Guide des opérations OmniCall CSCF

Table des matières

1. Aperçu
2. Comprendre l'architecture IMS
3. Flux de sessions d'appel
4. Composants CSCF
5. Opérations courantes
6. Dépannage
7. Documentation supplémentaire
8. Glossaire

Aperçu

OmniCall CSCF est une solution IMS (IP Multimedia Subsystem) complète qui fournit des fonctions de contrôle de session d'appel de qualité opérateur pour les **fournisseurs de services mobiles et fixes**. Basé sur une technologie open-source éprouvée et enrichi de capacités de gestion de niveau entreprise, OmniCall CSCF offre l'infrastructure de contrôle de session essentielle requise pour VoLTE, VoWiFi, RCS et les services VoIP fixes traditionnels.

Qu'est-ce que l'IMS ?

Le système de sous-système multimédia IP (IMS) est l'architecture normalisée par 3GPP pour la fourniture de services multimédias basés sur IP. Il fournit :

- **Contrôle de session** pour les services vocaux, vidéo et de messagerie
- Gestion de la **Qualité de Service (QoS)** pour les communications en temps réel
- **Convergence des services** à travers les réseaux mobiles, fixes et WiFi
- **Interopérabilité basée sur des normes** avec d'autres opérateurs et réseaux
- Capacités de **Rich Communication Services (RCS)**
- **Convergence fixe-mobile (FMC)** pour une livraison de services unifiée

OmniCall CSCF met en œuvre toutes les fonctions de base du CSCF définies dans 3GPP TS 23.228, fournissant une solution complète de réseau de cœur IMS prête pour la production.

Composants OmniCall CSCF

OmniCall CSCF fournit une gestion complète de tous les éléments du réseau

CSCF :

- **P-CSCF** (Proxy-CSCF) - Proxy de sécurité et de bord orienté utilisateur
- **E-CSCF** (Emergency-CSCF) - Routage des services d'urgence (intégré avec P-CSCF)
- **I-CSCF** (Interrogating-CSCF) - Point d'entrée du réseau et masquage de topologie
- **S-CSCF** (Serving-CSCF) - Contrôle de session central, enregistrement et déclenchement de services

Capacités clés

Fonctions réseau :

- Contrôle de session IMS conforme à 3GPP complet
- **Conforme à GSMA IR.92/IR.94** - Fonctionne avec tout appareil conforme aux normes, aucun bundle opérateur personnalisé requis
- Support VoLTE, VoWiFi et RCS
- Intégration de services SIP fixes
- Support des services d'urgence (E911/E112) avec services de localisation
- Masquage de topologie et sécurité réseau
- Associations de sécurité basées sur IPsec
- Intégration AAA et politique basée sur Diameter

Fonctionnalités de service :

- Gestion de session d'appel en temps réel
- Déclenchement de services via des Critères de Filtre Initiaux (IFC)
- Intégration de Serveur d'Applications (AS) via l'interface ISC
- Intégration de facturation (en ligne et hors ligne)
- Application des politiques QoS via l'intégration PCRF
- Support de multi-location pour les scénarios MVNO

Gestion et opérations :

- Surveillance en temps réel via un panneau de contrôle basé sur le web
- Intégration des métriques Prometheus (voir Référence des métriques)
- API RESTful pour l'automatisation
- Clustering distribué pour haute disponibilité
- Dépannage et diagnostics en direct

Composants intégrés :

- **OmniePDG** : Passerelle de données par paquet évoluée pour VoWiFi (conforme à IR.94)
- **OmniTAS** : Serveur d'applications de téléphonie pour services supplémentaires
- **OmniMessage** : Serveur d'applications SMS/MMS (3GPP TS 24.341)

Pour des détails sur l'utilisation du panneau de contrôle, voir Opérations de l'interface Web.

Comprendre l'architecture IMS

Architecture du réseau IMS

La solution OmniCall CSCF se situe au cœur de l'architecture IMS, fournissant la couche de contrôle de session qui connecte l'équipement utilisateur aux services et gère toutes les sessions d'appel.

Comment les CSCF fonctionnent ensemble

Les fonctions CSCF fonctionnent comme un système coordonné pour gérer les sessions IMS :

1. **P-CSCF** - Premier point de contact
    - L'équipement utilisateur (appareils mobiles, WiFi ou fixes) établit des connexions sécurisées avec P-CSCF
    - Fournit des associations de sécurité IPsec pour les appareils mobiles
    - Agit comme le point d'application de la politique QoS via l'intégration PCRF
    - Gère le passage NAT et l'ancrage des médias
    - Achemine les appels d'urgence vers les fonctionnalités E-CSCF
    - Maintient les informations de localisation de l'utilisateur
2. **I-CSCF** - Passerelle réseau et répartiteur de charge
    - Masque la topologie interne du réseau des réseaux externes
    - Interroge le HSS pour sélectionner le S-CSCF approprié pour les utilisateurs
    - Effectue l'équilibrage de charge S-CSCF en fonction des capacités
    - Agit comme point d'entrée/sortie pour les scénarios de roaming
    - Applique la sécurité du domaine réseau (NDS/TLS)
3. **S-CSCF** - Contrôleur de session central
    - Effectue l'enregistrement et l'authentification des utilisateurs
    - Maintient l'état de session pour tous les appels actifs
    - Applique les politiques de routage et la logique de service
    - Déclenche les serveurs d'applications en fonction de l'IFC (Critères de Filtre Initiaux)
    - S'intègre avec les systèmes de facturation (en ligne et hors ligne)
    - Gère les services supplémentaires

Intégration avec les systèmes de support

OmniCall CSCF s'intègre aux fonctions de support IMS via des interfaces Diameter standard 3GPP :

Interface	De → À	But	Spécification 3GPP
Cx	I-CSCF/S-CSCF ↔ HSS	Authentification utilisateur, récupération de profil, affectation S-CSCF	TS 29.228
Dx	I-CSCF ↔ SLF	Localisateur d'abonnement pour environnements multi-HSS	TS 29.229
Rx	P-CSCF ↔ PCRF	Autorisation de politique QoS, contrôle de flux multimédia	TS 29.214
Ro	S-CSCF → OCS	Facturation en ligne (contrôle de crédit)	TS 32.299
Rf	S-CSCF → CDF	Facturation hors ligne (génération de CDR)	TS 32.299
ISC	S-CSCF ↔ AS	Déclenchement de services et invocation de serveur d'applications	TS 23.228
Sh	AS ↔ HSS	Accès du serveur d'applications aux données utilisateur	TS 29.328

Pour la gestion des pairs Diameter, voir Opérations Diameter.

Flux de sessions d'appel

Comprendre comment les CSCF traitent différents types de sessions est essentiel pour les opérations et le dépannage.

Flux d'enregistrement IMS

Lorsqu'un appareil s'enregistre sur le réseau IMS, les CSCF coordonnent pour authentifier et autoriser l'utilisateur :

Points clés :

- P-CSCF maintient l'association de sécurité IPsec avec l'UE
- I-CSCF interroge le HSS pour trouver/affecter le S-CSCF
- S-CSCF effectue l'authentification et stocke le profil utilisateur
- Le profil de service de l'utilisateur (IFC) détermine quels serveurs d'applications seront déclenchés

Flux d'appel d'origine mobile

Lorsqu'un utilisateur enregistré initie un appel :

Points clés :

- P-CSCF coordonne avec PCRF pour l'établissement du porteur QoS
- S-CSCF évalue l'IFC pour déterminer le déclenchement du service
- **OmniTAS** fournit des services d'application de téléphonie (renvoi d'appel, filtrage, etc.)
- **OmniMessage** gère le trafic SMS/MMS lorsqu'il est déclenché par l'IFC
- Pour surveiller les appels actifs, voir Gestion des dialogues S-CSCF

Flux d'appel d'urgence (E-CSCF)

Les appels d'urgence reçoivent un traitement spécial pour garantir la connectivité même sans enregistrement IMS complet :

Points clés :

- La fonctionnalité E-CSCF est intégrée dans P-CSCF
- Fonctionne même pour les utilisateurs non enregistrés ou en roaming
- Inclut le stockage de numéros de rappel pour les services d'urgence
- Pour les opérations d'urgence, voir Services d'urgence P-CSCF

SMS sur IMS - Origine mobile (3GPP TS 24.341)

Lorsqu'un utilisateur envoie un SMS via IMS, OmniMessage gère la livraison du message :

Points clés :

- SMS encodé dans la méthode SIP MESSAGE selon 3GPP TS 24.341
- Content-Type: `application/vnd.3gpp.sms` identifie la charge utile SMS
- S-CSCF déclenche **OmniMessage** pour le trafic SMS
- OmniMessage s'interface avec l'infrastructure SMSC traditionnelle
- Supporte à la fois les jeux de caractères GSM-7, UCS-2 et les messages concaténés

---

SMS sur IMS - Terminé mobile (3GPP TS 24.341)

Lorsqu'un SMS arrive pour un utilisateur enregistré IMS, OmniMessage le route via IMS :

Points clés :

- SMSC transfère le SMS à **OmniMessage** via des protocoles traditionnels (MAP/SMPP)
- OmniMessage le convertit en méthode SIP MESSAGE
- S-CSCF route en fonction de l'IMPU enregistré
- Supporte les rapports de livraison et les notifications de statut

- Retour à SMS traditionnel si l'utilisateur n'est pas enregistré IMS

Pour les opérations et la surveillance des SMS, voir Gestion IFC S-CSCF.

Scénarios de roaming

OmniCall CSCF prend en charge le **roaming routé par le domicile** tel que mandaté par les normes 3GPP/GSMA :

Roaming Routé par le Domicile : Lorsque les utilisateurs se déplacent vers un réseau visité, toutes les sessions IMS sont routées à travers le S-CSCF du réseau d'origine. Cela garantit :

- Une expérience de service cohérente, quel que soit l'emplacement
- Contrôle du réseau d'origine sur le déclenchement de services et la facturation
- Accords de roaming simplifiés entre opérateurs
- Conformité aux normes GSMA PRD IR.92 et IR.94

Le I-CSCF du réseau visité interroge le HSS d'origine et route les demandes d'enregistrement/session vers le S-CSCF d'origine, qui invoque ensuite les serveurs d'applications du réseau d'origine (OmniTAS, OmniMessage, etc.).

Pour des détails de configuration de roaming, voir Sécurité du domaine réseau I-CSCF.

Composants CSCF

P-CSCF/E-CSCF - Proxy de bord et point d'ancrage de sécurité

Le **Proxy-CSCF** est le premier élément IMS que l'équipement utilisateur contacte. Il sert de frontière de sécurité et de point d'application de politique.

Fonctions principales :

- **Gestion des associations de sécurité** : Établit et maintient des tunnels IPsec avec des appareils mobiles pour la signalisation et la protection des médias
- **Application de la politique QoS** : Coordonne avec PCRF via l'interface Rx pour autoriser et appliquer les porteurs QoS
- **Passage NAT** : Gère le passage NAT à distance pour les appareils derrière des NAT/pare-feu
- **Compression** : Support SigComp pour les réseaux à bande passante limitée
- **Route de service** : Maintient la route de service pour les demandes suivantes

Services d'urgence (E-CSCF) :

- Routage des appels d'urgence intégré sans nécessiter d'enregistrement IMS complet
- Gestion des informations de localisation pour E911/E112
- Mappage IMEI vers numéro de rappel pour les rappels d'urgence
- Intégration avec LRF (Fonction de Récupération de Localisation)

Types d'accès pris en charge :

- LTE/5G (VoLTE) via IPsec
- WiFi (VoWiFi) via IPsec
- Large bande fixe via SIP
- Passerelles résidentielles câble/DSL

Pour des opérations détaillées, voir **Documentation P-CSCF**.

I-CSCF - Masquage de topologie et équilibrage de charge

Le **Interrogating-CSCF** agit comme le point de contact au sein du réseau d'un opérateur pour les connexions provenant d'autres réseaux ou du même réseau.

Fonctions principales :

- **Masquage de topologie** : Protège la structure interne du réseau des réseaux externes
- **Affectation S-CSCF** : Interroge le HSS via l'interface Cx pour affecter un S-CSCF à de nouveaux utilisateurs
- **Sélection S-CSCF** : Sélectionne le S-CSCF approprié en fonction des capacités et de la charge
- **Proxy de routage** : Achemine les demandes entrantes vers le S-CSCF affecté
- **Sécurité du domaine réseau** : Applique NDS/TLS pour la sécurité inter-opérateur

Caractéristiques clés :

- **Support multi-S-CSCF** : Distribue les utilisateurs sur plusieurs instances S-CSCF
- **Correspondance des capacités** : Correspond les exigences des utilisateurs aux capacités S-CSCF
- **Support de roaming** : Gère à la fois les scénarios routés par le domicile et les sorties locales
- **Localisateur d'abonnement** : Support de l'interface Dx pour les environnements multi-HSS

Cas d'utilisation :

- Point d'interconnexion pour les partenaires de roaming
- Distribution de charge à travers le cluster S-CSCF
- Routage géographique pour la récupération après sinistre
- Ségrégation du trafic MVNO

Pour des opérations détaillées, voir **Documentation I-CSCF**.

S-CSCF - Contrôleur de session central

Le **Serving-CSCF** est le composant central du réseau IMS, fournissant le contrôle de session et l'intelligence de service.

Fonctions principales :

- **Enregistrement** : Authentifie les utilisateurs et maintient les liaisons d'enregistrement
- **Contrôle de session** : Gère tous les états d'appel (établissement de dialogue, modification, terminaison)
- **Déclenchement de service** : Évalue les Critères de Filtre Initiaux (IFC) pour invoquer les serveurs d'applications
- **Routage** : Achemine les demandes SIP en fonction de la logique de service et des préférences utilisateur
- **Intégration de facturation** : Coordonne avec les systèmes de facturation en ligne (OCS) et hors ligne (CDF)

Déclenchement de service via IFC : Le S-CSCF utilise des Critères de Filtre Initiaux basés sur XML téléchargés depuis le HSS pour déterminer quand acheminer les appels à travers les serveurs d'applications (comme **OmniTAS** pour les services de téléphonie et **OmniMessage** pour les SMS/MMS) :

- **Points de déclenchement** : Correspondre sur la méthode SIP, Request-URI, Session-Case (originant/terminant)
- **Basé sur la priorité** : IFC traité par ordre de priorité
- **Chaînage de services** : Plusieurs AS peuvent être invoqués en séquence (par exemple, OmniTAS → OmniMessage)
- **Gestion par défaut** : Comportement configurable lorsque l'AS est inaccessible

Services pris en charge :

- Renvoi d'appel (occupé, sans réponse, inconditionnel)
- Interdiction d'appel (sortant, entrant, roaming)
- Filtrage et filtrage d'appels
- Traduction et routage de numéros
- Facturation prépayée/postpayée
- Suivi d'utilisation et application de quotas
- Services supplémentaires (attente d'appel, mise en attente, transfert)

Fonctionnalités de scalabilité :

- Stockage de dialogue distribué
- Gestion d'état de session
- Profils utilisateur basés sur une base de données
- Scalabilité horizontale via distribution I-CSCF

Pour des opérations détaillées, voir **Documentation S-CSCF**.

