list` (plus nécessaire)
- Supprimé : `selection_list` intégré dans les configurations de pair
- Toutes les définitions de UPF vont maintenant dans les règles et le pool de secours de `upf_selection`

Comment Fonctionnent les Pools de UPF :

- Sélection Consciente de la Santé** : Seuls les UPFs sains reçoivent du trafic

- Sain = association PFCP active + moins de 3 battements consécutifs manqués
- Les UPFs non sains sont automatiquement filtrés
- Recul vers tous les UPFs si aucun n'est sain (échec rapide)

2. Support Actif/Standy : Utilisez weight: 0 pour les UPFs de secours

- **UPFs Actifs** (poids > 0) : Reçoivent du trafic lorsqu'ils sont sains
- **UPFs de Secours** (poids == 0) : Reçoivent du trafic uniquement lorsque tous les UPFs actifs sont en panne
- Les UPFs de secours sont traités comme weight: 1 lorsqu'ils sont activés

3. Sélection Aléatoire Pondérée : Chaque session est assignée aléatoirement à un UPF sain basé sur les poids

- Dans l'exemple ci-dessus : 70% vont à .21, 20% à .22, 10% à .23
- Poids plus élevé = plus de sessions assignées à cet UPF
- Poids égaux = distribution égale

4. Enregistrement Automatique : Tous les UPFs dans les pools sont automatiquement enregistrés au démarrage

- Noms générés automatiquement : "UPF-<ip>:<port>"
- Paramètres par défaut : association PFCP passive, battements de 5 secondes
- Suivi de santé immédiat pour tous les UPFs configurés

Sélection Consciente de la Santé avec Actif/Standy

Sélection Aléatoire Pondérée Exemple :

```
Pool: [
    UPF-A: poids 50, sain ✓
    UPF-B: poids 30, sain ✓
    UPF-C: poids 20, sain ✓
]
```

Poids Total: 50 + 30 + 20 = 100

Plages de Poids :

UPF-A:	0-49	(50%)
UPF-B:	50-79	(30%)
UPF-C:	80-99	(20%)

Nombre aléatoire : 63 → Sélectionne UPF-B

Nombre aléatoire : 15 → Sélectionne UPF-A

Nombre aléatoire : 91 → Sélectionne UPF-C

Échec de Bascelage Actif/Standy Exemple :

```
Pool Initial : [
    UPF-A: poids 100, sain ✓ (Actif)
    UPF-B: poids 0, sain ✗ (Standby)
]

Scénario 1 : UPF-A Sain
→ Utiliser le Pool Actif : [UPF-A: 100]
→ Tout le trafic vers UPF-A

Scénario 2 : UPF-A Échoue
→ Aucun UPF actif sain
→ Activer Standby : [UPF-B: 1]
→ Tout le trafic bascule vers UPF-B
→ Journaliser : "Tous les UPFs actifs en panne, activation des UPFs de secours"

Scénario 3 : Les Deux Non Sains
→ Aucun UPF sain
→ Utiliser le pool complet : [UPF-A: 100, UPF-B: 0]
→ Sélectionner avec des poids (tentative de connexion, peut échouer)
→ Journaliser : "Aucun UPF sain dans le pool, utilisation du pool complet comme secours"
```

Modèles de Poids Courants :

```
# Distribution égale (25% chacun)
upf_pool: [
    %{remote_ip_address: "10.0.1.1", remote_port: 8805, weight: 1},
    %{remote_ip_address: "10.0.1.2", remote_port: 8805, weight: 1},
    %{remote_ip_address: "10.0.1.3", remote_port: 8805, weight: 1},
    %{remote_ip_address: "10.0.1.4", remote_port: 8805, weight: 1}
]

# Charge équilibrée primaire/sauvegarde (90% / 10%)
upf_pool: [
    %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight: 90},
    %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 10}
]

# Actif/Standy (100% primaire, 0% standby jusqu'à ce que le primaire échoue)
upf_pool: [
    %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight: 100},
    # Actif
    %{remote_ip_address: "10.0.1.22", remote_port: 8805, weight: 0}
    # Standby (uniquement lorsque actif en panne)
]
```

```

# Actif avec plusieurs standby (charge équilibrée lorsqu'activée)
upf_pool: [
    %{remote_ip_address: "10.0.1.1", remote_port: 8805, weight: 100},
# Actif
    %{remote_ip_address: "10.0.1.2", remote_port: 8805, weight: 0},
# Standby 1
    %{remote_ip_address: "10.0.1.3", remote_port: 8805, weight: 0}
# Standby 2
]
# Résultat : Actif obtient 100%. Si actif échoue, les standby obtiennent 50/50%.

# Test A/B (50% / 50%)
upf_pool: [
    %{remote_ip_address: "10.0.1.100", remote_port: 8805, weight: 50},
# Ancienne version
    %{remote_ip_address: "10.0.1.200", remote_port: 8805, weight: 50}
# Nouvelle version
]

```

Cas d'Utilisation :

- **Échec de Bascelage Actif/Standby** : Utilisez `weight: 0` pour les UPFs de secours chauds qui ne s'activent que lorsque les primaires échouent
- **HA Consciente de la Santé** : Basculement automatique lorsque les UPFs perdent l'association PFCP ou manquent des battements
- **Mise à l'Échelle Horizontale** : Distribuer la charge entre plusieurs UPFs pour augmenter la capacité
- **Haute Disponibilité** : Distribution automatique empêche la surcharge d'un seul UPF
- **Déploiements Progressifs** : Utilisez des poids pour les déploiements canaris (par exemple, 95% ancien, 5% nouveau)
- **Optimisation des Coûts** : Diriger plus de trafic vers des UPFs de plus grande capacité
- **Distribution Géographique** : Équilibrer les sessions entre les UPFs de bord

Remplacements PCO (Options de Configuration de Protocole) :

Chaque règle de sélection de UPF peut spécifier des valeurs PCO personnalisées qui remplacent la configuration PCO par défaut pour les sessions correspondantes. Cela permet à différents APNs ou types de trafic de recevoir différents paramètres réseau.

Comment Fonctionnent les Remplacements PCO :

1. **Remplacements Partiels** : Spécifiez uniquement les champs PCO que vous souhaitez remplacer

2. **Fallback par Défaut** : Les champs non spécifiés utilisent les valeurs de la configuration PCO principale
3. **Spécifique à la Règle** : Chaque règle peut avoir des remplacements PCO différents
4. **Fusion par Priorité** : Le PCO de la règle a la priorité sur le PCO global

Hiérarchie de Population de PCO

Ordre de Priorité pour Chaque Champ PCO :

1. **Remplacement PCO de Règle** (Priorité Élevée)
2. **Découverte DNS P-CSCF** (uniquement pour les adresses P-CSCF)
3. **Configuration PCO Globale** (Priorité la Plus Basse / Fallback)

Exemple : La Règle IMS Remplace DNS, La Règle Entreprise Remplace Tout

Session IMS (correspond à la règle "Trafic IMS"):

- └ Serveurs DNS : DE LA CONFIGURATION GLOBALE (non remplacé dans la règle)
- └ P-CSCF : DE LA DÉCOUVERTE DNS (`p_cscf_discovery_fqdn` défini dans la règle)
 - └ Fallback : DE LA RÈGLE si DNS échoue
 - └ MTU : DE LA CONFIGURATION GLOBALE (non remplacé dans la règle)

Session Entreprise (correspond à la règle "Trafic Entreprise"):

- └ Serveurs DNS : DE LA RÈGLE (192.168.1.10, 192.168.1.11)
- └ P-CSCF : DE LA CONFIGURATION GLOBALE (non remplacé dans la règle)
- └ MTU : DE LA RÈGLE (1500)

Session par Défaut (aucune règle correspondante) :

- └ Serveurs DNS : DE LA CONFIGURATION GLOBALE
- └ P-CSCF : DE LA CONFIGURATION GLOBALE ou DNS si la découverte globale est activée
- └ MTU : DE LA CONFIGURATION GLOBALE

Champs de Remplacement PCO Disponibles :

- `primary_dns_server_address` - Adresse IP du serveur DNS principal
- `secondary_dns_server_address` - Adresse IP du serveur DNS secondaire
- `primary_nbns_server_address` - Adresse IP du serveur WINS principal
- `secondary_nbns_server_address` - Adresse IP du serveur WINS secondaire
- `p_cscf_ipv4_address_list` - Liste des serveurs P-CSCF (pour IMS) - Voir [Configuration PCO](#) et [Surveillance P-CSCF](#) pour la découverte dynamique de P-CSCF
- `ipv4_link_mtu_size` - Taille MTU en octets

Découverte P-CSCF par Règle :

En plus des remplacements PCO, les règles de sélection de UPF peuvent spécifier la découverte dynamique de P-CSCF :

- `p_cscf_discovery_fqdn` - (Chaîne) FQDN pour la découverte P-CSCF basée sur DNS (par exemple, "pcscf.mnc380.mcc313.3gppnetwork.org")

Lorsque ce paramètre est défini :

1. PGW-C effectue une recherche DNS pour le FQDN spécifié lors de l'établissement de session
2. Le serveur DNS renvoie une liste d'adresses IP P-CSCF
3. Les adresses P-CSCF découvertes sont envoyées à l'UE via PCO
4. Si la recherche DNS échoue, on revient à `p_cscf_ipv4_address_list` du remplacement PCO (si spécifié) ou à la configuration PCO globale
5. Voir [Surveillance P-CSCF](#) pour suivre les taux de succès/échec de découverte

Ceci est particulièrement utile pour :

- **APNs IMS** - Différents réseaux IMS avec différents serveurs P-CSCF
- **Déploiements multi-locataires** - Différentes entreprises avec une infrastructure P-CSCF dédiée
- **Routage Géographique** - DNS renvoie le P-CSCF le plus proche basé sur la localisation de l'UE
- **Haute Disponibilité** - DNS renvoie automatiquement uniquement les serveurs P-CSCF sains

Exemple : Trafic IMS avec P-CSCF Personnalisé :

```
rules: [
  %{
    name: "Trafic IMS",
    priority: 20,
    match_field: :apn,
    match_regex: "^ims",
    upf_pool: [
      %{remote_ip_address: "10.100.2.21", remote_port: 8805, weight: 80},
      %{remote_ip_address: "10.100.2.22", remote_port: 8805, weight: 20}
    ],
    # Découverte P-CSCF : Interroger dynamiquement DNS pour les
    # adresses P-CSCF
    # La recherche DNS renvoie les IPs P-CSCF actuelles basées sur ce
    # FQDN
    p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org",
    # Les sessions IMS obtiennent des serveurs P-CSCF personnalisés
    # (utilisés comme fallback si DNS échoue)
    pco: %{
```

```

        p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
        # DNS, NBNS, MTU utiliseront les valeurs par défaut de la
configuration PCO principale
    }
}
]

```

Exemple : Trafic Entreprise avec DNS Personnalisé :

```

rules: [
  %{
    name: "Trafic Entreprise",
    priority: 15,
    match_field: :apn,
    match_regex: "^(enterprise|corporate)\.apn",
    upf_pool: [
      %{remote_ip_address: "10.100.3.21", remote_port: 8805, weight:
100}
    ],
    # Les sessions d'entreprise obtiennent des DNS d'entreprise et un
MTU personnalisé
    pco: %{
      primary_dns_server_address: "192.168.1.10",
      secondary_dns_server_address: "192.168.1.11",
      ipv4_link_mtu_size: 1500
      # P-CSCF, NBNS utiliseront les valeurs par défaut de la
configuration PCO principale
    }
  }
]

```

Exemple : Remplacement Complet (Tous les Champs PCO) :

```

rules: [
  %{
    name: "APN IoT - Entièrement Personnalisé",
    priority: 10,
    match_field: :apn,
    match_regex: "^iot\.m2m",
    upf_pool: [
      %{remote_ip_address: "10.100.5.21", remote_port: 8805, weight:
100}
    ],
    # Les sessions IoT obtiennent un PCO complètement personnalisé
    pco: %{
      primary_dns_server_address: "8.8.8.8",
      secondary_dns_server_address: "8.8.4.4",
      primary_nbns_server_address: "10.0.0.100",
      secondary_nbns_server_address: "10.0.0.101",
    }
  }
]

```

```

    p_cscf_ipv4_address_list: [], # Pas de P-CSCF pour IoT
        ipv4_link_mtu_size: 1280      # MTU plus petit pour les
appareils contraints
    }
}
]

```

Cas d'Utilisation :

- **IMS/VoLTE** : Fournir des serveurs P-CSCF spécifiques au transporteur pour les services vocaux
- **APNs Entreprise** : Routage du trafic d'entreprise via des serveurs DNS d'entreprise
- **IoT/M2M** : Utiliser des DNS publics et un MTU optimisé pour les appareils à faible bande passante
- **Roaming** : Fournir des serveurs DNS locaux pour les abonnés en visite
- **Différenciation de Service** : Différents paramètres réseau par type de service

Sélection Basée sur DNS de UPF :

Activer la sélection dynamique de UPF basée sur les Informations de Localisation de l'Utilisateur (ULI) en utilisant des requêtes NAPTR DNS. Les paramètres DNS sont maintenant configurés dans la section `upf_selection`.

Remarque : Cela fournit une sélection de UPF basée sur la géographie ou la topologie. Voir [Interface PFCP](#) pour la configuration de l'association PFCP avec des UPFs découverts dynamiquement et [Gestion de Session](#) pour les flux d'établissement de session.

```

upf_selection: %{
    # Activer la sélection basée sur DNS
    dns_enabled: true,

    # Types de localisation à interroger par ordre de priorité
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],

    # Suffixe DNS pour les requêtes NAPTR 3GPP
    dns_suffix: "epc.3gppnetwork.org",

    # Délai d'attente de requête DNS en millisecondes
    dns_timeout_ms: 5000,
    # ... règles et fallback_pool ...
}

```

La sélection basée sur DNS fonctionne comme suit :

1. **Priorité** : La sélection DNS est utilisée uniquement lorsque **AUCUNE**

règle statique ne correspond (priorité inférieure)

2. **Génération de Requête** : Construit des requêtes NAPTR DNS basées sur la localisation de l'UE :
 - Requête ECGI : eci-<hex>.ecgi.epc.mnc<MNC>.mcc<MCC>.epc.3gppnetwork.org
 - Requête TAI : tac-lb<hex>.tac-hb<hex>.tac.epc.mnc<MNC>.mcc<MCC>.epc.3gppnetwork.org
 - Les requêtes RAI, SAI, CGI suivent un format similaire à celui de la norme 3GPP TS 23.003
3. **Hiérarchie de Fallback** : Essaie chaque type de localisation par ordre de priorité jusqu'à ce qu'une correspondance soit trouvée
4. **Correspondance des Pairs** : Les résultats DNS sont filtrés par rapport à la liste des pairs configurés
5. **Sélection** : Choisit le pair correspondant (actuellement première correspondance, sélection basée sur la charge à venir)

Exemples d'Enregistrements DNS (configurer sur votre serveur DNS) :

```
; Enregistrement NAPTR pour TAC 100 dans PLMN 313-380
tac-lb64.tac-hb00.tac.epc.mnc380.mcc313.epc.3gppnetwork.org IN NAPTR
10 50 "a" "x-3gpp-upf:x-sxb" "" upf-edge-1.example.com.
```

```
; Enregistrement A pour le UPF
upf-edge-1.example.com IN A 10.100.1.21
```

Cas d'Utilisation :

- **MEC/Edge Computing** : Routage des sessions vers les UPFs de bord géographiquement les plus proches
- **Découverte Dynamique de UPF** : Ajouter/retirer des UPFs sans reconfigurer PGW-C
- **Équilibrage de Charge** : Distribuer la charge entre les UPFs en fonction de la localisation
- **Slicing de Réseau** : Routage de différentes tranches vers différents UPFs par localisation

Surveillance de la Santé de UPF

Sélection Consciente de la Santé Automatique : Le PGW-C surveille en continu la santé de tous les UPFs et exclut automatiquement les UPFs non sains de la sélection.

Critères de Vérification de Santé

Un UPF est considéré comme **sain** lorsque TOUTES les conditions suivantes sont remplies :

1. **Association PFCP Active** : Le UPF a une association PFCP établie

2. **Réactivité des Battements** : Moins de 3 battements consécutifs manqués
3. **Processus Actif** : Le processus GenServer du pair UPF est en cours d'exécution

Un UPF est considéré comme **non sain** si L'UNE des affirmations suivantes est vraie :

- L'association PFCP n'est pas établie (`associated: false`)
- 3 ou plus de délais d'attente de battement consécutifs
- Le processus du pair UPF a échoué ou est non réactif

Mécanisme de Surveillance

Pour les UPFs Configurés (dans `upf_selection`) :

- Le suivi de santé commence immédiatement au démarrage
- L'association PFCP est surveillée en continu
- Des battements sont envoyés toutes les 5 secondes
- Le compteur `missed_heartbeats_consecutive` suit les échecs consécutifs
- Tous les UPFs des règles et du pool de secours sont automatiquement enregistrés

Pour les UPFs Découverts par DNS (enregistrement dynamique) :

- Considéré comme sain jusqu'à la première tentative de session
- Enregistré automatiquement lors de la première utilisation
- Le suivi de santé commence après l'enregistrement

Comportement de Sélection

Mode Actif/Standy (lors de l'utilisation de `weight: 0`) :

1. Filtrer vers seulement les UPFs sains
2. Séparer en **actifs** (`poids > 0`) et **standby** (`poids == 0`)
3. Utiliser les UPFs actifs si l'un d'eux est sain
4. Activer les UPFs de secours (traiter comme poids 1) si tous les actifs sont non sains
5. Recul vers le pool complet si aucun UPF sain n'existe

Mode Équilibré par Charge (tous poids > 0) :

1. Filtrer vers seulement les UPFs sains
2. Effectuer une sélection aléatoire pondérée parmi les UPFs sains
3. Recul vers le pool complet si aucun UPF sain n'existe

Journalisation :

```
[debug] Utilisation du pool UPF actif (2/3 UPFs sains, 1 standby)
```

```
[info] Tous les UPFs actifs en panne, activation des UPFs de secours  
(1 UPFs standby, traitement du poids 0 comme 1)  
[warning] Aucun UPF sain dans le pool (3 au total), utilisation du  
pool complet comme secours
```

Vérification de la Santé de UPF

Programmatique :

```
# Vérifier si un UPF spécifique est sain  
iex> PGW_C.PFCP_Node.is_peer_healthy?({10, 100, 1, 21})  
true  
  
# Obtenir des informations détaillées sur la santé  
iex> PGW_C.PFCP_Node.get_peer_health({10, 100, 1, 21})  
%{  
    associated: true,  
    missed_heartbeats: 0,  
    healthy: true,  
    registered: true  
}
```

Via l'Interface Web :

- Naviguer vers /upf_selection dans le panneau de contrôle
- Voir l'état de santé en temps réel pour tous les UPFs dans chaque pool
- Badges d'état : ◊ Actif-UP, ◊ Standby-Prêt, ◊ Actif-ÉCHOUÉ, ◊ Non Associé
- Badges de rôle : ACTIF (poids > 0), STANDBY (poids == 0), DYNAMIQUE (découvert par DNS, non dans la config)
- Compteur de battements manqués affiché pour les UPFs associés

Meilleures Pratiques de Surveillance de la Santé

1. **Configurer les UPFs dans upf_selection** : Tous les UPFs dans les règles et les pools de secours sont automatiquement surveillés

```
upf_selection: %{  
    rules: [  
        %{  
            name: "Trafic Internet",  
            priority: 10,  
            match_field: :apn,  
            match_regex: "^internet",  
            upf_pool: [  
                %{remote_ip_address: "10.100.1.21", remote_port: 8805,  
            weight: 100}  
            ]
```

```

        }
    ],
    fallback_pool: [
        %{remote_ip_address: "10.100.2.21", remote_port: 8805,
weight: 100}
    ]
}
# Tous les UPFs obtiennent automatiquement :
# - Battements de 5 secondes
# - Suivi de santé depuis le démarrage
# - Noms générés automatiquement

```

2. **Utiliser des UPFs de secours** : Configurer des secours chauds avec weight: 0 pour un basculement automatique

```

upf_pool: [
    %{remote_ip_address: "10.1.1.1", remote_port: 8805, weight:
100}, # Actif
    %{remote_ip_address: "10.1.1.2", remote_port: 8805, weight: 0}
# Standby
]

```

3. **Surveiller via l'Interface Web** : Vérifiez régulièrement l'état de santé des UPFs dans le panneau de contrôle
4. **Ajuster le seuil de battement** : Ajustez le seuil < 3 de battements manqués dans le code si nécessaire
 - Situé dans : lib/core/pfcp_node/impl/peer.ex fonction is_peer_healthy?/1
 - Seuil plus bas = détection plus rapide des pannes mais plus sensible aux perturbations réseau
 - Seuil plus élevé = plus tolérant mais détection plus lente des pannes

Enregistrement Dynamique de UPF

Fonctionnalité : Le PGW-C enregistre et surveille automatiquement les UPFs découverts via DNS, même s'ils ne sont pas dans la configuration upf_selection.

Comment Cela Fonctionne

Lorsque n'importe quelle méthode de sélection (règles statiques, pools ou DNS) renvoie un UPF qui n'est pas déjà enregistré, le système automatiquement :

1. **Crée un Pair PFCP** : Génère une configuration de pair par défaut pour le UPF inconnu
2. **Initie l'Association PFCP** : Tente d'établir une association PFCP avec le UPF

3. **Enregistre dans le Registre des Pairs** : Ajoute le UPF au système de suivi interne des pairs
4. **Commence la Surveillance des Battements** : Commence les échanges de battements périodiques (intervalles de 10 secondes)
5. **Suit la Vitalité** : Surveille le UPF pour des pannes et des récupérations

Configuration par Défaut pour les UPFs Dynamiques

Lorsqu'un UPF est enregistré dynamiquement, il reçoit la configuration par défaut suivante :

```
%{
    name: "Dynamic-UPF-<IP>",                      # par exemple, "Dynamic-
    UPF-10-100-1-21"
    remote_ip_address: <discovered_ip>,            # IP depuis DNS ou sélection
    remote_port: 8805,                                # Port PFCP standard
    (remplaçable)
    initiate_pfcp_association_setup: true,          # PGW-C initie l'association
    heartbeat_period_ms: 10_000                         # Intervalle de battement de
10 secondes
}
```

Remarque : Les UPFs dynamiques sont enregistrés uniquement pour la gestion de l'association. Ils sont utilisés comme cibles dans les règles de `upf_selection`, pas comme sources de logique de sélection.

Exemple : DNS Renvoie un UPF Inconnu

```
# La requête DNS renvoie : upf-edge-2.example.com -> 10.200.5.99
# Ce UPF n'est PAS dans votre configuration upf_selection

# Flux d'enregistrement dynamique :
# 1. Le système détecte le UPF inconnu 10.200.5.99
# 2. Journalise : "UPF {10, 200, 5, 99} non pré-configuré, tentative
d'enregistrement dynamique..."
# 3. Envoie la Requête d'Établissement d'Association PFCP à
10.200.5.99:8805
# 4. Si le UPF répond : Association établie, la session continue
normalement
# 5. Si le UPF ne répond pas : La session échoue proprement avec un
message d'erreur clair
```

Avantages

- ◊ **Véritable Découverte Dynamique** : La sélection de UPF basée sur DNS fonctionne maintenant sans pré-configuration
- ◊ **Mise à l'Échelle Automatique** : Ajoutez des UPFs à votre réseau sans redémarrer PGW-C

- ◊ **Dégradation Propre** : Si l'association échoue, les sessions échouent proprement (pas de plantages)
- ◊ **Compatible avec les Versions Précédentes** : Les UPFs préconfigurés continuent de fonctionner exactement comme avant
- ◊ **Surveillance Complète** : Les UPFs dynamiques reçoivent le même suivi de battement que les pairs statiques

Gestion des Échecs

Si un UPF découvert dynamiquement ne répond pas à la Requête d'Établissement d'Association PFCP :

```
[error] Échec de l'Établissement d'Association PFCP pour le UPF
dynamique {10, 200, 5, 99} : :timeout
[error] Échec de l'enregistrement dynamique du UPF {10, 200, 5, 99} :
:timeout.
```

La création de session échouera

Format du Registre de Données de Facturation (CDR)

Facturation Hors Ligne pour PGW-C et SGW-C

Table des Matières

1. [Aperçu](#)
2. [Format du Fichier CDR](#)
3. [Champs CDR](#)
4. [Événements CDR](#)
5. [Structure du Fichier](#)
6. [Configuration](#)
7. [Flux de Génération CDR](#)
8. [Détails des Champs](#)
9. [Exemples](#)
10. [Intégration](#)

Aperçu

Le format **CDR de Données (Registre de Données de Facturation)** fournit des capacités de facturation hors ligne pour le Plan de Contrôle de la Passerelle de Paquet (PGW-C) et le Plan de Contrôle de la Passerelle de Service (SGW-C). Les CDR sont générés pour enregistrer les événements de session de porteur, l'utilisation des données et les informations sur les abonnés à des fins de facturation et d'analyse.

Ce format commun est utilisé par les deux éléments du réseau pour garantir la cohérence des enregistrements de facturation à travers l'infrastructure EPC.

Caractéristiques Clés

- **Format basé sur CSV** - Valeurs séparées par des virgules simples et lisibles par l'homme
- **Enregistrement basé sur les événements** - Capture les événements de début, de mise à jour et de fin de porteur
- **Mesure de volume** - Enregistre l'utilisation des données en amont et en aval
- **Rotation automatique** - Rotation de fichier configurable basée sur des intervalles de temps
- **Conforme à la 3GPP** - Suit les spécifications 3GPP TS 32.251 (facturation du domaine PS) et TS 32.298 (encodage CDR)

Cas d'Utilisation

Cas d'Utilisation	Description
Facturation Hors Ligne	Générer des CDR pour la facturation postpayée
Analytique	Analyser les modèles d'utilisation des abonnés
Piste d'Audit	Suivre tous les événements de session de porteur
Planification de Capacité	Surveiller l'utilisation des ressources réseau
Dépannage	Déboguer les problèmes de session et de porteur

Format du Fichier CDR

Convention de Nommage des Fichiers

<epoch_timestamp>

Exemple :

1726598022

Le nom du fichier est le timestamp Unix (en secondes) du moment où le fichier a été créé.

Emplacement du Fichier

Répertoires par défaut :

- PGW-C : /var/log/pgw_c/cdr/
- SGW-C : /var/log/sgw_c/cdr/

Configuré via le paramètre directory dans la configuration du rapporteur CDR.

En-tête du Fichier

Chaque fichier CDR commence par un en-tête multi-lignes contenant des métadonnées :

```
# Fichier CDR de Données :
# Heure de Début du Fichier : HH:MM:SS (unix_timestamp)
# Heure de Fin du Fichier : HH:MM:SS (unix_timestamp)
# Nom de la Passerelle : <gateway_name>
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,eci,sgw_ip,ue_ip,pgw_ip,apn,qci,octets_in,octets_out
```

Champs de l'En-tête :

- **Heure de Début du Fichier** - Quand le fichier CDR a été créé (lisible par l'homme et timestamp Unix)
- **Heure de Fin du Fichier** - Quand la rotation du fichier aura lieu (lisible par l'homme et timestamp Unix)
- **Nom de la Passerelle** - Identifiant pour l'instance de la passerelle (PGW-C ou SGW-C)
- **En-têtes de Colonne** - Noms des champs CSV pour les enregistrements de données

Champs CDR

Résumé des Champs

Position	Nom du Champ	Type	Description
0	epoch	entier	Timestamp de l'événement (secondes Unix)
1	imsi	chaîne	Identité Internationale de l'Abonné Mobile
2	event	chaîne	Type d'événement CDR (par exemple, "default_bearer_start")
3	charging_id	entier	Identifiant de facturation unique pour le porteur
4	msisdn	chaîne	Numéro ISDN de la Station Mobile (numéro de téléphone)
5	ue_imei	chaîne	Identité Internationale de l'Équipement Mobile
6	timezone_raw	chaîne	Fuseau horaire UE (réservé, actuellement vide)
7	plmn	entier	Identifiant du Réseau Mobile Terrestre Public
8	tac	entier	Code de Zone de Suivi
9	eci	entier	Identifiant de Cellule E-UTRAN
10	sgw_ip	chaîne	Adresse IP du Plan de Contrôle S5/S8 de SGW-C (ou IP S5/S8 de PGW-C pour les CDR PGW)
11	ue_ip	chaîne	Adresse IP de l'UE (format IPv4 IPv6)
12	pgw_ip	chaîne	Adresse IP du Plan de Contrôle S5/S8 de PGW-C
13	apn	chaîne	Nom du Point d'Accès
14	qci	entier	Identifiant de Classe QoS
15	octets_in	entier	Volume de données en aval (octets)
16	octets_out	entier	Volume de données en amont (octets)

Événements CDR

Types d'Événements

Les CDR sont générés pour trois types d'événements :

Type d'Événement	Format	Description	Quand Généré
Début de Porteur	<type>_bearer_start	Établissement du porteur	Réponse de Création de Session envoyée
Mise à Jour de Porteur	<type>_bearer_update	Rapport d'utilisation durant la session	Rapports d'utilisation périodiques du plan utilisateur
Fin de Porteur	<type>_bearer_end	Terminaison du porteur	Demande/Réponse de Suppression de Session

Types de Porteurs :

- default - Porteur par défaut (un par connexion PDN)
- dedicated - Porteur dédié (zéro ou plusieurs par connexion PDN)

Exemples d'Événements

default_bearer_start	- Porteur par défaut établi
default_bearer_update	- Mise à jour de l'utilisation du porteur par défaut
default_bearer_end	- Porteur par défaut terminé
dedicated_bearer_start	- Porteur dédié établi
dedicated_bearer_update	- Mise à jour de l'utilisation du porteur dédié
dedicated_bearer_end	- Porteur dédié terminé

Structure du Fichier

Exemple de Fichier CDR

```
# Fichier CDR de Données :
# Heure de Début du Fichier : 18:53:42 (1726598022)
# Heure de Fin du Fichier : 19:53:42 (1726601622)
# Nom de la Passerelle : pgw-c-prod-01
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,ecii,sgw_ip,ue_ip,pgw_ip,apn,qci,octets_in,octets_out
1726598022,3102601234567899,default_bearer_start,12345,15551234567,123456789012345,,349552,1234,5678,10.0.1.10,172.16.1.100|2001:db8::1,10.0.1.20,internet,9,0,0
1726598322,3102601234567899,default_bearer_update,12345,15551234567,123456789012345,,349552,1234,5678,10.0.1.10,172.16.1.100|2001:db8::1,10.0.1.20,internet,9,1048576,524288
1726598622,3102601234567899,default_bearer_update,12345,15551234567,123456789012345,,349552,1234,5678,10.0.1.10,172.16.1.100|2001:db8::1,10.0.1.20,internet,9,5242880,2097152
1726598922,3102601234567899,default_bearer_end,12345,15551234567,123456789012345,,349552,1234,5678,10.0.1.10,172.16.1.100|2001:db8::1,10.0.1.20,internet,9,10485766,5242880
```

Rotation des Fichiers

Les fichiers CDR sont automatiquement tournés en fonction de la durée configurée :

Processus de Rotation :

- Fermer le fichier CDR actuel
- Créer un nouveau fichier avec le timestamp actuel
- Écrire l'en-tête dans le nouveau fichier
- Continuer à enregistrer les CDR dans le nouveau fichier

Configuration

Paramètres de Configuration

Paramètre	Type	Description	Par Défaut	Recommandé
gateway_name	chaîne	Identifiant de l'instance de la passerelle	-	Utiliser le nom d'hôte ou l'ID de l'instance
duration	entier	Intervalle de rotation du fichier (ms)	-	3600000 (1 heure)
directory	chaîne	Chemin du répertoire de sortie CDR	-	/var/log/{pgw,sgw}_c/cdrs

Exemples de Configuration

Production :

- gateway_name** : "pgw-c-prod-01" ou "sgw-c-prod-01"
- duration** : 3,600,000 ms (rotation de 1 heure)
- directory** : "/var/log/pgw_c/cdrs" ou "/var/log/sgw_c/cdrs"

Développement :

- gateway_name** : "pgw-c-dev" ou "sgw-c-dev"
- duration** : 300,000 ms (rotation de 5 minutes pour les tests)
- directory** : "/tmp/pgw_c_cdrs" ou "/tmp/sgw_c_cdrs"

Haut Volume :

- gateway_name** : "pgw-c-prod-heavy" ou "sgw-c-prod-heavy"
- duration** : 1,800,000 ms (rotation de 30 minutes)
- directory** : "/mnt/fast-storage/cdrs"

Flux de Génération CDR

Événements CDR du Cycle de Vie du Porteur

Génération CDR SGW-C :

Génération CDR PGW-C :

Événements de Génération CDR

1. Début de Porteur :

- Quand** : La réponse de création de session est envoyée
- But** : Enregistre l'établissement du porteur avec une utilisation nulle
- octets_in** : 0
- octets_out** : 0

2. Mise à Jour de Porteur :

- Quand** : Demande de rapport de session PFCP reçue du plan utilisateur
- But** : Enregistre l'utilisation des données incrémentale
- octets_in** : Octets en aval cumulés depuis le début du porteur
- octets_out** : Octets en amont cumulés depuis le début du porteur