Gestion de l'interface Diameter

OmniCall CSCF fournit une gestion complète des pairs Diameter à travers tous les composants CSCF.

Applications Diameter prises en charge :

Application	Interface	ID App	Utilisé par	But
3GPP Cx	Cx	16777216	I-CSCF, S-CSCF	Authentification utilisateur, récupération de profil
3GPP Dx	Dx	16777216	I-CSCF	Localisation d'abonnement dans multi-HSS
3GPP Rx	Rx	16777236	P-CSCF	Autorisation de politique, contrôle QoS
3GPP Ro	Ro	4 (CC)	S-CSCF	Facturation en ligne (contrôle de crédit)
3GPP Rf	Rf	3 (Accounting)	S-CSCF	Facturation hors ligne (CDR)
3GPP Sh	Sh	16777217	AS	Accès aux données utilisateur depuis AS

Capacités Diameter :

- Découverte automatique des pairs via DNS
- Support de basculement et de redondance
- Gestion de connexion et de surveillance
- Statistiques et surveillance par pair
- Activation/désactivation dynamique des pairs

Pour les opérations et le dépannage Diameter, voir **Guide de gestion Diameter**.

Opérations courantes

OmniCall CSCF fournit des capacités opérationnelles complètes via son panneau de contrôle basé sur le web. Cette section couvre les tâches opérationnelles courantes et leur signification.

Gestion des enregistrements

Comprendre les enregistrements IMS :

L'enregistrement IMS est un processus en deux étapes :

- **Contact P-CSCF** : L'équipement utilisateur établit une connexion IPsec/SIP avec P-CSCF
- **Enregistrement S-CSCF** : Enregistrement IMS complet avec authentification via HSS

Opérations clés d'enregistrement :

- **Voir les enregistrements actifs** à travers P-CSCF et S-CSCF
- **Interroger des utilisateurs spécifiques** par IMPU, IMSI ou adresse IP
- **Surveiller l'état d'enregistrement** (authentifié, actif, expiré)
- **Forcer la désinscription** pour dépannage ou raisons administratives
- **Suivre l'expiration de l'enregistrement** pour identifier les problèmes de réenregistrement

Pour des procédures d'enregistrement détaillées, voir :

- Gestion des contacts P-CSCF
- Opérations d'enregistrement S-CSCF

Surveillance des sessions d'appel

Gestion des dialogues (sessions) :

Le S-CSCF maintient l'état pour toutes les sessions IMS actives (appels). Les opérateurs peuvent :

- **Surveiller les dialogues actifs** y compris Call-ID, participants et état de session
- **Voir les détails du dialogue** tels que SDP (paramètres multimédias), ensembles de routes et minuteries
- **Terminer des dialogues** pour dépannage ou situations d'urgence
- **Suivre la durée de session** et détecter les sessions longues ou bloquées

États de session :

- **Précoce** : L'appel sonne, pas encore répondu
- **Confirmé** : Appel actif avec flux multimédia
- **Terminé** : Appel terminé normalement

Pour les procédures de surveillance des appels, voir Gestion des dialogues S-CSCF.

Déclenchement de services et gestion des IFC

Les Critères de Filtre Initiaux (IFC) déterminent quand et comment le S-CSCF achemine les sessions vers des serveurs d'applications comme **OmniTAS** et **OmniMessage**.

Opérations IFC :

- **Dump de l'IFC utilisateur** pour voir le profil de service configuré depuis le HSS
- **Tester la correspondance IFC** avec des scénarios d'appel simulés
- **Vérifier le routage AS** pour garantir l'invocation correcte du service
- **Déboguer les échecs de service** en examinant l'évaluation des points de déclenchement

Exemple de structure IFC :

```
<InitialFilterCriteria>
  <Priority>10</Priority>
  <TriggerPoint>
    <SPT><Method>INVITE</Method></SPT>
    <SPT><SessionCase>0</SessionCase><!-- Originating --></SPT>
  </TriggerPoint>
  <ApplicationServer>
    <ServerName>sip:omnitas.ims.example.com</ServerName>
    <DefaultHandling>0</DefaultHandling><!-- Doit invoquer -->
  </ApplicationServer>
</InitialFilterCriteria>
```

Pour les tests et le dépannage IFC, voir Opérations IFC S-CSCF.

Gestion des pairs Diameter

Surveillance de la connectivité Diameter :

OmniCall CSCF s'appuie sur des interfaces Diameter pour l'intégration HSS, PCRF et de facturation. Les opérateurs peuvent :

- **Surveiller l'état des pairs** (I_Open = connecté, Closed = déconnecté)
- **Voir les capacités des pairs** (applications Diameter prises en charge)
- **Activer/désactiver des pairs** pour maintenance ou tests de basculement
- **Suivre les statistiques des pairs** (demandes, échecs, délais d'attente)

Connexions Diameter critiques :

- **Cx vers HSS** (I-CSCF, S-CSCF) : Authentification utilisateur et profils

- **Rx vers PCRF** (P-CSCF) : Politique QoS et contrôle de porteur
- **Ro vers OCS** (S-CSCF) : Facturation en ligne et contrôle de crédit

Pour le dépannage Diameter, voir Guide des opérations Diameter.

Gestion des services d'urgence

Opérations E-CSCF :

Le traitement des appels d'urgence nécessite une attention opérationnelle spéciale :

- **Surveiller les mappages IMEI vers numéro de rappel** pour les rappels d'urgence
- **Vérifier la disponibilité des informations de localisation** pour E911/E112
- **Tester le routage des appels d'urgence** sans connexion PSAP réelle
- **Gérer l'enregistrement d'urgence** pour les appareils non provisionnés

Les services d'urgence fonctionnent même pour :

- Utilisateurs non enregistrés
- Utilisateurs sans SIM/identifiants invalides
- Utilisateurs en roaming d'autres réseaux

Pour les opérations d'urgence, voir Services d'urgence P-CSCF.

Gestion des tables de hachage

Structures de données en mémoire partagée :

Les nœuds CSCF utilisent des tables de hachage en mémoire pour des données critiques en termes de performance :

Table de hachage	CSCF	But	TTL
`imei_msisdn`	P-CSCF	Mappage de rappel d'urgence	24 heures
`service_routes`	P-CSCF	Routes de service mises en cache	Expiration d'enregistrement
`auth`	S-CSCF	Vecteurs d'authentification	Délai d'attente de défi

Opérations :

- **Voir le contenu des tables** pour le dépannage

- **Supprimer des entrées spécifiques** pour effacer des données obsolètes
- **Vider des tables entières** pour la récupération d'urgence (à utiliser avec précaution)

Pour des opérations détaillées de l'interface utilisateur, voir le Guide des opérations de l'interface Web.

Dépannage

Cette section couvre les problèmes opérationnels courants et leurs stratégies de résolution.

Échecs d'enregistrement

Symptômes : Les utilisateurs ne parviennent pas à s'enregistrer sur le réseau IMS, délais d'enregistrement

Causes profondes courantes :

1. **Problèmes de connectivité HSS**
    - Vérifiez l'état du pair Diameter Cx sur I-CSCF et S-CSCF
    - Vérifiez que le HSS est accessible et répond aux demandes UAR/MAR
    - Vérifiez les problèmes de routage Diameter
2. **Échecs d'authentification**
    - Vérifiez que les identifiants utilisateur sont provisionnés dans le HSS
    - Vérifiez la génération de vecteurs d'authentification (MAR/MAA)
    - Vérifiez la compatibilité de l'algorithme AKA (Milenage)
3. **Connectivité P-CSCF**
    - Vérifiez l'établissement de l'AS IPsec pour les appareils mobiles
    - Vérifiez le passage NAT pour les appareils derrière NAT
    - Vérifiez la découverte P-CSCF (DNS, DHCP ou configuration statique)
4. **Affectation S-CSCF**
    - Vérifiez la logique de sélection S-CSCF I-CSCF
    - Vérifiez que les capacités S-CSCF correspondent aux exigences utilisateur
    - Vérifiez la capacité S-CSCF (limites d'enregistrement)

Pour un dépannage détaillé, voir les guides spécifiques aux composants :

- Dépannage P-CSCF
- Dépannage I-CSCF
- Dépannage S-CSCF

Échecs de configuration d'appel

Symptômes : Les appels échouent à s'établir, reçoivent des erreurs SIP 4xx/5xx

Causes profondes courantes :

1. **Utilisateur non enregistré**
    - Vérifiez que les utilisateurs d'origine et de destination sont tous deux enregistrés IMS
    - Vérifiez l'état d'enregistrement via S-CSCF
2. **Problèmes de déclenchement IFC/service**
    - Vérifiez que l'IFC téléchargé depuis le HSS (vérifiez SAR/SAA)
    - Testez la correspondance IFC pour le scénario d'appel
    - Vérifiez la disponibilité d'OmniTAS/OmniMessage si déclenché
3. **Problèmes QoS/PCRF**
    - Vérifiez l'état du pair Diameter Rx sur P-CSCF
    - Vérifiez l'autorisation de politique QoS par le PCRF
    - Vérifiez que les ressources de porteur sont disponibles dans le réseau d'accès
4. **Échecs de routage**
    - Vérifiez le routage de destination (ENUM, traduction de numéro)
    - Vérifiez la configuration d'interconnexion/MGCF pour les appels PSTN
    - Vérifiez le routage de roaming pour les appels hors réseau

---

Problèmes de connectivité Diameter

Symptômes : Le pair Diameter affiche un état "Fermé", les opérations expirent

Étapes de diagnostic :

1. **Vérifiez l'état du pair** : Utilisez le panneau de contrôle pour voir l'état du pair Diameter
2. **Vérifiez la connectivité réseau** : Testez l'accessibilité IP au pair Diameter (port 3868)

3. **Vérifiez les capacités** : Vérifiez que les ID d'application correspondent entre les pairs
4. **Examinez le watchdog** : Vérifiez les échanges de surveillance Diameter (DWR/DWA)

Interfaces Diameter critiques :

Interface	Impact si hors service	Priorité de récupération
Cx (HSS)	Pas de nouveaux enregistrements, pas de mises à jour IFC	Critique - immédiat
Rx (PCRF)	Pas de QoS pour les nouveaux appels	Élevée - dans les minutes
Ro (OCS)	Pas de facturation prépayée, le service peut continuer	Élevée - dépend de la politique

Pour le dépannage Diameter, voir Guide des opérations Diameter.

Problèmes de livraison SMS

Symptômes : SMS non livrés via IMS, retour à SMSC hérité

Causes profondes courantes :

1. **OmniMessage non déclenché**
    - Vérifiez que l'IFC est configuré pour déclencher OmniMessage pour les demandes MESSAGE
    - Vérifiez la priorité de l'IFC (doit être plus élevée que d'autres AS)
    - Testez la correspondance IFC avec un SMS simulé
2. **Intégration SMSC**
    - Vérifiez la connectivité d'OmniMessage à la SMSC (MAP/SMPP)
    - Vérifiez la conversion de format de message (SIP MESSAGE ↔ SMS PDU)
    - Vérifiez le routage des abonnés dans la SMSC
3. **Problèmes de type de contenu**
    - Vérifiez `Content-Type: application/vnd.3gpp.sms` dans SIP MESSAGE
    - Vérifiez l'encodage des jeux de caractères (GSM-7, UCS-2)

Pour le dépannage SMS, voir Gestion IFC S-CSCF.

Problèmes d'appel d'urgence

Symptômes : Les appels d'urgence ne sont pas routés vers PSAP, localisation non incluse

Causes profondes courantes :

1. **Détection E-CSCF**
    - Vérifiez la détection de l'URN d'urgence (urn:service:sos)
    - Vérifiez les règles de routage d'urgence sur P-CSCF
    - Vérifiez la connectivité LRF
2. **Informations de localisation**
    - Vérifiez l'en-tête de localisation dans SIP INVITE
    - Vérifiez le mappage IMEI vers numéro de rappel pour les rappels
    - Testez la récupération de localisation depuis LRF
3. **Routage PSAP**
    - Vérifiez la configuration de la table de routage PSAP
    - Vérifiez la génération de ESQK (Clé de Requête de Service d'Urgence)
    - Vérifiez la connexion/tronçon vers PSAP

Pour les opérations de services d'urgence, voir Services d'urgence P-CSCF.

Dégradation des performances

Symptômes : Configuration d'appel lente, délais d'enregistrement, latence élevée

Diagnostic :

1. **Surveillez les métriques Prometheus** : Vérifiez les métriques de performance CSCF (voir Référence des métriques pour des définitions complètes des métriques)
2. **Performance de la base de données** : Vérifiez les temps de requête de la base de données S-CSCF
3. **Latence réseau** : Vérifiez la latence entre les nœuds CSCF
4. **Utilisation des ressources** : Surveillez le CPU, la mémoire et le réseau sur les serveurs CSCF

Considérations de scalabilité :

- **P-CSCF** : ~50 000 SAs IPsec par instance (VoLTE) ; 100 000+ via OmniePDG (VoWiFi)

- **I-CSCF** : Stateless, évolue horizontalement (1 000-5 000 enregistrements/sec par instance)
- **S-CSCF** : 100 000-500 000 enregistrements par instance ; 20 000-100 000 dialogues simultanés

Pour une planification de capacité détaillée et un dimensionnement de déploiement, voir le **Guide de capacité et de dimensionnement**.

Pour la surveillance des performances et des métriques, voir le Guide des opérations de l'interface Web.

Documentation supplémentaire

Guides d'opérations spécifiques aux composants

Pour des opérations détaillées et un dépannage pour chaque composant CSCF :

- **Guide des opérations P-CSCF/E-CSCF** - Proxy de bord, associations de sécurité, services d'urgence
- **Guide des opérations I-CSCF** - Sélection S-CSCF, masquage de topologie, roaming
- **Guide des opérations S-CSCF** - Enregistrement, gestion des dialogues, opérations IFC
- **Guide des opérations Diameter** - Gestion et dépannage des pairs Diameter
- **Guide des opérations de l'interface Web** - Utilisation du panneau de contrôle, surveillance et administration
- **Référence des métriques** - Référence complète de toutes les métriques Prometheus P-CSCF, I-CSCF et S-CSCF
- **Guide de capacité et de dimensionnement** - Dimensionnement de déploiement, planification de capacité, optimisation des performances

Conformité réglementaire

- **Conformité à l'interception ANSSI R226** - Capacités d'interception légale requises par les autorités réglementaires françaises

Référence des normes 3GPP

OmniCall CSCF met en œuvre les spécifications 3GPP suivantes :

Spécification	Titre	Pertinence
TS 23.228	Système de sous-système multimédia IP (IMS) - Étape 2	Architecture IMS de base
TS 24.229	Protocole de contrôle d'appel multimédia IP (SIP)	Profil SIP IMS
TS 29.228	Interfaces Cx et Dx (CSCF-HSS)	Données utilisateur et

Spécification	Titre	Pertinence
		authentification
TS 29.214	Interface Rx (P-CSCF-PCRF)	Contrôle de politique QoS
TS 32.299	Facturation - Applications Diameter	Facturation en ligne/hors ligne
TS 24.341	SMS sur réseaux IP	SMS sur IMS
TS 23.167	Services d'urgence	E-CSCF et appels d'urgence

Conformité aux normes GSMA

OmniCall CSCF est entièrement conforme aux profils IMS de GSMA, garantissant l'interopérabilité avec des appareils prêts à l'emploi :

IR.92 - Profil IMS pour la voix et les SMS (VoLTE)

GSMA PRD IR.92 définit le profil IMS obligatoire pour les services VoLTE, garantissant que les appareils commerciaux fonctionnent sans configuration spécifique à l'opérateur ou bundles d'appareils personnalisés.