3. Fin de Porteur :

- Quand** : Réponse de suppression de session PFCP reçue (avec utilisation finale)
- But** : Enregistre l'utilisation finale des données avant la terminaison de la session
- octets_in** : Total final des octets en aval
- octets_out** : Total final des octets en amont

Détails des Champs

1. epoch (Timestamp)

Type : Timestamp Unix (secondes)

Description : Le moment où l'événement CDR s'est produit

Exemple :

1726598022 → 2025-09-17 18:53:42 UTC

Source : DateTime.utcnow() |> DateTime.to_unix()

2. imsi (Identité de l'Abonné)

Type : Chaîne (jusqu'à 15 chiffres)

Format : MCCMNC + MSIN

Description : Identité Internationale de l'Abonné Mobile identifiant de manière unique l'abonné

Exemple :

310260123456789
└── └── └──
MCC MNC MSIN
(310) (260) (123456789)

Source : Contexte UE, reçu dans la demande de création de session

3. event (Type d'Événement CDR)

Type : Chaîne

Format : <bearer_type>_bearer_<event>

Valeurs :

- default_bearer_start
- default_bearer_update
- default_bearer_end
- dedicated_bearer_start
- dedicated_bearer_update
- dedicated_bearer_end

Détermination :

- Si EBI (Identifiant de Porteur EPS) est égal à LBI (Identifiant de Porteur Lié) : default
- Si EBI n'est pas égal à LBI : dedicated

Source : Contexte de porteur (comparaison EBI vs LBI)

4. charging_id (Identifiant de Facturation)

Type : Entier non signé 32 bits

Description : Identifiant unique pour la corrélation de facturation à travers les éléments du réseau

Exemple :

12345

Source : Assigné par PGW-C, reçu dans la réponse de création de session

Utilisation :

- Corrèle les événements de facturation à travers SGW et PGW
- Utilisé dans les interfaces de facturation Diameter Gy/Gz
- Unique par porteur

5. msisdn (Numéro de Téléphone)

Type : Chaîne (format E.164)

Description : Numéro ISDN de la Station Mobile (numéro de téléphone de l'abonné)

Format : Code du pays + numéro national

Exemple :

15551234567
└── └──
CC National
(1) (5551234567)

Source : Contexte UE, généralement provenant de HSS via MME

6. ue_imei (Identité de l'Équipement)

Type : Chaîne (15 chiffres)

Format : TAC (8) + SNR (6) + Spare (1)

Description : Identité Internationale de l'Équipement Mobile (identifiant de l'appareil)

Exemple :

123456789012345
└── └── └──
TAC SNR S

Source : Contexte UE, reçu de MME

7. timezone_raw (Fuseau Horaire UE)

Type : Chaîne (actuellement réservé/vide)

Description : Champ réservé pour les informations de fuseau horaire de l'UE

Statut Actuel : Non peuplé (champ vide dans le CSV)

Utilisation Future : Peut inclure le décalage horaire et le drapeau d'heure d'été

Exemple :

, (champ vide)

8. plmn (Identifiant du Réseau)

Type : Entier (format hérité)

Description : Identifiant du Réseau Mobile Terrestre Public encodé en hexadécimal little-endian

Processus d'Encodage :

MCC: 505, MNC: 57
↓
"50557"
↓
Échanger les paires : "055570"
↓
Hex à décimal : 0x055570 = 349552

Exemple :

349552 → MCC: 505, MNC: 57

Source : Informations de localisation de l'UE provenant de MME

Remarque : Il s'agit d'un format d'encodage hérité pour la compatibilité ascendante

9. tac (Code de Zone de Suivi)

Type : Entier non signé 16 bits

Description : Le Code de Zone de Suivi identifie la zone de suivi où se trouve l'UE

Plage : 0 - 65535

Exemple :

1234

Source : Informations de localisation de l'UE, reçues de MME dans la demande de création de session

Utilisation :

- Identifie la zone de gestion de mobilité
- Utilisé pour la recherche et les mises à jour de localisation
- Partie de l'Identité de Zone de Suivi (TAI)

10. eci (Identifiant de Cellule E-UTRAN)

Type : Entier non signé 28 bits

Description : L'Identifiant de Cellule E-UTRAN identifie de manière unique la cellule servant l'UE

Format : ID eNodeB (20 bits) + ID de Cellule (8 bits)

Plage : 0 - 268,435,455

Exemple :

5678

Source : Informations de localisation de l'UE provenant de MME

Utilisation :

- Identifie une tour de cellule spécifique et un secteur
- Utilisé pour le transfert et la gestion de mobilité
- Informations de localisation granulaires

11. sgw_ip (IP du Plan de Contrôle de la Passerelle)

Type : Chaîne (adresse IPv4 ou IPv6)

Description : Adresse IP du Plan de Contrôle S5/S8 de la Passerelle (F-TEID)

- Pour les CDR SGW-C : IP du plan de contrôle S5/S8 de SGW-C
- Pour les CDR PGW-C : IP du plan de contrôle S5/S8 de PGW-C (F-TEID local)

Format : Décimal pointé (IPv4) ou hexadécimal à deux-points (IPv6)

Exemple :

10.0.1.10 (IPv4)
2001:db8::10 (IPv6)

Source :

- SGW-C : Configuration locale, assignée à l'interface S5/S8
- PGW-C : Configuration locale, assignée à l'interface S5/S8

Remarque : Malgré le nom de champ "sgw_ip", cela contient l'adresse IP de la passerelle locale pour les CDR PGW et SGW

12. ue_ip (Adresse IP de l'UE)

Type : Chaîne (format IPv4|IPv6)

Description : Adresse IP assignée à l'UE pour la connexion PDN

Format : <ipv4>|<ipv6>

Exemples :

172.16.1.100	(IPv4 uniquement)
2001:db8::1	(IPv6 uniquement)
172.16.1.100 2001:db8::1	(Dual-stack)

Source : Allocation d'Adresse PDN (PAA) de PGW-C

Remarques :

- IPv4 vide : Aucune adresse IPv4 attribuée
- IPv6 vide : Aucune adresse IPv6 attribuée
- Les deux présents : Connexion PDN en double pile

13. pgw_ip (IP de la Passerelle Pair)

Type : Chaîne (adresse IPv4 ou IPv6)

Description : Adresse IP du Plan de Contrôle S5/S8 de la Passerelle Pair (F-TEID)

- Pour les CDR SGW-C : IP du plan de contrôle S5/S8 de PGW-C (F-TEID distant)
- Pour les CDR PGW-C : IP du plan de contrôle S5/S8 de SGW-C (F-TEID distant)

Format : Décimal pointé (IPv4) ou hexadécimal à deux-points (IPv6)

Exemple :

10.0.1.20 (IPv4)
2001:db8::20 (IPv6)

Source :

- SGW-C : Reçu dans la réponse de création de session de PGW-C
- PGW-C : Reçu dans la demande de création de session de SGW-C

Remarque : Malgré le nom de champ "pgw_ip", cela contient l'adresse IP de la passerelle pair

14. apn (Nom du Point d'Accès)

Type : Chaîne (jusqu'à 100 caractères)

Description : Nom du Point d'Accès identifiant le réseau externe (PDN)

Format : Format de label similaire à DNS

Exemples :

internet
ims
mms
enterprise.corporate

Source : Reçu dans la demande de création de session de MME

Utilisation :

- Détermine quel réseau externe connecter
- Conduit les règles de politique et de facturation
- Peut déterminer le pool d'adresses IP

15. qci (Identifiant de Classe QoS)

Type : Entier non signé 8 bits

Description : L'Identifiant de Classe QoS définit la qualité de service du porteur

Plage : 1 - 9 (standardisé), 128-254 (spécifique à l'opérateur)

Valeurs QCI Standardisées :

QCI	Type de Ressource	Priorité	Délai de Paquet	Perte de Paquet	Service	Exemple
1	GBR	2	100 ms	10^-2	Voix Conversationnelle	
2	GBR	4	150 ms	10^-3	Vidéo Conversationnelle	
3	GBR	3	50 ms	10^-3	Jeux en Temps Réel	
4	GBR	5	300 ms	10^-6	Vidéo Non Conversationnelle	
5	Non-GBR	1	100 ms	10^-6	Signification IMS	
6	Non-GBR	6	300 ms	10^-6	Vidéo (tamponnée)	
7	Non-GBR	7	100 ms	10^-3	Voix, Vidéo, Jeux	
8	Non-GBR	8	300 ms	10^-6	Vidéo (tamponnée)	
9	Non-GBR	9	300 ms	10^-6	Porteur par Défaut	

Exemple :

9 → Porteur par défaut (meilleure effort)

Source : Paramètres QoS du porteur provenant de PGW-C

16. octets_in (Volume en Aval)

Type : Entier non signé 64 bits

Description : Nombre d'octets transmis dans la direction aval (réseau → UE)

Unités : Octets

Exemple :

1048576 → 1 Mo en aval

Source : Mesure de Volume PFCP du plan utilisateur (PGW-U ou SGW-U)

Remarques :

- Cumulatif pour les événements update
- Total final pour les événements end
- Toujours 0 pour les événements start

17. octets_out (Volume en Amont)

Type : Entier non signé 64 bits

Description : Nombre d'octets transmis dans la direction amont (UE → réseau)

Unités : Octets

Exemple :

524288 → 512 Ko en amont

Source : Mesure de Volume PFCP du plan utilisateur (PGW-U ou SGW-U)

Remarques :

- Cumulatif pour les événements update
- Total final pour les événements end
- Toujours 0 pour les événements start

Exemples

Exemple 1 : Session de Base avec Mise à Jour Unique

Chronologie :

1. Porteur établi
2. 5 minutes plus tard : Mise à jour d'utilisation (10 Mo en aval, 5 Mo en amont)
3. Session terminée

Sortie CDR :

```
# Fichier CDR de Données :
# Heure de Début du Fichier : 10:00:00 (1726570800)
# Heure de Fin du Fichier : 11:00:00 (1726574400)
# Nom de la Passerelle : pgw-c-01
# epoch,imsi,event,charging_id,msisdn,ue_imei,timezone_raw,plmn,tac,eci,sgw_ip,ue_ip,pgw_ip,apn,qci,octets_in,octets_out
1726570800,310260111111111,15551111111,1111111111111111,,349552,1000,2000,10.0.1.1,172.16.1.1|,10.0.2.1,internet,9,0,0
1726571100,310260111111111,15551111111,1111111111111111,,349552,1000,2000,10.0.1.1,172.16.1.1|,10.0.2.1,internet,9,10485760,5242880
1726571400,310260111111111,15551111111,1111111111111111,,349552,1000,2000,10.0.1.1,172.16.1.1|,10.0.2.1,internet,9,10485760,5242880
```

Exemple 2 : Session en Double Pile avec Plusieurs Mises à Jour

Chronologie :

1. Porteur en double pile établi (IPv4 + IPv6)
2. Plusieurs mises à jour d'utilisation
3. Session terminée

Sortie CDR :

```
1726570800,310260222222222,15552222222,222222222222222,,349552,1001,2001,10.0.1.1,172.16.1.2|2001:db8::2,10.0.2.1,internet,9,0,0
1726571100,310260222222222,15552222222,222222222222222,,349552,1001,2001,10.0.1.1,172.16.1.2|2001:db8::2,10.0.2.1,internet,9,2097152,1048576
1726571400,310260222222222,15552222222,222222222222222,,349552,1001,2001,10.0.1.1,172.16.1.2|2001:db8::2,10.0.2.1,internet,9,8388608,4194304
1726571700,310260222222222,15552222222,222222222222222,,349552,1001,2001,10.0.1.1,172.16.1.2|2001:db8::2,10.0.2.1,internet,9,20971520,10485760
1726572000,310260222222222,15552222222,222222222222222,,349552,1001,2001,10.0.1.1,172.16.1.2|2001:db8::2,10.0.2.1,internet,9,31457280,15728640
```

Exemple 3 : Session avec Porteur Dédié

Chronologie :

1. Porteur par défaut établi (QCI 9)
2. Porteur dédié créé pour la vidéo (QCI 6)
3. Mises à jour d'utilisation pour les deux porteurs
4. Porteur dédié supprimé
5. Porteur par défaut terminé

Sortie CDR :

```
1726570800,310260333333333,15553333333,333333333333333,,1258248,1002,2002,10.0.1.1,172.16.1.3|,10.0.2.1,internet,9,0,0
1726571100,310260333333333,15553333333,333333333333333,,1258248,1002,2002,10.0.1.1,172.16.1.3|,10.0.2.1,internet,6,0,0
1726571400,310260333333333,15553333333,333333333333333,,1258248,1002,2002,10.0.1.1,172.16.1.3|,10.0.2.1,internet,9,5242880,2097152
1726571700,310260333333333,15553333333,333333333333333,,1258248,1002,2002,10.0.1.1,172.16.1.3|,10.0.2.1,internet,6,104857600,1048576
1726572000,310260333333333,15553333333,333333333333333,,1258248,1002,2002,10.0.1.1,172.16.1.3|,10.0.2.1,internet,6,209715200,2097152
1726572300,310260333333333,15553333333,333333333333333,,1258248,1002,2002,10.0.1.1,172.16.1.3|,10.0.2.1,internet,9,10485760,4194304
```

Analyse :

- Le porteur par défaut (10003) transporte le trafic de fond (10 Mo en aval, 4 Mo en amont)
- Le porteur dédié (10004) transporte le trafic vidéo (200 Mo en aval, 2 Mo en amont)
- Différentes valeurs QCI (9 vs 6) reflètent un traitement QoS différent

Intégration

Pipeline de Traitement CDR

Méthodes de Collecte CDR

1. Collecte Basée sur Fichiers :

```
# Surveiller le répertoire CDR (exemple PGW-C)
inotifywait -m /var/log/pgw_c/cdrs/ -e close_write | while read path action file; do
    # Rotation du fichier terminée, traiter le CDR
    process_cdr "$path$file"
done

# Surveiller le répertoire CDR (exemple SGW-C)
inotifywait -m /var/log/sgw_c/cdrs/ -e close_write | while read path action file; do
    # Rotation du fichier terminée, traiter le CDR
    process_cdr "$path$file"
done
```

2. Streaming en Temps Réel :

```
# Suivre et streamer vers le pipeline de traitement
tail -F /var/log/pgw_c/cdrs/* /var/log/sgw_c/cdrs/* | process_cdr_stream
```

Documentation Connexe

Facturation

- [Interface Diameter Gy](#) - Facturation en ligne pour les abonnés prépayés
- [Interface Diameter Gx](#) - Contrôle de politique et règles de facturation dans les CDR
- [Guide de Configuration](#) - Configuration de la facturation en ligne

Sources de Données

- [Interface PFPCP](#) - Rapport d'utilisation de PGW-U via URRs
- [Interface S5/S8](#) - Informations sur le porteur pour les CDR
- [Gestion de Session](#) - Cycle de vie de la session et déclencheurs de CDR
- [Allocation IP de l'UE](#) - Adresses IP de l'UE enregistrées dans les CDR

Opérations

- [Guide de Surveillance](#) - Métriques de génération CDR, suivi de l'intégration de facturation
- [Configuration PCO](#) - Paramètres réseau contextuels pour les CDR

Références 3GPP :

- TS 32.251 - Facturation du domaine de commutation de paquets (PS)
- TS 29.274 - Système de Paquet Évolué (EPS) ; Protocole de Tunnel de Service Général Évolué (GPRS) pour le Plan de Contrôle (GTPv2-C)
- TS 29.244 - Interface entre les nœuds du Plan de Contrôle et du Plan Utilisateur (PFPCP)



Documentation de l'Interface Diameter Gx

Fonction de Règles de Politique et de Facturation (PCRF)

Table des Matières

1. [Aperçu](#)
 2. [Bases de l'Interface Gx](#)
 3. [Protocole Diameter](#)
 4. [Messages de Contrôle de Crédit](#)
 5. [Règles de Politique et de Facturation](#)
 6. [Configuration](#)
 7. [Flux de Messages](#)
 8. [Gestion des Erreurs](#)
 9. [Dépannage](#)
-

Aperçu

L'**interface Gx** connecte le PGW-C au **PCRF (Fonction de Règles de Politique et de Facturation)** ou **PCF (Fonction de Contrôle de Politique)** dans les réseaux 5G. Cette interface permet :

- **Contrôle de Politique Dynamique** - Application en temps réel de la QoS et des politiques
- **Contrôle de Facturation** - Autorisation de crédit et suivi de l'utilisation
- **Connaissance du Service** - Différenciation du trafic au niveau des applications
- **Gestion des Profils d'Abonnés** - Application de politiques par utilisateur

Gx dans l'Architecture Réseau

Fonctions Clés

Fonction	Description
Provisionnement de Politique	Le PCRF fournit des règles PCC définissant comment gérer le trafic
Contrôle de QoS	Ajustement dynamique des débits et des paramètres QoS

Fonction	Description
Contrôle de Facturation	Autorisation de crédit pour les scénarios prépayés/postpayés
Contrôle de Gating	Activer/désactiver les flux de trafic en fonction de la politique
Surveillance de l'Utilisation	Suivi de la consommation de données par service

Bases de l'Interface Gx

Référence 3GPP

- **Spécification :** 3GPP TS 29.212
- **ID d'Application Diameter :** 16777238 (Gx)
- **Protocole :** Protocole de Base Diameter (RFC 6733)

Concept de Session

Chaque connexion PDN de l'UE a une **session Gx** correspondante identifiée par un **Session-ID**. Cette session :

- Créée lorsque l'UE s'attache (CCR-Initial)
- Mise à jour pendant la durée de la connexion (CCR-Update) - optionnelle
- Terminée lorsque l'UE se détache (CCR-Termination)

Format de l'ID de Session

Session-ID: <Origin-Host>;<high32>;<low32>[;<optional>]

Exemple: omni-

pgw_c.epc.mnc999.mcc999.3gppnetwork.org;1234567890;98765

Composants :

- **Origin-Host** : Identité Diameter du PGW-C
- **high32** : 32 bits supérieurs de l'identifiant unique
- **low32** : 32 bits inférieurs de l'identifiant unique

Protocole Diameter

Structure des Messages

Les messages Diameter sont encodés en binaire avec la structure suivante :

En-tête Diameter (20 octets)
|— Version (1 octet) = 1

```
└── Longueur du Message (3 octets)
└── Drapeaux (1 octet)
    ├── R : Demande (1) / Réponse (0)
    ├── P : Proxiable
    ├── E : Erreur
    └── T : Potentiellement retransmis
└── Code de Commande (3 octets)
└── ID d'Application (4 octets) = 16777238 (Gx)
└── ID Hop-by-Hop (4 octets)
└── ID End-to-End (4 octets)
```

AVPs (Paires Attribut-Valeur)

```
└── En-tête AVP
    ├── Code AVP
    ├── Drapeaux (V, M, P)
    ├── Longueur AVP
    └── ID de Fournisseur (optionnel)
└── Données AVP
```

Concepts Clés de Diameter

AVP (Attribut-Valeur) :

- Unité de données de base dans Diameter
- Contient un code, des drapeaux et une valeur
- Peut être imbriqué (AVP Groupé)

Commande :

- Paire Demande/Réponse
- CCR (Demande de Contrôle de Crédit) / CCA (Réponse de Contrôle de Crédit)

Codes de Résultat :

- 2001 - DIAMETER_SUCCESS
- 3xxx - Erreurs de protocole
- 4xxx - Échecs transitoires
- 5xxx - Échecs permanents

Messages de Contrôle de Crédit

Le PGW-C utilise l'**Application de Contrôle de Crédit Diameter** (RFC 4006) pour Gx.

Types de Messages

CCR-Initial (Demande de Contrôle de Crédit - Initial)

Quand : L'UE crée une nouvelle connexion PDN

But :

- Demander des règles de politique et de facturation initiales
- Fournir le contexte de l'UE et du réseau au PCRF
- Obtenir des paramètres QoS et une autorisation de facturation

AVPs Clés Envoyés par le PGW-C :

Nom AVP	Code AVP	Type	Description
Session-Id	263	UTF8String	Identifiant de session Gx unique
Auth-Application-Id	258	Unsigned32	16777238 (Gx)
Origin-Host	264	DiamIdent	Identité Diameter du PGW-C
Origin-Realm	296	DiamIdent	Domaine Diameter du PGW-C
Destination-Realm	283	DiamIdent	Domaine du PCRF
CC-Request-Type	416	Enumerated	1 = INITIAL_REQUEST
CC-Request-Number	415	Unsigned32	Numéro de séquence (commence à 0)
Subscription-Id	443	Grouped	Identifiant de l'UE (IMSI/MSISDN)
Called-Station-Id	30	UTF8String	Nom de l'APN
Framed-IP-Address	8	OctetString	Adresse IPv4 allouée à l'UE
IP-CAN-Type	1027	Enumerated	5 = 3GPP-EPS
RAT-Type	1032	Enumerated	1004 = EUTRAN
QoS-Information	1016	Grouped	QoS actuelle (AMBR)
Network-Request-Support	1024	Enumerated	Procédures initiées par le réseau
Supported-Features	628	Grouped	Liste des fonctionnalités Gx

Exemple de Structure CCR-I :

```
CCR (Code de Commande : 272, Demande)
└── Session-Id: "pgw_c.example.com;123;456"
└── Auth-Application-Id: 16777238
└── Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
└── Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
└── Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
└── CC-Request-Type: INITIAL_REQUEST (1)
└── CC-Request-Number: 0
└── Subscription-Id (Groupé)
    └── Subscription-Id-Type: END_USER_IMSI (1)
```

```

    └ Subscription-Id-Data: "310260123456789"
    └ Called-Station-Id: "internet"
    └ Framed-IP-Address: 100.64.1.42
    └ IP-CAN-Type: 3GPP-EPS (5)
    └ RAT-Type: EUTRAN (1004)
    └ QoS-Information (Groupé)
        └ APN-Aggregate-Max-Bitrate-UL: 100000000 (100 Mbps)
        └ APN-Aggregate-Max-Bitrate-DL: 50000000 (50 Mbps)
    └ Network-Request-Support: 1
    └ Supported-Features: [...]

```

CCA-Initial (Réponse de Contrôle de Crédit - Initial)

Envoyé par : PCRF en réponse à CCR-I

But :

- Autoriser ou rejeter la session
- Fournir des règles PCC pour la gestion du trafic
- Spécifier les paramètres QoS

AVPs Clés Reçus par le PGW-C :

Nom AVP	Code AVP	Description
Result-Code	268	Succès (2001) ou code d'erreur
Experimental-Result	297	Codes de résultat spécifiques au fournisseur
QoS-Information	1016	QoS autorisée (peut différer de la demande)
Charging-Rule-Install	1001	Règles PCC à activer
Charging-Rule-Definition	1003	Définitions de règles en ligne
Default-EPS-Bearer-QoS	1049	QoS pour le porteur par défaut

Exemple de Réponse de Succès :

```

CCA (Code de Commande : 272, Réponse)
    └ Session-Id: "pgw_c.example.com;123;456"
    └ Result-Code: DIAMETER_SUCCESS (2001)
    └ Origin-Host: "pcrf.example.com"
    └ Origin-Realm: "example.com"
    └ Auth-Application-Id: 16777238
    └ CC-Request-Type: INITIAL_REQUEST (1)
    └ CC-Request-Number: 0
    └ QoS-Information (Groupé)
        └ APN-Aggregate-Max-Bitrate-UL: 50000000 (50 Mbps - réduit)
        └ APN-Aggregate-Max-Bitrate-DL: 100000000 (100 Mbps - augmenté)
    └ Charging-Rule-Install (Groupé)
        └ Charging-Rule-Name: "default_internet_rule"
        └ Charging-Rule-Name: "video_streaming_rule"
    └ Charging-Rule-Definition (Groupé)

```

```
└─ Charging-Rule-Name: "default_internet_rule"  
└─ QoS-Information: {...}  
└─ Precedence: 1000
```

CCR-Termination (Demande de Contrôle de Crédit - Terminaison)

Quand : L'UE se détache ou la connexion PDN est supprimée

But :

- Notifier le PCRF de la terminaison de la session
- Enregistrement final de comptabilité/facturation

Différences Clés par Rapport à CCR-I :

- CC-Request-Type: TERMINATION_REQUEST (3)
- Peut inclure des statistiques d'utilisation
- Ensemble AVP simplifié

Exemple CCR-T :

```
CCR (Code de Commande : 272, Demande)  
└─ Session-Id: "pgw_c.example.com;123;456"  
└─ Auth-Application-Id: 16777238  
└─ Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"  
└─ Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"  
└─ Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"  
└─ CC-Request-Type: TERMINATION_REQUEST (3)  
└─ CC-Request-Number: 1  
└─ Termination-Cause: DIAMETER_LOGOUT (1)
```

CCA-Termination

Envoyé par : PCRF en réponse à CCR-T

But :

- Accuser réception de la terminaison de la session
- Aucune règle de politique retournée

Exemple CCA-T :

```
CCA (Code de Commande : 272, Réponse)  
└─ Session-Id: "pgw_c.example.com;123;456"  
└─ Result-Code: DIAMETER_SUCCESS (2001)  
└─ Origin-Host: "pcrf.example.com"  
└─ Origin-Realm: "example.com"
```

```
└── Auth-Application-Id: 16777238
└── CC-Request-Type: TERMINATION_REQUEST (3)
└── CC-Request-Number: 1
```

Règles de Politique et de Facturation

Structure de la Règle PCC

Une **Règle PCC (Contrôle de Politique et de Facturation)** définit comment gérer des flux de trafic spécifiques :

Composants de la Règle

1. Nom de la Règle :

- Identifiant unique pour la règle
- Exemple : "video_streaming_rule"

2. Précérence :

- Un nombre plus bas = une priorité plus élevée
- Plage : 0-65535
- Utilisé lorsque plusieurs règles correspondent

3. Filtres de Flux (TFT - Modèle de Flux de Trafic) :

- Définit quels paquets correspondent à cette règle
- Exemples :
 - IP 5-tuple : Protocole, Src/Dst IP, Src/Dst Port
 - "permit out ip from any to 8.8.8.8 80"

4. Informations QoS :

- **QCI (Identifiant de Classe QoS)** : 1-9 (normalisé), 128-254 (spécifique à l'opérateur)
 - QCI 1 : Voix Conversationnelle
 - QCI 5 : Signalisation IMS
 - QCI 9 : Internet par Défaut
- **ARP (Priorité d'Allocation et de Rétention)** : Capacité de préemption
- **MBR/GBR** : Débits Maximum/Garantis

5. Informations de Facturation :

- **Groupe de Tarification** : Identifie la catégorie de facturation (utilisé par OCS - voir [Interface Diameter Gy](#))
- **Méthode de Mesure** : Volume, temps ou événement
- **Facturation en Ligne/Hors Ligne** : OCS (prépayé via [Diameter Gy](#)) vs.

CDRs hors ligne (postpayé - voir [Format de CDR de Données](#))

6. Statut de Gating :

- **OUVERT** : Autoriser le trafic
- **FERMÉ** : Bloquer le trafic

Provisionnement Dynamique de Règles

Le PCRF peut fournir des règles de deux manières :

1. Règles Prédéfinies (par nom) :

```
Charging-Rule-Install (Groupé)
└─ Charging-Rule-Name: "gold_subscriber_internet"
└─ Charging-Rule-Name: "video_qos_boost"
```

2. Règles Dynamiques (définition en ligne) :

```
Charging-Rule-Definition (Groupé)
└─ Charging-Rule-Name: "dynamic_rule_123"
└─ Precedence: 100
└─ Flow-Information (Groupé)
    └─ Flow-Description: "permit out ip from any to 192.0.2.0/24"
        └─ Flow-Direction: DOWLINK
└─ QoS-Information (Groupé)
    └─ QoS-Class-Identifier: 5
    └─ Max-Requested-Bandwidth-UL: 10000000
        └─ Max-Requested-Bandwidth-DL: 50000000
└─ Rating-Group: 1000
```

AVP d'Informations QoS

APN-AMBR (Débit Maximum Agrégé) :

S'applique à tous les porteurs non-GBR pour cet APN :

```
QoS-Information (Groupé)
└─ APN-Aggregate-Max-Bitrate-UL: 100000000 # 100 Mbps
└─ APN-Aggregate-Max-Bitrate-DL: 200000000 # 200 Mbps
```

Réponse du PGW-C :

- Met à jour l'état interne AMBR
- Envoie une Demande de Modification de Session au PGW-U avec le QER mis à jour

Configuration

Configuration de Base Gx

Modifier config/runtime.exs :

```
config :pgw_c,
diameter: %{
  # Adresse IP à écouter pour les connexions Diameter
  listen_ip: "0.0.0.0",

  # Identité Diameter du PGW-C (Origin-Host)
  host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",

  # Domaine Diameter du PGW-C (Origin-Realm)
  realm: "epc.mnc999.mcc999.3gppnetwork.org",

  # Liste des pairs PCRF
  peer_list: [
    %{
      # Identité Diameter du PCRF
      host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",

      # Domaine du PCRF (généralement le même que le domaine du
      # PGW-C)
      realm: "epc.mnc999.mcc999.3gppnetwork.org",

      # Adresse IP du PCRF
      ip: "10.0.0.30",

      # Si le PGW-C initie la connexion au PCRF
      # true = PGW-C se connecte au PCRF
      # false = Attendre que le PCRF se connecte
      initiate_connection: true
    }
  ]
}
```

Plusieurs Pairs PCRF

Pour la redondance ou la distribution géographique :

```
config :pgw_c,
diameter: %{
  listen_ip: "0.0.0.0",
  host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
  realm: "epc.mnc999.mcc999.3gppnetwork.org",
  peer_list: [
```

```

%{
    host: "pcrf-primary.example.com",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    ip: "10.0.1.30",
    initiate_connection: true
},
%{
    host: "pcrf-backup.example.com",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    ip: "10.0.2.30",
    initiate_connection: true
}
]
}

```

Équilibrage de Charge :

- Le protocole Diameter gère la sélection des pairs
- Les demandes sont distribuées en fonction de la disponibilité
- Basculement automatique en cas de défaillance d'un pair

Résolution de Noms d'Hôtes

Les Identités Diameter doivent être des FQDN (Noms de Domaine Entièrement Qualifiés) :

```

# CORRECT - format FQDN
host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org"

# INCORRECT - Pas une Identité Diameter valide
host: "pgw_c"
host: "10.0.0.20" # Les adresses IP ne sont pas autorisées

```

Format de Domaine :

- Doit être un nom de domaine valide
- Correspond généralement au format PLMN 3GPP : epc.mncXXX.mccYYY.3gppnetwork.org

Flux de Messages

Établissement de Session Réussi

Remarque : Les paramètres QoS du PCRF sont traduits en QERs (Règles d'Application de QoS) et programmés dans le PGW-U via PFCP. Voir [Interface PFCP](#) pour les détails des QER.