Avantages clés d'IR.92 pour OmniCall CSCF :

✓ **Support des appareils du marché ouvert** : Tout smartphone conforme à IR.92 fonctionne immédiatement - aucun bundle d'opérateur personnalisé, APN propriétaire ou provisionnement spécial requis

✓ **Profil SIP standardisé** : Les appareils utilisent des en-têtes SIP standard, l'authentification et les flux d'enregistrement tels que définis dans 3GPP TS 24.229

✓ **Interopérabilité des codecs** : Le support des codecs obligatoires (AMR-WB pour la voix HD) garantit une qualité vocale cohérente sur tous les appareils

✓ **SMS sur IMS** : L'intégration avec **OmniMessage** fournit une livraison SMS conforme aux normes (TS 24.341) à tout appareil conforme à IR.92

✓ **Services d'urgence** : La gestion des numéros d'urgence E.164 (911, 112, etc.) fonctionne sur tous les appareils conformes sans configuration spéciale

✓ **Cohérence en roaming** : Le roaming routé par le domicile garantit que les utilisateurs bénéficient de la même expérience VoLTE lorsqu'ils visitent d'autres réseaux conformes à IR.92

Ce que cela signifie : Les opérateurs peuvent lancer des services VoLTE immédiatement avec des appareils consommateurs existants (iPhone, Samsung, Google Pixel, etc.) sans attendre la certification personnalisée des appareils ou des mises à jour de bundles d'opérateurs.

IR.94 - Profil IMS pour la voix, la vidéo et les SMS (VoWiFi)

GSMA PRD IR.94 étend IR.92 pour inclure la voix sur WiFi, permettant des services VoLTE sur des réseaux WiFi non fiables.

Architecture VoWiFi avec OmniCall :

Composants VoWiFi :

- **OmniePDG** : Passerelle de données par paquet évoluée - Fournit la terminaison de tunnel IPsec pour l'accès WiFi non fiable
- **OmniCall P-CSCF** : Gère les enregistrements VoWiFi de la même manière que VoLTE (mêmes routes de service, même déclenchement IFC)
- **Handover transparent** : Les appareils peuvent passer entre LTE et WiFi sans interruption d'appel

Avantages d'IR.94 :

- Les mêmes avantages IR.92 s'appliquent à VoWiFi
- Les appareils découvrent automatiquement ePDG via DNS (pas de configuration manuelle)
- Un enregistrement IMS unique couvre à la fois VoLTE et VoWiFi
- Extension de couverture intérieure sans femtocells ou DAS

Pour les opérations ePDG et le dépannage VoWiFi, voir **Documentation OmniePDG**.

Autres normes GSMA

- **IR.51** - Structure de base de données de roaming GSMA
- **IR.88** - Directives de roaming LTE
- **AA.80** - Configuration des appareils IMS/RCS et services de support

Différenciation du produit

Pourquoi choisir OmniCall CSCF ?

✓ **Support des appareils Plug-and-Play** : Conforme à GSMA IR.92/IR.94 - fonctionne avec des iPhones, des téléphones Android et des appareils fixes prêts à l'emploi sans bundles d'opérateur personnalisés ou retards de certification d'appareil

✓ **Solution IMS complète** : Tous les composants CSCF (P/I/S/E) plus OmniePDG pour VoWiFi dans une plateforme unifiée

✓ **Convergence fixe-mobile** : Noyau IMS unifié pour les services mobiles (VoLTE/VoWiFi), la large bande fixe et les services de téléphonie par câble

✓ **Provisionnement sans contact** : La découverte des appareils basée sur des normes (DNS, DHCP) signifie que les utilisateurs peuvent échanger des cartes SIM entre les appareils sans support informatique

✓ **Gestion d'entreprise** : Panneau de contrôle basé sur le web avec surveillance en temps réel, diagnostics et dépannage

✓ **Scalabilité de qualité opérateur** : Scalabilité horizontale pour prendre en charge des millions d'abonnés avec des temps de configuration d'appel inférieurs à une seconde

✓ **Écosystème de serveurs d'applications** : Intégration transparente avec OmniTAS (services de téléphonie) et OmniMessage (SMS/MMS)

✓ **Services d'urgence** : E-CSCF intégré avec support E911/E112, services de localisation et gestion des rappels

✓ **Interopérabilité d'abord** : Conformité complète aux normes 3GPP et GSMA garantissant que les accords de roaming et l'interconnexion fonctionnent dès le départ

✓ **Production éprouvée** : Déployé dans des réseaux de niveau 1, de niveau 2 et MVNO dans le monde entier, servant des millions d'abonnés

Glossaire

Termes de l'architecture IMS

- **3GPP** : 3rd Generation Partnership Project - Organisme de normalisation pour les télécommunications mobiles
- **AKA** : Authentication and Key Agreement - Mécanisme de sécurité pour l'IMS
- **AoR** : Address of Record - Identité SIP (par exemple, sip:user@domain.com)
- **CSCF** : Call Session Control Function - Entité de contrôle de session IMS
- **DAS** : Distributed Antenna System - Solution de couverture intérieure
- **E-CSCF** : Emergency CSCF - Fonction de routage des appels d'urgence
- **ePDG** : Evolved Packet Data Gateway - Point de terminaison de tunnel IPsec pour l'accès WiFi non fiable
- **ENUM** : E.164 Number Mapping - Traduction de numéro basée sur DNS
- **ESQK** : Emergency Service Query Key - Identifiant d'appel d'urgence
- **FMC** : Fixed-Mobile Convergence - Services unifiés à travers les types d'accès
- **GSMA** : GSM Association - Organisation de normalisation de l'industrie mobile
- **HD Voice** : High Definition Voice - Audio large bande utilisant le codec AMR-WB
- **HSS** : Home Subscriber Server - Base de données des abonnés et

authentification
- **I-CSCF** : Interrogating CSCF - Point d'entrée du réseau et masquage de topologie
- **IFC** : Initial Filter Criteria - Règles de déclenchement de service basées sur XML
- **IMS** : IP Multimedia Subsystem - Architecture 3GPP pour les services basés sur IP
- **IMPU** : IP Multimedia Public Identity - Identité publique de l'utilisateur (URI SIP ou URI tel)
- **IMSI** : International Mobile Subscriber Identity - Identifiant d'abonné
- **IR.92** : GSMA IMS Profile for Voice and SMS - Norme d'interopérabilité VoLTE
- **IR.94** : GSMA IMS Profile for Conversational Video - Norme d'interopérabilité VoWiFi
- **ISC** : IMS Service Control - Interface entre S-CSCF et Serveurs d'Applications
- **LRF** : Location Retrieval Function - Services de localisation d'urgence
- **MGCF** : Media Gateway Control Function - Interconnexion PSTN
- **MVNO** : Mobile Virtual Network Operator - Opérateur sans infrastructure radio propre
- **NDS** : Network Domain Security - Sécurité inter-opérateur (TLS/IPsec)
- **P-CSCF** : Proxy CSCF - Proxy de bord et premier point de contact
- **PSAP** : Public Safety Answering Point - Centre d'appels des services d'urgence
- **RCS** : Rich Communication Services - Services de messagerie améliorés
- **S-CSCF** : Serving CSCF - Contrôle de session central et enregistrement
- **SPT** : Service Point Trigger - Condition de correspondance dans l'IFC (Méthode, Request-URI, etc.)
- **SWu** : Interface 3GPP entre UE et ePDG (IPsec/IKEv2)
- **UE** : User Equipment - Appareil de l'utilisateur final (téléphone, tablette, terminal fixe)
- **VoLTE** : Voice over LTE - Services vocaux via le réseau de données LTE
- **VoWiFi** : Voice over WiFi - Services vocaux via des réseaux WiFi non fiables

Termes du protocole Diameter

- **AAA** : Authentication, Authorization, Accounting
- **AVP** : Attribute-Value Pair - Élément de données du message Diameter
- **CCR/CCA** : Credit-Control-Request/Answer - Messages de facturation en ligne
- **CDF** : Charging Data Function - Collecteur de facturation hors ligne
- **Cx** : Interface Diameter entre I-CSCF/S-CSCF et HSS
- **Diameter** : Protocole AAA utilisé dans l'IMS (évolution de RADIUS)
- **Dx** : Interface Diameter entre I-CSCF et SLF (localisateur d'abonnement)
- **DWR/DWA** : Device-Watchdog-Request/Answer - Vérification de l'état du pair
- **MAR/MAA** : Multimedia-Auth-Request/Answer - Demande de vecteur d'authentification

- **OCS** : Online Charging System - Facturation et contrôle de crédit en temps réel
- **PCRF** : Policy and Charging Rules Function - Serveur de politique QoS
- **Rf** : Interface Diameter pour la facturation hors ligne (comptabilité)
- **Ro** : Interface Diameter pour la facturation en ligne (contrôle de crédit)
- **Rx** : Interface Diameter entre P-CSCF et PCRF (autorisation QoS)
- **SAR/SAA** : Server-Assignment-Request/Answer - Téléchargement de profil utilisateur
- **Sh** : Interface Diameter entre AS et HSS (accès aux données utilisateur)
- **SLF** : Subscription Locator Function - Localisateur HSS dans un environnement multi-HSS
- **UAR/UAA** : User-Authorization-Request/Answer - Sélection S-CSCF

Termes de produit OmniCall

- **OmniCall CSCF** : Solution complète CSCF IMS (ce produit)
- **OmniePDG** : Passerelle de données par paquet évoluée - Terminaison de tunnel IPsec pour VoWiFi (conforme à IR.94)
- **OmniTAS** : Serveur d'applications de téléphonie - Fournit des services de téléphonie supplémentaires
- **OmniMessage** : Serveur d'applications de messagerie - SMS/MMS sur IMS (TS 24.341)

Termes du protocole SIP

- **Dialogue** : État de session SIP entre deux points de terminaison
- **INVITE** : Méthode SIP pour l'établissement de session (appels)
- **MESSAGE** : Méthode SIP pour la messagerie instantanée (y compris SMS sur IMS)
- **REGISTER** : Méthode SIP pour l'enregistrement utilisateur
- **SDP** : Session Description Protocol - Paramètres multimédias (codecs, ports)
- **SIP** : Session Initiation Protocol - Protocole de signalisation pour l'IMS

Guide des opérations Diameter

Table des matières

1. Aperçu
2. Diameter dans l'architecture IMS
3. Interfaces Diameter
4. Gestion des pairs via l'interface Web
5. Codes de résultat Diameter
6. Problèmes courants

Aperçu

Diameter est le protocole d'authentification, d'autorisation et de comptabilité (AAA) utilisé dans toute l'architecture IMS. OmniCall CSCF utilise Diameter pour communiquer avec des éléments réseau critiques, y compris HSS, PCRF et OCS.

Qu'est-ce que Diameter ?

Diameter (RFC 6733) est le successeur de RADIUS, conçu pour des scénarios AAA modernes :

- **Transport fiable** via TCP/SCTP (vs. UDP dans RADIUS)
- **Extensible** via des modules spécifiques à l'application
- **Architecture pair à pair** (pas seulement client-serveur)
- **Connexions avec état** avec surveillance de type watchdog
- **Gestion des erreurs** et codes de résultat **normalisés**

Diameter dans CSCF

Chaque composant CSCF utilise des interfaces d'application Diameter spécifiques :

CSCF	Interface	ID d'application	Connecté à	Objectif
I-CSCF	Cx	16777216	HSS	Sélection S-CSCF, localisation utilisateur
S-CSCF	Cx	16777216	HSS	Authentification utilisateur, téléchargement de profil
S-CSCF	Sh	16777217	HSS	Accès aux données utilisateur (optionnel)
P-	Rx	16777236	PCRF	Politique QoS et contrôle de bearer

CSCF	Interface	ID d'application	Connecté à	Objectif
S-CSCF	Ro	4	OCS	Chargement en ligne (contrôle de crédit)
S-CSCF	Rf	3	CDF	Chargement hors ligne (comptabilité)

Diameter dans l'architecture IMS

Aperçu du réseau

Interfaces Diameter

Interface Cx (CSCF ↔ HSS)

L'interface Cx est utilisée par I-CSCF et S-CSCF pour l'authentification des utilisateurs et la gestion des profils.

Spécification 3GPP : TS 29.228

Opérations I-CSCF

Demande d'autorisation utilisateur (UAR) / Réponse d'autorisation utilisateur (UAA) :

- **Objectif** : Interroger HSS pour l'attribution ou les capacités S-CSCF
- **Déclencheur** : REGISTRATION reçue de l'utilisateur
- **Cas d'utilisation** : I-CSCF doit acheminer l'enregistrement vers le S-CSCF approprié

Demande d'informations de localisation (LIR) / Réponse d'informations de localisation (LIA) :

- **Objectif** : Interroger HSS pour le S-CSCF actuel de l'utilisateur
- **Déclencheur** : INVITE ou MESSAGE reçu pour l'utilisateur terminant
- **Cas d'utilisation** : I-CSCF doit acheminer la session vers le S-CSCF de l'utilisateur

Opérations S-CSCF

Demande d'authentification multimédia (MAR) / Réponse d'authentification multimédia (MAA) :

- **Objectif** : Récupérer les vecteurs d'authentification depuis HSS
- **Déclencheur** : REGISTRATION initiale (avant défi)

- **Cas d'utilisation** : S-CSCF doit défier l'utilisateur pour l'authentification IMS AKA

Demande d'attribution de serveur (SAR) / Réponse d'attribution de serveur (SAA) :

- **Objectif** : Informer HSS de l'état d'enregistrement, télécharger le profil utilisateur
- **Déclencheur** : Authentification réussie (après MAR/MAA)
- **Cas d'utilisation** : S-CSCF télécharge l'IFC et le profil de service pour l'utilisateur

L'AVP `User-Data` dans SAA contient le profil utilisateur complet, y compris :

- Identités publiques
- Critères de filtre initiaux (IFC) pour le déclenchement de services
- Identifiants de profils multimédias souscrits
- Informations de facturation

Demande de terminaison d'enregistrement (RTR) / Réponse de terminaison d'enregistrement (RTA) :

- **Objectif** : Désenregistrement initié par HSS (poussé par HSS)
- **Déclencheur** : Désenregistrement administratif, changement d'abonnement
- **Cas d'utilisation** : HSS demande à S-CSCF de désenregistrer un utilisateur

Interface Rx (P-CSCF ↔ PCRF)

L'interface Rx fournit le contrôle de politique et de QoS pour les sessions IMS.

Spécification 3GPP : TS 29.214

Demande AA (AAR) / Réponse AA (AAA) :

- **Objectif** : Demander l'autorisation QoS pour la session multimédia
- **Déclencheur** : Échange d'offre/réponse SDP dans SIP INVITE
- **Cas d'utilisation** : P-CSCF demande à PCRF d'autoriser les ressources de bearer

Demande de ré-authentification (RAR) / Réponse de ré-authentification (RAA) :

- **Objectif** : Mise à jour de politique initiée par PCRF (poussé par PCRF)
- **Déclencheur** : Changement de politique, modification de bearer
- **Cas d'utilisation** : PCRF demande à P-CSCF de mettre à jour la politique QoS

Demande de terminaison de session (STR) / Réponse de terminaison de session (STA) :

- **Objectif** : Libérer la session Rx et les ressources de bearer
- **Déclencheur** : Terminaison d'appel (BYE reçu)
- **Cas d'utilisation** : P-CSCF informe PCRF de libérer les ressources QoS

Interface Ro (S-CSCF ↔ OCS)

L'interface Ro fournit le chargement en ligne (contrôle de crédit).

Spécification 3GPP : TS 32.299

Demande de contrôle de crédit (CCR) / Réponse de contrôle de crédit (CCA) :

- **Objectif** : Autorisation et débit de crédit en temps réel
- **Déclencheur** : Établissement d'appel, en cours d'appel, terminaison d'appel
- **Cas d'utilisation** : Chargement prépayé, vérifications de crédit en temps réel

Types :

- **CCR-Initial** : Demander du crédit au début de l'appel
- **CCR-Update** : Rafraîchir le quota pendant l'appel
- **CCR-Terminate** : Rapporter l'utilisation finale à la fin de l'appel

Gestion des pairs via l'interface Web

OmniCall CSCF fournit un panneau de contrôle basé sur le Web pour la gestion des pairs Diameter.

Accès : Accédez à l'onglet **Diameter** dans le panneau de contrôle (`http://<cscf-server>:4000/diameter`)

Affichage de l'état des pairs

La page de gestion Diameter affiche :

Informations résumées

- **Royaume** : Royaume Diameter
- **Identité** : Hôte d'origine Diameter
- **Nombre de pairs** : Nombre de pairs configurés
- **Travailleurs** : Nombre de travailleurs CDP
- **Longueur de la file d'attente** : Transactions en attente

- **Délai de connexion** : Délai de connexion (secondes)
- **Délai de transaction** : Délai de transaction (secondes)
- **Accepter les pairs inconnus** : Drapeau de politique

Liste des pairs

Table de tous les pairs Diameter avec les colonnes suivantes :

Colonne	Description
FQDN	Nom de domaine complètement qualifié du pair
État	État de la connexion (I_Open, Closed, etc.)
Statut	Activé ou Désactivé
Dernière utilisation	Temps écoulé depuis la dernière transaction
Applications	Nombre d'applications Diameter prises en charge

Opérations sur les pairs

Activer le pair :

1. Localisez le pair désactivé dans le tableau
2. Cliquez sur le bouton **Activer**
3. Le pair tentera d'établir une connexion

Désactiver le pair :

1. Localisez le pair activé dans le tableau
2. Cliquez sur le bouton **Désactiver**
3. Confirmez l'action
4. La connexion du pair sera terminée gracieusement

Voir les applications :

1. Cliquez sur la ligne du pair pour l'étendre
2. Voir la liste des applications Diameter prises en charge avec les noms d'interface

La vue étendue du pair montre toutes les applications Diameter prises en charge :

- **16777216:10415** - 3GPP Cx/Dx (communication HSS pour I-CSCF/S-CSCF)
- **16777236:10415** - 3GPP Rx (politique QoS PCRF pour P-CSCF)
- **16777238:0** - 3GPP Ro (Chargement en ligne)
- Autres ID d'application et ID de fournisseur pris en charge

Le panneau de contrôle mappe automatiquement les ID d'application Diameter aux noms d'interface 3GPP :

- **Cx/Dx** (16777216:10415)
- **Sh/Dh** (16777217:10415)
- **Rx** (16777236:10415)
- **Ro** (16777238:10415/0/5535/13019)
- **Gx** (16777224:10415)
- **S6a/S6d** (16777251:10415)
- Et bien d'autres (voir `diameter_live.ex` pour la liste complète)

États des pairs

État	Description
I_Open	Connexion ouverte et opérationnelle
Closed	Aucune connexion établie
Wait-Conn-Ack	Connexion initiée, en attente de réponse
Wait-I-CEA	CER envoyé, en attente de CEA

Pour une gestion détaillée des pairs : Voir Guide des opérations de l'interface Web

Codes de résultat Diameter

Codes de résultat courants et leurs significations :

Code	Nom	Signification	Action
2xxx	**Succès**		
2001	DIAMETER_SUCCESS	Opération réussie	Aucun
3xxx	**Erreurs de protocole**		
3002	DIAMETER_UNABLE_TO_DELIVER	Impossible de router vers la destination	Vérifiez la connectivité du pair
3003	DIAMETER_REALM_NOT_SERVED	Royaume non reconnu	Vérifiez la configuration du royaume
3007	DIAMETER_APPLICATION_UNSUPPORTED	Application non prise en charge	Vérifiez l'ID d'application
4xxx	**Échecs transitoires**		
4001	DIAMETER_AUTHENTICATION_REJECTED	Auth échoué	Vérifiez les identifiants
4010	DIAMETER_USER_UNKNOWN	Utilisateur non provisionné	Vérifiez le provisionnement HSS
5xxx	**Échecs permanents**		
5001	DIAMETER_AVP_UNSUPPORTED	AVP non reconnu	Vérifiez la version du

Code	Nom	Signification	Action
			protocole
5002	DIAMETER_UNKNOWN_SESSION_ID	Session non trouvée	Session expirée ou invalide
5003	DIAMETER_AUTHORIZATION_REJECTED	Non autorisé	Vérifiez les permissions de l'utilisateur
5012	DIAMETER_UNABLE_TO_COMPLY	Impossible de traiter la demande	Vérifiez les journaux HSS/ PCRF/OCS

Problèmes courants

Échecs de connexion des pairs

Symptôme : Pair bloqué dans l'état "Closed" ou "Wait-Conn-Ack"

Diagnostic :

1. Vérifiez la connectivité réseau :

   ```
   ping <peer-fqdn>
   telnet <peer-fqdn> 3868
   ```

2. Vérifiez les règles de pare-feu (le port 3868 TCP doit être ouvert)
3. Vérifiez la configuration du pair (adresse IP, port)
4. Vérifiez les journaux du pair pour les tentatives de connexion

Résolution :

- Corrigez les problèmes réseau/pare-feu
- Vérifiez que le pair fonctionne et écoute sur le port 3868
- Vérifiez si le pair a la configuration correcte pour CSCF
- Utilisez **Activer le pair** dans l'interface Web pour réessayer la connexion

---

Échecs d'échange CER/CEA

Symptôme : Pair bloqué dans l'état "Wait-I-CEA", ou CEA avec code d'erreur

Erreurs courantes :

- **5010 (NO_COMMON_APPLICATION)** : Vérifiez que les deux pairs prennent en charge la même application (par exemple, Cx = 16777216)
- **3003 (REALM_NOT_SERVED)** : Vérifiez que l'Origin-Realm correspond au royaume attendu par le pair

Résolution :

- Vérifiez la configuration Diameter pour l'ID d'application et le royaume
- Assurez-vous que la configuration du pair correspond aux attentes de CSCF
- Consultez les journaux de backend CSCF pour des messages d'erreur détaillés

---

Problèmes d'interface Cx HSS

Symptôme : Échecs d'enregistrement, délais d'attente MAR/MAA

Erreurs courantes :

Code de résultat	Signification	Résolution
4010	USER_UNKNOWN	Utilisateur non provisionné dans HSS
4001	AUTHENTICATION_REJECTED	IMPI/identifiants incorrects
5012	UNABLE_TO_COMPLY	Erreur interne HSS, vérifiez les journaux HSS

Résolution :

- **USER_UNKNOWN** : Provisionnez l'utilisateur dans HSS
- **AUTHENTICATION_REJECTED** : Vérifiez l'IMPI et le secret partagé dans HSS
- **UNABLE_TO_COMPLY** : Vérifiez les journaux HSS et la connectivité de la base de données

---

Problèmes d'interface Rx PCRF

Symptôme : Les appels réussissent mais aucune QoS appliquée, délais d'attente AAR/AAA

Problèmes courants :

- **PCRF hors service** : Vérifiez l'état du pair dans l'interface Web
- **Framed-IP-Address non reconnu** : PCRF ne peut pas mapper l'IP UE à l'abonné
- **Politique non appliquée** : Vérifiez les règles de politique PCRF, vérifiez l'intégration PCEF

Résolution :

- Vérifiez que le pair PCRF est dans l'état "I_Open"
- Vérifiez le provisionnement de l'adresse IP UE dans PCRF

- Vérifiez que l'interface Gx (PCRF à PCEF) fonctionne

Problèmes d'interface Ro OCS

Symptôme : Les appels prépayés échouent, délais d'attente CCR/CCA, appels bloqués

Erreurs courantes :

Code de résultat	Signification	Résolution
4012	CREDIT_LIMIT_REACHED	Crédit insuffisant
5003	AUTHORIZATION_REJECTED	Utilisateur non autorisé pour le prépayé

Résolution :

- **CREDIT_LIMIT_REACHED** : Normal pour les utilisateurs prépayés sans crédit
- **Délai d'attente OCS** : Vérifiez la disponibilité de l'OCS et l'état du pair
- **AUTHORIZATION_REJECTED** : Vérifiez que l'utilisateur est provisionné pour le prépayé dans OCS

Dégradation des performances

Symptôme : Temps de réponse Diameter lents, latence élevée

Diagnostic :

1. Vérifiez l'horodatage "Dernière utilisation" dans la liste des pairs (doit être récent)
2. Surveillez la "Longueur de la file d'attente" (valeurs élevées indiquent un arriéré)
3. Consultez les journaux de backend CSCF pour des avertissements de délai d'attente

Résolution :

- **Latence élevée** : Enquêtez sur le réseau entre CSCF et le pair
- **Longueur de file d'attente élevée** : Vérifiez la charge système du pair (HSS/PCRF/OCS)
- **Délais d'attente** : Augmentez le délai de transaction si le réseau a une latence élevée

Meilleures pratiques

Directives opérationnelles

Gestion des pairs :

- Surveillez l'état des pairs via le tableau de bord de l'interface Web
- Configurez une surveillance externe pour les événements de pair hors service
- Testez la connectivité des pairs pendant les fenêtres de maintenance

Planification de capacité :

- Estimez le taux de transaction Diameter en fonction des enregistrements et du volume d'appels
- Assurez-vous que HSS/PCRF/OCS peut gérer les taux de transaction de pointe
- Envisagez des agents de routage Diameter (DRA) pour les grandes déploiements

Dépannage :

- Vérifiez d'abord l'état des pairs lors de l'investigation des échecs d'enregistrement ou d'appel
- Corrélez les échecs Diameter avec les échecs SIP (même Call-ID ou utilisateur)
- Consultez les journaux de backend CSCF pour des traces de transaction Diameter détaillées

Sécurité :

- Utilisez TLS pour les connexions Diameter en production (si pris en charge)
- Restreignez l'accès des pairs Diameter via le pare-feu (seuls les pairs connus)
- Examinez régulièrement les journaux d'audit d'activation/désactivation des pairs

Limitations et améliorations futures

Mise en œuvre actuelle

Le panneau de contrôle fournit :

- ✅ Visualisation de l'état des pairs en temps réel
- ✅ Opérations d'activation/désactivation des pairs
- ✅ Mapping des ID d'application aux noms d'interface
- ✅ Actualisation automatique toutes les 5 secondes

Pas encore implémenté

Les fonctionnalités suivantes ne sont **pas actuellement disponibles** mais pourraient être ajoutées dans de futures versions :

- **Inspecteur de messages Diameter** : Voir les transactions Diameter récentes et les détails des AVP
- **Tableau de bord des métriques Diameter** : Intégration Grafana pour la latence, les taux d'erreur, etc.
- **Statistiques des pairs** : Comptes de messages, taux de succès, latence moyenne par pair
- **Surveillance watchdog** : État DWR/DWA en temps réel
- **Reconnecter manuellement** : Forcer la reconnexion du pair via l'interface Web

Solutions de contournement

Pour l'inspection des messages : Consultez les journaux de backend CSCF ou activez la journalisation de débogage Diameter

Pour des statistiques détaillées : Interrogez les métriques à partir du point de terminaison Prometheus (voir Référence des métriques pour les définitions complètes des métriques CDP/Diameter et Guide des opérations de l'interface Web pour la configuration de la surveillance)

Pour la reconnexion manuelle : Utilisez l'interface Web pour désactiver puis réactiver le pair

Documentation connexe

- **Guide des opérations P-CSCF** - Opérations de l'interface Rx P-CSCF
- **Guide des opérations I-CSCF** - Opérations de l'interface Cx I-CSCF
- **Guide des opérations S-CSCF** - Interfaces Cx, Ro S-CSCF
- **Guide des opérations de l'interface Web** - Gestion des pairs Diameter via le panneau de contrôle
- **Guide des opérations CSCF** - Opérations générales CSCF

Spécifications 3GPP

- **TS 29.228** : Interfaces Cx et Dx (CSCF-HSS)
- **TS 29.214** : Interface Rx (P-CSCF-PCRF)
- **TS 32.299** : Applications de facturation Diameter (Ro, Rf)
- **RFC 6733** : Protocole de base Diameter

Détails techniques

Mise en œuvre

- **Pile Diameter** : Pile de protocole Diameter intégrée
- **Interface de gestion** : Protocole RPC vers le backend CSCF
- **Interface Web** : Phoenix LiveView (`lib/cscf_web/web/diameter_live.ex`)

Configuration

Les pairs Diameter sont configurés dans les fichiers de configuration du backend CSCF, et non via le panneau de contrôle. Le panneau de contrôle fournit uniquement une surveillance et un contrôle opérationnel (activation/désactivation).

Guide de Capacité et de Dimensionnement d'OmniCall CSCF

Aperçu

Ce guide fournit des informations sur la planification de la capacité et le dimensionnement pour les déploiements d'OmniCall CSCF. Les chiffres de capacité présentés ici sont des **lignes directrices basées sur l'analyse du code source et l'expérience en production**, et non des limites strictes.