Mise à Jour de Politique (Initiée par le Réseau)

Terminaison de Session

Gestion des Erreurs

Codes de Résultat

Le PGW-C gère divers codes de résultat Diameter dans les messages CCA :

Codes de Succès :

Code	Nom	Action
2001	DIAMETER_SUCCESS	Continuer l'établissement de la session

Échecs Permanents (5xxx) :

Code	Nom	Action PGW-C
5002	DIAMETER_UNKNOWN_SESSION_ID	Journaliser l'erreur, échouer la session
5030	DIAMETER_USER_UNKNOWN	Rejeter la session (Utilisateur Inconnu)
5140	DIAMETER_ERROR_INITIAL_PARAMETERS	Journaliser l'erreur, réessayer ou échouer
5003	DIAMETER_AUTHORIZATION_REJECTED	Rejeter la session (Non Autorisé)

Échecs Transitoires (4xxx) :

Code	Nom	Action PGW-C
4001	DIAMETER_AUTHENTICATION_REJECTED	Réessayer ou échouer la session
4010	DIAMETER_TOO_BUSY	Réessayer avec un temps d'attente
4012	DIAMETER_UNABLE_TO_COMPLY	Journaliser l'erreur, peut réessayer

Codes de Résultat Expérimentaux

Codes d'erreur spécifiques au fournisseur :

```
Experimental-Result (Groupé)
└─ Vendor-Id: 10415 (3GPP)
└─ Experimental-Result-Code: <code spécifique au fournisseur>
```

Codes Expérimentaux 3GPP Courants :

Code	Nom	Signification
5065	IP_CAN_SESSION_NOT_AVAILABLE	Le PCRF ne peut pas établir de session
5143	INVALID_SERVICE_INFORMATION	Données de service invalides

Gestion des Délais d'Attente

Délai d'Attente CCR-I :

Si le PCRF ne répond pas à CCR-Initial dans le délai imparti :

1. Le PGW-C attend le délai configuré (par exemple, 5 secondes)
2. Si aucun CCA reçu :
 - Journaliser : "Délai d'attente CCR-Initial pour Session-ID : ..."
 - Répondre au SGW-C avec un code d'erreur
 - Nettoyer les ressources allouées
3. Le SGW-C reçoit : Réponse de Création de Session (Cause : Pair Distant Non Répondant)

Réponse d'Erreur au SGW-C :

Fichier : /lib/session/impl/message_handlers.ex

```
{:error, :credit_control_initial_request_timeout} ->
Procedures.do_gtp_c_error_response(
  from,
  :create_session_response,
  seq_num,
  :remote_peer_not_responding
)
```

Scénarios d'Échec

Scénario 1 : Le PCRF Rejette la Session (Utilisateur Inconnu)

Scénario 2 : PCRF Temporairement Indisponible

Dépannage

Problèmes Courants

1. Échec de Connexion au Pair Diameter

Symptômes :

- Journal : "Pair Diameter non connecté"
- Aucun CCR-Initial envoyé

Causes Possibles :

- PCRF non accessible
- IP du PCRF incorrect dans la configuration
- Pare-feu bloquant le port Diameter (3868)
- Identités Diameter incorrectes (hôte/domaine)

Résolution :

```
# Tester la connectivité réseau
ping <pcrf_ip>

# Tester le port Diameter (TCP 3868)
telnet <pcrf_ip> 3868

# Vérifier la configuration de l'identité Diameter
# Assurez-vous que l'hôte et le domaine sont des FQDN, pas des IP
```

Vérifiez la Configuration :

```
config :pgw_c,
diameter: %{
    # Doit être un FQDN, pas une IP
    host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    peer_list: [
        %{
            host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
            ip: "10.0.0.30"
        }
    ]
}
```

2. Délais d'Attente CCR-Initial

Symptômes :

- La Demande de Création de Session échoue
- Journal : "Délai d'attente CCR-Initial"

Causes Possibles :

- PCRF surchargé
- Latence réseau
- PCRF ne répond pas à cet ID de session

Résolution :

1. Vérifiez les journaux du PCRF pour des erreurs
2. Vérifiez que le PCRF traite les demandes
3. Vérifiez la latence réseau : ping <pcrf_ip>
4. Augmentez le délai d'attente si la latence réseau est élevée

3. Sessions Rejetées par le PCRF

Symptômes :

- CCA-Initial avec Result-Code != 2001
- La Réponse de Création de Session échoue

Codes de Résultat Courants :

Code de Résultat	Cause Probable	Résolution
5030	IMSI non dans la base de données des abonnés	Provisionner l'abonné dans HSS/SPR
5003	Autorisation rejetée	Vérifier les autorisations de l'abonné
4010	PCRF trop occupé	Réessayer ou ajouter de la capacité au PCRF

Vérifiez les Journaux :

```
# Les journaux du PGW-C montrent :  
[error] Erreur Diameter Gx : Result-Code 5030 (DIAMETER_USER_UNKNOWN)  
[error] IMSI 3102609999999999 rejeté par le PCRF
```

4. QoS Non Appliquée

Symptômes :

- Session établie mais mauvaise QoS
- Les débits ne correspondent pas aux valeurs attendues

Étapes de Débogage :

1. Vérifiez CCA-Initial :

- Vérifiez que l'AVP QoS-Information est présent
- Vérifiez les valeurs APN-Aggregate-Max-Bitrate-UL/DL

2. Vérifiez l'Établissement de Session PFCP :

- Vérifiez que le QER a été créé avec les bonnes valeurs MBR

- Vérifiez les journaux du PGW-U pour l'installation du QER

3. Vérifiez la Politique du PCRF :

- Vérifiez la configuration du PCRF
- Vérifiez que le profil d'abonné inclut la bonne QoS

5. Problèmes de Routage Diameter

Symptômes :

- Les messages Diameter n'atteignent pas le PCRF
- Journal : "Aucun itinéraire vers le Domaine de Destination"

Cause :

- Mismatch de domaine entre la configuration et les messages

Résolution :

Assurez-vous de la cohérence :

```
# Tous doivent correspondre
config :pgw_c,
diameter: %{
    realm: "epc.mnc999.mcc999.3gppnetwork.org", # Domaine du PGW-C
    peer_list: [
        %{
            realm: "epc.mnc999.mcc999.3gppnetwork.org" # Domaine du PCRF
            (généralement le même)
        }
    ]
}
```

Dans CCR-Initial :

```
Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
```

Surveillance de la Santé Gx

Métriques Clés :

```
# Taux de messages Gx
rate(gx_inbound_messages_total{message_type="cca"}[5m])

# Taux d'erreurs Gx
rate(gx_inbound_errors_total[5m])
```

```
# Compte des sessions Gx
session_id_registry_count

# Durée de traitement des messages Gx
histogram_quantile(0.95,
rate(gx_inbound_handling_duration_bucket[5m]))
```

Exemples d'Alerte :

```
# Alerte sur un taux d'erreur Gx élevé
- alert: GxErrorRateHigh
  expr: rate(gx_inbound_errors_total[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Taux d'erreur Gx élevé détecté"

# Alerte sur un délai d'attente Gx
- alert: GxTimeout
  expr: rate(gx_inbound_errors_total{error_type="timeout"}[5m]) >
0.05
  for: 2m
  annotations:
    summary: "Des délais d'attente Gx se produisent"

# Alerte sur le rejet de session Gx
- alert: GxSessionRejection
  expr: rate(gx_inbound_errors_total{result_code="5030"}[5m]) > 0.01
  for: 5m
  annotations:
    summary: "Le PCRF rejette les sessions (USER_UNKNOWN)"
```

Journalisation de Débogage

Activer la journalisation verbose de Diameter :

```
# config/runtime.exs
config :logger, level: :debug

# Ou à l'exécution
iex> Logger.configure(level: :debug)
```

Recherchez :

- [debug] Envoi de CCR-Initial pour Session-ID : ...
 - [debug] Reçu CCA-Initial : Result-Code 2001
 - [error] Erreur Diameter : ...
-

Interface Web - Surveillance des Pairs Diameter

OmniPGW inclut une interface Web en temps réel pour surveiller les connexions et l'état des pairs Diameter.

Page des Pairs Diameter

Accès : `http://<omnipgw-ip>:<web-port>/diameter`

But : Surveiller la connectivité des pairs Diameter Gx au PCRF en temps réel

Fonctionnalités :

1. Vue d'Ensemble de la Connexion des Pairs

- **Compte Connecté** - Nombre de pairs PCRF avec connexion active
- **Compte Déconnecté** - Nombre de pairs configurés mais non connectés
- Actualisation automatique toutes les 1 seconde (taux d'actualisation le plus rapide de toutes les pages)

2. Informations de Statut par Pair

Pour chaque pair PCRF configuré :

- **Hôte** - Identité Diameter (Origin-Host)
- **Adresse IP** - IP du PCRF
- **Port** - Port Diameter (par défaut 3868)
- **Statut** - Connecté (vert) / Déconnecté (rouge)
- **Transport** - TCP ou SCTP
- **Initiation de Connexion** - Qui initie (PGW ou PCRF)
- **Domaine** - Domaine Diameter
- **Nom du Produit** - Identifiant de produit PCRF (s'il est annoncé)
- **IDs d'Application** - Applications Diameter prises en charge (par exemple, Gx = 16777238)

3. Détails Développables

Cliquez sur n'importe quelle ligne de pair pour voir :

- Configuration complète du pair
- Détails de l'Échange de Capacités (CER/CEA)
- Fonctionnalités prises en charge
- État de connexion complet

Cas d'Utilisation Opérationnels

Surveiller la Connectivité du PCRF :

1. Ouvrir la page Diameter dans le navigateur
2. Vérifier que tous les pairs PCRF affichent "Connecté"
3. Vérifier que l'Initiation de Connexion correspond à la configuration

4. Vérifier que les IDs d'Application incluent Gx (16777238)

Dépanner les Échecs de Création de Session (Problèmes Gx) :

1. Les sessions utilisateur échouent avec des erreurs "Délai d'attente PCRF"
2. Ouvrir la page Diameter
3. Vérifier le statut du pair :
 - Déconnecté ?
 - Vérifier la connectivité réseau
 - Vérifier que le PCRF fonctionne
 - Vérifier les règles de pare-feu pour TCP 3868
 - Connecté mais les sessions échouent ?
 - Le problème est au niveau de l'application (vérifier les journaux)
 - Le PCRF peut rejeter les abonnés

Vérifier la Configuration Diameter :

1. Après avoir configuré un nouveau pair PCRF
2. Ouvrir la page Diameter
3. Vérifier que le pair apparaît dans la liste
4. Vérifier que le statut change en "Connecté"
5. Développer le pair pour vérifier :
 - Le domaine correspond à la configuration
 - Les IDs d'Application incluent Gx
 - Le Nom du Produit montre l'identifiant du PCRF

Surveiller le Basculement :

Scénario : Le PCRF principal échoue

1. La page Diameter montre "Déconnecté" pour le principal
2. Vérifier que le PCRF de secours est toujours "Connecté"
3. Les nouvelles sessions utilisent automatiquement le secours
4. Lorsque le principal se rétablit, le statut revient à "Connecté"

Déetecter les Problèmes de Routage Diameter :

- Le pair affiche "Connecté" mais le mauvais domaine
- Les IDs d'Application n'incluent pas Gx (16777238)
- Le Nom du Produit ne correspond pas au PCRF attendu

Identifier les Mismatches de Configuration :

L'interface Web montre :

Initiation de Connexion : "Le pair initie"

Mais la configuration dit :

initiate_connection: true

Cela indique :

- OmniPGW tente de se connecter
- Mais le PCRF initie également
- Peut causer des conditions de course de connexion

Avantages :

- **Taux d'actualisation le plus rapide** - Mises à jour toutes les 1 seconde
- **Statut de connexion visuel** - Indication immédiate rouge/verte
- **Aucun outil Diameter nécessaire** - Pas besoin d'outils CLI diameter
- **Configuration du pair visible** - Vérifiez les paramètres sans consulter les fichiers de configuration
- **Détails au niveau de l'application** - Voir les applications Diameter prises en charge
- **Vérification de domaine** - Confirmer la configuration de routage Diameter

Intégration avec les Métriques

Bien que l'interface Web fournit un statut en temps réel, combinez-la avec Prometheus pour :

- Taux d'erreurs Gx historiques
- Comptes de messages CCR/CCA
- Tendances de latence

Interface Web = "Est-ce que ça fonctionne en ce moment ?" Métriques = "Comment ça a fonctionné dans le temps ?"

Documentation Connexe

Configuration et Politique

- [**Guide de Configuration**](#) - Configuration Diameter, configuration des pairs PCRF
- [**Interface PFCP**](#) - Application de QoS via QERs des règles PCC
- [**Gestion des Sessions**](#) - Cycle de vie de la session avec intégration de la politique
- [**Gestion de la QoS & des Porteurs**](#) - Configuration détaillée de la QoS et configuration des porteurs

Intégration de Facturation

- [**Interface Diameter Gy**](#) - Facturation en ligne déclenchée par les règles PCC
- [**Format de CDR de Données**](#) - Enregistrements de facturation hors ligne avec informations de politique

- [**Configuration PCO**](#) - Livraison P-CSCF pour le contrôle de politique IMS

Opérations

- [**Guide de Surveillance**](#) - Métriques Gx, suivi des politiques, alertes de connectivité PCRF
 - [**Interface S5/S8**](#) - Intégration de la gestion des porteurs avec la politique
-

[**Retour au Guide des Opérations**](#)

Diamètre de Facturation en Ligne (Interface Gy/Ro)

Système de Facturation en Ligne (OCS)

Table des Matières

1. [Aperçu](#)
2. [Architecture de Facturation 3GPP](#)
3. [Notions de Base de l'Interface Gy/Ro](#)
4. [Messages de Contrôle de Crédit](#)
5. [Flux de Facturation en Ligne](#)
6. [Contrôle de Facturation des Porteuses](#)
7. [Contrôle de Crédit pour Plusieurs Services](#)
8. [Configuration](#)
9. [Flux de Messages](#)
10. [Gestion des Erreurs](#)
11. [Intégration avec Gx](#)
12. [Dépannage](#)

Aperçu

L'interface Gy (également appelée **interface Ro** dans les contextes IMS) connecte le PGW-C au **Système de Facturation en Ligne (OCS)** pour le contrôle de crédit en temps réel. Cela permet :

- **Facturation Prépayée** - Autorisation et déduction de crédit en temps réel
- **Contrôle de Crédit en Temps Réel** - Accorder un quota avant la livraison du service
- **Facturation Basée sur le Service** - Facturation différente pour la voix, les données, les SMS, etc.
- **Mises à Jour de Compte Immédiates** - Mises à jour du solde de crédit en temps réel
- **Refus de Service** - Bloquer le service lorsque le crédit est épuisé

Facturation en Ligne vs. Hors Ligne

Aspect	Facturation en Ligne (Gy/Ro)	Facturation Hors Ligne (Gz/Rf)
Temps	En temps réel, avant le service	Après la livraison du service
Cas d'Utilisation	Abonnés prépayés	Abonnés postpayés
Vérification de Crédit	Oui, avant d'accorder le service	Non, facture générée plus tard
Système	OCS (Système de Facturation en Ligne) CGF/CDF (Fonction de Données de Facturation)	
Risque	Pas de perte de revenus	Risque de factures impayées
Complexité	Élevée (exigences en temps réel)	Inférieure (traitement par lots)
Impact sur l'Utilisateur	Service refusé si pas de crédit	Service toujours disponible

Voir aussi : [Format CDR de Données](#) pour les enregistrements de facturation hors ligne (facturation postpayée)

Voir aussi : [Gestion des Sessions](#) pour le cycle de vie complet de la session PDN, y compris l'intégration de la facturation

Gy dans l'Architecture Réseau

Fonctions Clés

Fonction	Description
Authorisation de Crédit	Demander un quota à l'OCS avant de permettre le trafic
Gestion de Quota	Suivre les unités accordées (octets, temps, événements)
Détection d'Épuisement de Crédit	Surveiller le quota restant
Ré-autorisation	Demander un quota supplémentaire lorsque le seuil est atteint
Interruption de Service	Arrêter le service lorsque le crédit est épuisé
Règlement Final	Rapporter l'utilisation réelle à la fin de la session

Architecture de Facturation 3GPP

Points de Référence de Facturation

Fonction de Déclenchement de Facturation (CTF)

Le PGW-C agit comme un **CTF (Fonction de Déclenchement de Facturation)**, responsable de :

1. Détecter les événements facturables - Début de session, utilisation des données, fin de session
2. Demander l'autorisation de crédit - Avant de permettre le service
3. Suivre la consommation de quota - Surveiller les unités accordées
4. Générer des événements de facturation - Déclencher des demandes de crédit
5. Appliquer le contrôle de crédit - Bloquer le trafic lorsque le quota est épuisé

Fonction de Facturation en Ligne (OCF)

L'OCS met en œuvre la **OCF (Fonction de Facturation en Ligne)** :

1. **Gestion du solde de compte** - Suivre le crédit de l'abonné
2. **Tarification** - Déterminer le prix par unité (par Mo, par seconde, etc.)
3. **Réservation de Crédit** - Réserver du crédit pour le quota accordé
4. **Déduction de Crédit** - Déduire lors du rapport d'utilisation
5. **Décisions de Politique** - Accorder ou refuser en fonction du solde

Notions de Base de l'Interface Gy/Ro

Référence 3GPP

- Spécification : 3GPP TS 32.229 (Architecture de facturation)
- Protocole : 3GPP TS 32.251 (Facturation du domaine PS)
- ID d'Application Diamètre : 4 (Gy/Ro - Application de Contrôle de Crédit)
- Protocole de Base : RFC 4006 (Application de Contrôle de Crédit Diamètre)

Concept de Session

Chaque connexion PDN UE nécessitant une facturation en ligne a une **session Gy/Ro** identifiée par un **Session-ID**. Cette session :

- Créeée lorsque la porteuse nécessite une facturation en ligne (CCR-Initial)
- Mise à jour lorsque le quota est consommé (CCR-Update)
- Terminée lorsque la session se termine (CCR-Termination)

Format de l'ID de Session

Session-ID: <Origin-Host>;<high32>;<low32>[;<optional>]
Exemple: omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org;9876543210;12345;gy

Composants :

- **Origin-Host** : Identifie le PGW-C
- **high32** : 32 bits supérieurs de l'identifiant unique
- **low32** : 32 bits inférieurs de l'identifiant unique
- **optional** : Identifiant supplémentaire (par exemple, "gy" pour distinguer de Gx)

Messages de Contrôle de Crédit

Types de Messages

CCR-Initial (Demande de Contrôle de Crédit - Initial)

Quand : L'UE crée une connexion PDN et la porteuse nécessite une facturation en ligne

But :

- Demander une autorisation de crédit initiale à l'OCS
- Réserver un quota pour la livraison du service
- Établir une session Gy/Ro

AVPs Clés Envoyés par PGW-C :

Nom AVP	Code AVP	Type	Description
Session-Id	263	UTF8String	Identifiant unique de session Gy
Auth-Application-Id	258	Unsigned32	4 (Contrôle de Crédit)
Origin-Host	264	DiamIdent	Identité Diamètre du PGW-C
Origin-Realm	299	DiamIdent	Domaine Diamètre du PGW-C
Destination-Realm	283	DiamIdent	Domaine de l'OCs
CC-Request-Type	416	Enumerated1	= INITIAL_REQUEST
CC-Request-Number	415	Unsigned32	Numéro de séquence (commence à 0)
Subscription-Id	443	Grouped	Identifiant de l'UE (IMSI/MSISDN)
Service-Context-Id	461	UTF8String	Identifiant de contexte de facturation
Multiple-Services-Credit-Control	456	Grouped	Demandes de crédit spécifiques au service
Requested-Service-Unit	437	Grouped	Quota demandé (octets, temps, etc.)
Used-Service-Unit	446	Grouped	Quota utilisé (0 pour initial)
Service-Identifier	439	Unsigned32	Identifiant de type de service
Rating-Group	432	Unsigned32	Identifiant de catégorie de facturation

Exemple de Structure CCR-I :

```
CCR (Code de Commande : 272, Demande)
└─ Session-Id: "pgw_c_example.com;123;456;gy"
  └─ Auth-Application-Id: 4
  └─ Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
  └─ Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
  └─ Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
  └─ CC-Request-Type: INITIAL_REQUEST (1)
  └─ CC-Request-Number: 0
  └─ Subscription-Id: (Grouped)
    └─ Subscription-Id-Type: END_USER_IMSI (1)
    └─ Subscription-Id-Data: "3102601234567899"
  └─ Subscription-Id: (Grouped)
    └─ Subscription-Id-Type: END_USER_E164 (0)
    └─ Subscription-Id-Data: "+15551234567"
  └─ Service-Context-Id: "3225163gpp.org"
  └─ Multiple-Services-Credit-Control (Grouped)
    └─ Service-Identifier: 1
    └─ Rating-Group: 100
    └─ Requested-Service-Unit (Grouped)
      └─ CC-Total-Octets: 10000000 (demande 10 Mo)
    └─ Used-Service-Unit (Grouped)
      └─ CC-Total-Octets: 0 (aucune utilisation encore)
```

CCA-Initial (Réponse de Contrôle de Crédit - Initial)

Envoyé par : OCS en réponse à CCR-I

But :

- Accorder ou refuser l'autorisation de crédit
- Fournir un quota pour la livraison du service
- Spécifier les paramètres de tarification et de facturation

AVPs Clés Reçus par PGW-C :

Nom AVP	Code AVP	Description
Result-Code	268	Succès (2001) ou code d'erreur
Multiple-Services-Credit-Control	456	Accords de crédit spécifiques au service
Granted-Service-Unit	431	Quota accordé (octets, temps, etc.)
Validity-Time	448	Période de validité du quota (secondes)
Result-Code	268	Code de résultat par service
Final-Unit-Indication	430	Action lorsque le quota est épuisé
Volume-Quota-Threshold	-	Seuil pour ré-autorisation

Exemple de Réponse de Succès :

```
CCA (Code de Commande : 272, Réponse)
└─ Session-Id: "pgw_c_example.com;123;456;gy"
  └─ Result-Code: DIAMETER_SUCCESS (2001)
  └─ Origin-Host: "ocs.example.com"
  └─ Origin-Realm: "example.com"
  └─ Auth-Application-Id: 4
  └─ CC-Request-Type: INITIAL_REQUEST (1)
  └─ CC-Request-Number: 0
  └─ Multiple-Services-Credit-Control (Grouped)
    └─ Result-Code: DIAMETER_SUCCESS (2001)
    └─ Service-Identifier: 1
    └─ Rating-Group: 100
    └─ Granted-Service-Unit (Grouped)
      └─ CC-Total-Octets: 10000000 (accordé 10 Mo)
    └─ Validity-Time: 3600 (quota valide pour 1 heure)
    └─ Volume-Quota-Threshold: 8000000 (ré-accès à 8 Mo utilisés, 80%)
```

CCR-Update (Demande de Contrôle de Crédit - Mise à Jour)

Quand :

- Seuil de quota accordé atteint (par exemple, 80 % consommé)
- Temps de validité expiré
- Changement de service nécessitant une ré-autorisation
- Changement de temps de tarif

But :

- Demander un quota supplémentaire
- Rapporter l'utilisation du quota précédemment accordé
- Mettre à jour les paramètres de facturation

Définitions Clés par Rapport à CCR-I :

- CC-Request-Type: UPDATE_REQUEST (2)
- CC-Request-Number incrémenté
- Used-Service-Unit contient l'utilisation réelle
- Requested-Service-Unit pour plus de quota

Exemple de Structure CCR-U :

```
CCR (Code de Commande : 272, Demande)
└─ Session-Id: "pgw_c_example.com;123;456;gy"
  └─ Auth-Application-Id: 4
  └─ Origin-Host: "omni-pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
  └─ Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
  └─ Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
  └─ CC-Request-Type: UPDATE_REQUEST (2)
  └─ CC-Request-Number: 1
  └─ Multiple-Services-Credit-Control (Grouped)
    └─ Service-Identifier: 1
    └─ Rating-Group: 100
    └─ Used-Service-Unit (Grouped)
      └─ CC-Total-Octets: 8000000 (8 Mo utilisés jusqu'à présent)
    └─ Requested-Service-Unit (Grouped)
      └─ CC-Total-Octets: 10000000 (demander encore 10 Mo)
```

CCA-Update (Réponse de Contrôle de Crédit - Mise à Jour)

Envoyé par : OCS en réponse à CCR-U

But :

- Accorder un quota supplémentaire (si crédit disponible)
- Accuser réception de l'utilisation
- Mettre à jour les paramètres de facturation

Résultats Possibles :

1. Plus de Quota Accordé :

```
CCA (Mise à Jour)
└─ Multiple-Services-Credit-Control
    └─ Result-Code: DIAMETER_SUCCESS (2001)
    └─ Granted-Service-Unit
        └─ CC-Total-Octets: 10000000 (encore 10 Mo)
    └─ Validity-Time: 3600
```

2. Quota Final (Crédit Épuisé) :

```
CCA (Mise à Jour)
└─ Multiple-Services-Credit-Control
    └─ Result-Code: DIAMETER_SUCCESS (2001)
    └─ Granted-Service-Unit
        └─ CC-Total-Octets: 1000000 (il reste seulement 1 Mo)
    └─ Final-Unit-Indication
        └─ Final-Unit-Action: TERMINATE (0)
```

3. Pas de Crédit Disponible :

```
CCA (Mise à Jour)
└─ Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)
└─ Multiple-Services-Credit-Control
    └─ Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012)
    └─ Final-Unit-Indication
        └─ Final-Unit-Action: TERMINATE (0)
```

CCR-Termination (Demande de Contrôle de Crédit - Terminaison)

Quand :

- L'UE se détache
- Connexion PDN supprimée
- Session terminée pour une raison quelconque

But :

- Rapport final d'utilisation
- Fermer la session Gy/Ro
- Règlement final

Differences Clés :

- CC-Request-Type: TERMINATION_REQUEST (3)
- Used-Service-Unit contient l'utilisation finale
- Pas de Requested-Service-Unit (plus de quota nécessaire)
- Inclut Termination-Cause

Exemple de Structure CCR-T :

```
CCR (Code de Commande : 272, Demande)
└─ Session-Id: "pgw_c.example.com;123;456;gy"
└─ Auth-Application-Id: 4
└─ Origin-Host: "pgw_c.epc.mnc999.mcc999.3gppnetwork.org"
└─ Origin-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
└─ Destination-Realm: "epc.mnc999.mcc999.3gppnetwork.org"
    CC-Request-Type: TERMINATION_REQUEST (3)
    CC-Request-Number: 5
    Termination-Cause: DIAMETER_LOGOUT (1)
    Multiple-Services-Credit-Control (Grouped)
        └─ Service-Identifier: 1
            └─ Rating-Group: 100
            └─ Used-Service-Unit (Grouped)
                └─ CC-Total-Octets: 18500000 (18,5 Mo d'utilisation totale)
```

CCA-Termination (Réponse de Contrôle de Crédit - Terminaison)

Envoyé par : OCS en réponse à CCR-T

But :

- Accuser réception de la terminaison de session
- Compléter la comptabilité
- Libérer le crédit réservé

Exemple CCA-T :

```
CCA (Code de Commande : 272, Réponse)
└─ Session-Id: "pgw_c.example.com;123;456;gy"
└─ Result-Code: DIAMETER_SUCCESS (2001)
└─ Origin-Host: "ocs.example.com"
└─ Origin-Realm: "example.com"
└─ Auth-Application-Id: 4
└─ CC-Request-Type: TERMINATION_REQUEST (3)
└─ CC-Request-Number: 5
```

Flux de Facturation en Ligne

Types d'Unités de Service

L'OCS peut accorder un quota dans différentes unités :

Type d'Unité	AVP	Description	Cas d'Utilisation
Temps	CC-Time	Secondes	Appels vocaux, durée de session
Volume	CC-Total-Octets	Octets (total montant montant)	Services de données
Volume (séparé)	CC-Input-Octets, CC-Output-Octets	Octets (séparés)	Facturation asymétrique
Spécifique au Service	CC-Service-Specific-Units	Unités personnalisées	SMS, MMS, appels API
Événements	-	Événements comptés	Services payants à l'utilisation

Gestion du Seuil de Quota

Problème : Comment PGW-C sait-il quand demander plus de quota ?

Solution : L'OCS fournit un **Volume-Quota-Threshold** ou **Time-Quota-Threshold**. PGW-C surveille l'utilisation via les Rapports de Session PFCP de PGW-U (voir [Interface PFCP](#)).

Exemple de Flux :

1. L'OCS accorde un quota de 10 Mo avec un seuil de 80 % (8 Mo)
2. PGW-C surveille l'utilisation via les rapports d'utilisation de PGW-U (Rapports de Session PFCP)
3. Lorsque l'utilisation atteint 8 Mo :
 - PGW-C envoie CCR-Update
 - Continue à permettre le trafic (n'attend pas de réponse)
4. L'OCS répond avec plus de quota
5. Si le quota est épuisé avant l'envoi de CCR-Update :
 - PGW-C doit bloquer le trafic

Calcul du Seuil :

Granted-Service-Unit: 10000000 octets (10 Mo)
Volume-Quota-Threshold: 8000000 octets (8 Mo)

Lorsque 8 Mo consommés → Déclencher CCR-Update
Tampon restant : 2 Mo (permet du temps pour la réponse de l'OCS)

Surveillance de PGW-C :

PGW-C surveille l'utilisation via **Rapports de Session PFCP** de PGW-U :

Indication de l'Unité Finale

Que se passe-t-il lorsque le crédit est épuisé ?

L'OCS inclut l'AVP **Final-Unit-Indication** dans CCA pour spécifier l'action :

Final-Unit-Action	Valeur	Comportement de PGW-C
TERMINATE	0	Bloquer tout le trafic, initier la terminaison de session
REDIRECT	1	Rediriger le trafic vers le portail (par exemple, page de recharge)
RESTRICT_ACCESS	2	Autoriser l'accès uniquement à des services spécifiques (par exemple, serveur de recharge)

Exemple : Unité Finale avec Redirection

```

CCA (Mise à Jour)
└─ Multiple-Services-Credit-Control
    └─ Result-Code: DIAMETER_SUCCESS (2001)
        └─ Granted-Service-Unit
            └─ CC-Total-Octets: 1000000 (dernier 1 Mo)
                └─ Final-Unit-Indication
                    └─ Final-Unit-Action: REDIRECT (1)
                        └─ Redirect-Server (Grouped)
                            └─ Redirect-Address-Type: URL (2)
                                └─ Redirect-Server-Address: "http://topup.example.com"

```

Actions de PGW-C :

1. TERMINATE : Envoyer CCR-T, supprimer la porteuse
2. REDIRECT : Installer une règle PFCP pour rediriger HTTP vers l'URL de recharge
3. RESTRICT_ACCESS : Installer des règles PFCP permettant uniquement les IP sur liste blanche

Contrôle de Facturation des Porteuses

Qu'est-ce qui Contrôle si une Porteuse est Facturée ?

Spécification 3GPP : TS 23.203, TS 29.212, TS 32.251

La facturation des porteuses est contrôlée par des **Règles PCC** fournies par le PCRF via l'interface Gx. Voir [Interface Diamètre Gx](#) pour la documentation complète des règles PCC.

Flux de Décision de Facturation :

Règle PCC avec Informations de Facturation

Réponse PCRF (CCA-I sur Gx) :

```

CCA (Interface Gx)
└─ Charging-Rule-Definition (Grouped)
    └─ Charging-Rule-Name: "prepaid_data_rule"
        └─ Rating-Group: 100
        └─ Online: 1 (activer la facturation en ligne)
        └─ Offline: 0 (désactiver la facturation hors ligne)
        └─ Metering-Method: VOLUME (1)
        └─ Precedence: 100
        └─ Flow-Information: [...]
        └─ QoS-Information: [...]

```

AVPs de Facturation Clés dans les Règles PCC :

Nom AVP	Code AVP	Valeurs	Description
Rating-Group	432	Unsigned32	Catégorie de facturation (correspond à un tarif dans l'OCS)
Online	1009	0=Désactiver, 1=Activer	Activer la facturation en ligne (Gy)
Offline	1008	0=Désactiver, 1=Activer	Activer la facturation hors ligne (Gz)
Metering-Method	1007	0=Durée, 1=Volume, 2=Les Deux	Ce qu'il faut mesurer
Reporting-Level	1011	0=Service, 1=Groupe de Tarification	Granularité des rapports d'utilisation

Matrice de Décision de Facturation des Porteuses

En Ligne	Hors Ligne	Rating-Group	Comportement
1	0	Présent	Facturation en ligne uniquement (prépayé)
0	1	Présent	Facturation hors ligne uniquement (postpayé)
1	1	Présent	Facturation en ligne et hors ligne (convergente)
0	0	-	Pas de facturation (service gratuit)

Groupes de Tarification Multiples

Une seule connexion PDN peut avoir **plusieurs porteuses avec différents groupes de tarification** :

Scénario d'Exemple :

Porteuse par Défaut (Internet)

```

└─ Rating-Group: 100 (Données Standard)
    └─ En Ligne: 1

```

Porteuse Dédiée 1 (Streaming Vidéo)

```

└─ Rating-Group: 200 (Service Vidéo)
    └─ En Ligne: 1

```

Porteuse Dédiée 2 (Voix IMS)

```

└─ Rating-Group: 300 (Voix)
    └─ En Ligne: 1

```

Comportement Gy de PGW-C :

- Un seul CCR-I avec plusieurs sections MSCC (Multiple-Services-Credit-Control) :

```

CCR-Initial
└─ Session-Id: "..."
    └─ Multiple-Services-Credit-Control
        └─ [Rating-Group: 100] → Données Standard
        └─ [Rating-Group: 200] → Service Vidéo
        └─ [Rating-Group: 300] → Voix

```

Réponse de l'OCS :

```

CCA-Initial
└─ Multiple-Services-Credit-Control
    └─ [Rating-Group: 100] → Accordé : 10 Mo
    └─ [Rating-Group: 200] → Accordé : 5 Mo (vidéo plus cher)
    └─ [Rating-Group: 300] → Accordé : 60 secondes

```

Application de la Facturation par Service

PGW-C suit le quota par Rating-Group :

```

# Pseudocode
state.charging_quotas = {
    100 => %{granted: 10_000_000, used: 0, threshold: 8_000_000},
    200 => %{granted: 5_000_000, used: 0, threshold: 4_000_000},
    300 => %{granted: 60_000, used: 0, threshold: 48_000} # millisecondes
}

```

Surveillance de l'Utilisation par Porteuse :

Contrôle de Crédit pour Plusieurs Services

AVP MSCC (Multiple-Services-Credit-Control)

But : Regrouper les informations de facturation pour un service/groupe de tarification spécifique

Structure :

```

Multiple-Services-Credit-Control (Grouped, AVP 456)
└─ Service-Identifier (Unsigned32, AVP 439)
└─ Rating-Group (Unsigned32, AVP 432)
└─ Requested-Service-Unit (Grouped, AVP 437)
    └─ CC-Time (Unsigned32, AVP 420)
    └─ CC-Total-Octets (Unsigned64, AVP 421)
    └─ CC-Input-Octets (Unsigned64, AVP 412)
    └─ CC-Output-Octets (Unsigned64, AVP 414)

```

Used-Service-Unit (Grouped, AVP 446)
└ [Même structure que Requested-Service-Unit]
Granted-Service-Unit (Grouped, AVP 431)
└ [Même structure que Requested-Service-Unit]
Validity-Time (Unsigned32, AVP 448)
Result-Code (Unsigned32, AVP 268)
Final-Unit-Indication (Grouped, AVP 430)
└ Final-Unit-Action (Enumerated, AVP 449)

Service-Identifier vs. Rating-Group

Attribut	Service-Identifier	Rating-Group
But	Identifie le type de service	Identifie la catégorie de facturation
Exemple	1=Données, 2=Voix, 3=SMS	100=Régulier, 200=Premium
Granularité	Classification large	Tarif spécifique
Requis	Optionnel	Requis pour la facturation
Mapping	Peut correspondre à plusieurs RG	Tarif unique dans l'OCS

Exemple :

Service-Identifier: 1 (Service de Données)
└ Rating-Group: 100 (Données Standard - 0,01 \$/Mo)
└ Rating-Group: 200 (Données Premium - 0,05 \$/Mo)
Service-Identifier: 2 (Voix)

└ Rating-Group: 300 (Appels Vocaux - 0,10 \$/min)

Configuration

Configuration de Base de Gy

Modifier config/runtime.exs :

```
config :pgw_c,
  online_charging: %{
    # Activer ou désactiver la facturation en ligne globalement
    enabled: true,
    # Délai de connexion OCS (millisecondes)
    timeout_ms: 5000,
    # Quota par défaut demandé (octets) s'il n'est pas spécifié par le PCRF
    default_requested_quota: 10_000_000, # 10 Mo
    # Pourcentage de seuil pour ré-autorisation
    # (0.8 = déclencher CCR-Update à 80 % de quota consommé)
    quota_threshold_percentage: 0.8,
    # Action lorsque le délai d'attente OCS se produit
    # Options : :block, :allow
    timeout_action: :block,
    # Action lorsque l'OCS ne retourne pas de crédit
    # Options : :terminate, :redirect
    no_credit_action: :terminate,
    # URL de redirection pour la recharge (utilisée si no_credit_action: :redirect)
    topup_redirect_url: "http://topup.example.com"
  },
  diameter: %{
    listen_ip: "0.0.0.0",
    host: "omni-pgw.c.epc.mnc999.mcc999.3gppnetwork.org",
    realm: "epc.mnc999.mcc999.3gppnetwork.org",
    # Configuration du pair OCS
    peer_list: [
      # PCRF pour le contrôle de politique (Gx)
      %{
        host: "pcrf.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.30",
        initiate_connection: true
      },
      # OCS pour la facturation en ligne (Gy)
      %{
        host: "ocs.epc.mnc999.mcc999.3gppnetwork.org",
        realm: "epc.mnc999.mcc999.3gppnetwork.org",
        ip: "10.0.0.40",
        initiate_connection: true
      }
    ]
  }
```

Explication des Paramètres de Configuration

enabled

- true : Facturation en ligne active, messages CCR envoyés à l'OCS
- false : Facturation en ligne désactivée, pas de messages Gy

timeout_ms

- Temps d'attente pour la réponse CCA de l'OCS
- Recommandé : 3000-5000 ms

default_requested_quota

- Quota par défaut à demander si le PCRF ne spécifie pas
- Valeurs typiques : 1-100 Mo

quota_threshold_percentage

- Déclencher CCR-Update lorsque ce % de quota est consommé
- Recommandé : 0.75-0.85 (75%-85%)
- Plus élevé = moins de messages, mais risque d'épuisement de quota
- Plus bas = plus de messages, mais plus sûr

timeout_action

- :block - Bloquer le trafic si l'OCS ne répond pas (plus sûr, empêche la perte de revenus)
- :allow - Autoriser le trafic si l'OCS ne répond pas (meilleure expérience utilisateur, risque de revenus)

no_credit_action

- :terminate - Supprimer la porteuse lorsque le crédit est épuisé
- :redirect - Rediriger vers le portail de recharge

Configuration Spécifique à l'Environnement

Production (abonnés prépayés) :

```
config :pgw_c,
  online_charging: %{
    enabled: true,
    timeout_action: :block,
    no_credit_action: :terminate,
    quota_threshold_percentage: 0.8
  }
```

Test/Développement :

```
config :pgw_c,
  online_charging: %{
    enabled: false # Désactiver pour les tests
  }
```

Hybride (certains prépayés, certains postpayés) :

```
config :pgw_c,
  online_charging: %
    enabled: true, # Contrôlé par abonné par le PCRF
    timeout_action: :allow, # Ne pas bloquer le postpayé en cas d'échec de l'OCS
    no_credit_action: :terminate
}
```

Flux de Messages

Session Réussie avec Facturation en Ligne

Ré-autorisation de Quota (CCR-Update)

Épuisement de Crédit (Unité Finale)

Gestion des Délais d'Attente de l'OCS

Gestion des Erreurs

Codes de Résultat

Codes de Succès :

Code	Nom	Action
2001	DIAMETER_SUCCESS	Continuer avec le quota accordé

Échecs Transitoires (4xxx) :

Code	Nom	Action PGW-C
4010	DIAMETER_TOO_BUSY	Réessayer avec un retour
4011	DIAMETER_UNABLE_TO_COMPLY	Journaliser l'erreur, peut réessayer
4012	DIAMETER_CREDIT_LIMIT_REACHED	Terminer ou rediriger

Échecs Permanents (5xxx) :

Code	Nom	Action PGW-C
5003	DIAMETER_AUTHORIZATION_REJECTED	Rejeter la session
5031	DIAMETER_USER_UNKNOWN	Rejeter la session (abonné invalide)

Codes de Résultat par Service

Important : Le Result-Code peut apparaître à deux niveaux :

1. Niveau de message - Résultat global
2. Niveau MSCC - Résultat par service

Exemple :

```
CCA-Initial
└─ Result-Code: DIAMETER_SUCCESS (2001) ← Niveau de message : OK
  └─ Multiple-Services-Credit-Control
    └─ [Rating-Group: 100]
      └─ Result-Code: DIAMETER_SUCCESS (2001) ← RG 100 : OK
        └─ [Rating-Group: 200]
          └─ Result-Code: DIAMETER_CREDIT_LIMIT_REACHED (4012) ← RG 200 : Pas de crédit
```

Comportement de PGW-C :

- Autoriser le trafic pour le Rating-Group 100
- Bloquer le trafic pour le Rating-Group 200

Intégration avec Gx

L'interface Gx (contrôle de politique PCRF) détermine si la facturation en ligne est requise et fournit le Rating-Group qui entraîne la facturation Gy. Voir [Interface Diamètre Gx](#) pour la documentation complète sur le contrôle de politique.

Relation entre Gx et Gy

Flux d'Intégration

1. Configuration de Porteuse :

PGW-C reçoit la Demande de Création de Session

↓

Envoyer CCR-I au PCRF (Gx)

↓

Recevoir CCA-I avec Règles PCC

↓

Analysé les Règles PCC :

- La règle a-t-elle un Rating-Group ?

- En Ligne = 1 ?

↓

Si OUI :

Envoyer CCR-I à l'OCS (Gy) avec Rating-Group

↓

Recevoir CCA-I avec quota

↓

Si quota accordé : Procéder

Si pas de crédit : Rejeter la porteuse

Si NON :

Procéder sans facturation en ligne

2. Mise à Jour de Politique Dynamique (RAR du PCRF) :

Le PCRF envoie RAR (Re-Auth-Request) sur Gx

↓

Nouvelle Règle PCC ajoutée avec En Ligne=1, Rating-Group=200

↓

PGW-C envoie CCR-U à l'OCS (Gy)

- Ajouter MSCC pour Rating-Group 200

↓

L'OCS accorde un quota pour le nouveau service

↓

Installer une porteuse dédiée avec facturation en ligne

Dépannage

Problèmes Courants

1. Délais d'Attente CCR-Initial vers OCS

Symptômes :

- Les sessions échouent avec "délai d'attente OCS"
- Journal : "CCR-Initial (Gy) délai d'attente"

Causes Possibles :

- OCS non accessible
- IP OCS incorrect dans la configuration
- Pare-feu bloquant le port Diamètre (3868)
- OCS surcharge

Résolution :

Tester la connectivité réseau

```

ping <ocs_ip>
# Tester le port Diamètre (TCP 3868)
telnet <ocs_ip> 3868
# Vérifier la configuration
# Assurez-vous que le paire OCS est configuré dans peer_list

```

2. Sessions Rejetées par l'OCS

Symptômes :

- CCA-I avec Result-Code != 2001
- Échec de la Réponse à la Création de Session

Codes de Résultat Courants :

Code de Résultat	Cause Probable	Résolution
4012	Limite de crédit atteinte	L'abonné doit recharger
5003	Autorisation rejetée	Vérifier les permissions de l'abonné
5031	Utilisateur inconnu	Provisionner l'abonné dans l'OCS

Étapes de Débogage :

1. Vérifier les journaux de l'OCS pour la raison du rejet
2. Vérifier le solde de l'abonné dans l'OCS
3. Vérifier que l'IMSI/MSISDN dans CCR-I correspond à l'enregistrement de l'abonné

3. Épuisement de Quota Non Détecté

Symptômes :

- L'utilisateur continue d'utiliser des données après épuisement du solde
- Aucun CCR-Update envoyé

Causes Possibles :

- URR (Règles de Rapport d'Utilisation) non installée dans PGW-U
- Seuil non configuré correctement
- Rapports de Session PFPCP non reçus

Étapes de Débogage :

1. Vérifier URR dans l'établissement de Session PFPCP :

```

Créer URR
└── URR-ID: 1
    ├── Measurement-Method: VOLUME
    ├── Volume-Threshold: 8000000 (8 Mo)
    └── Reporting-Triggers: VOLUME_THRESHOLD

```

2. Vérifier les journaux de PGW-U pour les rapports d'utilisation
3. Vérifier quota_threshold_percentage dans la configuration

4. Rating-Group Incorrect

Symptômes :

- L'OCS rejette avec "Rating-Group Inconnu"
- Les sessions échouent

Cause :

- Rating-Group dans CCR-I ne correspond pas à la configuration de l'OCS
- PCRF a provisionné un Rating-Group invalide

Résolution :

1. Vérifier le Rating-Group dans la Régule PCC du PCRF
2. Vérifier la configuration de l'OCS pour les Rating-Groups valides
3. Assurez-vous que le mapping entre les Règles PCC et les tarifs de l'OCS est correct

Surveillance

Métriques Clés

```

# Taux de messages Gy
rate(gy_inbound_messages_total{message_type="cca"}[5m])
rate(gy_outbound_messages_total{message_type="ccr"}[5m])

# Taux d'erreurs Gy
rate(gy_inbound_errors_total[5m])

# Événements d'épuisement de quota
rate(gy_quota_exhausted_total[5m])

# Taux de délai d'attente OCS
rate(gy_timeout_total[5m])

# Durée de traitement des messages Gy
histogram_quantile(0.95, rate(gy_inbound_handling_duration_bucket[5m]))

```

Alertes

```

# Alert sur un taux d'erreur Gy élevé
- alert: GyErrorRateHigh
  expr: rate(gy_inbound_errors_total[5m]) > 0.1
  for: 5m
  annotations:
    summary: "Taux d'erreur Gy élevé détecté"

# Alert sur délai d'attente OCS
- alert: OcsTimeout
  expr: rate(gy_timeout_total[5m]) > 0.05
  for: 2m
  annotations:
    summary: "Délai d'attente OCS en cours"

# Alert sur pic d'épuisement de crédit
- alert: CreditExhaustionSpike
  expr: rate(gy_quota_exhausted_total[5m]) > 10
  for: 5m
  annotations:
    summary: "Taux élevé d'épuisement de crédit"

```

Interface Web - Simulateur de Contrôle de Crédit Gy

OmniPGW inclut un simulateur Gy/Ro intégré pour tester la fonctionnalité de facturation en ligne sans nécessiter un OCS externe.

Accès : http://<omnipgw-ip>:<web-port>/gy_simulator

PGW-C v0.1.0

Licensed to: Omnitouch
© 2025 Omnitouch

- [Resources](#)
- [Configuration](#)
- [Topology](#)
- [UE Search](#)
- [PGW Sessions](#)
- [Session History](#)
- [IP Pools](#)
- [Diameter](#)
- [PFCP Sessions](#)
- [UPF Status](#)
- [UPF Selection](#)
- [P-CSCF Monitor](#)
- [Gy Simulator](#)
- [Logs](#)



Gy Credit Control Simulator

Request Parameters

IMSI	<input type="text" value="e.g., 318170123456789"/>		
MSISDN	<input type="text" value="e.g., 14155551234"/>		
Requested Units (bytes)	Service ID	Rating Group	
<input type="text" value="1000000"/>	<input type="text" value="1"/>	<input type="text" value="1"/>	<button style="background-color: #007bff; color: white; padding: 5px 10px;">Send CCR-I</button>

But : Tester et simuler des scénarios de facturation en ligne pour les abonnés prépayés

Fonctionnalités :

1. Paramètres de Demande

- **IMSI** - Identité de l'abonné (par exemple, "310170123456789")
- **MSISDN** - Numéro de téléphone (par exemple, "14155551234")
- **Unités Demandées** - Montant du quota à demander (en octets)
- **ID de Service** - Identifiant de type de service
- **Groupe de Tarification** - Catégorie de facturation

2. Simulation CCR-I

- Envoyer CCR-Initial (Demande de Contrôle de Crédit Initial)
- Simule la demande de quota initiale lors de l'établissement de session
- Teste l'intégration de l'OCS sans trafic en direct

3. Cas d'Utilisation

- **Tests de Développement** - Tester l'interface Gy pendant le développement
- **Intégration OCS** - Vérifier la connectivité et les réponses de l'OCS
- **Tests de Quota** - Tester différents scénarios de quota
- **Dépannage** - Déboguer les problèmes de facturation
- **Démonstration** - Démontrer la facturation en ligne aux parties prenantes

Comment Utiliser :

1. Entrer les détails de l'abonné (IMSI, MSISDN)
2. Définir les unités demandées (par exemple, 1000000 pour 1 Mo)
3. Configurer l'ID de Service et le Groupe de Tarification
4. Cliquer sur "Envoyer CCR-I"
5. Voir la réponse de l'OCS et le quota accordé

Avantages :

- Pas besoin d'un OCS externe pendant les tests
- Validation rapide de la logique de facturation
- Environnement de test sécurisé
- Utile pour la formation et les démonstrations

Documentation Connexe

Facturation et Politique

- [Interface Diamètre Gx](#) - Contrôle de politique PCRF, règles PCC qui déclenchent la facturation en ligne
- [Format CDR de Données](#) - Enregistrements de facturation hors ligne pour la facturation postpayée
- [Guide de Configuration](#) - Paramètres de configuration complets pour la facturation en ligne

Gestion des Sessions

- [Gestion des Sessions](#) - Cycle de vie de la session PDN, gestion des porteuses
- [Interface PFCP](#) - Rapport d'utilisation de PGW-U via URR
- [Interface S5/S8](#) - Configuration et démontage de la porteuse GTP-C

Opérations

- [Guide de Surveillance](#) - Métriques Gy, suivi de quota, alertes de délai d'attente OCS
- [Allocation d'IP UE](#) - Configuration de pool d'IP pour les sessions facturées

[Retour au Guide des Opérations](#)



Guide de Surveillance et de Métriques d'OmniPGW

Intégration Prometheus et Surveillance Opérationnelle

par Omnitouch Network Services

Table des Matières

1. [Aperçu](#)
 2. [Point de Terminaison des Métriques](#)
 3. [Métriques Disponibles](#)
 4. [Configuration de Prometheus](#)
 5. [Tableaux de Bord Grafana](#)
 6. [Alertes](#)
 7. [Surveillance des Performances](#)
 8. [Dépannage des Métriques](#)
-

Aperçu

OmniPGW fournit deux approches de surveillance complémentaires :

1. Interface Web en Temps Réel (couverte brièvement ici, détaillée dans les documents d'interface respectifs)

- Visualiseur de session en direct
- État des pairs PFCP
- Connectivité des pairs Diameter
- Inspection de session individuelle

2. Métriques Prometheus (principal objectif de ce document)

- Tendances historiques et analyses
- Alertes et notifications
- Métriques de performance
- Planification de capacité

Ce document se concentre sur les **métriques Prometheus**. Pour les détails de l'interface Web, voir :

- [Gestion des Sessions - Interface Web](#)
- [Interface PFCP - Interface Web](#)
- [Diameter Gx - Interface Web](#)

Aperçu des Métriques Prometheus

OmniPGW expose des **métriques compatibles avec Prometheus** pour une surveillance complète de la santé, de la performance et de la capacité du système. Cela permet aux équipes opérationnelles de :

- **Surveiller la Santé du Système** - Suivre les sessions actives, les allocations et les erreurs
- **Planification de Capacité** - Comprendre les tendances d'utilisation des ressources
- **Analyse de Performance** - Mesurer la latence de traitement des messages
- **Alertes** - Notification proactive des problèmes
- **Débogage** - Identifier les causes profondes des problèmes

Architecture de Surveillance

Point de Terminaison des Métriques

Configuration

Activez les métriques dans config/runtime.exs :

```
config :pgw_c,
  metrics: %{
    enabled: true,
    ip_address: "0.0.0.0", # Lier à toutes les interfaces
    port: 9090,           # Port HTTP
    registry_poll_period_ms: 5_000 # Intervalle de sondage
  }
```

Accès aux Métriques

Point de Terminaison HTTP :

```
http://<omnippgw_ip>:<port>/metrics
```

Exemple :

```
curl http://10.0.0.20:9090/metrics
```

Format de Sortie

Les métriques sont exposées au format **texte Prometheus** :

```
# HELP teid_registry_count Le nombre de TEID enregistrés pour les sessions
# TYPE teid_registry_count gauge
teid_registry_count 150

# HELP address_registry_count Le nombre d'adresses enregistrées pour les sessions
# TYPE address_registry_count gauge
address_registry_count 150

# HELP s5s8_inbound_messages_total Le nombre total de messages reçus des pairs S5/S8
# TYPE s5s8_inbound_messages_total counter
s5s8_inbound_messages_total{message_type="create_session_request"} 1523
s5s8_inbound_messages_total{message_type="delete_session_request"} 1487
```

Métriques Disponibles

OmniPGW expose les catégories de métriques suivantes :

Métriques de Session

Comptes de Sessions Actives :

Nom de la Métrique	Type	Description
teid_registry_count	Gauge	Sessions S5/S8 actives (nombre de TEID)
seid_registry_count	Gauge	Sessions PFCP actives (nombre de SEID)
session_id_registry_count	Gauge	Sessions Gx actives (nombre d'ID de Session Diameter)
address_registry_count	Gauge	Adresses IP UE allouées
charging_id_registry_count	Gauge	IDs de facturation actifs (voir Format CDR de Données pour les enregistrements de facturation CDR)

Utilisation :

```
# Sessions actives actuelles
teid_registry_count
```

```
# Taux de création de session (par seconde)
rate(teid_registry_count[5m])

# Sessions maximales au cours de la dernière heure
max_over_time(teid_registry_count[1h])
```

Compteurs de Messages

Messages S5/S8 (GTP-C) :

Nom de la Métrique	Type	Étiquettes	Description
s5s8_inbound_messages_total	Counter	message_type	Nombre total de messages S5/S8 entrants
s5s8_outbound_messages_total	Counter	message_type	Nombre total de messages S5/S8 sortants
s5s8_inbound_errors_total	Counter	message_type	Erreurs de traitement S5/S8

Types de Messages :

- create_session_request
- create_session_response
- delete_session_request
- delete_session_response
- create_bearer_request
- delete_bearer_request

Messages Sxb (PFCP) :

Nom de la Métrique	Type	Étiquettes	Description
sxb_inbound_messages_total	Counter	message_type	Nombre total de messages PFCP entrants
sxb_outbound_messages_total	Counter	message_type	Nombre total de messages PFCP sortants
sxb_inbound_errors_total	Counter	message_type	Erreurs de traitement PFCP

Types de Messages :

- association_setup_request
- association_setup_response
- heartbeat_request
- heartbeat_response
- session_establishment_request
- session_establishment_response
- session_modification_request
- session_deletion_request

Messages Gx (Diameter) :

Nom de la Métrique	Type	Étiquettes	Description
gx_inbound_messages_total	Counter	message_type	Nombre total de messages Diameter entrants
gx_outbound_messages_total	Counter	message_type	Nombre total de messages Diameter sortants
gx_inbound_errors_total	Counter	message_type	Erreurs de traitement Diameter

Types de Messages :

- cca (Réponse de Contrôle de Crédit)
- ccr_initial
- ccr_termination

Métriques de Latence

Durée de Traitement des Messages :

Nom de la Métrique	Type	Étiquettes	Description
s5s8_inbound_handling_duration	Histogram	request_message_type	Temps de traitement des messages S5/S8
sxb_inbound_handling_duration	Histogram	request_message_type	Temps de traitement des messages

Nom de la Métrique	Type	Étiquettes	Description
gx_inbound_handling_duration	Histogram	request_message_type Diameter	PFCP Temps de traitement des messages

Seaux (microsecondes) :

- Valeurs typiques : 100µs, 500µs, 1ms, 5ms, 10ms, 50ms, 100ms, 500ms, 1s, 5s

Utilisation :

```
# Latence S5/S8 au 95e percentile
histogram_quantile(0.95,
  rate(s5s8_inbound_handling_duration_bucket[5m])
)

# Latence PFCP moyenne
rate(sxb_inbound_handling_duration_sum[5m]) /
rate(sxb_inbound_handling_duration_count[5m])
```

Métriques Système

Métriques de la VM Erlang :

Nom de la Métrique	Type	Description
vm_memory_total	Gauge	Mémoire totale de la VM (octets)
vm_memory_processes	Gauge	Mémoire utilisée par les processus
vm_memory_system	Gauge	Mémoire utilisée par le système
vm_system_process_count	Gauge	Nombre total de processus Erlang
vm_system_port_count	Gauge	Nombre total de ports ouverts

Configuration de Prometheus

Configuration de Scrape

Ajoutez OmniPGW au fichier `prometheus.yml` de Prometheus :

```
# prometheus.yml
global:
  scrape_interval: 15s
  evaluation_interval: 15s

scrape_configs:
  - job_name: 'omnipgw'
    static_configs:
      - targets: ['10.0.0.20:9090']
        labels:
          instance: 'omnipgw-01'
          environment: 'production'
          site: 'datacenter-1'
```

Plusieurs Instances OmniPGW

```
scrape_configs:
  - job_name: 'omnipgw'
    static_configs:
      - targets:
          - '10.0.0.20:9090'
          - '10.0.0.21:9090'
          - '10.0.0.22:9090'
        labels:
          environment: 'production'
```

Découverte de Service

Kubernetes :

```
scrape_configs:
  - job_name: 'omnipgw'
    kubernetes_sd_configs:
      - role: pod
    relabel_configs:
      - source_labels: [__meta_kubernetes_pod_label_app]
        action: keep
        regex: omnipgw
      - source_labels: [__meta_kubernetes_pod_ip]
        target_label: __address__
        replacement: '${1}:9090'
```

Vérification

Test de scrape :

```
# Vérifiez les cibles de Prometheus
curl http://prometheus:9090/api/v1/targets

# Interrogez une métrique
curl 'http://prometheus:9090/api/v1/query?query=teid_registry_count'
```

Tableaux de Bord Grafana

Configuration du Tableau de Bord

1. Ajouter la Source de Données Prometheus :

Configuration → Sources de Données → Ajouter une source de données → Prometheus
URL : http://prometheus:9090

2. Importer le Tableau de Bord :

Créez un nouveau tableau de bord ou importez depuis JSON.

Panneaux Clés

Panneau 1 : Sessions Actives

```
# Requête
teid_registry_count

# Type de Panneau : Gauge
# Seuils :
#   Vert : < 5000
#   Jaune : 5000-8000
#   Rouge : > 8000
```

Panneau 2 : Taux de Session

```
# Requête
rate(s5s8_inbound_messages_total{message_type="create_session_request"}[5m])

# Type de Panneau : Graphique
# Unité : requêtes/sec
```

Panneau 3 : Utilisation du Pool IP

```
# Requête (pour un sous-réseau /24 avec 254 IPs)
(address_registry_count / 254) * 100

# Type de Panneau : Gauge
# Unité : pourcentage (0-100)
# Seuils :
#   Vert : < 70%
#   Jaune : 70-85%
#   Rouge : > 85%
```

Panneau 4 : Latence des Messages (95e Percentile)

```
# Requête
histogram_quantile(0.95,
rate(s5s8_inbound_handling_duration_bucket{request_message_type="create_session_request"}[5m])

# Type de Panneau : Graphique
# Unité : millisecondes
```

Panneau 5 : Taux d'Erreur

```
# Requête
rate(s5s8_inbound_errors_total[5m])

# Type de Panneau : Graphique
# Unité : erreurs/sec
# Seuil d'Alerte : > 0.1
```

Panneau 6 : État d'Association PFCP

```
# Requête
pfcp_peer_associated

# Type de Panneau : Stat
# Mappages :
#   1 = "UP" (Vert)
#   0 = "DOWN" (Rouge)
```

Exemple Complet de Tableau de Bord

```
{
  "dashboard": {
    "title": "OmniPGW - Tableau de Bord des Opérations",
    "panels": [
      {
        "title": "Sessions Actives",
        "targets": [
          {
            "expr": "teid_registry_count",
            "legendFormat": "Sessions Actives"
          }
        ],
        "type": "graph"
      },
      {
        "title": "Taux de Création de Session",
        "targets": [
          {
            "expr": "rate(s5s8_inbound_messages_total{message_type=\"create_session_request\"}[5m])",
            "label": "Taux de Création de Session"
          }
        ],
        "type": "gauge"
      }
    ]
  }
}
```

```

        "legendFormat": "Sessions/sec"
    },
],
"type": "graph"
},
{
"title": "Utilisation du Pool IP",
"targets": [
{
"expr": "(address_registry_count / 254) * 100",
"legendFormat": "Utilisation du Pool %"
}
],
"type": "gauge"
},
{
"title": "Latence des Messages (p95)",
"targets": [
{
"expr": "histogram_quantile(0.95,
rate(s5s8_inbound_handling_duration_bucket[5m]))",
"legendFormat": "S5/S8 p95"
},
{
"expr": "histogram_quantile(0.95,
rate(sxb_inbound_handling_duration_bucket[5m]))",
"legendFormat": "PFCP p95"
}
],
"type": "graph"
}
]
}
}

```

Alertes

Règles d'Alerte

Créez omnipgw_alerts.yml :

```

groups:
- name: omnipgw
  interval: 30s
  rules:
    # Alertes de Compte de Session
    - alert: OmniPGW_HighSessionCount
      expr: teid_registry_count > 8000
      for: 5m
      labels:
        severity: warning
      annotations:
        summary: "Nombre élevé de sessions OmniPGW"
        description: "{{ $value }} sessions actives (seuil : 8000)"

    - alert: OmniPGW_SessionCountCritical
      expr: teid_registry_count > 9500
      for: 2m
      labels:
        severity: critical
      annotations:
        summary: "Nombre critique de sessions OmniPGW"
        description: "{{ $value }} sessions actives approchant de la capacité"

```

```

# Alertes de Pool IP
- alert: OmniPGW_IPPoolUtilizationHigh
  expr: (address_registry_count / 254) * 100 > 80
  for: 10m
  labels:
    severity: warning
  annotations:
    summary: "Utilisation élevée du pool IP OmniPGW"
    description: "Pool IP {{ $value }}% utilisé"

- alert: OmniPGW_IPPoolExhausted
  expr: address_registry_count >= 254
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "Pool IP OmniPGW épuisé"
    description: "Aucune IP disponible pour allocation"

# Alertes de Taux d'Erreur
- alert: OmniPGW_HighErrorRate
  expr: rate(s5s8_inbound_errors_total[5m]) > 0.1
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Taux d'erreur élevé OmniPGW"
    description: "{{ $value }} erreurs/sec sur l'interface S5/S8"

- alert: OmniPGW_GxErrorRate
  expr: rate(gx_inbound_errors_total[5m]) > 0.05
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Erreurs Gx OmniPGW"
    description: "{{ $value }} erreurs Diameter/sec"

# Alertes PFCP
- alert: OmniPGW_PFCPAssociationDown
  expr: pfcp_peer_associated == 0
  for: 1m
  labels:
    severity: critical
  annotations:
    summary: "Pair PFCP {{ $labels.peer }} hors ligne"
    description: "Association PFCP perdue"

- alert: OmniPGW_PFCPHeartbeatFailures
  expr: pfcp_consecutive_heartbeat_failures > 2
  for: 30s
  labels:
    severity: warning
  annotations:
    summary: "Échecs de battement PFCP"
    description: "{{ $value }} échecs consécutifs pour {{ $labels.peer }}"

# Alertes de Latence
- alert: OmniPGW_HighLatency
  expr: |
    histogram_quantile(0.95,
      rate(s5s8_inbound_handling_duration_bucket[5m])
    ) > 100000
  for: 5m
  labels:

```

```

    severity: warning
  annotations:
    summary: "Latence élevée des messages OmniPGW"
    description: "Latence p95 {{ $value }}µs (> 100ms)"

# Alertes Système
- alert: OmniPGW_HighMemoryUsage
  expr: vm_memory_total > 2000000000
  for: 10m
  labels:
    severity: warning
  annotations:
    summary: "Utilisation élevée de la mémoire OmniPGW"
    description: "VM utilisant {{ $value | humanize }}B de mémoire"

- alert: OmniPGW_HighProcessCount
  expr: vm_system_process_count > 100000
  for: 10m
  labels:
    severity: warning
  annotations:
    summary: "Nombre élevé de processus OmniPGW"
    description: "{{ $value }} processus Erlang (fuite potentielle)"

```

Configuration du Gestionnaire d'Alerte

```

# alertmanager.yml
global:
  resolve_timeout: 5m

route:
  receiver: 'ops-team'
  group_by: ['alertname', 'instance']
  group_wait: 10s
  group_interval: 10s
  repeat_interval: 12h

  routes:
    - match:
        severity: critical
        receiver: 'pagerduty'

    - match:
        severity: warning
        receiver: 'slack'

receivers:
  - name: 'ops-team'
    email_configs:
      - to: 'ops@example.com'

  - name: 'slack'
    slack_configs:
      - api_url: 'https://hooks.slack.com/services/YOUR/SLACK/WEBHOOK'
        channel: '#omnipgw-alerts'
        title: 'Alerte OmniPGW : {{ .GroupLabels.alertname }}'
        text: '{{ range .Alerts }}{{ .Annotations.description }}{{ end }}'

  - name: 'pagerduty'
    pagerduty_configs:
      - service_key: 'YOUR_PAGERDUTY_KEY'

```

Surveillance des Performances

Indicateurs Clés de Performance (KPI)

Requêtes de Débit

Taux de Configuration de Session :

```
rate(s5s8_inbound_messages_total{message_type="create_session_request"}[5m])
```

Taux de Suppression de Session :

```
rate(s5s8_inbound_messages_total{message_type="delete_session_request"}[5m])
```

Croissance Nette des Sessions :

```
rate(s5s8_inbound_messages_total{message_type="create_session_request"}[5m]) -  
rate(s5s8_inbound_messages_total{message_type="delete_session_request"}[5m])
```

Analyse de Latence

Latence de Traitement des Messages (Percentiles) :

```
# p50 (Médiane)  
histogram_quantile(0.50,  
    rate(s5s8_inbound_handling_duration_bucket[5m])  
)  
  
# p95  
histogram_quantile(0.95,  
    rate(s5s8_inbound_handling_duration_bucket[5m])  
)  
  
# p99  
histogram_quantile(0.99,  
    rate(s5s8_inbound_handling_duration_bucket[5m])  
)
```

Répartition de la Latence par Type de Message :

```
histogram_quantile(0.95,  
    rate(s5s8_inbound_handling_duration_bucket[5m])  
) by (request_message_type)
```

Tendance de Capacité

Tendance de Croissance des Sessions (24h) :

```
teid_registry_count -  
teid_registry_count offset 24h
```

Capacité Restante :

```
# Pour une capacité maximale de 10 000 sessions  
10000 - teid_registry_count
```

Temps jusqu'à l'Épuisement de la Capacité :

```
# Jours jusqu'à l'épuisement de la capacité (basé sur le taux de croissance sur 1h)  
(10000 - teid_registry_count) /  
(rate(teid_registry_count[1h]) * 86400)
```

Dépannage des Métriques

Identification des Problèmes

Problème : Taux de Rejet de Session Élevé

Requête :

```
rate(s5s8_inbound_errors_total[5m]) by (message_type)
```

Action :

- Vérifiez les journaux d'erreurs
- Vérifiez la connectivité PCRF (erreurs Gx)
- Vérifiez l'épuisement du pool IP

Problème : Configuration de Session Lente

Requête :

```
histogram_quantile(0.95,  
rate(s5s8_inbound_handling_duration_bucket{request_message_type="create_session_request"}[5m])
```

Action :

- Vérifiez la latence Gx (temps de réponse PCRF)
- Vérifiez la latence PFCP (temps de réponse PGW-U)
- Examinez l'utilisation des ressources système

Problème : Fuite de Mémoire Suspectée

Requêtes :

```
# Tendance de la mémoire totale  
rate(vm_memory_total[1h])  
  
# Tendance de la mémoire des processus  
rate(vm_memory_processes[1h])  
  
# Tendance du nombre de processus  
rate(vm_system_process_count[1h])
```

Action :

- Vérifiez les sessions obsolètes
- Examinez les comptes de registre
- Redémarrez si la fuite est confirmée

Requêtes de Débogage

Trouver le Moment de Pic des Sessions :

```
max_over_time(teid_registry_count[24h])
```

Comparer Actuel vs. Historique :

```
teid_registry_count /  
avg_over_time(teid_registry_count[7d])
```

Identifier les Anomalies :

```
abs(
```

```
teid_registry_count -  
avg_over_time(teid_registry_count[1h])  
) > 100
```

Meilleures Pratiques

Collecte de Métriques

1. **Intervalle de Scrape** : 15-30 secondes (équilibrer granularité et charge)
2. **Rétention** : 15+ jours pour analyse historique
3. **Étiquettes** : Utilisez un étiquetage cohérent (instance, environnement, site)

Conception de Tableau de Bord

1. **Tableau de Bord d'Aperçu** - KPIs de haut niveau pour le NOC
2. **Tableaux de Bord Détails** - Plongée approfondie par interface
3. **Tableau de Bord de Dépannage** - Métriques d'erreurs et journaux

Conception d'Alerte

1. **Éviter la Fatigue d'Alerte** - Alertez uniquement sur des problèmes exploitables
 2. **Escalade** - Avertissement → Critique avec sévérité croissante
 3. **Contexte** - Inclure des liens vers des manuels d'exploitation dans les descriptions d'alerte
-

Documentation Connexe

Configuration et Mise en Place

- [Guide de Configuration](#) - Configuration des métriques Prometheus, mise en place de l'interface Web
- [Guide de Dépannage](#) - Utilisation des métriques pour le débogage

Métriques d'Interface

- [Interface PFCP](#) - Métriques de session PFCP, surveillance de la santé UPF
- [Interface Diameter Gx](#) - Métriques de politique Gx, suivi de l'interaction PCRF
- [Interface Diameter Gy](#) - Métriques de facturation Gy, suivi des quotas, délais OCS
- [Interface S5/S8](#) - Métriques de messages GTP-C, communication SGW-C

Surveillance Spécialisée

- [Surveillance P-CSCF](#) - Métriques de découverte P-CSCF, santé IMS
 - [Gestion des Sessions](#) - Sessions actives, métriques du cycle de vie des sessions
 - [Allocation IP UE](#) - Métriques d'utilisation du pool IP
-

[Retour au Guide des Opérations](#)



Options de Configuration du Protocole (PCO)

Paramètres Réseau Fournis au UE

OmniPGW par Omnitouch Network Services

Vue d'ensemble

PCO (Options de Configuration du Protocole) sont des paramètres réseau envoyés au UE (appareil mobile) lors de l'établissement de la connexion PDN. Ces paramètres permettent au UE d'accéder à des services réseau tels que DNS, IMS, et de configurer les paramètres réseau.