Stratégie de Mise à l'Échelle Horizontale

OmniCall CSCF atteint une échelle pratiquement illimitée grâce à la mise à l'échelle horizontale - il suffit de déployer des instances supplémentaires à mesure que votre base d'abonnés croît. Il n'y a pas de limite supérieure pratique à la capacité totale du réseau.

Principes Clés de Mise à l'Échelle :

✓ **Ajoutez des instances, pas de la complexité** : Besoin de supporter 1 million d'abonnés ? Déployez 3-4 instances S-CSCF au lieu d'un serveur massif

✓ **Composants indépendants** : Chaque instance P-CSCF, I-CSCF et S-CSCF fonctionne indépendamment

✓ **Distribution de charge** : I-CSCF distribue automatiquement les utilisateurs entre les instances S-CSCF ; DNS ou équilibreurs de charge distribuent le trafic vers P-CSCF et I-CSCF

✓ **Pas d'affinité de session requise** : Les utilisateurs peuvent être répartis entre différentes instances CSCF

✓ **Distribution géographique** : Déployez des instances CSCF dans plusieurs centres de données pour la résilience et l'optimisation de la latence

Exemple de Chemin de Mise à l'Échelle :

- **10K abonnés** : 1 P-CSCF, 1 I-CSCF, 1 S-CSCF
- **50K abonnés** : 2 P-CSCF, 2 I-CSCF, 2 S-CSCF
- **200K abonnés** : 6 P-CSCF, 4 I-CSCF, 4 S-CSCF
- **1M abonnés** : 30 P-CSCF, 10 I-CSCF, 10 S-CSCF
- **10M abonnés** : 300 P-CSCF, 50 I-CSCF, 50 S-CSCF

Mise à l'Échelle Économique : Matériel standard + mise à l'échelle horizontale = CapEx inférieur à des solutions coûteuses de "big iron".

À Propos de Ces Lignes Directrices

Les chiffres de capacité dans ce document sont des **estimations conservatrices** conçues pour :

- Fournir une marge de manœuvre pour les pics de trafic (tempêtes d'enregistrement, événements d'appels massifs)
- Tenir compte du traitement IFC complexe et des intégrations multiples de serveurs d'application
- Assurer des temps de réponse inférieurs à une seconde même sous charge
- Supporter des configurations à haute disponibilité avec capacité de basculement

Votre expérience peut varier en fonction de :

- Spécifications matérielles (vitesse du CPU, RAM, bande passante réseau)
- Complexité de l'IFC et nombre de serveurs d'application
- Minuteurs d'expiration d'enregistrement (plus courts = réenregistrements plus fréquents)
- Temps de maintien des appels et modèles de trafic aux heures de pointe

Recommandation : Utilisez ces lignes directrices comme point de départ, puis surveillez les métriques de production pour optimiser le nombre d'instances et la configuration pour votre déploiement spécifique.

Table des Matières

1. Résumé Exécutif
2. Capacité P-CSCF
3. Capacité I-CSCF
4. Capacité S-CSCF
5. Dimensionnement du Déploiement
6. Optimisation des Performances
7. Surveillance et Alertes
8. Résumé : Échelle Illimitée Grâce à la Mise à l'Échelle Horizontale

---

Résumé Exécutif

Contraintes Clés de Capacité

Type de CSCF	Contrainte Principale	Maximum par Instance	Déploiement Typique
P-CSCF	Associations de Sécurité IPsec	**~50,000 UEs**	10,000-30,000 UEs
I-CSCF	CPU/Réseau (sans état)	**Limité par le débit**	100,000+ req/sec
S-CSCF	Enregistrements d'Utilisateurs	**~500,000 IMPUs**	100,000-300,000 IMPUs
Dialogues	État d'Appel Actif	**~100,000 dialogues**	20,000-50,000 simultanés

Limites Techniques (Par Instance)

OmniCall CSCF a certaines limites techniques par instance. Ce ne sont **pas des limites de déploiement** - la capacité totale est illimitée grâce à la mise à l'échelle horizontale :

Limite	Valeur	Ce que cela signifie	Solution
Suivi de Hash SPI	**10,000 entrées**	Structure de suivi interne pour les SPI IPsec	Cela ne limite PAS les enregistrements à 10K. P-CSCF peut gérer 40K-50K enregistrements avec une configuration appropriée. Déployez plus de VMs P-CSCF pour une échelle plus élevée.
Contacts par IMPU	**100**	Maximum de contacts SIP par identité publique	Rarement atteint en pratique (typique : 1-5 contacts par utilisateur). Ajoutez des VMs S-CSCF si nécessaire.
Routes de Service	**10 par contact**	Maximum d'en-têtes de route de service	Utilisation typique : 1-3. Pas une contrainte.
Taille du Corps NOTIFY	**16 Ko**	Taille maximale du message de notification	Divisez les grandes listes d'abonnés entre les instances S-CSCF.

Clarification sur la Limite de Hash SPI :

- La limite de 10,000 SPI hash est une **structure de suivi interne**, pas une limite d'enregistrement stricte
- Les instances P-CSCF gèrent régulièrement **40,000-50,000 enregistrements simultanés** en production

- Le hash SPI est utilisé pour des recherches rapides ; les SAs IPsec réels sont gérés séparément par le noyau
- Si vous approchez des limites de capacité, déployez simplement des VMs P-CSCF supplémentaires

Point Clé : Ce sont des limites d'ingénierie pour une seule instance VM. Pour une échelle illimitée, déployez plus de VMs.

Capacité P-CSCF

Le **Proxy-CSCF** est généralement le composant le plus contraint en capacité en raison de la surcharge des associations de sécurité IPsec.

Facteurs de Capacité

1. Associations de Sécurité IPsec

Empreinte Mémoire par UE :

```
Chaque SA IPsec consomme environ :
- Suivi SPI : ~200 octets (entrée de table de hachage)
- Liaison de socket : ~1-2 Ko (ressources du noyau)
- État de contact : ~500-1000 octets (données d'enregistrement)
- Total par UE : ~2-3 Ko en mémoire partagée
```

Lignes Directrices de Capacité par Instance :

- **Agressive** : 40,000-50,000 UEs (approche de la limite de hash SPI)
- **Recommandé** : 20,000-30,000 UEs (performance équilibrée et marge de manœuvre)
- **Conservateur** : 10,000-15,000 UEs (marge de manœuvre maximale HA pour le basculement)

Mise à l'Échelle au-delà d'une Instance Unique :

- **100K abonnés** : Déployez 3-5 instances P-CSCF derrière un équilibrage de charge DNS
- **500K abonnés** : Déployez 15-25 instances P-CSCF sur plusieurs sites
- **1M+ abonnés** : Déployez 30-50+ instances P-CSCF avec distribution géographique

Remarque : Ce sont des lignes directrices, pas des limites. Les déploiements en production ont réussi à faire fonctionner des instances P-CSCF à 40K+ UEs avec un réglage approprié.

2. Services d'Urgence

Le traitement des appels d'urgence utilise un stockage en mémoire pour les mappages IMEI-vers-retour d'appel (TTL de 24 heures) pour supporter les retours d'appel d'urgence.

Exigences VM P-CSCF

Spécification VM Standard : 8 vCPU, 8 Go de RAM minimum

Taille de Déploiement	UEs par VM	VMs Nécessaires pour Exemples de Déploiements
Conservateur	10,000-15,000	10K abonnés = 1 VM, 50K abonnés = 4 VMs, 100K abonnés = 7 VMs
Recommandé	20,000-30,000	10K abonnés = 1 VM, 50K abonnés = 2 VMs, 100K abonnés = 4 VMs
Agressif	40,000-50,000	10K abonnés = 1 VM, 50K abonnés = 1 VM, 100K abonnés = 2 VMs

VoWiFi avec OmniePDG :

- OmniePDG termine IPsec, P-CSCF gère uniquement SIP
- La capacité augmente à **80,000-100,000 UEs par VM P-CSCF**
- 100K utilisateurs VoWiFi = 1-2 VMs P-CSCF (contre 4 VMs pour VoLTE)

Capacité I-CSCF

Le **Interrogating-CSCF** est sans état et principalement limité par le CPU et le débit réseau plutôt que par la mémoire.

Facteurs de Capacité

1. Conception Sans État

- **Pas d'état de session** : I-CSCF ne maintient pas les enregistrements d'utilisateurs ou les dialogues
- **Requêtes HSS** : Chaque enregistrement nécessite un échange Cx UAR/UAA
- **Basé sur le débit** : Limité par le taux de traitement REGISTER/INVITE

Débit Typique :

- **Taux d'Enregistrement** : 1,000-5,000 enregistrements/seconde (en fonction de la latence HSS)
- **Taux de Mise en Place d'Appels** : 5,000-10,000 INVITE/seconde

- **Abonnés Simultanés** : Effectivement illimité (aucun état maintenu)

2. Sélection S-CSCF

I-CSCF maintient un pool d'instances S-CSCF disponibles (typiquement 2-10) pour l'équilibrage de charge basé sur les capacités et la charge actuelle.

Exigences VM I-CSCF

Spécification VM Standard : 4 vCPU, 8 Go de RAM minimum

Taille de Déploiement	Débit par VM	VMs Nécessaires pour Exemples de Déploiements
Conservateur	1,000 reg/sec	10K abonnés = 1 VM, 100K abonnés = 2 VMs, 500K abonnés = 4 VMs
Recommandé	2,000 reg/sec	10K abonnés = 1 VM, 100K abonnés = 1 VM, 500K abonnés = 2 VMs
Agressif	5,000 reg/sec	10K abonnés = 1 VM, 100K abonnés = 1 VM, 500K abonnés = 1 VM

Stratégie de Mise à l'Échelle : Déployez plusieurs instances I-CSCF derrière un équilibrage de charge DNS en round-robin ou un équilibreur de charge matériel. Chaque instance est indépendante et sans état.

Capacité S-CSCF

Le **Serving-CSCF** maintient l'état d'enregistrement et les dialogues actifs, ce qui en fait le composant central de la scalabilité.

Facteurs de Capacité

1. Enregistrements d'Utilisateurs

Empreinte Mémoire par IMPU :

```
Chaque IMPU enregistré consomme environ :
- Entrée de hachage : ~1-2 Ko (IMPU, contacts, expiration)
- IFC (Critères de Filtrage Initiaux) : ~5-20 Ko (profil de service du HSS)
- Vecteurs d'authentification : ~1-2 Ko
- Total par IMPU : ~7-25 Ko selon la complexité du service
```

Lignes Directrices de Capacité par Instance :

- **Agressive** : 400,000-500,000 IMPUs (avec hash_size=14+, matériel haut

de gamme)
- **Recommandé** : 200,000-300,000 IMPUs (charge équilibrée, complexité IFC typique)
- **Conservateur** : 100,000-150,000 IMPUs (IFC complexe, plusieurs AS, marge de manœuvre HA)

Mise à l'Échelle pour de Grands Déploiements :

- **1M abonnés** : Déployez 3-5 instances S-CSCF, I-CSCF distribue via HSS
- **5M abonnés** : Déployez 15-25 instances S-CSCF dans plusieurs centres de données
- **10M+ abonnés** : Déployez 30-50+ instances S-CSCF

Remarque : Ce sont des lignes directrices de départ. La capacité réelle dépend de la complexité de l'IFC, de l'intégration AS et des spécifications matérielles. Certains déploiements en production fonctionnent avec 400K+ IMPUs par instance avec des configurations optimisées.

2. Dialogues Actifs (Sessions d'Appel)

Empreinte Mémoire par Dialogue :

```
Chaque dialogue actif consomme environ :
- État de dialogue : ~2-4 Ko (Call-ID, tags From/To, ensemble de
routes)
- Informations SDP : ~1-2 Ko (paramètres médias)
- Profils/variables : ~1-2 Ko
- Total par dialogue : ~4-8 Ko
```

Lignes Directrices de Capacité par Instance :

- **Agressive** : 80,000-100,000 dialogues simultanés (avec dlg_hash_size=15+)
- **Recommandé** : 40,000-60,000 dialogues simultanés (déploiement typique)
- **Conservateur** : 20,000-30,000 dialogues simultanés (marge de manœuvre HA maximale)

Mise à l'Échelle pour un Volume d'Appels Élevé :

- **100K appels simultanés** : Déployez 2-3 instances S-CSCF
- **500K appels simultanés** : Déployez 10-15 instances S-CSCF
- **1M+ appels simultanés** : Déployez 20-30+ instances S-CSCF

Remarque : La capacité des dialogues est souvent supérieure à celle des enregistrements puisque les dialogues sont de courte durée (secondes à minutes) tandis que les enregistrements sont de longue durée (minutes à heures). Surveillez les taux d'appels simultanés réels aux heures de pointe pour optimiser.

3. Traitement des Critères de Filtrage Initiaux (IFC)

Impact de la Complexité de l'IFC :

- IFC simple (1-5 points de déclenchement) : Surcharge minimale
- IFC complexe (10+ points de déclenchement, plusieurs AS) : 5-10 ms de traitement supplémentaire par appel
- Mémoire : 5-20 Ko par utilisateur selon la complexité du profil de service

Exigences VM S-CSCF

Spécification VM Standard : 8 vCPU, 8 Go de RAM minimum

Taille de Déploiement	IMPUs par VM	Dialogues Simultanés par VM	VMs Nécessaires pour Exemples de Déploiements
Conservateur	100,000-150,000	20,000-30,000	10K abonnés = 1 VM, 100K abonnés = 1 VM, 500K abonnés = 4 VMs
Recommandé	200,000-300,000	40,000-60,000	10K abonnés = 1 VM, 100K abonnés = 1 VM, 500K abonnés = 2 VMs
Agressif	400,000-500,000	80,000-100,000	10K abonnés = 1 VM, 100K abonnés = 1 VM, 500K abonnés = 1 VM

Dimensionnement du Déploiement

Petit Déploiement (< 10,000 Abonnés)

Scénario : MVNO, petite entreprise, environnement de laboratoire/test

Composant	Nombre de VMs	Spécification des VMs	Capacité par VM
P-CSCF	1	8 vCPU, 8 Go de RAM	10,000-15,000 UEs
I-CSCF	1	4 vCPU, 8 Go de RAM	1,000-2,000 reg/sec
S-CSCF	1	8 vCPU, 8 Go de RAM	100,000-200,000 IMPUs
Total VMs	**3**		
Capacité Totale			**Jusqu'à 15,000 abonnés**

Déploiement Moyen (10,000-100,000 Abonnés)

Scénario : Opérateur régional, opérateur de niveau 2, grande entreprise

Dimensionnement Conservateur (100K abonnés) :

Composant	Nombre de VMs	Spécification des VMs	Capacité par VM
P-CSCF	4	8 vCPU, 8 Go de RAM	25,000 UEs chacune
I-CSCF	2	4 vCPU, 8 Go de RAM	2,000 reg/sec chacune
S-CSCF	2	8 vCPU, 8 Go de RAM	150,000 IMPUs chacune
Total VMs	**8**		
Capacité Totale			**100,000 abonnés**

Dimensionnement Recommandé (100K abonnés) :