Éléments d'Information PCO :

Nom IE	ID de Conteneur	Description	Requis
Adresse IPv4 du Serveur DNS	0x000D	DNS Principal	Oui
Adresse IPv4 du Serveur DNS	0x000D	DNS Secondaire	Optionnel
Adresse IPv4 du P-CSCF	0x000C	P-CSCF pour IMS	Optionnel (IMS)
MTU de Lien IPv4	0x0010	Unité de transmission maximale	Recommandé
Adresse IPv4 du Serveur NBNS	0x0011	Serveur de noms NetBIOS	Optionnel

Configuration

Configuration de Base

```
# config/runtime.exs
config :pgw_c,
  pco: %{
    # Serveurs DNS (requis)
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",
```

```

# Serveurs NBNS (optionnel, pour appareils Windows)
primary_nbns_server_address: nil,
secondary_nbns_server_address: nil,

# Adresses P-CSCF pour IMS/VoLTE (optionnel)
p_cscf_ipv4_address_list: [],

# Découverte Dynamique P-CSCF (optionnel)
p_cscf_discovery_enabled: false,
p_cscf_discovery_dns_server: nil,
p_cscf_discovery_timeout_ms: 5000,

# Taille MTU IPv4 (octets)
ipv4_link_mtu_size: 1400
}

```

Paramètres PCO

Adresses des Serveurs DNS

DNS Principal et Secondaire :

```

pco: %{
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4"
}

```

Fournisseurs DNS Courants :

Fournisseur	Principal	Secondaire
Google	8.8.8.8	8.8.4.4
Cloudflare	1.1.1.1	1.0.0.1
Quad9	9.9.9.9	149.112.112.112
OpenDNS	208.67.222.222	208.67.220.220

DNS Privé :

```

pco: %{
  primary_dns_server_address: "10.0.0.10",
  secondary_dns_server_address: "10.0.0.11"
}

```

Adresses P-CSCF (IMS)

Pour les Services IMS/VoLTE :

```

pco: %{
    p_cscf_ipv4_address_list: [
        "10.0.0.50", # P-CSCF Principal
        "10.0.0.51" # P-CSCF Secondaire
    ]
}

```

P-CSCF (Fonction de Contrôle de Session d'Appel Proxy) :

- Point d'entrée pour la signalisation IMS
- Requis pour VoLTE, VoWiFi, RCS
- UE utilise SIP via ce serveur

Découverte Dynamique P-CSCF

Découverte P-CSCF Basée sur DNS :

OmniPGW prend en charge la découverte dynamique de P-CSCF via des requêtes DNS comme défini dans 3GPP TS 23.003 et TS 24.229. Lorsqu'elle est activée, PGW-C peut interroger DNS pour les adresses P-CSCF au lieu d'utiliser une configuration statique.

```

pco: %{
    # Activer la découverte dynamique P-CSCF
    p_cscf_discovery_enabled: true,

    # Serveur DNS pour les requêtes P-CSCF (sous forme de tuple)
    p_cscf_discovery_dns_server: {10, 179, 2, 177},

    # Délai d'attente pour les requêtes DNS (millisecondes)
    p_cscf_discovery_timeout_ms: 5000,

    # Liste statique de P-CSCF (utilisée comme secours si DNS échoue)
    p_cscf_ipv4_address_list: ["10.0.0.50"]
}

```

Comment Ça Fonctionne :

1. Lorsque `p_cscf_discovery_enabled: true`, PGW-C effectue des requêtes DNS pour les adresses P-CSCF
2. La requête DNS est envoyée au `p_cscf_discovery_dns_server` configuré
3. Si la requête DNS réussit, les adresses P-CSCF découvertes sont envoyées au UE via PCO
4. Si la requête DNS échoue ou expire, elle revient à la liste statique `p_cscf_ipv4_address_list`
5. Voir [Surveillance P-CSCF](#) pour des détails sur la surveillance et les métriques

Flux de Découverte P-CSCF

Priorité de Découverte :

1. **Découverte FQDN par Règle** (Priorité la Plus Élevée) - p_cscf_discovery_fqdn dans la règle de sélection UPF
2. **Découverte DNS Globale** - p_cscf_discovery_enabled: true dans la configuration PCO globale
3. **Liste Statique PCO de Règle** - p_cscf_ipv4_address_list dans le remplacement PCO de règle
4. **Liste Statique PCO Globale** (Secours) - p_cscf_ipv4_address_list dans la configuration PCO globale

Surveillance :

Tous les essais de découverte P-CSCF sont enregistrés et suivis avec des métriques :

- Taux de succès/échec des requêtes DNS
- Latence de découverte
- Statistiques d'utilisation des secours
- Métriques de découverte par règle et globale

Voir [Surveillance P-CSCF](#) pour des détails complets sur la surveillance.

Options de Configuration :

Paramètre	Type	Par Défaut	Description
p_cscf_discovery_enabled	Booléen	false	Activer la découverte dynamique P-CSCF basée sur DNS
p_cscf_discovery_dns_server	tuple (IP)	nil	Adresse IP du serveur DNS sous forme de tuple à 4 éléments (ex. : {10, 179, 2, 177})
p_cscf_discovery_timeout_ms	Entier	5000	Délai d'attente pour les requêtes DNS en millisecondes

Cas d'Utilisation :

- **Déploiements IMS Dynamiques** - Les adresses P-CSCF changent en fonction de la configuration DNS
- **Équilibrage de Charge Géographique** - DNS renvoie les serveurs P-CSCF les plus proches
- **Haute Disponibilité** - DNS renvoie automatiquement les serveurs P-CSCF disponibles
- **Environnements Multi-Tenants** - Différents abonnés obtiennent différents serveurs P-CSCF

Exemple : IMS en Production avec Découverte DNS

```
pco: %{
    primary_dns_server_address: "10.0.0.10",
    secondary_dns_server_address: "10.0.0.11",

    # Activer la découverte dynamique P-CSCF
    p_cscf_discovery_enabled: true,
    p_cscf_discovery_dns_server: {10, 179, 2, 177}, # Serveur DNS IMS
    p_cscf_discovery_timeout_ms: 3000,

    # Adresses P-CSCF de secours (si DNS échoue)
    p_cscf_ipv4_address_list: [
        "10.0.0.50", # Secours principal
        "10.0.0.51" # Secours secondaire
    ],
    ipv4_link_mtu_size: 1400
}
```

Découverte P-CSCF par Règle :

La découverte P-CSCF peut également être configurée par règle de sélection UPF. Cela permet à différents APN d'utiliser différents serveurs DNS pour la découverte P-CSCF :

```
# Dans la configuration de sélection upf
rules: [
    %{
        name: "Trafic IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [...],

        # Découverte P-CSCF par règle
        p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org"
    }
]
```

Voir [Configuration de Sélection UPF](#) pour des détails sur la découverte P-CSCF par règle.

Voir aussi : [Surveillance P-CSCE](#) pour la surveillance de la découverte P-CSCF et de la santé

Serveurs NBNS (NetBIOS)

Pour la Compatibilité des Appareils Windows :

```
pco: %{
    primary_nbns_server_address: "10.0.0.20",
    secondary_nbns_server_address: "10.0.0.21"
}
```

Quand Utiliser :

- Réseaux d'entreprise avec des appareils Windows
- Support d'applications héritées
- Résolution de noms NetBIOS requise

Taille MTU de Lien

Unité de Transmission Maximale :

```
pco: %{
    ipv4_link_mtu_size: 1400 # octets
}
```

Valeurs MTU Courantes :

MTU Cas d'Utilisation

1500 Ethernet Standard (sans tunneling)

1400 Surcharge de tunneling GTP prise en compte

1420 Surcharge réduite

1280 MTU minimum IPv6

1360 Environnements VPN/tunnel

Recommandation : Utiliser **1400** pour LTE afin de tenir compte de la surcharge GTP-U.

Exemples de Configuration

APN Internet

```
pco: %{
    primary_dns_server_address: "8.8.8.8",
    secondary_dns_server_address: "8.8.4.4",
    ipv4_link_mtu_size: 1400
}
```

APN IMS

```
pco: %{
    primary_dns_server_address: "10.0.0.10",
    secondary_dns_server_address: "10.0.0.11",
    p_cscf_ipv4_address_list: [
        "10.0.0.50",
        "10.0.0.51"
    ],
    ipv4_link_mtu_size: 1400
}
```

Voir : [Surveillance P-CSCF](#) pour surveiller les taux de réussite d'enregistrement IMS et la santé P-CSCF

APN Entreprise

```
pco: %{
    primary_dns_server_address: "10.100.0.10",
    secondary_dns_server_address: "10.100.0.11",
    primary_nbns_server_address: "10.100.0.20",
    secondary_nbns_server_address: "10.100.0.21",
    ipv4_link_mtu_size: 1400
}
```

PCO dans les Messages GTP-C

Réponse de Crédation de Session

OmniPGW inclut PCO dans le message **Réponse de Crédation de Session** :

```
Réponse de Crédation de Session
└─ Cause : Demande acceptée
└─ Adresse IP UE : 100.64.1.42
└─ PCO (Options de Configuration du Protocole)
    └─ Adresse IPv4 du Serveur DNS : 8.8.8.8
    └─ Adresse IPv4 du Serveur DNS : 8.8.4.4
    └─ Adresse IPv4 du P-CSCF : 10.0.0.50
    └─ Adresse IPv4 du P-CSCF : 10.0.0.51
    └─ MTU de Lien IPv4 : 1400
```

Traitemetn UE

Le UE reçoit PCO et :

1. Configure le résolveur DNS avec les serveurs fournis

-
2. S'enregistre auprès du P-CSCF pour les services IMS
 3. Définit la MTU d'interface à la valeur spécifiée

Dépannage

Problème : UE Ne Peut Pas Résoudre DNS

Symptômes :

- UE a une adresse IP mais ne peut pas accéder à Internet
- Les recherches DNS échouent

Causes Possibles :

1. Adresses de serveur DNS incorrectes dans la configuration PCO
2. Serveurs DNS non accessibles depuis le pool IP de l'UE
3. Pare-feu bloquant le trafic DNS

Résolution :

```
# Tester la connectivité du serveur DNS
ping 8.8.8.8

# Tester la résolution DNS depuis le réseau UE
nslookup google.com 8.8.8.8

# Vérifier la configuration PCO
grep "primary_dns_server_address" config/runtime.exs
```

Problème : Échec de l'Enregistrement IMS

Symptômes :

- Les appels VoLTE échouent
- UE affiche "Pas d'enregistrement IMS"

Causes Possibles :

1. Configuration P-CSCF manquante
2. Adresses IP P-CSCF incorrectes
3. P-CSCF non accessible

Résolution :

```
# Vérifier la configuration P-CSCF
pco: %{
  p_cscf_ipv4_address_list: ["10.0.0.50"]  # S'assurer qu'elle n'est
```

```
pas vide  
}
```

Problème : Problèmes de MTU

Symptômes :

- Certains sites Web se chargent, d'autres non
- Les transferts de gros fichiers échouent
- Problèmes de fragmentation

Causes Possibles :

- MTU trop grande pour la surcharge de tunneling
- MTU trop petite causant une fragmentation excessive

Résolution :

```
# Recommandé : 1400 pour le tunneling GTP  
pco: %{  
    ipv4_link_mtu_size: 1400  
}  
  
# Si des problèmes persistent, essayer plus bas  
pco: %{  
    ipv4_link_mtu_size: 1360  
}
```

Meilleures Pratiques

Configuration DNS

1. Utiliser des Serveurs DNS Fiables

- Public : Google (8.8.8.8), Cloudflare (1.1.1.1)
- Privé : DNS interne pour l'entreprise

2. Toujours Configurer un Secondaire

- Fournit de la redondance
- Améliore la fiabilité

3. Considérer la Sécurité DNS

- Résolveurs compatibles DNSSEC
- Filtrage DNS pour la sécurité

Configuration IMS

1. Fournir Plusieurs P-CSCF

- Au moins 2 pour la redondance
- Distribution géographique si possible

2. Assurer la Connectivité

- P-CSCF doit être accessible depuis le pool IP de l'UE
- Tester la connectivité SIP

Optimisation MTU

1. Tenir Compte de la Surcharge

- GTP-U : 36 octets (IPv4)
- IPsec : Variable (50-100 octets)

2. MTU Standard LTE

- Recommandé : **1400 octets**
- Équilibre entre débit et compatibilité

3. Tester de Bout en Bout

- Découverte de MTU de chemin
 - Tester avec de gros paquets
-

Documentation Connexe

Guides de Configuration

- [**Guide de Configuration**](#) - Référence complète de runtime.exs, sélection UPF avec remplacements PCO
- [**Attribution d'IP UE**](#) - Gestion des pools IP, attribution basée sur APN
- [**Surveillance P-CSCF**](#) - Surveillance de la découverte P-CSCF, suivi de la santé, métriques

Gestion des Sessions et Interfaces

- [**Gestion des Sessions**](#) - Cycle de vie de la session PDN, établissement de porteurs
- [**Interface S5/S8**](#) - Protocole GTP-C, encodage et livraison PCO
- [**Interface PFCP**](#) - Établissement de session de plan utilisateur

IMS et VoLTE

- [**Interface Diameter Gx**](#) - Contrôle de politique pour les porteurs IMS
 - [**Guide de Surveillance**](#) - Métriques et tableaux de bord liés à PCO
-

[**Retour au Guide des Opérations**](#)

Configuration PCO OmniPGW - par Omnitouch Network Services



Découverte et Surveillance du P-CSCF

Découverte Dynamique du Serveur P-CSCF avec Surveillance en Temps Réel

OmniPGW par Omnitouch Network Services

Aperçu

La Découverte et la Surveillance du P-CSCF (Fonction de Contrôle de Session d'Appel Proxy) fournit une découverte dynamique des serveurs P-CSCF IMS en utilisant des requêtes DNS SRV avec vérification de santé SIP OPTIONS en temps réel. Cette fonctionnalité permet :

- **Découverte P-CSCF par Règle** : Différents serveurs P-CSCF pour différents types de trafic
- **Surveillance Automatique** : Un processus en arrière-plan surveille en continu la résolution DNS (toutes les 60 secondes)
- **Vérifications de Santé SIP OPTIONS** : Vérifie que les serveurs P-CSCF sont actifs via des pings SIP OPTIONS
 - **TCP d'abord** : Tente SIP OPTIONS via TCP (préféré pour la fiabilité)
 - **Repli UDP** : Repli à UDP si TCP échoue
 - **Suivi de Statut** : Marque chaque serveur comme **up** ou **down** en fonction de la réponse
- **Suivi de Santé Temps Réel** : L'interface Web affiche le statut de résolution, les IP découvertes et le statut de santé
- **Repli Gracieux** : Stratégie de repli à trois niveaux pour une fiabilité maximale
- **Métriques Prometheus** : Observabilité complète via les métriques Prometheus

Table des Matières

1. [Démarrage Rapide](#)
2. [Configuration](#)
3. [Comment Ça Marche](#)
4. [Surveillance de l'Interface Web](#)
5. [Monitoring et Observabilité](#)
6. [Stratégies de Repli](#)
7. [Configuration DNS](#)
8. [Dépannage](#)
9. [Meilleures Pratiques](#)

Démarrage Rapide

Configuration de Base

```
# config/runtime.exs

# Configuration globale du PCO (serveur DNS pour la découverte du P-CSCF)
config :ppw_c,
  pco: %{
    p_cscf_discovery_dns_server: "10.179.2.177",
    p_cscf_discovery_enabled: true,
    p_cscf_discovery_timeout_ms: 5000
  },
  upf_selection: %{
    rules: [
      # Trafic IMS - Découverte dynamique du P-CSCF
      %{
        name: "Trafic IMS",
        priority: 20,
        match_field: :apn,
        match_regex: "^ims",
        upf_pool: [...],
        %>remote_ip_address: "10.100.2.21", remote_port: 8805, weight: 80
      },
      # FQDN de découverte du P-CSCF (voir le Guide de Configuration pour plus de règles de sélection UPF)
      p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org",
      # Repli statique (voir le Guide de Configuration du PCO)
      pco: %{
        p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
      }
    ]
  }
}
```

Voir le [Guide de Configuration](#) pour la configuration complète des règles de sélection UPF et le [PCO Configuration](#) pour les options de repli statique du P-CSCF.

Surveillance d'Accès

1. Démarrer OmniPGW
2. Naviguer vers **Web UI → P-CSCF Monitor** (https://localhost:8086/pcscf_monitor)
3. Voir l'état de résolution en temps réel et les IP découvertes

Configuration

Paramètres Globaux de Découverte du P-CSCF

Configurer le serveur DNS utilisé pour la découverte du P-CSCF dans la section PCO :

```
pco: %{
  # Serveur DNS pour la découverte du P-CSCF (séparé du DNS donné à l'UE)
  p_cscf_discovery_dns_server: "10.179.2.177",

  # Activer la fonctionnalité de découverte DNS du P-CSCF
  p_cscf_discovery_enabled: true,

  # Décalage d'expiration pour les requêtes DNS SRV (millisecondes)
  p_cscf_discovery_timeout_ms: 5000,

  # Adresses P-CSCF statiques (repli global)
  p_cscf_ipv4_address_list: ["10.101.2.146"]
}
```

FQDNs P-CSCF par Règle

Chaque règle de sélection UPF peut spécifier son propre FQDN de découverte P-CSCF :

```
upf_selection: %{
  rules: [
    # Trafic IMS - P-CSCF spécifique à l'IMS
    %{
      name: "Trafic IMS",
      match_field: :apn,
      match_regex: "^ims",
      upf_pool: [...],
      p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org",
      pco: %{
        p_cscf_ipv4_address_list: ["10.101.2.100"] # Repli
      }
    },
    # Entreprise - P-CSCF spécifique à l'entreprise
    %{
      name: "Trafic Entreprise",
      match_field: :apn,
      match_regex: "^enterprise",
      upf_pool: [...],
      p_cscf_discovery_fqdn: "pcscf.enterprise.example.com",
      pco: %{
        p_cscf_ipv4_address_list: ["192.168.1.50"] # Repli
      }
    },
  ]
}
```

```

# Internet - Pas de découverte P-CSCF (utilise la configuration globale)
%{
    name: "Trafic Internet",
    match_field: :apn,
    match_regex: "^internet",
    upf_pool: [...]
} # Pas de p_cscf_discovery_fqdn - utilise la configuration PCO globale
}

```

Comment Ça Marche

Processus de Démarrage

1. L'application démarre
 - Le GenServer de surveillance P-CSCF s'initialise
 - Le parseur de configuration extrait tous les FQDN P-CSCF uniques des règles de sélection UPF
2. Enregistrement des FQDN
 - Chaque FQDN unique est enregistré avec le moniteur
 - Le moniteur effectue une requête DNS SRV initiale pour chaque FQDN
 - Vérification de Santé SIP OPTIONS (en parallèle pour tous les serveurs découverts) :
 - Essayer TCP d'abord (SIP/2.0/TCP sur le port 5060)
 - Si TCP échoue, repli sur UDP (SIP/2.0/UDP sur le port 5060)
 - Marquer chaque serveur comme : up (répond) ou : down (pas de réponse/délai d'attente)
 - Les résultats (IPs, statut de santé ou erreurs) sont mis en cache avec des horodatages

3. Surveillance Périodique (toutes les 60 secondes)

- Le moniteur rafraîchit tous les FQDN
- Les requêtes DNS s'exécutent en arrière-plan sans bloquer
- Pour chaque serveur découvert :
 - Envoyer SIP OPTIONS via TCP (délai d'attente : 5 secondes)
 - Si TCP échoue, essayer UDP (délai d'attente : 5 secondes)
 - Mettre à jour le statut de santé en fonction de la réponse
- Le cache est mis à jour avec les derniers résultats DNS et le statut de santé

Flux de Crédation de Session

Processus de Requête DNS

Le moniteur utilise les **enregistrements DNS SRV** pour la découverte directe du P-CSCF :

1. **Requête SRV** : Requête des enregistrements SRV à _sip._tcp.{fqdn}
2. **Tri par Priorité** : Trier par priorité et poids
3. **Extraction de Cible** : Extraire les noms d'hôtes cibles des enregistrements SRV
4. **Résolution de Nom d'Hôte** : Résoudre les noms d'hôtes cibles en adresses IP (enregistrements A/AAAA)
5. **Mise en Cache** : Mettre en cache les IP résolus avec statut et horodatage

Précédence de Sélection d'Adresse P-CSCF

Lorsque le FQDN et le PCO statique sont configurés sur une règle, le FQDN a la priorité :

```

%{
    name: "Trafic IMS",
    p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org", # ← Essayer D'ABORD
    pco: %{
        p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"] # ← Repli
    }
}

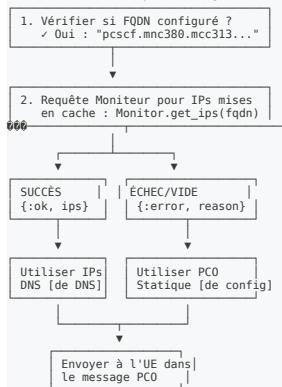
```

Logique de Sélection :

Condition	Source P-CSCF	IPs Utilisées	Message de Log
Le FQDN se réduit avec succès	Découverte DNS (Moniteur)	IPs découvertes via DNS	"Utilisation des adresses P-CSCF du FQDN pcscf.example.com"
Le FQDN échoue à se résoudre	Remplacement PCO de la Règle	IPs statiques de pco.p_cscf_ipv4.address_list	"Échec d'obtention des IPs P-CSCF du FQDN..., repli sur la configuration statique"
Le FQDN renvoie une liste vide	Remplacement PCO de la Règle	IPs statiques de pco.p_cscf_ipv4.address_list	Repli déclenché
Moniteur indisponible	Remplacement PCO de la Règle	IPs statiques de pco.p_cscf_ipv4.address_list	L'erreur déclenche le repli
Aucun FQDN configuré	Remplacement PCO de la Règle ou GlobalIPs statiques de la règle ou configuration globale	GlobalIPs statiques de la règle ou configuration globale	Utilise directement la configuration statique

Flux d'Exemple :

Création de Session pour la Règle de Trafic IMS :



Scénarios du Monde Réel :

Scénario 1 : La Découverte DNS Fonctionne ◊

Configuration :
`p_cscf_discovery_fqdn: "pcscf.ims.example.com"
pco.p_cscf_ipv4_address_list: ["10.101.2.100"]`

Résultat DNS : [10.101.2.150, 10.101.2.151]
 L'UE reçoit : [10.101.2.150, 10.101.2.151] ~ Du DNS
 Remarque : Le PCO statique est ignoré lorsque DNS réussit

Scénario 2 : DNS Échoue, Repli Gracieux ▲

Configuration :
`p_cscf_discovery_fqdn: "pcscf.ims.example.com"
pco.p_cscf_ipv4_address_list: ["10.101.2.100"]`

Résultat DNS : ERREUR :no_naptr_records
 L'UE reçoit : [10.101.2.100] ~ Du PCO statique
 Remarque : La session réussit malgré l'échec de DNS

Scénario 3 : Aucun FQDN Configuré

Configuration :
`# Pas de p_cscf_discovery_fqdn
pco.p_cscf_ipv4_address_list: ["192.168.1.50"]`

L'UE reçoit : [192.168.1.50] ← Du PCO statique
Remarque : La découverte DNS n'est pas tentée

Pourquoi ce Design ?

1. **Préférer Dynamique** : DNS offre flexibilité, équilibrage de charge et routage conscient de la localisation
2. **Assurer la Fiabilité** : Le repli statique garantit que les sessions ne échouent jamais en raison de problèmes DNS
3. **Aucune Intervention Manuelle** : Basculement automatique sans intervention de l'opérateur
4. **Sécurisé en Production** : Le meilleur des deux mondes - agilité avec stabilité

Recommandation : Toujours configurer à la fois le FQDN et le PCO statique pour les déploiements en production :

```
# ✓ RECOMMANDÉ : Dynamique avec repli
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com", # Préféré
  pco: %{
    p_cscf_ipv4_address_list: ["10.101.2.100"]      # Filet de sécurité
  }
}

# △ RISQUÉ : Dynamique uniquement (repli sur PCO global)
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com"
  # Pas de repli spécifique à la règle !
}

# ✓ VALIDE : Statique uniquement (pas de surcharge DNS)
%{
  pco: %{
    p_cscf_ipv4_address_list: ["192.168.1.50"]
  }
}
```

Surveillance de l'Interface Web

Page de Surveillance du P-CSCF

Accédez à l'interface de surveillance à : https://localhost:8086/pcscf_monitor

Fonctionnalités :

- **Statistiques d'Aperçu**
 - Total des FQDN surveillés
 - FQDN résolus avec succès
 - Résolutions échouées
 - Total des IPs P-CSCF découvertes
- **Tableau des FQDN**
 - FQDN surveillé
 - Statut de résolution (✓ Résolu / ✘ Échoué / ⚡ En attente)
 - Nombre d'IPs découvertes
 - Liste des adresses IP résolues (avec détails du serveur extensibles)
 - Horodatage de la dernière mise à jour
 - Bouton de rafraîchissement manuel par FQDN
 - **Statut de Santé** : Chaque serveur découvert montre :
 - Adresse IP et port
 - Nom d'hôte (à partir de la cible DNS SRV)
 - Indicateur de santé en temps réel (✓ Actif / ✘ Hors ligne)
- **Contrôles de Rafraîchissement**
 - Bouton **Rafraîchir Tout** : Déclenche une nouvelle requête immédiate de tous les FQDN
 - **Rafraîchissement par FQDN** : Rafraîchir les FQDN individuels à la demande
 - Auto-rafrachissement : La page se met à jour toutes les 5 secondes
- **Tableau de Bord des Métriques de Surveillance**
 - **Total des FQDN** : Nombre de FQDN uniques enregistrés pour la surveillance
 - **Résolus avec Succès** : FQDN qui se sont résolus avec succès via DNS
 - **Échecs de Résolution DNS** : FQDN qui ont échoué à se résoudre
 - **Total des Serveurs P-CSCF** : Nombre total de serveurs découverts à travers tous les FQDN
 - **✓ Sains (SIP OPTIONS UP)** : Serveurs répondant aux vérifications de santé SIP OPTIONS
 - **✗ Malades (SIP OPTIONS DOWN)** : Serveurs ne répondant pas aux SIP OPTIONS
 - **Taux de Réussite DNS** : Pourcentage de résolutions DNS réussies
 - **Intervalle de Vérification de Santé** : Fréquence des vérifications de santé SIP OPTIONS (60s, délai de 5s)

The screenshot shows the PGW-C v0.1.0 web interface with the following details:

- Header:** PGW-C v0.1.0, Licensed to: Omnitouch, © 2025 Omnitouch.
- Left Sidebar:** Resources, Configuration, Topology, UE Search, PGW Sessions, Session History, IP Pools, Diameter, PCP, Sessions, UPF Status, UPF Selection, P-CSCF Monitor, Gy Simulator, Logs.
- Main Content:**
 - P-CSCF Discovery Monitor**
 - Last updated: 00:41:56
 - 1 Resolved, 0 Failed, 1 / 2 Healthy
 - Refresh All
 - Resolved Addresses**

FQDN	Status	Servers	Responding
pcscf.mnc[REDACTED].3gppnetwork.org	✓ Resolved	2	1 / 2
 - Resolved P-CSCF Servers (2)**

10.179.4.165.5060 Hostname: omni[REDACTED] pcscf01.mnc[REDACTED] 3gppnetwork.org	✓ Up
10.179.4.166.5060 Hostname: omni[REDACTED] pcscf02.mnc[REDACTED] 3gppnetwork.org	✗ Down
 - Monitoring Metrics**

Total FQDNs: 1	Successfully Resolved: 1	Failed DNS Resolutions: 0	Total P-CSCF Servers: 2	✓ Healthy (SIP OPTIONS UP): 1	✗ Unhealthy (SIP OPTIONS DOWN): 1	DNS Success Rate: 100.0%
Health Check Interval: 60s (5s timeout)						

Le tableau de bord des métriques fournit une visibilité en temps réel sur la santé de la résolution DNS et la disponibilité des serveurs P-CSCF via SIP OPTIONS.

Intégration de la Page de Sélection UPF

La page de Sélection UPF (/upf_selection) affiche le statut de découverte P-CSCF pour chaque règle :

```
✗ Trafic IMS (Priorité 20)
Correspondance : APN correspondant à ^ims
```

```

Pool : UPF-IMS-Primary (10.100.2.21:8805)
  ◊ Découverte P-CSCF
    FQDN : pscf.mnc380.mcc313.3gppnetwork.org
    Statut : ✓ Résolu (2 IPs)
    IPs Résolues : 10.101.2.100, 10.101.2.101
  ◊ Remplacements PCO
    DNS Principal : 10.103.2.195
    P-CSCF (repli statique) : 10.101.2.100, 10.101.2.101

```

Métriques et Observabilité

Métriques Prometheus

Le système de surveillance P-CSCF expose des métriques via Prometheus (port 42069 par défaut) :

Métriques de Type Gauge

```

# Métriques au niveau FQDN
pscfc_fqdns_total          # Nombre total de FQDN surveillés
pscfc_fqdns_resolved        # FQDN résolus avec succès (DNS réussi)
pscfc_fqdns_failed          # Échecs de résolutions de FQDN (DNS échoué)

# Métriques au niveau serveur (agrégées)
pscfc_servers_total          # Nombre total de serveurs P-CSCF découverts via DNS SRV
pscfc_servers_healthy         # Serveurs répondant aux SIP OPTIONS (agrégés)
pscfc_servers_unhealthy       # Serveurs ne répondant pas aux SIP OPTIONS (agrégés)

# Métriques au niveau serveur (par FQDN avec étiquette)
pscfc_servers_healthy(fqdn="...") # Serveurs sains pour un FQDN spécifique
pscfc_servers_unhealthy(fqdn="...") # Serveurs malades pour un FQDN spécifique

```

Détails de Vérification de Santé :

- **healthy** : Le serveur a répondu au ping SIP OPTIONS (TCP ou UDP)
- **unhealthy** : Le serveur n'a pas répondu aux SIP OPTIONS (délai de 5s par transport)

Exemples de Métriques

Métriques de Résolution DNS :

```

# Requête des FQDN résolus avec succès
pscfc_fqdns_resolved

# Calculer le taux de réussite DNS
(pscfc_fqdns_resolved / pscfc_fqdns_total) * 100

# Total des serveurs découverts
pscfc_servers_total

```

Métriques de Santé SIP OPTIONS :

```

# Total des serveurs sains à travers tous les FQDN
pscfc_servers_healthy

# Total des serveurs malades
pscfc_servers_unhealthy

# Calculer le taux de réussite de la vérification de santé
(pscfc_servers_healthy / pscfc_servers_total) * 100

# Serveurs sains pour un FQDN spécifique
pscfc_servers_healthy(fqdn="pscfc.mnc380.mcc313.3gppnetwork.org")

# Alerte si tous les serveurs sont hors ligne
pscfc_servers_healthy == 0 AND pscfc_servers_total > 0

```

Exemples d'Alerte Prometheus :

```

# Alerte lorsque tous les serveurs P-CSCF sont hors ligne
- alert: AllPCSCFServersDown
  expr: pscfc_servers_healthy == 0 AND pscfc_servers_total > 0
  for: 5m
  labels:
    severity: critical
  annotations:
    summary: "Tous les serveurs P-CSCF sont malades"
    description: "{{ $value }} serveurs sains (0) - tous les contrôles SIP OPTIONS échoués"

# Alerte lorsque plus de 50 % des serveurs sont hors ligne
- alert: MajorityPCSCFServersDown
  expr: (pscfc_servers_healthy / pscfc_servers_total) < 0.5
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "La majorité des serveurs P-CSCF sont malades"
    description: "Seulement {{ $value }}% des serveurs répondent aux SIP OPTIONS"

# Alert sur les échecs de résolution DNS
- alert: PCSCFDNSResolutionFailed
  expr: pscfc_fqdns_failed > 0
  for: 5m
  labels:
    severity: warning
  annotations:
    summary: "Échecs de résolution DNS du P-CSCF"
    description: "{{ $value }} FQDN(s) échouent à se résoudre"

```

Journalisation

Le moniteur enregistre des événements clés :

```

[info] Moniteur P-CSCF démarré
[info] Enregistrement de 2 FQDN P-CSCF uniques pour la surveillance : ["pscfc.ims.example.com", "pscfc.enterprise.example.com"]
[info] Moniteur P-CSCF : Enregistrement du FQDN pscfc.ims.example.com
[debug] Moniteur P-CSCF : Résolution réussie de pscfc.ims.example.com en 2 IPs
[warning] Moniteur P-CSCF : Echec de la résolution de pscfc.enterprise.example.com : :nxdomain
[débog] Utilisation des adresses P-CSCF du FQDN pscfc.ims.example.com : {10, 101, 2, 100}, {10, 101, 2, 101}

```

Stratégie de Repli

Le système utilise une **stratégie de repli à trois niveaux** pour une fiabilité maximale :

Niveau 1 : Découverte DNS (Préférée)

```
p_cscf_discovery_fqdn: "pscfc.ims.example.com"
```

- Le moniteur interroge DNS et met en cache les IP résolues
- La session utilise les IP mises en cache si disponibles
- **Avantage** : Dynamique, équilibré, conscient de la localisation

Niveau 2 : PCO Statique Spécifique à la Règle (Repli)

```
pco: %{
  p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
}
```

- Utilisé si la découverte DNS échoue ou ne renvoie pas d'IPs
- Configuration statique spécifique à la règle
- **Avantage** : Repli spécifique à la règle, prévisible

Niveau 3 : Configuration PCO Globale (Dernier Recours)

```
# Configuration PCO globale
pco: %{
    p_cscf_ipv4_address_list: ["10.101.2.146"]
}



- Utilisé si aucune configuration spécifique à la règle et que DNS échoue
- Adresses P-CSCF par défaut globales
- Avantage : Toujours disponible, empêche l'échec de session

```

Exemple de Logique de Repli

La session correspond à la règle "Trafic IMS" :

- Essayer la découverte DNS pour "pcscf.ims.example.com"
 - Succès → Utiliser [10.101.2.100, 10.101.2.101] ✓
 - Échec → Essayer le niveau suivant
- Essayer le remplacement PCO de la règle
 - Configuré → Utiliser [10.101.2.100, 10.101.2.101] ✓
 - Non configuré → Essayer le niveau suivant
- Utiliser la configuration PCO globale
 - Utiliser [10.101.2.146] ✓ (Réussit toujours)

Configuration DNS

Configuration du Serveur DNS

Configurer le serveur DNS avec des enregistrements SRV et A/AAAA pour la découverte du P-CSCF :

```
; Enregistrements SRV pour le P-CSCF (_sip._tcp préfixe est interrogé automatiquement)
_sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org. IN SRV 10 50 5060 pcscf1.example.com.
_sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org. IN SRV 20 50 5060 pcscf2.example.com.

; Enregistrement A
pcscf1.example.com. IN A 10.101.2.100
pcscf2.example.com. IN A 10.101.2.101
```

Important : OmniPGW préfixe automatiquement _sip._tcp. au FQDN configuré. Si vous configurez p_cscf_discovery_fqdn: "pcscf.mnc380.mcc313.3gppnetwork.org", le système interrogera _sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org.

Format des Enregistrements SRV

Les enregistrements SRV suivent ce format :

```
_service._proto.domain. IN SRV priority weight port target.
```

- Priorité** : Les valeurs plus basses ont une priorité plus élevée (10 avant 20)
- Poids** : Pour l'équilibrage de charge parmi la même priorité (plus élevé = plus de trafic)
- Port** : Port SIP (typiquement 5060 pour TCP, 5060 pour UDP)
- Cible** : Nom d'hôte à résoudre en adresse IP

Tester la Configuration DNS

```
# Interroger les enregistrements SRV (notez le préfixe _sip._tcp)
dig SRV _sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org @10.179.2.177

# Sortie attendue :
#_sip._tcp.pcscf.mnc380.mcc313.3gppnetwork.org. 300 IN SRV 10 50 5060 pcscf1.example.com.

# Résoudre le nom d'hôte P-CSCF en IP
dig A pcscf1.example.com @10.179.2.177

# Sortie attendue :
# pcscf1.example.com. 300 IN A 10.101.2.100
```

Dépannage

Problème : FQDN Affiche un Statut "Échoué"

Symptômes :

- L'interface Web affiche un statut ✘ Échoué
- Erreur : :nxdomain, :timeout, ou :no_naptr_records

Causes Possibles :

- Serveur DNS non accessible
- FQDN n'existe pas dans DNS
- Aucun enregistrement NAPTR configuré
- Délai d'attente du serveur DNS

Résolution :

```
# 1. Tester la connectivité du serveur DNS
ping 10.179.2.177

# 2. Tester la requête NAPTR manuellement
dig NAPTR pcscf.mnc380.mcc313.3gppnetwork.org @10.179.2.177

# 3. Vérifier les journaux d'OmniPGW
grep "P-CSCF" /var/log/pgw_c.log

# 4. Vérifier la configuration
grep "p_cscf_discovery_dns_server" config/runtime.exs

# 5. Rafraîchissement manuel dans l'interface Web
# Cliquez sur le bouton "Rafraîchir" à côté du FQDN échoué
```

Problème : Aucune IP Renvoie

Symptômes :

- L'interface Web affiche "0 IPs"
- Le statut peut être ✓ Résolu ou ✘ Échoué

Causes Possibles :

- Les enregistrements NAPTR existent mais les FQDN de remplacement ne se résolvent pas
- Le champ de service ne correspond pas au modèle IMS/SIP
- Enregistrements A/AAAA manquants

Résolution :

```
# Vérifier le champ de service de l'enregistrement NAPTR
dig NAPTR pcscf.example.com @10.179.2.177

# Assurez-vous que le service contient "SIP" ou "IMS" :
# CORRECT : "SIP+D2U", "x-3gpp-ims:sip"
# FAUX : "H3IP", "FIP"

# Vérifier que les enregistrements A/AAAA existent
dig pcscf1.example.com A @10.179.2.177
```

Problème : Les Sessions Utilisent le Mauvais P-CSCF

Symptômes :

- L'UE reçoit des adresses P-CSCF inattendues
- Repli statique utilisé au lieu des IP découvertes

Causes Possibles :

- 1. La découverte DNS a échoué mais le repli fonctionne
- 2. Correspondance de règle incorrecte
- 3. FQDN non enregistré

Résolution :

```
# 1. Vérifier la page Moniteur P-CSCF
# Vérifier que le FQDN est enregistré et résolu

# 2. Vérifier les journaux de session
grep "Utilisation des adresses P-CSCF du FQDN" /var/log/pgw_c.log

# 3. Vérifier la page de Sélection UPF
# Vérifier que la règle montre le bon FQDN et statut

# 4. Tester la correspondance de règle
# Créer une session avec un APN spécifique et vérifier quelle règle correspond
```

Problème : Latence Élevée des Requêtes DNS

Symptômes :

- Création de session lente
- Les métriques montrent une haute `pcscf_discovery_query_duration_seconds`

Causes Possibles :

- 1. Problèmes de performance du serveur DNS
- 2. Latence réseau vers le serveur DNS
- 3. Délai d'attente trop élevé

Résolution :

```
# Réduire le délai d'expiration de la requête
pco: %{
  p_cscf_discovery_timeout_ms: 2000 # Réduire de 5000ms
}

# Envisager d'utiliser un serveur DNS plus proche
pco: %{
  p_cscf_discovery_dns_server: "10.0.0.10" # DNS local
}
```

Meilleures Pratiques

1. Sélection du Serveur DNS

Utiliser un Serveur DNS Dédié

```
pco: %{
  # DNS dédié pour la découverte du P-CSCF (pas le même que le DNS de l'UE)
  p_cscf_discovery_dns_server: "10.179.2.177",

  # Serveurs DNS de l'UE (données aux appareils mobiles)
  primary_dns_server_address: "8.8.8.8",
  secondary_dns_server_address: "8.8.4.4"
}
```

Pourquoi ?

- Séparer les préoccupations : DNS de l'UE vs. DNS IMS interne
- Différentes politiques d'accès et de sécurité
- Mise à l'échelle et fiabilité indépendantes

2. Toujours Configurer un Repli Statique

```
%{
  p_cscf_discovery_fqdn: "pcscf.ims.example.com", # Préféré
  pco: %{
    p_cscf_ipv4_address_list: ["10.101.2.100"] # Repli requis
  }
}
```

Pourquoi ?

- Garantit que les sessions réussissent même si DNS échoue
- Dégradation gracieuse
- Respecte les exigences SLA

3. Utiliser des FQDN Spécifiques par Type de Trafic

```
rules: [
  # IMS
  %{
    name: "IMS",
    match_regex: "^ims",
    p_cscf_discovery_fqdn: "pcscf.ims.mnc380.mcc313.3gppnetwork.org"
  },
  # Entreprise
  %{
    name: "Entreprise",
    match_regex: "^enterprise",
    p_cscf_discovery_fqdn: "pcscf.enterprise.example.com"
  }
]
```

Pourquoi ?

- Différents pools P-CSCF par service
- Meilleure distribution de charge
- Routage spécifique au service

4. Surveiller la Performance des Requêtes DNS

```
# Alert sur la latence élevée des requêtes P-CSCF
alert: HighPCSCFQueryLatency
expr: histogram_quantile(0.95, pcscf_discovery_query_duration_seconds_bucket) > 2
for: 5m
labels:
  severity: warning
annotations:
  summary: "Les requêtes DNS P-CSCF sont lentes (p95 > 2s)"
```

5. Vérifications de Santé DNS Régulières

- **Interface Web** : Vérifier la page Moniteur P-CSCF quotidiennement
- **Métriques** : Surveiller la métrique `pcscf_monitor_fqdns_failed`
- **Journaux** : Surveiller les erreurs DNS
- **Tests** : Vérifier périodiquement que les enregistrements DNS existent

6. Configurer un Délai d'Expiration Approprié

```
# Production : Équilibrer fiabilité et latence
pco: %{
  p_cscf_discovery_timeout_ms: 5000 # 5 secondes
}

# Haute performance : Favoriser la vitesse, s'appuyer sur le repli
pco: %{
  p_cscf_discovery_timeout_ms: 2000 # 2 secondes
}
```

7. Utiliser la Redondance DNS

Configurer des DNS primaire et secondaire :

```
# DNS P-CSCF principal  
pcscf.mnc380.mcc313.3gppnetwork.org. IN NAPTR 10 50 "s" "SIP+D2U" "" _sip._udp.pcscf1.example.com.  
# DNS P-CSCF secondaire  
pcscf.mnc380.mcc313.3gppnetwork.org. IN NAPTR 20 50 "s" "SIP+D2U" "" _sip._udp.pcscf2.example.com.
```

Documentation Connexe

- [Configuration PCO](#) - Options de Configuration de Protocole, paramètres DNS et P-CSCF
- [Guide de Configuration](#) - Référence complète de configuration d'OmniPGW
- [Surveillance](#) - Métriques, journalisation et observabilité
- [Gestion de Session](#) - Cycle de vie de la session et livraison du PCO
- [Interface PCP](#) - Communication de la Fonction de Plan Utilisateur

[Retour à la Documentation Principale](#)

Surveillance P-CSCF d'OmniPGW - par Omnitouch Network Services



Documentation de l'Interface PFCP/Sxb

Protocole de Contrôle de Transfert de Paquets - Communication entre PGW-C et PGW-U

Table des Matières

1. [Aperçu](#)
 2. [Bases du Protocole](#)
 3. [Gestion des Associations PFCP](#)
 4. [Gestion des Sessions PFCP](#)
 5. [Règles de Traitement des Paquets](#)
 6. [Configuration](#)
 7. [Sélection de UPF basée sur DNS](#)
 8. [Flux de Messages](#)
 9. [Dépannage](#)
 10. [Interface Web - Surveillance PFCP](#)
 11. [Documentation Connexe](#)
-

Aperçu

L'**interface Sxb** utilise le **PFCP (Protocole de Contrôle de Transfert de Paquets)** pour la communication entre le PGW-C (plan de contrôle) et le PGW-U (plan utilisateur). Cette séparation permet :

- **Plan de Contrôle (PGW-C)** - Gère la signalisation, la gestion des sessions, les décisions de politique
- **Plan Utilisateur (PGW-U)** - Gère le transfert de paquets réel à grande vitesse

Architecture PFCP

Bases du Protocole

Version PFCP

PGW-C implémente **PFCP Version 1** (3GPP TS 29.244).

Transport

- **Protocole** : UDP
- **Port par défaut** : 8805
- **Format de Message** : Codé binaire selon la spécification PFCP

Types d'ID de Nœud

Les pairs PFCP sont identifiés par l'ID de Nœud, qui peut être :

- **Adresse IPv4** - La plus courante
 - **Adresse IPv6**
 - **FQDN** (Nom de Domaine Entièrement Qualifié)
-

Gestion des Associations PFCP

Avant que la gestion des sessions puisse avoir lieu, une **association** PFCP doit être établie entre PGW-C et PGW-U.

Flux de Configuration de l'Association

Gestion de l'État des Pairs

Chaque pair PFCP maintient un état :

Champ	Description
is_associated	Booléen indiquant l'état de l'association
remote_node_id	ID de Nœud du pair (IP ou FQDN)
remote_ip_address	Adresse IP pour la communication
remote_port	Port UDP (par défaut 8805)
heartbeat_period_ms	Intervalle de cœur en millisecondes
missed_heartbeats_consecutive	Compte des cœurs manqués
up_function_features	Fonctionnalités du plan utilisateur prises en charge
up_recovery_time_stamp	Horodatage de récupération du pair

Mécanisme de Cœur

Objectif : Déetecter les pannes de pair et maintenir la vivacité de l'association

Configuration :

```
# Dans config/runtime.exs
sxb: %{
  local_ip_address: "10.0.0.20"
},
upf_selection: %{
  fallback_pool: [
    %{remote_ip_address: "10.0.0.21", remote_port: 8805, weight: 100}
  ]
}
# Tous les UPFs sont automatiquement enregistrés avec des cœurs de 5 secondes
```

Détection de Panne :

- Chaque cœur manqué incrémenté missed_heartbeats_consecutive
 - Généralement configuré pour échouer après 3 manqués consécutifs
 - L'association échouée empêche de nouvelles sessions vers ce pair
-

Gestion des Sessions PFCP

Les sessions PFCP sont créées pour chaque connexion PDN UE afin de programmer des règles

de transfert dans le plan utilisateur.

Cycle de Vie de la Session

Établissement de Session

Quand : L'UE s'attache et crée une connexion PDN

PGW-C envoie à PGW-U :

Demande d'Établissement de Session contenant :

- **SEID** (ID de Point de Terminaison de Session) - Identifiant de session unique
- **ID de Nœud** - ID de Nœud de PGW-C
- **F-SEID** - SEID Entièrement Qualifié (inclus IP + SEID)
- **PDRs** - Règles de Détection de Paquets (typiquement 2 : montante + descendante)
- **FARs** - Règles d'Action de Transfert (typiquement 2 : montante + descendante)
- **QERs** - Règles d'Application de QoS (limites de débit)
- **BAR** - Règle d'Action de Mise en Tampon (pour la mise en tampon descendante)

PGW-U répond :

Réponse d'Établissement de Session contenant :

- **Cause** - Raison de succès ou d'échec
- **F-SEID** - Point de terminaison de session de PGW-U
- **PDRs Crées** - Accusé de réception des règles créées
- **F-TEID** - TEID Entièrement Qualifié pour l'interface S5/S8

Modification de Session

Quand : Des changements de QoS, des mises à jour de politique ou des modifications de bearer se produisent

La modification peut inclure :

- Ajout de nouveaux PDRs, FARs, QERs
- Suppression de règles existantes
- Mise à jour des paramètres de règle

Suppression de Session

Quand : L'UE se détache ou la connexion PDN est terminée

Processus :

1. PGW-C envoie une Demande de Suppression de Session avec SEID
2. PGW-U supprime toutes les règles et libère les ressources
3. PGW-U répond avec une Réponse de Suppression de Session

Règles de Traitement des Paquets

PFCP utilise un ensemble de règles pour définir comment le plan utilisateur traite les paquets.

Architecture des Règles

PDR (Règle de Détection de Paquet)

Objectif : Identifier à quels paquets cette règle s'applique

Configuration Typique de PGW-C :

PDR #1 - Descendant :

```
ID de PDR : 1
Précédence : 100
PDI (Informations de Détection de Paquet) :
  - Interface Source : CORE (côté Internet)
  - Adresse IP de l'UE : 100.64.1.42/32
ID de FAR : 1 (règle de transfert associée)
```

PDR #2 - Montant :

```
ID de PDR : 2
Précédence : 100
PDI (Informations de Détection de Paquet) :
  - Interface Source : ACCESS (côté SGW)
  - F-TEID : <point de terminaison de tunnel S5/S8>
ID de FAR : 2 (règle de transfert associée)
ID de QER : 1 (application de QoS)
```

Champs Clés de PDR :

- **ID de PDR** - Identifiant unique de la règle (par session)
- **Précédence** - Priorité de correspondance de la règle (plus élevé = plus spécifique)
- **PDI** - Critères de correspondance (interface, IP, TEID, etc.)
- **Suppression de l'En-tête Externe** - Supprimer l'en-tête GTP-U à l'entrée
- **ID de FAR** - Action de transfert associée
- **ID de QER** - Application de QoS associée (optionnel)

FAR (Règle d>Action de Transfert)

Objectif : Définir quoi faire avec les paquets correspondants

FAR #1 - Descendant (Internet → UE) :

```
ID de FAR : 1
Appliquer l'Action : TRANSFÉRER
Paramètres de Transfert :
  - Interface de Destination : ACCESS (vers SGW)
  - Création de l'En-tête Externe : GTP-U/UDP/IPv4
  - F-TEID Distant : <point de terminaison de tunnel SGW S5/S8>
```

FAR #2 - Montant (UE → Internet) :

```
ID de FAR : 2
Appliquer l'Action : TRANSFÉRER
Paramètres de Transfert :
  - Interface de Destination : CORE (vers Internet)
  - (Pas d'en-tête externe - transfert IP simple)
```

Champs Clés de FAR :

- **ID de FAR** - Identifiant unique de la règle
- **Appliquer l'Action** - TRANSFÉRER, SUPPRIMER, METTRE EN TAMPO, NOTIFIER
- **Paramètres de Transfert :**
 - Interface de destination (ACCESS/CORE)
 - Création de l'En-tête Externe (ajouter un tunnel GTP-U)
 - Instance Réseau (VRF/table de routage)

QER (Règle d'Application de QoS)

Objectif : Appliquer des limites de débit et des paramètres de QoS. Les QER peuvent également suivre l'utilisation pour la gestion des quotas de facturation en ligne (voir [Interface Diameter Gy](#) pour le contrôle de crédit).

Exemple de QER :

```
ID de QER : 1
État de la Porte : OUVERT
Débit Maximum :
- Montant : 100 Mbps
- Descendant : 50 Mbps
Débit Garanti : (optionnel, pour les bearers GBR)
- Montant : 10 Mbps
- Descendant : 10 Mbps
```

Champs Clés de QER :

- **ID de QER** - Identifiant unique de la règle
- **État de la Porte** - OUVERT (autoriser) ou FERMÉ (bloquer)
- **MBR** - Débit Maximum (montant/descendant)
- **GBR** - Débit Garanti (pour les bearers dédiés)
- **QCI** - Identifiant de Classe de QoS (affecte la planification)

BAR (Règle d>Action de Mise en Tampon)

Objectif : Contrôler la mise en tampon des paquets descendants lorsque l'UE est inactif

Exemple de BAR :

```
ID de BAR : 1
Délai de Notification de Données Descendantes : 100ms
Nombre de Paquets Suggérés à Mettre en Tampon : 10
```

Utilisé pour : Optimisation DRX (Réception Discontinue) en mode inactif

Configuration

Configuration de Base de Sxb

Modifier config/runtime.exs :

```
config :pgw_c,
  sxb: %{
```

```

# Adresse IP locale pour la communication PFCP
local_ip_address: "10.0.0.20",

# Optionnel : Remplacer le port par défaut (8805)
local_port: 8805
},

# Sélection UPF - Tous les UPFs définis ici sont automatiquement enregistrés
upf_selection: %{
  fallback_pool: [
    %{
      # Adresse IP de PGW-U
      remote_ip_address: "10.0.0.21",

      # Port PFCP (par défaut : 8805)
      remote_port: 8805,

      # Poids pour l'équilibrage de charge (100 = normal, 0 = veille)
      weight: 100
    }
  ]
}

```

Plusieurs Pairs PGW-U

Pour l'équilibrage de charge ou la redondance :

```

config :pgw_c,
  sxb: %{
    local_ip_address: "10.0.0.20"
  },
  upf_selection: %{
    fallback_pool: [
      %{remote_ip_address: "10.0.1.21", remote_port: 8805, weight: 50}, # 50% du
trafic
      %{remote_ip_address: "10.0.2.21", remote_port: 8805, weight: 50} # 50% du
trafic
    ]
  }
# Les deux UPFs sont automatiquement enregistrés avec des coeurs de 5 secondes

```

Configuration de Sélection UPF

PGW-C utilise un **système de sélection UPF à trois niveaux** avec des règles basées sur la priorité :

1. **Règles Statique** (Priorité la Plus Élevée) - Correspondance basée sur les attributs de session
2. **Sélection Basée sur DNS** (Priorité Moyenne) - Routage conscient de la localisation via des requêtes DNS NAPTR
3. **Pool de Secours** (Priorité la Plus Basse) - Pool UPF par défaut lorsque aucune règle ne correspond

Exemple Complet de Sélection UPF

```
config :pgw_c,
```

```

# Interface PFCP
sxb: %{
    local_ip_address: "10.0.0.20"
} ,

# Sélection UPF : Tous les UPFs définis ici sont automatiquement enregistrés
upf_selection: %{
    # =====
    # Sélection Basée sur DNS (Routage Conscient de la Localisation)
    # =====
    # Interroge DNS en utilisant les Informations de Localisation de
l'Utilisateur (ULI)
    # Fournit une sélection dynamique de UPF basée sur la localisation de la
cellule
    dns_enabled: false,
    dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
    dns_suffix: "epc.3gppnetwork.org",
    dns_timeout_ms: 5000,

    # =====
    # Règles de Sélection Statique (Évaluées par Priorité)
    # =====
    # Les règles sont vérifiées de la priorité la plus élevée à la plus basse
    # La première règle correspondante détermine le pool UPF
    rules: [
        # Règle 1 : Trafic IMS - Priorité la Plus Élevée
        %{
            name: "Trafic IMS",
            priority: 20,
            match_field: :apn,
            match_regex: "^ims",
            upf_pool: [
                %{remote_ip_address: "10.100.2.21", remote_port: 8805, weight: 80},
                %{remote_ip_address: "10.100.2.22", remote_port: 8805, weight: 20}
            ],
            # Optionnel : Remplacements PCO pour cette règle
            pco: %{
                p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"]
            }
        },
        # Règle 2 : APN Entreprise - Haute Priorité
        %{
            name: "Trafic d'Entreprise",
            priority: 15,
            match_field: :apn,
            match_regex: "^(entreprise|corporate)\\.apn",
            upf_pool: [
                %{remote_ip_address: "10.100.3.21", remote_port: 8805, weight: 100}
            ],
            pco: %{
                primary_dns_server_address: "192.168.1.10",
                secondary_dns_server_address: "192.168.1.11",
                ipv4_link_mtu_size: 1500
            }
        },
    ],
}

```

```

# Règle 3 : Abonnés en Roaming - Priorité Moyenne
%{
    name: "Abonnés en Roaming",
    priority: 10,
    match_field: :serving_network_plmn_id,
    match_regex: "^(310|311|312|313)", # Réseaux américains
    upf_pool: [
        %{remote_ip_address: "10.100.4.21", remote_port: 8805, weight: 100}
    ]
},

# Règle 4 : Trafic Internet - Priorité Inférieure
%{
    name: "Trafic Internet",
    priority: 5,
    match_field: :apn,
    match_regex: "^internet",
    upf_pool: [
        %{remote_ip_address: "10.100.1.21", remote_port: 8805, weight: 33},
        %{remote_ip_address: "10.100.1.22", remote_port: 8805, weight: 33},
        %{remote_ip_address: "10.100.1.23", remote_port: 8805, weight: 34}
    ]
},
]

# =====
# Pool de Secours (Dernier Recours)
# =====
# Utilisé lorsque aucune règle ne correspond et que la sélection DNS échoue
ou est désactivée
fallback_pool: [
    %{remote_ip_address: "127.0.0.21", remote_port: 8805, weight: 100}
]
}

```

Champs de Correspondance Supportés

Champ de Correspondance	Description	Valeur Exemple
:imsi	Identifiant International de l'Abonné Mobile	"310260123456789"
:apn	Nom de Point d'Accès	"internet", "ims"
:serving_network_plmn_id	PLMN du réseau de service (MCC+MNC)	"310260" (opérateur américain)
:sgw_ip_address	Adresse IP de SGW (format chaîne)	"10.0.1.50"
:uli_tai_plmn_id	ID PLMN de la Zone de Suivi	"310260"
:uli_ecgi_plmn_id	ID PLMN de la Cellule E-UTRAN	"310260"

Pool UPF et Équilibrage de Charge

Chaque règle peut spécifier un **pool UPF** avec sélection aléatoire pondérée :

```
upf_pool: [
    %{remote_ip_address: "10.100.1.21", remote_port: 8805, weight: 50},
```

```

    %{remote_ip_address: "10.100.1.22", remote_port: 8805, weight: 30},
    %{remote_ip_address: "10.100.1.23", remote_port: 8805, weight: 20}
]

```

Comment Fonctionne la Sélection Pondérée :

1. Calculer le poids total : $50 + 30 + 20 = 100$
2. Générer un nombre aléatoire : 0.0 à 100.0
3. Sélectionner UPF basé sur les plages de poids cumulées :
 - 0-50 : UPF-1 (chance de 50%)
 - 50-80 : UPF-2 (chance de 30%)
 - 80-100 : UPF-3 (chance de 20%)

Cas d'Utilisation :

- **Distribution Équitable** : Tous les poids égaux (33, 33, 34)
- **Principal/Secours** : Poids élevé principal (80), faible poids secours (20)
- **Basé sur la Capacité** : Poids proportionnel à la capacité UPF

Remplacements PCO

Les règles peuvent remplacer les valeurs PCO (Options de Configuration de Protocole) :

```

%{
  name: "Trafic IMS",
  match_field: :apn,
  match_regex: "^ims",
  upf_pool: [...],
  pco: %{
    # Remplacer uniquement des champs spécifiques
    p_cscf_ipv4_address_list: ["10.101.2.100", "10.101.2.101"],
    # Autres champs utilisent les valeurs par défaut de la configuration
    principale de pco
  }
}

```

Champs de Remplacement PCO Disponibles :

- primary_dns_server_address
- secondary_dns_server_address
- primary_nbns_server_address
- secondary_nbns_server_address
- p_cscf_ipv4_address_list
- ipv4_link_mtu_size

Sélection Basée sur DNS

Lorsqu'elle est activée, PGW-C effectue des requêtes DNS NAPTR basées sur les Informations de Localisation de l'Utilisateur :

```

upf_selection: %{
  dns_enabled: true,
  dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
  dns_suffix: "epc.3gppnetwork.org",
  dns_timeout_ms: 5000
}

```

Priorité de Requête :

1. **ECGI** (Identifiant Global de Cellule E-UTRAN) - Le plus spécifique
2. **TAI** (Identifiant de Zone de Suivi) - Zone de cellule
3. **RAI** (Identifiant de Zone de Routage) - Zone 3G/2G
4. **SAI** (Identifiant de Zone de Service) - Zone de service 3G
5. **CGI** (Identifiant Global de Cellule) - Cellule 2G

Exemple de Requête DNS :

```
# Pour la requête ECGI :  
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org  
  
# Pour la requête TAI :  
tac-lb64.tac-hb00.tac.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Processus de Sélection DNS :

1. Essayer les requêtes dans l'ordre de priorité (ECGI d'abord, puis TAI, etc.)
2. Si DNS retourne des candidats, utiliser le premier résultat (enregistré dynamiquement si nécessaire)
3. Sélectionner le UPF retourné
4. Si aucune correspondance DNS ou DNS désactivé, passer au pool de secours

Voir [Sélection de UPF basée sur DNS](#) pour des informations détaillées.

Sélection de UPF basée sur DNS

Aperçu

La sélection de UPF basée sur DNS fournit un **routage conscient de la localisation** en effectuant des requêtes DNS NAPTR utilisant les Informations de Localisation de l'Utilisateur (ULI) de la cellule actuelle de l'UE.

Référence 3GPP : TS 23.003 - Procédures DNS pour la découverte de UPF

Avantages :

- Sélection automatique de UPF basée sur la localisation géographique
- Pas de configuration manuelle de règles par cellule
- Adaptation dynamique aux changements de topologie réseau
- Réduit le transport en dirigeant vers le UPF le plus proche

Comment Cela Fonctionne

Configuration

```
config :pgw_c,  
    upf_selection: %{  
        # Activer la sélection basée sur DNS  
        dns_enabled: true,  
  
        # Priorité de requête : essayer ECGI d'abord, puis TAI, puis RAI, etc.  
        dns_query_priority: [:ecgi, :tai, :rai, :sai, :cgi],
```

```

# Suffixe DNS pour les requêtes
dns_suffix: "epc.3gppnetwork.org",

# Délai d'expiration de la requête DNS
dns_timeout_ms: 5000,

# Les règles statiques prennent toujours la priorité sur DNS
rules: [...],

# Secours si DNS échoue
fallback_pool: [...]
}

```

Formats de Requête DNS

Les requêtes DNS sont construites en utilisant les Informations de Localisation de l'Utilisateur (ULI) du message GTP-C :

1. ECGI (Identifiant Global de Cellule E-UTRAN)

Le plus spécifique - Routage au niveau de la cellule LTE

Format :

```
eci-<HEX-ECI>.ecgi.epc.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemple :

```
# ID de Cellule : 0x1A2B3C (1,715,004 décimal)
# PLMN : MCC=999, MNC=999
eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Quand Utilisé : Réseaux LTE (4G)

2. TAI (Identifiant de Zone de Suivi)

Zone de cellule - Plusieurs cellules dans la même zone de suivi

Format :

```
tac-lb<LB>.tac-hb<HB>.tac.epc.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemple :

```
# TAC : 0x0064 (100 décimal)
# Octet bas : 0x64, Octet haut : 0x00
tac-lb64.tac-hb00.tac.epc.mnc999.mcc999.epc.3gppnetwork.org
```

Quand Utilisé : Zones de suivi LTE (4G)

3. RAI (Identifiant de Zone de Routage)

Zone de routage 3G/2G

Format :

```
rac<RAC>.lac-lb<LB>.lac-hb<HB>.lac.rai.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemple :

```
# RAC : 0x0A (10 décimal)
# LAC : 0x1234 (4660 décimal)
rac0a.lac-lb34.lac-hb12.lac.rai.mnc999.mcc999.epc.3gppnetwork.org
```

Quand Utilisé : Réseaux UMTS/GPRS 3G/2G

4. SAI (Identifiant de Zone de Service)

Zone de service 3G

Format :

```
sac<SAC>.lac-lb<LB>.lac-hb<HB>.lac.sai.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemple :

```
# SAC : 0x0001
# LAC : 0x1234
sac0001.lac-lb34.lac-hb12.lac.sai.mnc999.mcc999.epc.3gppnetwork.org
```

Quand Utilisé : Zones de service UMTS 3G

5. CGI (Identifiant Global de Cellule)

Niveau de cellule 2G

Format :

```
ci<CI>.lac-lb<LB>.lac-hb<HB>.lac.cgi.mnc<MNC>.mcc<MCC>.<dns_suffix>
```

Exemple :

```
# CI : 0x5678
# LAC : 0x1234
ci5678.lac-lb34.lac-hb12.lac.cgi.mnc999.mcc999.epc.3gppnetwork.org
```

Quand Utilisé : Cellules GSM 2G

Traitements des Réponses DNS

Format d'Enregistrement NAPTR :