Composant	Nombre de VMs	Spécification des VMs	Capacité par VM
P-CSCF	2	8 vCPU, 8 Go de RAM	50,000 UEs chacune
I-CSCF	1	4 vCPU, 8 Go de RAM	5,000 reg/sec
S-CSCF	1	8 vCPU, 8 Go de RAM	300,000 IMPUs
Total VMs	**4**		
Capacité Totale			**100,000 abonnés**

Haute Disponibilité :

- Déployez I-CSCF derrière un équilibrage de charge DNS ou un équilibreur de charge
- I-CSCF distribue les utilisateurs à travers le pool S-CSCF
- Distribution géographique recommandée pour la résilience

Grand Déploiement (500,000 Abonnés)

Scénario : Opérateur de niveau 1, opérateur national

Dimensionnement Conservateur :

Composant	Nombre de VMs	Spécification des VMs	Capacité par VM
P-CSCF	25	8 vCPU, 8 Go de RAM	20,000 UEs chacune
I-CSCF	4	4 vCPU, 8 Go de RAM	2,000 reg/sec chacune
S-CSCF	4	8 vCPU, 8 Go de RAM	150,000 IMPUs chacune
Total VMs	**33**		
Capacité Totale			**500,000 abonnés**

Dimensionnement Recommandé :

Composant	Nombre de VMs	Spécification des VMs	Capacité par VM
P-CSCF	15	8 vCPU, 8 Go de RAM	33,000 UEs chacune
I-CSCF	2	4 vCPU, 8 Go de RAM	5,000 reg/sec chacune
S-CSCF	2	8 vCPU, 8 Go de RAM	250,000 IMPUs chacune
Total VMs	**19**		
Capacité Totale			**500,000 abonnés**

Dimensionnement Agressif :

Composant	Nombre de VMs	Spécification des VMs	Capacité par VM
P-CSCF	10	8 vCPU, 8 Go de RAM	50,000 UEs chacune
I-CSCF	1	4 vCPU, 8 Go de RAM	5,000 reg/sec
S-CSCF	1	8 vCPU, 8 Go de RAM	500,000 IMPUs
Total VMs	**12**		
Capacité Totale			**500,000 abonnés**

Haute Disponibilité :

- P-CSCF actif-actif à travers les centres de données
- I-CSCF géo-redondant avec DNS ou BGP anycast
- Plusieurs instances S-CSCF avec distribution de charge I-CSCF

Considérations de Déploiement VoWiFi

Avec OmniePDG :

- La capacité P-CSCF augmente considérablement (pas de surcharge IPsec sur P-CSCF)
- ePDG gère la terminaison du tunnel IPsec
- P-CSCF peut supporter 100,000+ utilisateurs VoWiFi (limité par CPU/ réseau, pas IPsec)

Architecture :

```
VoWiFi UE → (IPsec) → OmniePDG → (SIP) → P-CSCF → I-CSCF → S-CSCF
VoLTE UE → (IPsec) → P-CSCF → I-CSCF → S-CSCF
```

Recommandation : Pour de grands déploiements VoWiFi (>50K utilisateurs), déployez des instances P-CSCF dédiées derrière OmniePDG sans module IPsec chargé pour un maximum de débit.

Optimisation des Performances

OmniCall CSCF est livré pré-optimisé pour une utilisation en production. L'optimisation des performances est gérée par l'ingénierie d'OmniCall lors du déploiement.

Configuration Standard des VMs

Toutes les VMs OmniCall CSCF sont configurées avec :

- **OS** : Tuning du noyau Linux pour un débit réseau élevé
- **Mémoire** : Allocation de mémoire partagée optimisée pour les tables de hachage et l'état de session
- **Réseau** : Tuning de la pile TCP/IP pour le trafic SIP et Diameter

Tuning Spécifique au Déploiement

Pour un tuning personnalisé basé sur vos exigences de déploiement spécifiques, contactez le support d'OmniCall. Les scénarios de tuning courants incluent :

- **Volume d'appels élevé** : Ajustement des processus de travail et de la capacité des dialogues
- **Grande base d'abonnés** : Optimisation des tables de hachage d'enregistrement
- **IFC complexe** : Tuning des processus de notification pour l'intégration des serveurs d'application
- **Distribution géographique** : Optimisation du basculement et de la redondance

---

Surveillance et Alertes

Indicateurs Clés de Performance (KPI)

Métriques P-CSCF

Métrique	Description	Seuil d'Alerte	Seuil Critique
Nombre de SA IPsec	Associations de sécurité actives	> 25,000	> 40,000
Utilisation du Hash SPI	Pourcentage de la plage SPI utilisée	> 70%	> 90%
Taux d'Enregistrement	Requêtes REGISTER/seconde	> 100/sec	> 500/sec
Charge du Hash de Contact	Contacts moyens par slot de hachage	> 20	> 50

Métrique	Description	Seuil d'Alerte	Seuil Critique
Utilisation de la Mémoire	Consommation de mémoire partagée	> 70%	> 90%

Requêtes Prometheus :

```
# Nombre de SA IPsec (à partir de la surveillance de la table de hachage)
ipsec_sa_count{cscf="pcscf01"}

# Taux d'enregistrement
rate(sip_register_requests_total{cscf="pcscf01"}[5m])
```

Métriques S-CSCF

Métrique	Description	Seuil d'Alerte	Seuil Critique
IMPUs Enregistrés	Total d'utilisateurs enregistrés	> 300,000	> 450,000
Dialogues Actifs	Sessions d'appel simultanées	> 40,000	> 70,000
Charge du Hash IMPU	IMPUs moyens par slot de hachage	> 50	> 100
Charge du Hash de Dialogue	Dialogues moyens par slot de hachage	> 10	> 20
Temps de Traitement IFC	Temps moyen d'évaluation de l'IFC	> 10 ms	> 50 ms

Requêtes Prometheus :

```
# Utilisateurs enregistrés
impu_registered_count{cscf="scscf01"}

# Dialogues actifs
dialog_active_count{cscf="scscf01"}
```

Métriques I-CSCF

Métrique	Description	Seuil d'Alerte	Seuil Critique
TPS d'Enregistrement	Transactions REGISTER/seconde	> 1,000/sec	> 2,000/sec
Latence de Requête HSS	Temps de réponse Diameter Cx	> 50 ms	> 200 ms
Taux d'Échec HSS	Pourcentage de requêtes HSS échouées	> 1%	> 5%

Vérifications de Santé

Surveillance de la Santé du Système : OmniCall CSCF exporte des métriques de santé complètes via le panneau de contrôle et les points de terminaison Prometheus (`http://<host>:9090/metrics`). Surveillez :

- Nombres de SA IPsec (P-CSCF)
- Nombres d'enregistrements (P-CSCF, S-CSCF)
- Nombres de dialogues actifs (S-CSCF)
- Utilisation de la mémoire
- Utilisation du CPU

Pour une liste complète de toutes les métriques disponibles, consultez la **Référence des Métriques**.

Règles d'Alerte (Prometheus/Alertmanager)

```
groups:
  - name: cscf_capacity
    rules:
      - alert: PCSCFIPsecSAHigh
        expr: ipsec_sa_count > 40000
        for: 5m
        annotations:
          summary: "P-CSCF {{ $labels.instance }} a un nombre élevé
de SA IPsec"

      - alert: SCSCFRegistrationHigh
        expr: impu_registered_count > 450000
        for: 10m
        annotations:
          summary: "S-CSCF {{ $labels.instance }} approche de la
capacité d'enregistrement"

      - alert: SCSCFDialogHigh
        expr: dialog_active_count > 70000
        for: 5m
        annotations:
          summary: "S-CSCF {{ $labels.instance }} a un nombre élevé
de dialogues actifs"
```

Annexe : Méthodologie de Planification de Capacité

Ce guide de dimensionnement est basé sur :

1. **Déploiements en Production** : Analyse des déploiements réels d'OmniCall CSCF allant de 5K à 500K+ abonnés
2. **Tests de Performance** : Tests de charge et benchmarking à travers diverses configurations matérielles
3. **Normes 3GPP** : Conformité aux spécifications 3GPP pour la capacité et la performance IMS
4. **Analyse d'Ingénierie** : Revue technique détaillée de l'architecture CSCF et de l'utilisation des ressources

Validation : Tous les chiffres de capacité ont été validés dans des réseaux de transport en production.

Résumé : Échelle Illimitée Grâce à la Mise à l'Échelle Horizontale

Points Clés à Retenir

1. **Pas de Limites Strictes sur la Capacité Totale** : Les limites par instance documentées dans ce guide sont des **lignes directrices conservatrices**, pas des plafonds absolus. La capacité totale du réseau est illimitée grâce à la mise à l'échelle horizontale.

2. **Modèle de Mise à l'Échelle Simple** :

   ```
   Besoin de plus de capacité ? → Déployez plus d'instances
   Atteignez une limite par instance ? → Ajoutez une autre instance
   Trafic en croissance ? → Lancez plus de VMs
   ```

3. **Prouvé à Grande Échelle** : Les déploiements d'OmniCall CSCF vont de :

   - Petits MVNO : 5K-10K abonnés sur 3-5 VMs
   - Opérateurs régionaux : 50K-200K abonnés sur 10-30 VMs
   - Opérateurs de niveau 1 : 1M+ abonnés sur 100+ VMs

4. **Croissance Économique** : Évoluez progressivement avec du matériel standard plutôt qu'avec des mises à niveau coûteuses. Ajoutez de la capacité à mesure que les revenus augmentent.

5. **Lignes Directrices, Pas Règles** : Les chiffres de capacité dans ce document sont :

   - ✅ Estimations conservatrices avec une marge de manœuvre intégrée
   - ✅ Basés sur l'analyse du code source et l'expérience en production
   - ✅ Points de départ utiles pour la planification
   - ✅ PAS des limites strictes qui ne peuvent pas être dépassées
   - ✅ PAS des prescriptions universelles

Exemple de Mise à l'Échelle dans le Monde Réel

Scénario : Passer de 10K à 1M abonnés en 3 ans

Année	Abonnés	P-CSCF	I-CSCF	S-CSCF	Action
Année 0	10,000	1	1	1	Déploiement initial (3 VMs)
Année 1	50,000	2	2	2	Croissance 2x : Ajoutez 3 VMs
Année 1.5	100,000	4	3	3	Croissance 2x : Ajoutez 4 VMs
Année 2	250,000	8	4	5	Croissance 2.5x : Ajoutez 6 VMs
Année 3	500,000	15	6	8	Croissance 2x : Ajoutez 13 VMs
Futur	1,000,000	30	10	10	Croissance 2x : Ajoutez 24 VMs

Investissement Total : Ajouts de VMs incrémentales à mesure que les revenus augmentent, pas de CapEx massif en amont.

Quand Ajouter des Instances

Surveillez ces signaux pour savoir quand évoluer horizontalement :

P-CSCF :

- Nombre de SA IPsec constamment >30K (>70% de la capacité recommandée)
- Utilisation du CPU >70% pendant l'heure de pointe
- Temps de réponse d'enregistrement >500ms

S-CSCF :

- Nombre d'IMPU constamment >250K (>70% de la capacité recommandée)
- Nombre de dialogues approchant 50K simultanés
- Utilisation du CPU >70% pendant l'heure de pointe

I-CSCF :

- Taux de requêtes constamment >2,000/sec par instance
- Utilisation du CPU >80% pendant l'heure de pointe
- Latence de requête HSS en augmentation

Action : Ajoutez 1-2 instances de manière proactive avant d'atteindre les limites. La mise à l'échelle horizontale est une assurance peu coûteuse contre les problèmes de capacité.

Philosophie de Configuration

Commencez Conservateur, Réglez au Fur et à Mesure :

1. Commencez avec les configurations recommandées de ce guide

2. Surveillez les métriques de production (voir Surveillance)
3. Réglez les tailles de hachage et les processus de travail en fonction de la charge réelle
4. Ajoutez des instances avant d'atteindre 80% des limites de capacité observées
5. Testez les configurations en staging avant le déploiement en production

Rappelez-vous : Ces lignes directrices fournissent un point de départ éprouvé, mais chaque déploiement est unique. Votre capacité réelle peut être plus élevée ou plus basse en fonction de votre environnement spécifique, des modèles de trafic et des exigences.

Guide des opérations I-CSCF

Table des matières

1. Aperçu
2. Rôle dans l'architecture IMS
3. Fonctions de l'I-CSCF
4. Opérations de l'interface Web
5. Flux d'appels
6. Dépannage

Aperçu

Le **I-CSCF** (Interrogating Call Session Control Function) sert de point d'entrée au réseau d'un opérateur IMS depuis des réseaux externes et depuis le P-CSCF. Sa principale responsabilité est d'interroger le HSS (Home Subscriber Server) pour découvrir le S-CSCF approprié pour un utilisateur et de cacher la topologie interne du réseau aux entités externes.

Spécifications 3GPP

- **3GPP TS 23.228** : Système multimédia IP (IMS) Étape 2
- **3GPP TS 24.229** : Protocole de contrôle d'appel IMS
- **3GPP TS 29.228** : Interface Cx (I-CSCF vers HSS)
- **3GPP TS 29.229** : Protocole Cx

Responsabilités clés

1. **Interrogation du HSS** : Interroge le HSS pour la localisation de l'utilisateur et l'attribution du S-CSCF
2. **Sélection du S-CSCF** : Choisit le S-CSCF approprié en fonction des capacités
3. **Masquage de la topologie** : Protège les adresses internes du S-CSCF de la vue externe
4. **Équilibrage de charge** : Distribue la charge sur plusieurs instances de S-CSCF
5. **Proxy de routage** : Achemine les demandes vers le S-CSCF sélectionné
6. **Point d'entrée réseau** : Premier saut pour les messages SIP externes

Caractéristiques clés

- **Fonctionnement sans état** : Rétention d'état minimale
- **Client Diameter** : Interface Cx vers HSS

- **Pas de gestion de médias** : Proxy de signalisation pur
- **Pas d'authentification** : Délègue au S-CSCF
- **Haut débit** : Optimisé pour les requêtes et le transfert

Rôle dans l'architecture IMS

Position dans le réseau

Points de référence 3GPP

Interface	Protocole	Objectif	Connecté à
Mw	SIP	P-CSCF/Externe à I-CSCF	P-CSCF, IMS Externe
Mw	SIP	I-CSCF à S-CSCF	S-CSCF
Cx	Diameter	Requêtes de données utilisateur	HSS

Fonctions de l'I-CSCF

1. Interrogation du HSS (Interface Cx)

L'I-CSCF utilise l'interface Diameter Cx pour interroger le HSS pour deux opérations principales :

Demande d'autorisation utilisateur (UAR)

Utilisée lors de **REGISTER** pour déterminer quel S-CSCF doit servir l'utilisateur.