DNS retourne des enregistrements NAPTR pointant vers des adresses IP de UPF :

```
ec1-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org.
    IN NAPTR 10 50 "a" "x-3gpp-upf:x-s5-gtp:x-s8-gtp" ""
upf1.epc.mnc999.mcc999.3gppnetwork.org.

upf1.epc.mnc999.mcc999.3gppnetwork.org.
    IN A 10.100.1.21
```

Traitements par PGW-C :

1. Analyser les enregistrements NAPTR pour extraire les adresses IP de UPF
2. Sélectionner le premier candidat de la réponse DNS
3. Enregistrer dynamiquement si non déjà configuré (ou mettre en œuvre une sélection basée sur la charge)

Exemple :

```
DNS retourne : [10.100.1.21, 10.100.5.99, 10.200.3.50]
```

```
Sélectionné : 10.100.1.21 (premier candidat)
```

```
Action : Enregistrer dynamiquement si non dans upf_selection
```

Exemple de Priorité de Sélection

Cas d'Utilisation

1. Équilibrage de Charge Géographique

Scénario : L'opérateur a des UPFs dans plusieurs villes

Configuration DNS :

```
# Cellule de Chicago
eci-aaa.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-Chicago (10.1.1.21)
```

```
# Cellule de New York
eci-bbb.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-NewYork (10.2.1.21)
```

```
# Cellule de Los Angeles
eci-ccc.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF-LosAngeles (10.3.1.21)
```

Avantage : Les utilisateurs sont automatiquement dirigés vers le UPF le plus proche, réduisant la latence et le transport

2. Informatique en Edge

Scénario : UPFs MEC (Multi-access Edge Computing) déployés sur les sites cellulaires

Configuration DNS :

```
# Chaque cellule pointe vers le UPF local en edge
eci-* .ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org → UPF Local en Edge
```

Avantage : Latence ultra-faible pour les applications en edge

3. Topologie Réseau Dynamique

Scénario : Les adresses UPF changent en raison de mises à niveau ou de maintenance

Avantage : Mettre à jour les enregistrements DNS sans changer la configuration PGW-C

Dépannage de la Sélection DNS

Échecs de Requête DNS

Symptômes :

- Journal : "Échec de la sélection UPF DNS : :nxdomain"
- Les sessions tombent dans le pool de secours

Causes Possibles :

1. Serveur DNS mal configuré
2. Zone DNS non peuplée pour les ID de cellules
3. ULI non présent dans le message GTP-C

Résolution :

```
# Tester la requête DNS manuellement
dig eci-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org NAPTR

# Vérifier les journaux PGW-C pour les requêtes DNS
grep "Sélection UPF DNS : interrogeant" /var/log/pgw_c.log

# Vérifier la présence de l'ULI dans la session
# Vérifier le champ "uli" dans l'état de la session
```

DNS Retourne un UPF Inconnu

Comportement :

- DNS retourne un UPF candidat qui n'est pas dans upf_selection
- Le système tente automatiquement l'enregistrement dynamique
- Si l'association PFCP réussit, le UPF est utilisé pour la session
- Si l'association PFCP échoue, il tombe dans le pool de secours

Exemple :

```
DNS retourne : [10.99.1.50]
upf_selection : [10.100.1.21, 10.100.1.22]

Action : Enregistrer dynamiquement 10.99.1.50
- Envoyer la Configuration de l'Association PFCP
- Si succès : Utiliser pour la session
- Si délai d'attente : Tomber dans le pool de secours
```

Options de Résolution :

1. Pré-configurer dans upf_selection pour une surveillance immédiate :

```
upf_selection: %{
    fallback_pool: [
        %{remote_ip_address: "10.99.1.50", remote_port: 8805, weight: 100}
    ]
}
```

2. Mettre à jour DNS pour retourner les IPs de UPF pré-configurées

3. Autoriser l'enregistrement dynamique (recommandé pour les scénarios MEC/edge)

Délai d'Attente de Requête

Symptômes :

- Journal : "Sélection UPF DNS : délai d'attente de requête"
- Les sessions prennent plus de temps à s'établir

Résolution :

```
upf_selection: %{
    dns_timeout_ms: 10000 # Augmenter le délai d'attente à 10 secondes
}
```

Surveillance de la Sélection DNS

Métriques :

```
# Taux de réussite des requêtes DNS
rate(upf_selection_dns_success_total[5m]) /
rate(upf_selection_dns_attempts_total[5m])

# Latence des requêtes DNS
histogram_quantile(0.95, rate(upf_selection_dns_duration_seconds_bucket[5m]))

# Utilisation du secours (indique des problèmes DNS)
rate(upf_selection_fallback_used_total[5m])
```

Journaux :

```
[debug] Sélection UPF DNS : interrogeant
ec1-1a2b3c.ecgi.epc.mnc999.mcc999.epc.3gppnetwork.org
[debug] Sélection UPF DNS : a obtenu 2 candidats de DNS
[info] Sélection UPF DNS : sélectionné 10.100.1.21
```

Flux de Messages

Flux Complet d'Établissement de Session

Flux de Modification de Session

Récupération après Échec de Cœur

Dépannage

Problèmes Courants

1. Échec de Configuration de l'Association

Symptômes :

- Message journal : "Échec de la Configuration de l'Association PFCP"
- Pas de réponse à la Demande de Configuration de l'Association

Causes Possibles :

- PGW-U non accessible (problème réseau)
- PGW-U non en cours d'exécution
- Pare-feu bloquant le port UDP 8805
- `remote_ip_address` incorrect dans la configuration

Résolution :

```
# Tester la connectivité
ping <pgw_u_ip_address>

# Tester le port UDP
nc -u -v <pgw_u_ip_address> 8805

# Vérifier le pare-feu
iptables -L -n | grep 8805
```

2. Échecs de Cœurs

Symptômes :

- Journal : "Échecs consécutifs de cœur : 3"
- Association marquée comme inactive

Causes Possibles :

- Latence réseau ou perte de paquets
- PGW-U surchargé
- Intervalle de cœur trop agressif

Résolution :

```
# Remarque : La période de cœur est fixée à 5 secondes
# Pour réduire la charge réseau, ajuster le seuil d'échec dans le code :
# lib/core/pfcp_node/impl/peer.ex - fonction is_peer_healthy?/1
# Changer : state.missed_heartbeats_consecutive < 3
# À : state.missed_heartbeats_consecutive < 5 (plus tolérant)
```

3. Échec de l'Établissement de Session

Symptômes :

- Réponse de Création de Session avec cause d'erreur
- Journal : "Échec de l'Établissement de Session PFCP"

Causes Possibles :

- Aucun pair PGW-U disponible
- Épuisement des ressources PGW-U
- Configuration de règle invalide

Vérifier :

1. Vérifier qu'au moins un pair a `is_associated = true`
2. Vérifier les journaux PGW-U pour des erreurs
3. Vérifier l'unicité du SEID

4. Erreurs de SEID Dupliqué

Symptômes :

- Réponse d'Établissement de Session : Cause "Contexte de session non trouvé"

Cause :

- Collision de SEID (très rare)
- Redémarrage de PGW-U sans connaissance de PGW-C

Résolution :

- Redémarrer l'association PFCP (déclenche un nouvel horodatage de récupération)
- PGW-C détectera le redémarrage de PGW-U et nettoiera les anciennes sessions

Surveillance de la Santé PFCP

Métriques à Surveiller :

```
# État d'association du pair PFCP
pfcp_peer_associated{peer="PGW-U Principal"} 1

# Sessions PFCP actives
seid_registry_count 150

# Taux de messages PFCP
rate(sxb_inbound_messages_total[5m])

# Erreurs PFCP
rate(sxb_inbound_errors_total[5m])

# Échecs de cœur
pfcp_consecutive_heartbeat_failures{peer="PGW-U Principal"} 0
```

Exemples d'Alerte :

```
# Alerte sur association inactive
- alert: PFCPAssociationDown
  expr: pfcp_peer_associated == 0
  for: 1m
  annotations:
    summary: "Le pair PFCP {{ $labels.peer }} est hors ligne"

# Alerte sur un taux élevé d'échecs d'établissement de session
- alert: PFCPSessionEstablishmentFailureHigh
  expr:
  rate(sxb_inbound_errors_total{message_type="session_establishment_response"}[5m])
> 0.1
  for: 5m
  annotations:
    summary: "Taux élevé d'échecs d'établissement de session PFCP"
```

Interface Web - Surveillance PFCP

OmniPGW fournit deux pages d'interface Web pour surveiller les opérations PFCP/Sxb en temps réel.

Page d'État UPF/Paire PFCP

Accès : `http://<omnipegw-ip>:<web-port>/upf_status`

Objectif : Surveiller l'état d'association PFCP avec tous les pairs PGW-U configurés

Fonctionnalités :

1. Vue d'Ensemble de l'État des Pairs

- **Nombre Associé** - Nombre de pairs avec une association PFCP active
- **Nombre Non Associé** - Nombre de pairs hors ligne ou non connectés
- Actualisation automatique toutes les 2 secondes

2. Informations par Pair

Pour chaque pair PGW-U configuré :

- **Nom du Pair** - Nom convivial de la configuration
- **Adresse IP** - IP distante de PGW-U
- **État de l'Association** - Associé (vert) ou Non Associé (rouge)
- **ID de Nœud** - Identifiant de Nœud PFCP
- **Horodatage de Récupération** - Dernière heure de redémarrage du pair
- **Période de Cœur** - Intervalle de cœur configuré
- **Cœurs Manqués Consécutifs** - Compte actuel des échecs
- **Fonctionnalités de la Fonction UP** - Capacités annoncées par PGW-U

3. Détails Développables

Cliquez sur n'importe quel pair pour voir :

- Configuration complète du pair
- Bitmap des fonctionnalités de la fonction UP
- Horodatages d'association
- tat complet du pair

Page des Sessions PFCP

Accès : `http://<omnipegw-ip>:<web-port>/pfcp_sessions`

Objectif : Voir les sessions PFCP actives entre OmniPGW et PGW-U

Fonctionnalités :

1. Nombre de Sessions Actives

- Nombre total de sessions PFCP actives
- Mise à jour en temps réel

2. Informations sur la Session

Pour chaque session PFCP :

- **Clé de Session** - Clé d'enregistrement interne
- **ID de Processus** - Identifiant du processus de session

- **IMSI** - Abonné associé (si disponible)
- **État** - État de la session

3. État Complet de la Session

Vue développable montrant :

- Contexte complet de la session PFCP
- PDRs, FARs, QERs, BARs (règles de transfert)
- F-SEIDs (identifiants de point de terminaison de session)
- Association de pair PGW-U

Cas d'Utilisation Opérationnels

Surveiller la Santé de l'Association PFCP :

1. Ouvrir la page d'État UPF
2. Vérifier que tous les pairs affichent "Associé"
3. Vérifier que le compte de coeurs manqués = 0
4. Si un pair affiche "Non Associé" :
 - Vérifier la connectivité IP du pair
 - Vérifier que le pair est en cours d'exécution
 - Vérifier le pare-feu (UDP 8805)

Dépanner les Échecs d'Établissement de Session :

1. La session utilisateur échoue à s'établir
2. Vérifier la page des Sessions PGW - la session existe-t-elle ?
3. Vérifier la page des Sessions PFCP - session PFCP créée ?
4. Si aucune session PFCP :
 - Vérifier l'État UPF - un pair est-il associé ?
 - Vérifier les journaux pour des erreurs PFCP
5. Si une session PFCP existe :
 - Inspecter les PDRs/FARs pour vérifier les règles programmées
 - Le problème est probablement en aval (PGW-U ou réseau)

Vérifier la Distribution de Charge des Pairs :

1. Avec plusieurs pairs PGW-U configurés
2. Vérifier la page des Sessions PFCP
3. Vérifier que les sessions sont distribuées entre les pairs
4. Identifier si un pair a une charge disproportionnée

Déetecter les Pannes de Pair :

- Un coup d'œil rapide à la page d'État UPF
- Badge rouge "Non Associé" immédiatement visible
- Le compteur de coeurs manqués montre la dégradation avant l'échec total
- Configurer des alertes de surveillance basées sur les données de l'interface Web

Avantages :

- **Surveillance en temps réel** - Pas besoin d'interroger des métriques ou de SSH
- **Statut visuel** - Couleur codée associé/non associé
- **Tendances de santé des pairs** - Le compteur de coeurs manqués montre un avertissement précoce
- **Inspection au niveau de la session** - Voir exactement les PDRs/FARs/QERs programmés

- **Aucun outil requis** - Juste un navigateur web
-

Documentation Connexe

Configuration

- [**Guide de Configuration**](#) - Sélection de UPF, surveillance de la santé, configuration PFCP
- [**Gestion des Sessions**](#) - Cycle de vie de la session PDN, établissement de bearer
- [**Gestion de QoS & Bearer**](#) - Configuration détaillée de QoS, programmation de QER

Facturation et Surveillance

- [**Interface Diameter Gx**](#) - Règles PCC qui pilotent l'application de QoS PFCP
- [**Interface Diameter Gy**](#) - Gestion des quotas de facturation en ligne via URRs
- [**Format de CDR de Données**](#) - Génération de CDR à partir des rapports d'utilisation PFCP
- [**Guide de Surveillance**](#) - Métriques PFCP, suivi des sessions, alertes de santé UPF

Interfaces Réseau

- [**Interface S5/S8**](#) - Gestion des bearers du plan de contrôle
 - [**Attribution IP UE**](#) - Attribution d'adresse UE via PFCP
-

[**Retour au Guide d'Opérations**](#)



Documentation de l'interface S5/S8

Communication GTP-C avec SGW-C

OmniPGW par Omnitouch Network Services

Aperçu

L'**interface S5/S8** connecte OmniPGW au SGW-C (plan de contrôle de la passerelle de service) en utilisant le protocole **GTP-C v2** (GPRS Tunnelling Protocol - plan de contrôle). Cette interface gère le signalement de gestion de session entre les passerelles.

Détails du protocole

GTP-C Version 2

- **Protocole :** GTP-C v2 (3GPP TS 29.274)
- **Transport :** UDP
- **Port :** 2123 (standard)
- **Type d'interface :** Plan de contrôle

TEID (Identifiant de point de terminaison de tunnel)

Chaque session a un **TEID** unique pour le routage des messages :

- **TEID local** - Alloué par OmniPGW pour les messages entrants
- **TEID distant** - Alloué par SGW-C pour les messages sortants

Message Flow:

```
SGW-C → OmniPGW: Destination TEID = TEID local d'OmniPGW  
OmniPGW → SGW-C: Destination TEID = TEID distant de SGW-C
```

Configuration

Configuration de base

```
# config/runtime.exs
config :pgw_c,
s5s8: %{
  # Adresse IPv4 locale pour l'interface S5/S8
  local_ipv4_address: "10.0.0.20",

  # Optionnel : Adresse IPv6 locale
  local_ipv6_address: nil,

  # Optionnel : Remplacer le port par défaut
  local_port: 2123
}
```

Exigences réseau

Règles de pare-feu :

```
# Autoriser GTP-C depuis le réseau SGW-C
iptables -A INPUT -p udp --dport 2123 -s <sgw_network>/24 -j ACCEPT
```

```
# Autoriser GTP-C sortant vers SGW-C  
iptables -A OUTPUT -p udp --dport 2123 -d <sgw_network>/24 -j ACCEPT
```

Routage :

```
# Assurez-vous d'une route vers le réseau SGW-C  
ip route add <sgw_network>/24 via <gateway_ip> dev eth0
```

Types de messages

L'interface S5/S8 gère le signalement GTP-C pour la gestion des sessions PDN. Pour un cycle de vie de session détaillé et la gestion des états, voir le [Guide de gestion des sessions](#).

Gestion des sessions

Demande de création de session

Direction : SGW-C → OmniPGW

But : Établir une nouvelle connexion PDN

Éléments d'information clés (IE) :

Nom de l'IE	Type	Description
IMSI	Identité	Identité internationale de l'abonné mobile
MSISDN	Identité	Numéro de téléphone mobile
APN	Chaîne	Nom du point d'accès (par exemple, "internet")
Type RAT	Enum	Technologie d'accès radio (EUTRAN)
Contexte de porteur	Groupé	Informations sur le porteur par défaut
Fuseau horaire UE	Horodatage	Fuseau horaire de l'UE
ULI	Groupé	Informations de localisation de l'utilisateur (TAI, ECGI)
Réseau de service	PLMN	MCC/MNC du réseau de service

Exemple :

```
Demande de création de session  
└─ IMSI: 310260123456789  
└─ MSISDN: 14155551234  
└─ APN: internet  
└─ Type RAT: EUTRAN (6)  
└─ Contexte de porteur  
    └─ EBI: 5  
        └─ QoS du porteur (QCI 9, ARP, débits)  
        └─ S5/S8 F-TEID (point de terminaison de tunnel SGW-U)  
└─ ULI  
    └─ TAI: MCC 310, MNC 260, TAC 12345  
    └─ ECGI: MCC 310, MNC 260, ECI 67890
```

Réponse à la création de session

Direction : OmniPGW → SGW-C

But : Accuser réception de la création de session

Éléments d'information clés :

Nom de l'IE	Type	Description
Cause	Résultat	Code de succès ou d'erreur
Contexte de porteur	Groupé	Informations sur le porteur
Allocation d'adresse PDNIP	Adresse IP	UE allouée (voir Allocation d'IP UE)
Restriction APN	Enum	Restrictions d'utilisation de l'APN

Nom de l'IE	Type	Description
PCO	Options	Options de configuration de protocole (voir Configuration PCO)

Réponse de succès :

```

Réponse à la création de session
└─ Cause: Demande acceptée (16)
└─ Allocation d'adresse PDN
    └─ IPv4: 100.64.1.42
└─ Contexte de porteur
    └─ EBI: 5
    └─ Cause: Demande acceptée
        └─ S5/S8 F-TEID (point de terminaison de tunnel PGW-U depuis PFCP)
└─ Restriction APN: Public-1 (1)
└─ PCO
    └─ Serveur DNS: 8.8.8.8
    └─ Serveur DNS: 8.8.4.4
    └─ MTU de lien: 1400

```

Demande de suppression de session

Direction : SGW-C → OmniPGW

But : Terminer la connexion PDN

Éléments d'information clés :

Nom de l'IE	Description
EBI	ID de porteur EPS à supprimer
EBI lié	Porteur associé (optionnel)

Réponse à la suppression de session

Direction : OmniPGW → SGW-C

But : Accuser réception de la suppression de session

Éléments d'information clés :

Nom de l'IE	Description
Cause	Code de succès ou d'erreur

Gestion des porteurs

Demande de création de porteur

Direction : OmniPGW → SGW-C

But : Créer un porteur dédié (initié par la politique PCRF)

Déclenché par :

- PCRF envoie une nouvelle règle PCC nécessitant un porteur dédié
- OmniPGW demande à SGW-C d'établir le porteur

Demande de suppression de porteur

Direction : OmniPGW → SGW-C ou SGW-C → OmniPGW

But : Supprimer le porteur dédié

Scénarios :

- **Initié par PGW** : Changement de politique PCRF supprime le porteur dédié
 - **Initié par SGW** : Libération de ressources radio
-

Flux de messages

Établissement de session

Résiliation de session

Codes de cause

Succès

Code	Nom	Description
16	Demande acceptée	Opération réussie

Erreurs (Échecs permanents)

Code	Nom	Quand utilisé
65	Utilisateur inconnu	PCRF rejeté (IMSI non trouvé)
66	Pas de ressources disponibles	Pool IP épuisé
93	Service non pris en charge	APN invalide
94	Erreur sémantique dans TFT	Modèle de flux de trafic invalide

Erreurs (Échecs transitoires)

Code	Nom	Quand utilisé
72	Pair distant ne répond pas	Délai d'attente PCRF/PGW-U
73	Collision avec une demande initiée par le réseau	Opérations simultanées

Surveillance

Métriques S5/S8

```
# Compteurs de messages
s5s8_inbound_messages_total{message_type="create_session_request"}
s5s8_inbound_messages_total{message_type="delete_session_request"}

# Compteurs d'erreurs
s5s8_inbound_errors_total

# Latence de traitement des messages
s5s8_inbound_handling_duration_bucket

# TEIDs actifs
teid_registry_count
```

Requêtes utiles

Taux de création de session :

```
rate(s5s8_inbound_messages_total{message_type="create_session_request"}[5m])
```

Taux d'erreur :

```
rate(s5s8_inbound_errors_total[5m])
```

Latence (p95) :

```
histogram_quantile(0.95,  
rate(s5s8_inbound_handling_duration_bucket{request_message_type="create_session_request"}[5m])  
)
```

Dépannage

Problème : Pas de réponse d'OmniPGW

Symptômes :

- SGW-C envoie une demande de création de session
- Pas de réponse reçue
- Délai d'attente à SGW-C

Causes :

1. Problème de connectivité réseau
2. OmniPGW ne répond pas à l'IP configurée
3. Pare-feu bloquant UDP 2123
4. Mauvais TEID dans la demande

Débogage :

```
# Vérifier qu'OmniPGW écoute  
netstat -ulpn | grep 2123  
  
# Vérifier les paquets entrants  
tcpdump -i any -n port 2123  
  
# Vérifier la configuration  
grep "local_ipv4_address" config/runtime.exs  
  
# Vérifier le pare-feu  
iptables -L -n | grep 2123
```

Problème : Échec de la création de session

Symptômes :

- Réponse de création de session avec cause d'erreur
- Session non établie

Causes courantes :

Cause 65 (Utilisateur inconnu) :

- PCRF a rejeté l'abonné
- Vérifier l'IMSI dans HSS/SPR

Cause 66 (Pas de ressources) :

- Pool IP épuisé
- Vérifier : curl http://pgw:9090/metrics | grep address_registry_count
- Étendre le pool IP

Cause 72 (Pair distant ne répond pas) :

- Délai d'attente PCRF ou PGW-U hors service
- Vérifier la connectivité Gx
- Vérifier l'association PFCP

Problème : Collision de TEID

Symptômes :

- Message routé vers la mauvaise session
- Comportement inattendu

Cause :

- TEID réutilisé avant nettoyage
- Bug dans l'allocation de TEID

Résolution :

- Assurer une allocation unique de TEID
 - Vérifier le registre de TEID pour les fuites
-

Meilleures pratiques

Conception réseau

1. Interface réseau dédiée

- Utiliser un VLAN séparé pour S5/S8
- Isoler du trafic de gestion

2. Optimisation de MTU

- S'assurer que le MTU prend en charge les en-têtes GTP
- MTU minimum : 1500 octets (1464 charge utile + 36 GTP)

3. Redondance

- Plusieurs instances d'OmniPGW
- Équilibrage de charge basé sur DNS depuis SGW-C

Performance

1. Tailles de tampon UDP

- Augmenter les tampons de socket pour une charge élevée
- Typique : 4-8 Mo par socket

2. Limites de connexion

- Planifier le nombre de sessions attendues
- Surveiller le compte du registre de TEID

Sécurité

1. Filtrage IP

- Autoriser uniquement GTP-C depuis des IP SGW-C connues
- Utiliser iptables ou des ACL réseau

2. Validation des messages

- OmniPGW valide tous les messages entrants
 - Rejette les paquets GTP-C mal formés
-

Documentation connexe

Fonctions principales

- [Guide de configuration](#) - Configuration de l'interface S5/S8, configuration de l'IP locale
- [Gestion des sessions](#) - Cycle de vie de la session PDN, établissement du porteur

- [**Allocation d'IP UE**](#) - Livraison d'adresse IP via la réponse de création de session
- [**Configuration PCO**](#) - Paramètres PCO dans les messages GTP-C

Interfaces connexes

- [**Interface PFCP**](#) - Coordination du plan utilisateur avec le plan de contrôle S5/S8
- [**Interface Diameter Gx**](#) - Intégration des politiques avec l'établissement du porteur
- [**Interface Diameter Gy**](#) - Intégration de facturation avec la gestion du porteur

Opérations

- [**Guide de surveillance**](#) - Métriques GTP-C S5/S8, suivi des messages
- [**Format de CDR de données**](#) - Génération de CDR à partir des sessions GTP-C

[Retour au guide des opérations](#)

Interface S5/S8 d'OmniPGW - par Omnitouch Network Services

Guide de Gestion des Sessions

Cycle de Vie et Opérations de Connexion PDN

OmniPGW par Omnitouch Network Services

Aperçu

Une Session PDN (Packet Data Network) représente la connexion de données d'un UE à travers OmniPGW. Chaque session coordonne plusieurs interfaces et ressources pour permettre la connectivité des données.

Composants de la Session

Identifiants de Session

Chaque session a plusieurs identifiants pour différentes interfaces :

Identifiant	Interface	Objectif
TEID	S5/S8 (GTP-C)	ID de point de terminaison de tunnel pour la communication SGW-C
SEID	Sxb (PPCP)	ID de point de terminaison de session pour la communication PGW-U
Session-ID	Gx (Diameter)	Session Diameter pour la communication PCRF
Charging-ID	Comptabilité	ID unique pour la facturation

Données de Session

Création de Session

Flux d'Appel

Étapes

1. Recevoir la Demande de Crédit de Session (S5/S8)

La création de session est initiée via le signalement GTP-C sur l'interface S5/S8. Voir [Interface S5/S8](#) pour les détails complets du protocole GTP-C et des formats de message.

Entrée :

- IMSI, MSISDN, IMEI
- APN (par exemple, "internet")
- Type de RA (EUTRAN)
- Localisation de l'UE (TAI, ECGI)
- Contexte de porteur (QoS, F-TEID)

2. Allocation de Ressources

- Allouer l'IP de l'UE à partir du pool APN
- Générer l'ID de facturation
- Générer l'ID de session Gx
- Allouer le TEID S5/S8
- Sélectionner le pair PGW-U

3. Demande de Politique (Gx)

Demandez une politique au PCRF :

- Envoyer CCR-Initial
- Recevoir CCA-Initial avec des règles QoS et PCC

4. Configuration du Plan Utilisateur (PFCP)

Programmer le PGW-U avec des règles de transfert :

- Envoyer la Demande d'Établissement de Session
- Inclure PDRs, FARs, QERs, BAR
- Recevoir F-TEID pour le tunnel S5/S8

5. Réponse au SGW-C

Envoyer la Réponse de Crédit de Session :

- Adresse IP de l'UE
- F-TEID S5/S8 (du PGW-U)
- PCO (DNS, P-CSCF, MTU)
- Contexte de porteur

Modification de Session

Déclencheurs

Les sessions peuvent être modifiées en raison de :

- Changements de QoS - Mises à jour des débits par le PCRF
- Opérations de Porteur - Ajouter/retirer des porteurs dédiés
- Transfert - Changement de SGW
- Mises à jour de Politique - Nouvelles règles PCC du PCRF

Flux de Modification de QoS

Suppression de Session

Flux d'Appel

Processus de Nettoyage

Ressources Libérées :

- Adresse IP de l'UE → retour au pool
- TEID → retiré du registre
- SEID → retiré du registre
- Session-ID → retiré du registre
- Charging-ID → libéré
- Processus de session terminé

Enregistrements de Facturation Générés :

- CDR final (Charging Data Record) écrit pour la facturation hors ligne - Voir [Format de CDR de Données](#)

État de Session

Machine d'État

Suivi de Session

Requêtes de Registre :

- Par TEID (S5/S8):
TEID 0x12345678 → Session PID
- Par SEID (Sxb):
SEID 0xABCD → Session PID
- Par Session-ID (Gx):

```
"pgw.example.com;123;456" → Session PID  
Par IP de l'UE:  
100.64.1.42 → Session PID  
Par IMSI + EBI:  
"310260123456789" + EBI 5 → Session PID
```

Surveillance des Sessions

Nombre de Sessions Actives

```
# Total des sessions actives  
teid_registry_count  
  
# Sessions PFCP  
seid_registry_count  
  
# Sessions Gx  
session_id_registry_count
```

Métriques de Session

```
# Taux de création de session  
rate(s5s8_inbound_messages_total{message_type="create_session_request"}[5m])  
  
# Taux de suppression de session  
rate(s5s8_inbound_messages_total{message_type="delete_session_request"}[5m])  
  
# Latence de création de session (p95)  
histogram.quantile(0.95,  
  rate(s5s8_inbound_handling_duration_bucket{request_message_type="create_session_request"}[5m]))
```

Problèmes Courants

Échecs de Création de Session

Causes :

1. Pool IP Épuisé - Aucune IP disponible
2. PCRF Injoignable - Délai d'attente Gx
3. PGW-U Hors Service - Aucun pair PFCP disponible
4. Rejet PCRF - Utilisateur inconnu, non autorisé

Débogage :

```
# Vérifier le pool IP  
curl http://pgw:9090/metrics | grep address_registry_count  
  
# Vérifier la connectivité PCRF  
# Vérifier les erreurs Gx dans les journaux  
  
# Vérifier l'association PGW-U  
# Vérifier l'état du pair PFCP
```

Session Bloquée/Obsolète

Symptômes :

- Session non supprimée correctement
- Ressources non libérées
- Registres montrent un nombre plus élevé que prévu

Causes :

1. Demande de suppression de session non reçue
2. Plantage du processus de session sans nettoyage
3. Fuite de registre

Résolution :

```
# Redémarrer OmniPGW (libère toutes les sessions)  
# Mettre en œuvre un mécanisme de délai d'attente de session
```

L'UE Ne Peut Pas Établir de Session

Symptômes :

- Échec de l'attachement de l'UE
- Réponse de création de session avec cause d'erreur

Causes et Réponses Courantes :

Valeur de Cause	Signification	Action
Utilisateur Inconnu	Rejet PCRF (IMSI non dans la base de données)	Provisionner l'abonné
Pas de Ressources Disponibles	Pool IP épuisé	Élargir le pool IP
Pair Distant Ne Répond Pas	Délai d'attente PCRF/PGW-U	Vérifier la connectivité
Service Non Supporté	APN invalide	Configurer le pool APN

Meilleures Pratiques

Limites de Session

Configurer une capacité appropriée :

Utilisateurs concurrents attendus : 10,000
Surcharge de session par utilisateur : -10 Ko RAM
RAM totale pour les sessions : -100 Mo

Paramètres de la VM Erlang :
- Max processus : 262,144 (par défaut)
- Taille du tas de processus : Ajuster en fonction de la charge

Nettoyage de Session

Assurer un nettoyage approprié :

1. Toujours répondre aux demandes de suppression de session
2. Mettre en œuvre un délai d'attente de session pour les sessions obsolètes
3. Surveiller les comptes de registre pour les fuites

Haute Disponibilité

Redondance de Session :

- Utiliser un design sans état (sessions liées à l'instance)
- Mettre en œuvre une base de données de session pour la HA (futur)
- DNS/équilibrage de charge pour la bascule

Éléments de Données de Session

Quelles Informations Une Session Stocke-t-elle ?

Chaque session PDN active maintient les informations suivantes :

Identification de l'UE :

- IMSI : "310260123456789" (identité de l'abonné)
- MSISDN : "14155551234" (numéro de téléphone)

- MEI/IMEI : Identifiant de l'appareil

Détails de la Connexion PDN :

- APN : "internet" (nom du réseau)
- Adresse IP de l'UE : 100.64.1.42 (IP allouée)
- Type de PDN : IPv4, IPv6, ou IPv4v6

Identifiants de Session :

- ID de facturation : Identifiant de facturation unique
- EBI de Porteur par Défaut : Identifiant de Porteur EPS (typiquement 5)

Paramètres QoS :

- APN-AMBR : Débit Maximum Agrégé
 - Montant : 100 Mbps
 - Descendant : 50 Mbps

Règles de Transfert :

- PDRs (Règles de Détection de Paquet) : Correspondre aux paquets
- FARs (Règles d'Action de Transfert) : Actions de transfert/abandon
- QERs (Règles d'Application de QoS) : Limitation de débit
- BAR (Règle d'Action de Mise en Mémoire) : Mise en mémoire descendante

Contexte d'Interface :

- État S5/S8 : TEIDs locaux/distant, adresse SGW-C
- État SxS : SEIDs locaux/distant, adresse PGW-U
- État Gx : Session-ID Diameter, compteur de requêtes

Interface Web - Surveillance des Sessions en Direct

OmniPGW comprend une **Interface Web** en temps réel pour surveiller les sessions actives sans avoir besoin de consulter des métriques ou des journaux.