Objectif :

- Vérifier si l'utilisateur est autorisé à s'enregistrer
- Obtenir le nom du S-CSCF s'il est déjà attribué
- Obtenir les capacités du S-CSCF s'il n'est pas attribué

Commande Diameter :

```
UAR (User-Authorization-Request)
  Session-Id
  Vendor-Specific-Application-Id
    Vendor-Id: 10415 (3GPP)
    Auth-Application-Id: 16777216 (Cx)
  Auth-Session-State: NO_STATE_MAINTAINED
  Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
  Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
  User-Name: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Visited-Network-Identifier: ims.mnc001.mcc001.3gppnetwork.org
```

```
  UAR-Flags: 0
```

Réponse HSS (UAA) :

```
UAA (User-Authorization-Answer)
  Result-Code: 2001 (DIAMETER_SUCCESS)
  Experimental-Result-Code: 2001 (FIRST_REGISTRATION)
  Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
  Server-Capabilities:
    Mandatory-Capability: 1
    Optional-Capability: 2
    Server-Name: sip:scscf-backup.ims.mnc001.mcc001.3gppnetwork.org
```

Codes de résultat :

- `2001` : Succès (utilisateur autorisé)
- `5003` : Utilisateur inconnu
- `5004` : Identités ne correspondent pas
- `5042` : Aucun S-CSCF disponible

Demande d'information de localisation (LIR)

Utilisée pour **INVITE** et d'autres demandes pour trouver quel S-CSCF sert actuellement l'utilisateur.

Objectif :

- Trouver le S-CSCF servant un utilisateur enregistré
- Acheminer correctement les appels terminants

Commande Diameter :

```
LIR (Location-Info-Request)
  Session-Id
  Vendor-Specific-Application-Id
    Vendor-Id: 10415 (3GPP)
    Auth-Application-Id: 16777216 (Cx)
  Auth-Session-State: NO_STATE_MAINTAINED
  Origin-Host: icscf.ims.mnc001.mcc001.3gppnetwork.org
  Origin-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Destination-Realm: ims.mnc001.mcc001.3gppnetwork.org
  Public-Identity: sip:user@ims.mnc001.mcc001.3gppnetwork.org
  Originating-Request: 0  # 0=terminating, 1=originating
```

Réponse HSS (LIA) :

```
LIA (Location-Info-Answer)
  Result-Code: 2001 (DIAMETER_SUCCESS)
```

```
Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
```

Codes de résultat :

- `2001` : Succès (utilisateur enregistré, S-CSCF retourné)
- `5401` : Utilisateur non enregistré
- `5003` : Utilisateur inconnu

2. Sélection du S-CSCF

Lorsque le HSS ne retourne pas un S-CSCF spécifique (par exemple, première inscription), l'I-CSCF doit en sélectionner un basé sur **l'adéquation des capacités**.

Algorithme d'adéquation des capacités

1. **Récupérer les capacités** du HSS UAA
2. **Interroger la base de données locale** pour les S-CSCF disponibles
3. **Faire correspondre les capacités obligatoires** (toutes doivent correspondre)
4. **Faire correspondre les capacités optionnelles** (meilleur effort)
5. **Appliquer l'équilibrage de charge** si plusieurs correspondances
6. **Sélectionner le S-CSCF** avec le meilleur ajustement

Structure de la base de données S-CSCF

L'I-CSCF maintient une base de donn��es avec deux tables liées :

Table S-CSCF : Stocke des informations sur les serveurs S-CSCF disponibles :

- **ID** : Identifiant unique pour chaque S-CSCF
- **Nom** : Nom descriptif (par exemple, "S-CSCF principal")
- **URI S-CSCF** : URI SIP du S-CSCF (par exemple, sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060;transport=tcp)

Table des capacités S-CSCF : Mappe les S-CSCF à leurs capacités prises en charge :

- **ID** : Identifiant unique pour le mappage des capacités
- **ID S-CSCF** : Référence le S-CSCF dans la première table
- **Capacité** : ID de capacité entier que ce S-CSCF prend en charge

Configuration d'exemple : Un déploiement typique pourrait avoir :

- S-CSCF #1 : "S-CSCF principal" avec URI sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
    - Prend en charge la capacité 0 (capacité obligatoire)
    - Prend en charge la capacité 1 (capacité optionnelle)

Vous pouvez consulter la liste actuelle des S-CSCF via : Interface Web → I-CSCF → Onglet Liste des S-CSCF

La liste des S-CSCF montre les serveurs S-CSCF disponibles et leurs capacités pour l'équilibrage de charge et l'attribution.

Logique de sélection

Processus de sélection du S-CSCF : L'I-CSCF effectue la sélection du S-CSCF basée sur les capacités en utilisant la logique suivante :

1. **Extraire les capacités** : Récupère les exigences de capacité obligatoires et optionnelles de la réponse UAA (User Authorization Answer) du HSS et les stocke dans des variables AVP

2. **Interrogation de la base de données** : Interroge la base de données avec les exigences de capacité pour trouver des serveurs S-CSCF qui correspondent aux capacités requises

3. **Gestion des résultats** :

    - Si un S-CSCF correspondant est trouvé, l'URI est stockée dans $avp(scscf_uri) et définie comme l'URI de destination ($du) pour le transfert de la demande
    - Si aucun S-CSCF correspondant n'est disponible, répond à la demande originale avec 503 Service Unavailable

3. Masquage de la topologie

L'I-CSCF protège les adresses internes du S-CSCF des réseaux externes en :

1. **Retirant Record-Route** : N'ajoute pas d'en-tête Record-Route
2. **Proxy des réponses** : Retire les en-têtes Via révélant le S-CSCF
3. **Réécriture de contact** : (optionnel) Remplace le contact S-CSCF par l'I-CSCF
4. **Suppression de chemin** : Supprime les informations de chemin internes

Exemple :

```
L'externe voit :
  Via: SIP/2.0/UDP icscf.example.com:5060

La réalité interne :
  Via: SIP/2.0/UDP scscf.example.com:5060
  Via: SIP/2.0/UDP icscf.example.com:5060
```

4. Logique de routage

Traitement de REGISTER

Traitement de INVITE (Terminant)

5. NDS (Sécurité du domaine réseau)

L'I-CSCF maintient une liste de **domaines de confiance** pour la sécurité inter-opérateur.

Base de données des domaines de confiance : Contient une liste de noms de domaine qui sont de confiance pour la communication inter-opérateur :

- **ID** : Identifiant unique pour chaque domaine de confiance
- **Domaine de confiance** : Nom de domaine (par exemple, "ims.mnc001.mcc001.3gppnetwork.org")

Configuration d'exemple : Un déploiement typique inclut le domaine IMS d'origine et tous les domaines de partenaires de peering :

- ims.mnc001.mcc001.3gppnetwork.org (réseau d'origine)
- ims.mnc002.mcc001.3gppnetwork.org (partenaire de roaming)

Objectif :

- Valider les demandes entrantes des réseaux de peering
- Appliquer des politiques de sécurité basées sur les relations de confiance
- Mettre en œuvre une limitation de taux par domaine
- Contrôler quels réseaux externes peuvent accéder au cœur IMS

Vous pouvez consulter les domaines de confiance via : Interface Web → I-CSCF → Onglet Domaines de confiance

6. Basculer et équilibrer la charge

Basculer le S-CSCF

Conditions de déclenchement - La bascule vers le S-CSCF suivant est déclenchée par :

- 408 Request Timeout
- Réponses d'erreur serveur 5xx
- Réponses d'échec global 6xx (sauf 600 Busy Everywhere, qui indique un rejet de l'utilisateur plutôt qu'une défaillance du serveur)

Logique de basculement : L'I-CSCF met en œuvre un basculement automatique

en utilisant une route de défaillance :

1. **Vérification de l'état** : Lorsqu'une réponse est reçue, vérifie si le code d'état correspond aux critères de basculement (408, 5xx ou 6xx)

2. **Sélection du S-CSCF suivant** : Si le basculement est déclenché, sélectionne le S-CSCF suivant disponible dans la liste

3. **Réessayer ou échouer** :

    - Si un autre S-CSCF est disponible, relaie la demande vers celui-ci
    - Si tous les S-CSCF ont été essayés et ont échoué, répond avec 503 Service Unavailable à l'initiateur

Gestion de la liste des S-CSCF avec état :

- La liste des S-CSCF candidats est conservée en mémoire de transaction
- La position dans la liste est maintenue à travers plusieurs tentatives
- La liste est effacée lorsqu'une réponse réussie finale est reçue (succès 2xx ou erreur client 4xx)
- La liste est préservée lors de la réception de 401 Unauthorized (défi d'authentification), car le même S-CSCF doit gérer la demande authentifiée suivante

Équilibrage de charge

Configuration de l'équilibrage de charge :

Lorsque plusieurs S-CSCF prennent en charge les mêmes capacités :

- S-CSCF 1 : sip:scscf1.example.com:5060 - capacité 0
- S-CSCF 2 : sip:scscf2.example.com:5060 - capacité 0
- S-CSCF 3 : sip:scscf3.example.com:5060 - capacité 0

L'I-CSCF utilise une sélection **round-robin** ou **aléatoire** pour répartir la charge uniformément sur tous les S-CSCF correspondants.

Consultez la distribution de la charge via : Interface Web → I-CSCF → Liste des S-CSCF (montre tous les serveurs configurés)

Opérations de l'interface Web

Accéder à la page I-CSCF

Naviguez vers : `https://<control-panel>/icscf`

Mise en page de la page

La page I-CSCF a quatre onglets principaux :

1. **Serveurs S-CSCF** - S-CSCF configurés et capacités
2. **Domaines de confiance NDS** - Sécurité du domaine réseau
3. **Sessions** - Sessions I-CSCF actives avec sélection de S-CSCF
4. **Tables de hachage** - Tables de mémoire partagée

Affichage des serveurs S-CSCF

Objectif : Voir quels S-CSCF sont disponibles pour l'attribution à l'utilisateur

Colonnes d'affichage :

- **ID** : ID de la base de données
- **Nom** : Nom descriptif
- **URI S-CSCF** : URI SIP du S-CSCF
- **Capacités** : IDs de capacité séparés par des virgules

Exemple de sortie :

```
ID   Nom                    URI S-CSCF
Capacités
1    S-CSCF principal
sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060   0, 1
2    S-CSCF secondaire
sip:scscf2.ims.mnc001.mcc001.3gppnetwork.org:5060  0, 1
```

Opérations :

- Voir la liste des S-CSCF
- Vérifier les capacités configurées
- Vérifier les URIs S-CSCF

Remarque : Pour ajouter/modifier des S-CSCF, coordonnez-vous avec les administrateurs système. Les nouvelles entrées S-CSCF nécessitent :

- Un nom (étiquette descriptive comme "Nouveau S-CSCF")
- L'URI S-CSCF (par exemple, sip:scscf3.example.com:5060;transport=tcp)
- Les IDs de capacité associés (par exemple, capacités 0 et 1)

Affichage des domaines de confiance NDS

Objectif : Surveiller quels domaines réseau sont de confiance pour le peering

Colonnes d'affichage :

- **ID** : ID de la base de données
- **Domaine de confiance** : FQDN du réseau de confiance

Exemple de sortie :

```
ID   Domaine de confiance
1    ims.mnc001.mcc001.3gppnetwork.org
2    ims.mnc002.mcc001.3gppnetwork.org
3    carrier.example.com
```

Opérations :

- Voir les domaines de confiance
- Vérifier les relations de peering

Ajout de domaines de confiance : Coordonnez-vous avec les administrateurs système pour ajouter de nouveaux domaines de confiance. Chaque entrée nécessite le nom de domaine entièrement qualifié (FQDN) du réseau de confiance (par exemple, partner.example.com).

Surveillance des sessions actives

Objectif : Voir en temps réel la prise de décision de l'I-CSCF et la sélection du S-CSCF

Informations d'affichage :

- **Call-ID** : SIP Call-ID
- **Identité utilisateur** : Identité publique étant interrogée
- **S-CSCF sélectionné** : Quel S-CSCF a été choisi
- **Correspondance des capacités** : Capacités qui ont correspondu
- **Résultat UAR/LIR** : Code de résultat Diameter
- **Horodatage** : Quand la session a été créée

Cas d'utilisation :

1. Vérifier que la sélection du S-CSCF fonctionne
2. Dépanner les problèmes de routage
3. Surveiller la distribution de la charge entre les S-CSCF
4. Analyser l'adéquation des capacités

Exemple :

```
Call-ID: 3c26700857a87f84@10.4.12.165
Utilisateur: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
S-CSCF sélectionné: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org:5060
Capacités: obligatoire=[0,1], optionnelles=[]
Opération: UAR (Enregistrement)
Résultat: 2001 (FIRST_REGISTRATION)
```

```
Horodatage: 2025-11-29 14:35:22
```

Gestion des tables de hachage

Similaire au P-CSCF, l'I-CSCF peut utiliser des tables de hachage pour la mise en cache ou la logique personnalisée.

Cas d'utilisation courants :

- Mise en cache des résultats UAR/LIR (TTL court)
- Limitation de taux par IP source
- Décisions de routage personnalisées

Opérations : Identiques à celles du P-CSCF (lister, vider, supprimer, vider)

Flux d'appels

Flux d'enregistrement avec I-CSCF

Flux d'appel terminant via I-CSCF

Flux de basculement S-CSCF

Dépannage

Problèmes de connectivité HSS

Pair Diameter fermé

Symptômes : Impossible d'interroger le HSS, tous les enregistrements échouent

Étapes de diagnostic :

1. Vérifiez l'état du pair Diameter dans l'interface Web :
    - Naviguez vers la page Diameter
    - Sélectionnez le nœud I-CSCF
    - Vérifiez l'état du pair HSS
2. Vérifiez la connectivité réseau vers le HSS (coordonnez-vous avec l'équipe réseau si nécessaire)
3. Essayez d'activer le pair via le panneau de contrôle :
    - Naviguez vers la page Diameter
    - Trouvez le pair HSS

    - Cliquez sur le bouton "Activer"

4. Consultez les journaux système via la page Journaux du panneau de contrôle pour les messages CER/CEA (Capabilities Exchange) et les erreurs Diameter

5. Coordonnez-vous avec les administrateurs système pour vérifier la configuration Diameter si nécessaire

Délai d'attente UAR/LIR

Symptômes : Les enregistrements/appels expirent, les journaux montrent un délai d'attente Diameter

Causes possibles :

- HSS surchargé
- Latence réseau
- Domaine de routage incorrect
- HSS ne répond pas à cet I-CSCF

Solutions :

1. Consultez les journaux système pour les erreurs de délai d'attente Diameter

2. Vérifiez que le pair HSS est connecté via le panneau de contrôle (page Diameter)

3. Coordonnez-vous avec les administrateurs système pour :

    - Augmenter le délai d'attente de transaction Diameter si nécessaire
    - Vérifier la configuration du domaine de destination
    - Vérifier les journaux HSS si accessibles

4. Surveillez le flux de messages Diameter via la page Journaux du panneau de contrôle

5. Coordonnez-vous avec l'équipe réseau pour vérifier qu'il n'y a pas de latence réseau ou de problèmes de routage vers le HSS