Recherche UE & Analyse Approfondie

Accès : http://<omnippgw-ip>:<web-port>/ue_search

Objectif : Rechercher des sessions UE spécifiques et voir des informations détaillées

Fonctionnalités :

1. Fonctionnalité de Recherche

- **IMSI** (par exemple, "310170123456789")
- **MSISDN** (numéro de téléphone)
- **Adresse IP** (par exemple, "100.64.1.42")

2. Options de Recherche

- Sélecteur déroulant pour choisir le type de recherche
- Recherche en temps réel avec résultats instantanés
- Interface claire avec des indices de recherche

3. Résultats d'Analyse Approfondie

Une fois trouvée, affiche des informations complètes sur la session, y compris :

- Détails complets de l'abonné
- Tous les points de terminaison de tunnel et identifiants
- Informations sur la QoS et le porteur
- État complet de la session

Cas d'Utilisation :

- Dépanner des problèmes spécifiques d'abonné
- Vérifier l'établissement de session
- Vérifier l'adresse IP assignée
- Inspecter les paramètres de session

Page des Sessions PGW

Accès : http://<omnippgw-ip>:<web-port>/pgw_sessions

Objectif : Vue en temps réel de toutes les sessions PDN actives

Fonctionnalités :

1. Aperçu de la Session

- Nombre de sessions en direct (mise à jour toutes les 2 secondes)
- Vue en grille de toutes les sessions actives
- Pas de rafraîchissement nécessaire - mises à jour automatiques

2. Informations Rapides sur la Session

Visibles pour chaque session :

- **IMSI** - Identité de l'abonné

- UE IP - Adresse IP allouée
- SGW TEID - ID de tunnel S5/S8 du SGW
- PGW TEID - ID de tunnel S5/S8 de l'OmniPGW
- APN - Nom du Point d'Accès

3. Fonctionnalité de Recherche

Rechercher des sessions par :

- IMSI (par exemple, "310260")
- Adresse IP de l'UE (par exemple, "100.64")
- MSISDN / numéro de téléphone
- Nom de l'APN

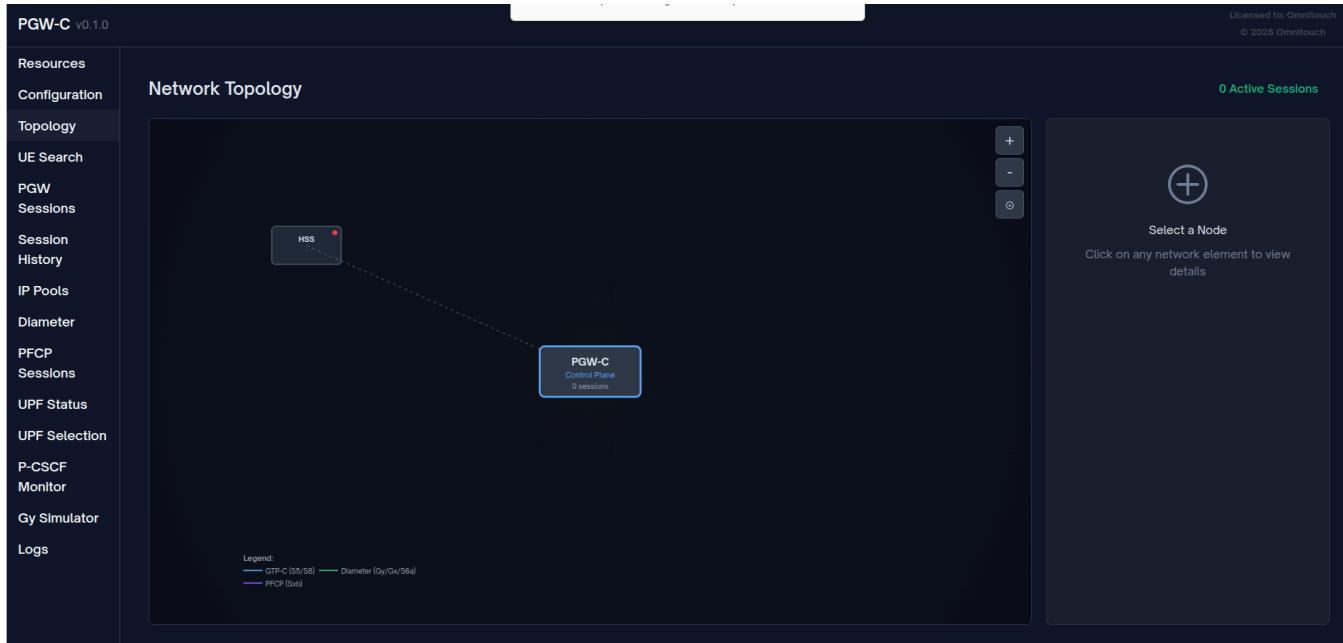
4. Détails Développables

Cliquez sur n'importe quelle ligne de session pour voir les détails complets :

- Informations complètes sur l'abonné (IMSI, MSISDN, IMEI)
- Contexte réseau (type de RAT, réseau de service MCC/MNC)
- Paramètres QoS (AMBR montant/descendant dans un format lisible)
- Identifiants de tunnel (les deux TEIDs en format hexadécimal)
- ID de processus pour le débogage
- État complet de la session (structure de données brute)

Vue de Topologie Réseau

Accès : <http://<omnippgw-ip>:<web-port>/topology>



Objectif : Représentation visuelle des connexions réseau et des sessions actives

Fonctionnalités :

1. Visualisation de la Topologie

- Graphique visuel des éléments du réseau
- Montre le nœud PGW-C (Plan de Contrôle)
- Pairs HSS (Home Subscriber Server) connectés
- Affichage du nombre de sessions actives

2. Éléments Interactifs

- Contrôles de zoom (+/-)
- Bouton de centrage de pairs
- Cliquez sur les nœuds pour des détails
- Montre l'état de connexion (vert = actif, rouge = hors service)

3. Compte de Sessions

- Compteur de sessions actives en temps réel
- Mises à jour automatiques
- Indication visuelle de la charge

Cas d'Utilisation :

- Comprendre l'architecture réseau d'un coup d'œil
- Vérifier les connexions de pairs
- Surveiller les changements de topologie
- Vérification rapide de la santé du réseau

Historique des Sessions & Journal d'Audit

Accès : http://<omnippgw-ip>:<web-port>/session_history

Objectif : Suivre les événements historiques de session et la piste d'audit

Fonctionnalités :

1. Filtrage des Événements

- Filtrer par type d'événement (Tous les Événements, Session Créeé, Session Supprimée, etc.)
- Sélection de plage de dates (De Date / À Date)
- Recherche par IMSI, MSISDN, adresse IP ou TEID

2. Fonctionnalité d'Exportation

- Exporter au format CSV pour analyse
- Inclut tous les résultats filtrés
- Utile pour la conformité et les rapports

3. Types d'Événements Suivis

- Événements de création de session
- Événements de suppression de session
- Événements de modification
- Événements d'erreur

Cas d'Utilisation :

- Piste d'audit pour la conformité
- Analyse historique des sessions
- Dépanner des problèmes passés
- Générer des rapports d'utilisation
- Suivre les modèles de session au fil du temps

Cas d'Utilisation Opérationnels

Vérification de Session :

1. L'utilisateur signale un problème de connectivité
2. Rechercher dans l'Interface Web par IMSI ou numéro de téléphone
3. Vérifier que la session existe et que l'UE a une adresse IP
4. Vérifier que les valeurs QoS correspondent au plan de l'abonné
5. Vérifier que les points de terminaison de tunnel sont établis

Surveillance de Capacité :

- Jeter un œil au nombre de sessions actives
- Comparer avec la capacité sous licence
- Identifier les modèles d'utilisation par APN

Dépannage :

- Trouver une session spécifique par n'importe quel identifiant
- Inspecter l'état complet de la session sans SSH/IE
- Vérifier que les TEIDs SGW et PGW correspondent entre les systèmes
- Vérifier les valeurs AMBR appliquées par le PCRF

Avantages par rapport aux Métriques :

- Voir les détails de session individuels (les métriques montrent des agrégats)
- Capacités de recherche et de filtrage
- Format lisible par l'homme (bande passante en Mbps, pas en bps)
- Inspection de l'état en temps réel
- Aucun accès à la ligne de commande requis

Documentation Connexe

Fonctions de Session de Base

- [Interface PFCP](#) - Établissement de session du plan utilisateur, PDRs, FARs, QERs, URRs
- [Allocation IP de l'UE](#) - Attribution d'adresse IP, gestion du pool APN
- [Configuration PCO](#) - Paramètres DNS, P-CSCF, MTU livrés à l'UE
- [Guide de Configuration](#) - Sélection de l'UPF, flux d'établissement de session

Politique et Facturation

- [Interface Diameter Gx](#) - Contrôle de politique PCRF, règles PCC, gestion de QoS
- [Interface Diameter Gy](#) - Facturation en ligne OCS, suivi des quotas
- [Format de CDR de Données](#) - Génération d'enregistrements de facturation hors ligne

Interfaces Réseau

- [Interface S5/S8](#) - Protocole GTP-C, communication SGW-C
- [Gestion de QoS & Porteurs](#) - Application de QoS des porteurs

Opérations

- [Guide de Surveillance](#) - Métriques de session, suivi des sessions actives, alertes
- [Surveillance P-CSCF](#) - Surveillance des sessions IMS

[Retour au Guide des Opérations](#)

Gestion des Sessions OmniPGW · par Omnitouch Network Services



Documentation sur l'allocation de pool IP UE

Gestion des adresses IP pour les appareils mobiles

Table des matières

1. [Aperçu](#)
2. [Concepts d'allocation IP](#)
3. [Configuration](#)
4. [Processus d'allocation](#)
5. [Sujets avancés](#)
6. [Surveillance](#)
7. [Dépannage](#)

Aperçu

Le PGW-C alloue des adresses IP aux appareils UE (User Equipment) lorsqu'ils établissent des connexions PDN (Packet Data Network). C'est une fonction critique qui permet aux appareils mobiles de communiquer avec des réseaux externes.

Pourquoi l'allocation IP est importante

Chaque UE reçoit une **adresse IP unique** du PGW-C qui :

- Identifie l'appareil sur le réseau
- Achemine le trafic vers/depuis l'appareil
- Permet la facturation et l'application des politiques
- Persiste pendant la durée de la connexion PDN

Versions IP prises en charge

Version IP	Support	Description
IPv4	◊ Complet	Adresses IPv4 standard
IPv6	◊ Complet	Adresses et préfixes IPv6
IPv4v6	◊ Complet	Dual-stack (IPv4 et IPv6)

Concepts d'allocation IP

Type de PDN

Lorsqu'un UE demande une connexion PDN, il spécifie un **Type de PDN** :

Type de PDN	Description	Adresses allouées
IPv4	Connexion uniquement IPv4	Adresse IPv4 unique
IPv6	Connexion uniquement IPv6	Préfixe IPv6 (par exemple, /64)
IPv4v6	Connexion dual-stack	Adresse IPv4 et préfixe IPv6

Méthodes d'allocation

Le PGW-C prend en charge deux méthodes d'allocation IP :

1. Allocation dynamique (la plus courante) :

- Le PGW-C sélectionne une IP dans le pool configuré
- Sélection aléatoire pour éviter la prévisibilité
- La détection de collision garantit l'unicité

2. Allocation statique :

- L'UE demande une IP spécifique dans le message GTP-C
- Le PGW-C valide la disponibilité
- Utile pour les appareils d'entreprise avec des IP fixes

Sélection de sous-réseau basée sur l'APN

Differents APN (Access Point Names) peuvent utiliser différents pools IP :

Avantages :

- **Séparation du trafic** - Différents APN acheminent vers différents réseaux
- **Différenciation des politiques** - Appliquer différentes politiques par APN
- **Planification de capacité** - Dimensionner les pools en fonction de l'utilisation prévue
- **Facturation** - Suivre l'utilisation par type de service

Registre d'adresses

Le **Registre d'adresses** suit les IP allouées :

Fonction	Description
Enregistrement	Map UE IP → PID de processus de session
Recherche	Trouver la session par UE IP
Désenregistrement	Libérer l'IP lorsque la session se termine
Détection de collision	Prévenir les allocations en double

Configuration

Configuration de base

Modifier config/runtime.exs :

```
config :pgw_c,
  ue: %{
    subnet_map: %{
      # L'APN "internet" utilise deux sous-réseaux
      "internet" => [
        "100.64.1.0/24",   # 254 IPs utilisables
        "100.64.2.0/24"   # 254 IPs utilisables
      ],
      # L'APN "ims" utilise un sous-réseau
      "ims" => [
        "100.64.10.0/24"
      ],
      # Pool par défaut pour les APN inconnus
      default: [
        "42.42.42.0/24"
      ]
    }
  }
```

Notation de sous-réseau

Notation CIDR : <network>/<prefix_length>

CIDR IPs utilisables	Plage d'exemple
/24 254	100.64.1.1 - 100.64.1.254
/23 510	100.64.0.1 - 100.64.1.254
/22 1022	100.64.0.1 - 100.64.3.254
/20 4094	100.64.0.1 - 100.64.15.254
/16 65534	100.64.0.1 - 100.64.255.254

Remarques :

- L'adresse réseau (par exemple, 100.64.1.0) n'est pas allouée
- L'adresse de diffusion (par exemple, 100.64.1.255) n'est pas allouée

- Le PGW-C alloue de <network> + 1 à <broadcast> - 1

Plusieurs sous-réseaux par APN

Équilibrage de charge entre sous-réseaux :

```
config :pgw_c,
ue: %{
    subnet_map: %{
        "internet" => [
            "100.64.1.0/24",
            "100.64.2.0/24",
            "100.64.3.0/24",
            "100.64.4.0/24"
        ]
    }
}
```

Méthode de sélection :

- Le PGW-C sélectionne aléatoirement un sous-réseau de la liste
- Fournit un équilibrage de charge de base
- Chaque session sélectionne indépendamment un sous-réseau

Avantages :

- Répartir la charge sur plusieurs sous-réseaux
- Expansion de capacité plus facile (ajouter de nouveaux sous-réseaux)
- Flexibilité pour les politiques de routage

Exemple du monde réel

```
config :pgw_c,
ue: %{
    subnet_map: %{
        # Accès général à Internet
        "internet" => [
            "100.64.0.0/20"      # 4094 IPs pour usage général
        ],
        # IMS (Voix sur LTE)
        "ims" => [
            "100.64.16.0/22"    # 1022 IPs pour IMS
        ],
        # APN d'entreprise
        "enterprise.corp" => [
            "10.100.0.0/16"     # 65534 IPs pour l'entreprise
        ],
        # Appareils IoT (débit faible)
        "iot.m2m" => [
            "100.64.20.0/22"    # 1022 IPs pour IoT
        ],
        # Fallback par défaut
        default: [
            "42.42.42.0/24"    # 254 IPs pour les APN inconnus
        ]
    }
}
```

Configuration IPv6

```
config :pgw_c,
ue: %{
    subnet_map: %{
        "internet" => [
            # Pools IPv4
            "100.64.1.0/24"
        ],
        "internet.ipv6" => [
            # Pools IPv6 (délégation de préfixe)
            "2001:db8:1::/48"
        ],
        default: [
            "42.42.42.0/24"
        ]
    }
}
```

Délégation de préfixe IPv6 :

- L'UE reçoit généralement un préfixe /64
- Permet à l'UE d'attribuer plusieurs IP (par exemple, pour le tethering)
- Exemple : L'UE reçoit 2001:db8:1:a::/64

Configuration Dual-Stack (IPv4v6)

```
config :pgw_c,
ue: %{
    subnet_map: %{
        "internet" => [
            "100.64.1.0/24",
            "2001:db8:1::/48"      # Pool IPv6 (sera utilisé pour l'allocation IPv6)
        ]
    }
}
```

Allocation Dual-Stack :

- L'UE demande un Type de PDN : IPv4v6
- Le PGW-C alloue à la fois une adresse IPv4 et un préfixe IPv6
- Les deux adresses sont actives simultanément

Processus d'allocation

L'allocation IP se produit lors de la création de session lorsque le PGW-C reçoit une Demande de création de session via l'interface S5/S8. Voir [Interface S5/S8](#) pour les détails du message GTP-C et [Gestion de session](#) pour le cycle de vie de la session.

Étape par étape : Allocation dynamique IPv4

Comment ça fonctionne

Processus d'allocation dynamique :

1. **Recherche de sous-réseau** : Le système récupère les sous-réseaux configurés pour l'APN demandé
2. **Sélection aléatoire** : Un sous-réseau est sélectionné aléatoirement dans la liste disponible
3. **Génération d'IP** : Une IP aléatoire est générée dans la plage du sous-réseau
4. **Vérification d'unicité** : Le système vérifie que l'IP n'a pas été allouée
5. **Logique de réessaï** : Si une collision est détectée, réessayer jusqu'à 100 fois avec une nouvelle IP aléatoire
6. **Enregistrement** : Une fois une IP unique trouvée, elle est enregistrée pour la session

Points de conception clés :

- **Max 100 tentatives** : Évite les boucles infinies lorsque le pool est presque épuisé
- **Sélection aléatoire** : Évite les modèles d'attribution IP prévisibles pour la sécurité
- **Opérations atomiques** : Le registre basé sur le processus garantit qu'il n'y a pas d'allocations en double
- **Fallback vers le par défaut** : Si l'APN n'est pas trouvé dans la config, utilise le pool par défaut

Gestion des collisions

Scénario : Deux sessions essaient d'allouer la même IP simultanément

Comment la prévention des collisions fonctionne :

- Le registre traite les demandes une à la fois (sérialisé)
- Aucune condition de course possible
- La première demande à enregistrer une IP réussit
- Les demandes suivantes pour la même IP sont rejetées
- Les sessions rejetées réessaient automatiquement avec une nouvelle IP aléatoire

Fallback vers le sous-réseau par défaut

Scénario : L'UE demande un APN inconnu

Configuration d'exemple :

```
# Config
subnet_map: %{
    "Internet" => ["100.64.1.0/24"],
    default: ["42.42.42.0/24"]
}
```

Comportement :

- L'UE demande l'APN : "unknown.apn"
- Le système recherche "unknown.apn" dans subnet_map
- Non trouvé, donc il revient au pool par défaut
- Alloue une IP de 42.42.42.0/24

Logique de fallback :

- D'abord, essayer de trouver le pool spécifique à l'APN dans la configuration
- Si non trouvé, utiliser le pool default
- Si aucun défaut configuré, l'allocation échoue

Désallocation à la fin de la session

Nettoyage automatique :

- Lorsque le processus de session se termine, le registre nettoie
- L'IP est immédiatement disponible pour de nouvelles allocations
- Aucune intervention manuelle requise

Sujets avancés

Épuisement du pool

Scénario : Toutes les IPs dans le pool sont allouées

```
Pool : 100.64.1.0/24 (254 IPs utilisables)
Allouées : 254 IPs
Nouvelle demande arrive → Épuisement
```

Que se passe-t-il :

- Le PGW-C tente 100 allocations aléatoires
- Toutes les tentatives trouvent l'IP déjà allouée
- Retourne : {error, ue_ip_address_allocation_failed}
- L'établissement de session échoue
- Le SGW-C reçoit une réponse d'erreur

Prévention :

```
# Surveiller l'utilisation du pool
address_registry_count / total_pool_size > 0.8 # Alerte à 80%
# Élargir le pool avant épuisement
"internet" => [
    "100.64.1.0/24",
    "100.64.2.0/24", # Ajouter un sous-réseau supplémentaire
    "100.64.3.0/24"
]
```

Allocation IP statique

Cas d'utilisation : L'appareil d'entreprise a besoin d'une IP fixe

Format de message GTP-C :

```
Demande de création de session
└─ IMSI : 310260123456789
└─ APN : enterprise.corp
└─ Allocation d'adresse PDN (IE)
    └─ Type de PDN : IPv4
        └─ Adresse IPv4 : 10.100.0.50 ← L'UE demande une IP spécifique
```

Traitement OmniPGW :

- Extraire l'IP demandée :** Analyser l'IE d'allocation d'adresse PDN de la demande
- Valider l'IP :** Vérifier si l'IP demandée est dans le pool configuré pour cet APN
- Vérifier la disponibilité :** Vérifier que l'IP n'est pas déjà allouée à une autre session
- Allouer ou rejeter :**
 - Si disponible : Allouer l'IP demandée à cette session
 - Si indisponible : Rejeter la session avec le code de cause approprié

Résultats possibles :

- Succès :** L'UE reçoit exactement l'adresse IP qu'elle a demandée
- Échec (IP en cours d'utilisation) :** Session rejettée - IP déjà allouée
- Échec (IP non dans le pool) :** Session rejettée - IP non dans la plage configurée

Délégation de préfixe IPv6

L'UE demande IPv6 :

```
Demande de création de session
└─ Type de PDN : IPv6
```

Le PGW-C alloue un préfixe /64 :

Préfixe alloué : 2001:db8:1:a::/64

L'UE peut utiliser :
- 2001:db8:1:a::1
- 2001:db8:1:a::2
... (18 quintillions d'adresses)

Avantages :

- L'UE peut attribuer plusieurs IP (par exemple, pour le tethering)
- Prend en charge SLAAC (Stateless Address Autoconfiguration)
- Élimine le besoin de NAT

Allocation Dual-Stack

L'UE demande IPv4v6 :

```
Demande de création de session
└─ Type de PDN : IPv4v6
```

Le PGW-C alloue les deux :

```
IPv4 : 100.64.1.42
IPv6 : 2001:db8:1:a::/64
```

Gestion du trafic :

- Le trafic IPv4 utilise l'adresse IPv4
- Le trafic IPv6 utilise le préfixe IPv6
- Les deux actifs simultanément

- Tunnels GTP séparés (ou tunnel dual-stack)

Adresses IP privées vs publiques

Pools IP privées (RFC 1918) :

```
# Non routables sur Internet public
subnet_map: %{
    "internet" => [
        "10.0.0.0/8",
        "172.16.0.0/12",
        "192.168.0.0/16
    ]
}
```

Nécessite NAT au PGW-U pour accéder à Internet

Pools IP publiques :

```
# IP publiques routables (exemple uniquement)
subnet_map: %{
    "internet" => [
        "203.0.113.0/24" # Bloc IP public
    ]
}
```

Aucun NAT requis - routage direct vers Internet

Recommandation :

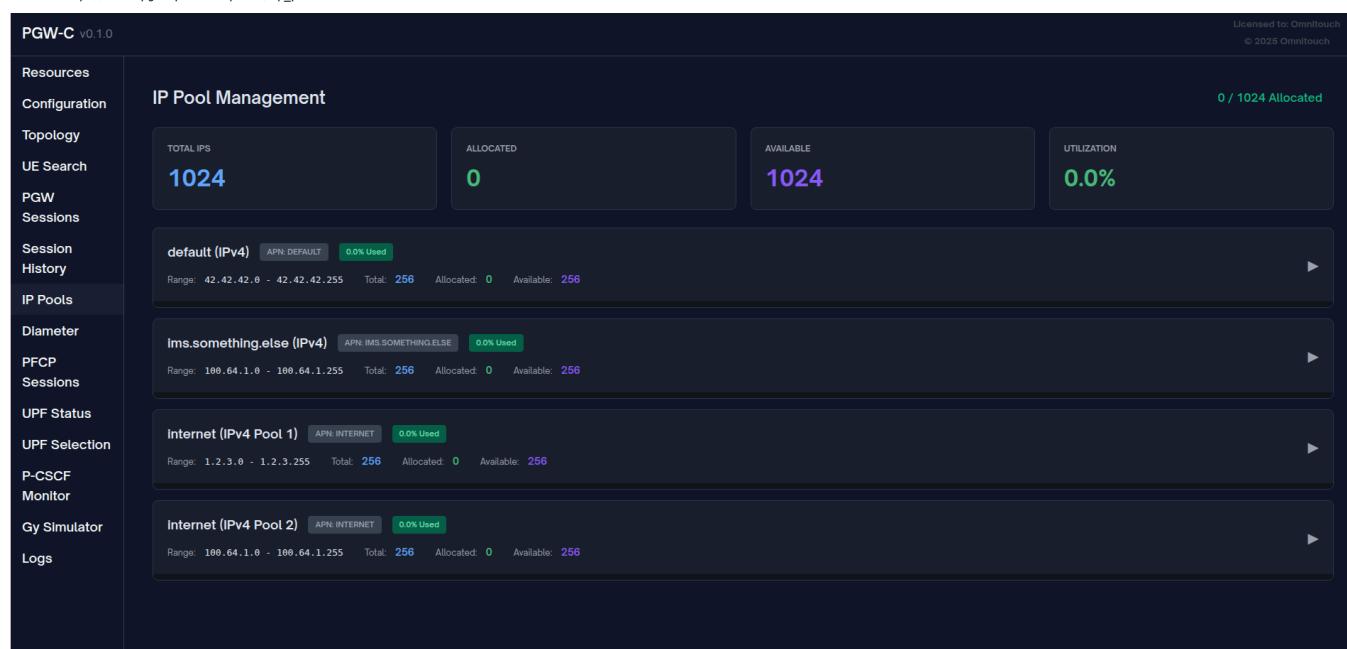
- Utiliser des IP privées (RFC 6598) : 100.64.0.0/10 (NAT de niveau opérateur)
- Réserver des IP publiques uniquement pour des services spéciaux

Surveillance

Interface Web - Gestion du pool IP

OmniPGW fournit une interface web en temps réel pour surveiller l'allocation et l'utilisation du pool IP.

Accès : http://<omnippgw-ip>:<web-port>/ip_pools



Fonctionnalités :

1. Vue d'ensemble du pool

- Total d'IPs dans tous les pools
- Adresses actuellement allouées
- IPs disponibles restantes
- Pourcentage d'utilisation en temps réel

2. Statut du pool par APN

- Chaque pool configuré affiche :
- Nom du pool** - Identifiant APN (par exemple, "default", "ims.something.else", "Internet")
 - Étiquette APN** - Badge du nom APN configuré
 - Plage IP** - Notation CIDR montrant la plage de sous-réseau
 - Utilisation** - Indicateur visuel montrant le pourcentage utilisé
 - Statistiques d'allocation :**
 - Total : Nombre d'IPs dans le pool
 - Allouées : IPs actuellement assignées
 - Disponibles : IPs restantes pour allocation

3. Mises à jour en temps réel

- Auto-rafrâchissement toutes les 2 secondes
- Aucun rechargement de page requis
- Suivi en direct de l'utilisation

Cas d'utilisation :

- Vérification rapide de la capacité avant la maintenance
- Identifier les pools approchant de l'épuisement
- Vérifier la configuration du pool
- Surveiller les modèles d'allocation par APN

Métriques clés

Compte du registre d'adresses :

```
# IPs actuellement allouées
address_registry_count

# Utilisation du pool (nécessite un calcul)
address_registry_count / <total_pool_size> * 100
```

Exemple :

```

Pool : 100.64.1.0/24 (254 IPs)
Allouées : 150 IPs
Utilisation : 150 / 254 = 59%

Alertes

# Alert sur une utilisation élevée du pool
- alert: UEIPpoolUtilizationHigh
  expr: address_registry_count > 200 # Pour le pool /24
  for: 1m
  annotations:
    summary: "Utilisation du pool IP UE au-dessus de 80%"
    description: "Actuel : {{ value }} / 254 IPs allouées"

# Alert sur l'épuisement du pool
- alert: UEIPpoolExhausted
  expr: address_registry_count >= 254 # Pour le pool /24
  for: 1m
  annotations:
    summary: "Pool IP UE épuisé - aucun IP disponible"

# Alert sur les échecs d'allocation
- alert: UEIPAllocationFailures
  expr: rate(ue_ip_allocation_failures_total[5m]) > 0
  for: 5m
  annotations:
    summary: "Échecs d'allocation IP UE en cours"

```

Tableau de bord Grafana

Panneau 1 : Utilisation du pool IP

```
# Jauge montrant le pourcentage
(address_registry_count / 254) * 100
```

Panneau 2 : IPs allouées au fil du temps

```
# Série temporelle
address_registry_count
```

Panneau 3 : Taux d'allocation

```
# Taux de nouvelles allocations
rate(address_registry_count{5m})
```

Panneau 4 : Risque d'épuisement du pool

```
# Jours jusqu'à épuisement (basé sur le taux actuel)
(254 - address_registry_count) / rate(address_registry_count{1h})
```

Dépannage

Problème 1 : Établissement de session échoue (Aucune IP disponible)

Symptômes :

- Réponse de création de session : Cause "Demande rejetée"
- Journal : "Échec de l'allocation d'adresse IP UE"

Causes possibles :

1. Pool épuisé

```
# Vérifier l'allocation actuelle
curl http://<pgw_c_ip>:42069/metrics | grep address_registry_count
```

2. Erreur de configuration

```
# Vérifier la configuration du sous-réseau
config :pgw_c,
  ue: '%
    subnet_map: %{
      "internet" => [
        "100.64.1.0/24" # Assurez-vous que CIDR est valide
      ]
    }
}
```

3. Mauvaise configuration de l'APN

```
# Si l'APN n'est pas trouvé, revient au par défaut
# Assurez-vous que le pool par défaut existe
subnet_map: %{
  default: ["42.42.42.0/24"]
}
```

Résolution :

- **Élargir le pool** : Ajouter plus de sous-réseaux
- **Nettoyer les sessions obsolètes** : Redémarrer le PGW-C pour libérer les IPs perdues
- **Vérifier la config** : Vérifier runtime.exe pour des fautes de frappe

Problème 2 : Collision d'adresse IP

Symptômes :

- Deux UEs reçoivent la même IP (très rare)
- Problèmes de routage

Cause :

- Bug dans le registre d'adresses (ne devrait pas se produire)

Débogage :

```
# Vérifier les IPs en double dans les journaux
grep "already_registered" /var/log/pgw_c.log
```

Résolution :

- Devrait se corriger tout seul (la deuxième session réessaie)
- Si persistant, signaler un bug

Problème 3 : Mauvais pool IP utilisé

Symptômes :

- L'UE reçoit une IP d'un sous-réseau inattendu
- L'APN "internet" obtient une IP du pool "ims"

Cause :

- Configuration incorrecte de subnet_map

Vérifiez :

```
# Vérifier la correspondance exacte de la chaîne APN
subnet_map: %{
  "internet" => [...], # Sensible à la casse
  "Internet" => [...] # APN différent !
}
```

Résolution :

- Assurez-vous que les noms d'APN correspondent exactement (sensible à la casse)
- Utilisez le pool par défaut pour attraper tout

Problème 4 : Échec de l'allocation IPv6

Symptômes :

- L'UE demande IPv6, reçoit une erreur

Causes possibles :

1. Aucun pool IPv6 configuré

```
# Sous-réseaux IPv6 manquants
subnet_map: %{
    "internet" => [
        "100.64.1.0/24" # Seulement IPv4
    ]
}
```

2. Préfixe IPv6 invalide

```
# Préfixe trop petit (devrait être /48 ou plus grand)
"internet" => [
    "2001:db8::/128" # Mauvais - pas de place pour l'allocation
]
```

Résolution :

```
# Ajouter un pool IPv6
subnet_map: %{
    "internet" => [
        "100.64.1.0/24",
        "2001:db8:1::/48" # Pool IPv6
    ]
}
```

Problème 5 : Utilisation élevée du pool

Symptômes :

- Proche de l'épuisement du pool
- address_registry_count approchant le maximum

Mesures proactives :

1. Ajouter des sous-réseaux :

```
"internet" => [
    "100.64.1.0/24", # Existant
    "100.64.2.0/24", # Nouveau sous-réseau (ajoute 254 IPs)
    "100.64.3.0/24" # Nouveau sous-réseau (ajoute 254 IPs)
]
```

2. Utiliser des sous-réseaux plus grands :

```
# Remplacer /24 par /22
"internet" => [
    "100.64.0.0/22" # 1022 IPs utilisables
]
```

3. Nettoyage des sessions :

- Surveiller les sessions obsolètes
- Assurer un traitement correct de la demande de suppression de session

Meilleures pratiques

Planification de capacité

Calculer la taille de pool requise :

```
Utilisateurs concurrents attendus : 10,000
Concurrence de pointe : 30% (3,000 sessions simultanées)
Marge de croissance : 50%
IPs requises : 3,000 * 1.5 = 4,500 IPs

Sous-réseau : /20 (4,094 IPs utilisables) - Trop petit
Sous-réseau : /19 (8,190 IPs utilisables) - Suffisant
```

Sélection de sous-réseau

Recommandé :

- Utiliser 100.64.0.0/10 (RFC 6598 - NAT de niveau opérateur)
- Fournit 4 millions d'IPs
- Réserve pour le NAT des fournisseurs de services

À éviter :

- IPs publiques (coûteuses, limitées)
- Plages privées courantes qui entrent en conflit avec les VPN d'entreprise

Disposition de la configuration

```
config :pgw_c,
ue: %{
    subnet_map: %{
        # APN principal Internet - grand pool
        "internet" => [
            "100.64.0.0/18" # 16,382 IPs
        ],
        # IMS - pool dédié plus petit
        "ims" => [
            "100.64.64.0/22" # 1,022 IPs
        ],
        # Entreprise - pool moyen
        "enterprise.corp" => [
            "100.64.68.0/22" # 1,022 IPs
        ],
        # IoT - grand pool pour de nombreux appareils
        "iot.m2m" => [
            "100.64.72.0/20" # 4,094 IPs
        ],
        # Par défaut - petit fallback
        default: [
            "100.64.127.0/24" # 254 IPs
        ]
    }
}
```

Documentation connexe

Configuration

- [Guide de configuration](#) - Configuration du pool IP UE, mappage de sous-réseau APN
- [Configuration PCO](#) - DNS, PCSCF, MTU livrés avec l'adresse IP
- [Gestion de session](#) - Cycle de vie de la session, allocation IP lors de la configuration PDN
- [Interface PFCP](#) - Attribution d'adresse UE via PFCP au UPF

Planification réseau

- [**Interface S5/S8**](#) - Livraison d'adresse IP via GTP-C
- [**Interface Diameter Gx**](#) - Contrôle des politiques pour l'allocation IP

Opérations

- [**Guide de surveillance**](#) - Métriques d'utilisation du pool IP, suivi des allocations
- [**Format de CDR de données**](#) - Adresses IP UE dans les CDR pour la corrélation de facturation

[Retour au guide des opérations](#)