Problèmes de sélection de S-CSCF

Aucun S-CSCF sélectionné

Symptômes : 503 Service Unavailable, les journaux montrent "Aucun S-CSCF disponible"

Étapes de diagnostic :

1. Vérifiez la liste des S-CSCF via le panneau de contrôle :
    - Naviguez vers I-CSCF → Onglet Serveurs S-CSCF
    - Vérifiez que les S-CSCF sont configurés avec les capacités appropriées
2. Consultez les journaux système pour les capacités UAA (User Authorization Answer) du HSS
3. Vérifiez la correspondance des capacités entre ce que retourne le HSS et ce qui est configuré dans la base de données I-CSCF
4. Coordonnez-vous avec les administrateurs système pour :
    - Vérifier la connectivité de la base de données
    - Ajouter les entrées S-CSCF manquantes si nécessaire
    - Vérifier que la configuration des capacités correspond aux attentes du HSS

Mauvais S-CSCF sélectionné

Symptômes : Les appels sont routés vers un S-CSCF inattendu

Causes possibles :

- Mismatch de capacité
- Problème d'équilibrage de charge
- Base de données désynchronisée avec le HSS

Solutions :

1. Surveillez le suivi des sessions via le panneau de contrôle :
    - Naviguez vers I-CSCF → Onglet Sessions
    - Consultez les décisions de sélection du S-CSCF
2. Consultez les journaux système pour vérifier si le HSS attribue un nom de S-CSCF spécifique (ce qui remplacerait la logique de sélection)
3. Vérifiez que la liste des S-CSCF et les capacités de la base de données I-CSCF correspondent aux attentes du HSS
4. Coordonnez-vous avec les administrateurs système pour examiner la configuration de correspondance des capacités

Problèmes de routage

Les demandes ne sont pas transférées au S-CSCF

Symptômes : L'I-CSCF reçoit la demande mais ne la transfère pas

Étapes de diagnostic :

1. Consultez les journaux système via la page Journaux du panneau de contrôle pour les erreurs de routage

2. Vérifiez que l'URI de destination S-CSCF est correctement définie (vérifiez les journaux pour les décisions de routage)

3. Vérifiez la connectivité réseau vers le S-CSCF (coordonnez-vous avec l'équipe réseau)

4. Vérifiez que le S-CSCF sélectionné est réellement accessible et répond

5. Coordonnez-vous avec les administrateurs système pour activer la journalisation de débogage si nécessaire pour une analyse plus approfondie

Le S-CSCF répond mais l'I-CSCF ne relaie pas

Symptômes : Wireshark montre une réponse à l'I-CSCF mais pas transférée

Causes possibles :

- Délai d'attente de transaction
- Mismatch d'en-tête Via
- Boucle Record-Route

Solutions :

1. Consultez les journaux système pour les erreurs de correspondance de transaction ou de détection de boucle

2. Vérifiez que les en-têtes Via sont traités correctement (vérifiez les journaux)

3. Coordonnez-vous avec les administrateurs système pour :

    - Augmenter le délai d'attente de transaction si nécessaire
    - Vérifier qu'il n'y a pas de boucles de routage SIP

Problèmes de base de données

Connexion à la base de données perdue

Symptômes : "Erreur de connexion à la base de données" dans les journaux

Solutions :

1. Coordonnez-vous avec les administrateurs système pour :
    - Vérifier que le service de base de données fonctionne
    - Tester la connectivité de la base de données
    - Activer la reconnexion automatique si ce n'est pas déjà configuré
    - Redémarrer le service I-CSCF si nécessaire

Mismatch du schéma de base de données

Symptômes : Erreurs SQL dans les journaux concernant des colonnes/tables manquantes

Solutions :

1. Coordonnez-vous avec les administrateurs système pour :
    - Vérifier que le schéma de la base de données correspond à la structure attendue
    - Vérifier que les tables s_cscf, s_cscf_capabilities et nds_trusted_domains existent et ont les bonnes colonnes
    - Recréer le schéma de la base de données si nécessaire

Meilleures pratiques

Haute disponibilité

1. **Déployer plusieurs instances I-CSCF** :
    - Utiliser DNS SRV pour l'équilibrage de charge
    - Chaque instance se connecte au même HSS
    - Partager la base de données (lecture seule pour la liste des S-CSCF)
2. **Configuration DNS SRV** :

```
_sip._udp.ims.example.com. SRV 10 50 5060 icscf01.example.com.
_sip._udp.ims.example.com. SRV 10 50 5060 icscf02.example.com.
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf01.example.com.
_sip._tcp.ims.example.com. SRV 10 50 5060 icscf02.example.com.
```

3. **Fonctionnement sans état** : L'I-CSCF ne maintient pas l'état de dialogue, ce qui rend le basculement transparent

Optimisation des performances

1. **Processus de travail** : Définir un nombre élevé de processus de travail pour un débit de requêtes optimal

    - children=64 (valeur élevée optimisée pour la charge de travail lourde en requêtes de l'I-CSCF)
    - tcp_children=8 pour gérer les connexions TCP

2. **Mise en pool de connexions à la base de données** : Utiliser des connexions persistantes pour réduire les frais de connexion

3. **Désactiver les fonctionnalités inutiles** pour réduire la surcharge de traitement :

    - Pas de gestion RTP (l'I-CSCF est uniquement de signalisation)
    - Pas de services de présence
    - Journalisation minimale en production (définir au niveau info ou avertissement uniquement)

4. **Optimiser Diameter** pour l'interface Cx à haut débit :

    - sessions_hash_size=4096 (table de hachage plus grande pour de meilleures performances de recherche de session)
    - workers=4 (threads de travail Diameter dédiés pour des opérations Cx concurrentes)

Sécurité

1. **Valider les domaines de confiance** : Vérifier les en-têtes Via/P-Visited-Network-ID

2. **Limitation de taux** : Prévenir les attaques DoS sur le HSS en limitant les requêtes UAR/LIR par IP source

    - Utiliser le module pike pour vérifier le taux de demande
    - Si la limite de taux est dépassée, répondre avec 503 Too Many Requests
    - Protège le HSS d'être submergé par des inondations de requêtes malveillantes

3. **TLS vers HSS** : Utiliser Diameter sur TLS (DTLS)

4. **Assainir les en-têtes** : Supprimer les P-en-têtes non fiables des réseaux externes

Surveillance

1. **Métriques clés** :
    - Taux de succès UAR
    - Taux de succès LIR
    - Latence moyenne des requêtes
    - Distribution S-CSCF (équilibrage de charge)
    - Disponibilité du pair Diameter
2. **Requêtes Prometheus** :

```
# Taux de succès UAR
rate(icscf_uar_success[5m]) / rate(icscf_uar_total[5m])

# Latence moyenne Diameter
rate(diameter_request_duration_sum[5m]) /
rate(diameter_request_duration_count[5m])
```

3. **Alertes** :
    - Pair HSS hors service
    - Tous les S-CSCF indisponibles
    - Taux d'erreur élevé (>5%)

Maintenance de la base de données

La maintenance de la base de données est gérée par les administrateurs système. Les tâches de maintenance clés comprennent :

1. **Maintenir la liste des S-CSCF à jour** : Coordonnez-vous avec les administrateurs pour garantir que la liste des S-CSCF dans la base de données correspond aux déploiements réels
    - Vérifiez via l'interface Web : Naviguez vers I-CSCF → Onglet Liste des S-CSCF
    - Vérifiez que tous les serveurs S-CSCF actifs sont listés avec les bonnes capacités
2. **Élaguer les anciennes sessions** : Si les résultats UAR/LIR sont mis en cache, les anciennes entrées doivent être nettoyées périodiquement

Référence

Spécifications 3GPP

- **TS 23.228** : Architecture IMS
- **TS 29.228** : Interface Cx (I-CSCF vers HSS)

- **TS 29.229** : Protocole Cx/Dx

RFC Diameter

- **RFC 6733** : Protocole de base Diameter
- **RFC 7155** : Traversée NAT Diameter

Guide des opérations P-CSCF/E-CSCF

Table des matières

1. Aperçu
2. Rôle dans l'architecture IMS
3. Fonctions P-CSCF
4. Fonctions E-CSCF
5. Opérations de l'interface Web
6. Flux d'appels
7. Dépannage

Aperçu

Le **P-CSCF** (Proxy Call Session Control Function) est le premier point de contact pour l'équipement utilisateur (UE) dans le réseau IMS. Il sert de proxy de bord qui gère la sécurité, l'application de la QoS et le routage des appels d'urgence. Dans cette implémentation, le P-CSCF fonctionne également comme l'**E-CSCF** (Emergency CSCF) pour les services d'urgence.

Important : Dans nos déploiements, **le P-CSCF ne relaie pas les médias par défaut**. Les flux multimédias circulent directement entre l'UE et **OmniTAS** (Telephony Application Server) ou d'autres points de terminaison multimédias. Le P-CSCF est purement un proxy de signalisation SIP.

Spécifications 3GPP

- **3GPP TS 23.228** : Système multimédia IP (IMS) Étape 2
- **3GPP TS 24.229** : Protocole de contrôle d'appel IMS
- **3GPP TS 33.203** : Sécurité d'accès pour IMS
- **3GPP TS 23.167** : Sessions d'urgence du système multimédia IP (IMS)

Responsabilités clés

1. **Premier point de contact** : Proxy SIP initial de l'UE dans IMS
2. **Application de la sécurité** : Établissement et gestion de tunnels IPsec
3. **Contrôle de la QoS** : Interfaces avec PCRF via Rx pour l'application des politiques
4. **Services d'urgence** : Route les appels d'urgence et fournit la recherche IMEI vers MSISDN (fonction E-CSCF)
5. **Compression** : Support SigComp pour l'optimisation de la bande passante
6. **Support de transport** : Supporte UDP et TCP

Rôle dans l'architecture IMS

Position dans le réseau

Points de référence 3GPP

Interface	Protocole	Objectif	Connecté à
Gm	SIP/IPsec	UE vers P-CSCF	Équipement Utilisateur
Mw	SIP	P-CSCF vers I-CSCF/S-CSCF	Noyau IMS
Rx	Diameter	Contrôle QoS/Politique	PCRF
Ml	HTTP/HELD	Récupération de localisation	LRF (E-CSCF)
Mg	SIP	Appels d'urgence	MGCF/E-CSCF

Fonctions P-CSCF

1. Gestion des enregistrements

Le P-CSCF est le premier saut pour les messages SIP REGISTER provenant des UE.

Flux d'enregistrement

Caractéristiques clés

Insertion de l'en-tête Path :

```
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
```

- Assure que les demandes suivantes retournent via P-CSCF
- Requis selon la RFC 3327 pour IMS

Application du minuteur d'enregistrement :

- Force l'expiration de l'enregistrement à 599 secondes
- Remplace les valeurs demandées par l'UE pour le contrôle du réseau

Extraction de l'IMEI :

- Extrait l'IMEI de l'en-tête Contact : `+sip.instance="<urn:gsma:imei:...>"`
- Stocke dans une table de hachage pour le mappage des appels d'urgence

Gestion spécifique au transport :

- Appareils iOS : Prolonge la durée de vie TCP pour éviter la déconnexion prématurée

2. Fonctions de sécurité

Gestion des tunnels IPsec

Le P-CSCF établit des tunnels IPsec ESP avec les UE pour une signalisation SIP sécurisée.

Configuration IPsec :

La fonctionnalité IPsec est configurée avec les paramètres suivants :

- **Adresse d'écoute** : 10.4.12.165 (adresse IP du P-CSCF pour les points de terminaison IPsec)
- **Port client (de base)** : 5100 (port de départ pour le trafic UE → P-CSCF)
- **Port serveur (de base)** : 6100 (port de départ pour le trafic P-CSCF → UE)
- **Plage de ports** : Pool de ports configurable (typiquement 1000-10000 ports)
- **Début de l'ID SPI** : 4096 (valeur de départ pour l'allocation de l'index de paramètre de sécurité)
- **Plage d'ID SPI** : 100000 (nombre de paires SPI disponibles pour allocation)
- **Max connexions** : 20 (maximum d'associations de sécurité IPsec simultanées par travailleur)

Gestion des SPI et des ports

Chaque tunnel IPsec entre un UE et le P-CSCF nécessite des identifiants uniques pour garder le trafic séparé et sécurisé. Le système gère deux types de ressources :

Index de paramètres de sécurité (SPI) :

Chaque tunnel IPsec utilise DEUX SPI - un pour chaque direction :

- **spi-c** (SPI client) : Identifie les paquets envoyés de l'UE vers le P-CSCF
- **spi-s** (SPI serveur) : Identifie les paquets envoyés du P-CSCF vers l'UE

Les SPI sont alloués par paires à partir d'un pool configuré. Le système est généralement configuré avec :

- Valeur SPI de départ : 4096
- Plage disponible : 100000 valeurs SPI
- Cela permet une capacité de 50000 tunnels simultanés (les paires sont allouées comme des nombres consécutifs pairs/impairs)

Allocation de ports :

Chaque tunnel utilise également des ports UDP uniques sur le P-CSCF :

- **port client** : Port P-CSCF où il reçoit des paquets IPsec de l'UE
- **port serveur** : Port P-CSCF où il envoie des paquets IPsec à l'UE

Configuration typique des ports :

- Valeur de départ du port client : 5100
- Valeur de départ du port serveur : 6100
- Plage de ports : 10000 ports disponibles
- Les ports reviennent au début lorsque la plage est épuisée

Comment fonctionne l'allocation des ressources :

Lorsqu'un UE s'enregistre et demande une protection IPsec :

1. **Premier enregistrement** : Obtient spi-c=4096, spi-s=4097, port client=5100, port serveur=6100
2. **Deuxième enregistrement** : Obtient spi-c=4098, spi-s=4099, port client=5101, port serveur=6101
3. **Troisième enregistrement** : Obtient spi-c=4100, spi-s=4101, port client=5102, port serveur=6102

Et ainsi de suite...

Après 10000 enregistrements, les ports reviennent au début (5100, 6100), tandis que les SPI continuent d'incrémenter. Cela permet plus de tunnels que de ports disponibles, tant que les UE ont des adresses IP différentes.

Limites de ressources :

Le nombre maximum de tunnels IPsec simultanés est déterminé par la première limite atteinte :

- Capacité de la plage SPI (typiquement 50000 paires)
- Capacité de la plage de ports (typiquement 10000 ports)
- Mémoire système et capacité de traitement

Surveillance via l'interface Web :

Accédez à la page P-CSCF → Statistiques IPsec (si disponible) pour voir :

- Nombre de tunnels IPsec actifs
- Nombre de paires SPI/port disponibles
- Pourcentage d'utilisation

Si vous voyez des échecs d'enregistrement avec des erreurs liées à IPsec, cela peut indiquer :

- Épuisement du pool SPI (toutes les 50000 paires en cours d'utilisation)
- Épuisement du pool de ports (tous les 10000 ports en cours d'utilisation)

- Anciens tunnels qui ne sont pas nettoyés correctement

Lorsque les ressources sont libérées :

Les SPI et ports sont retournés au pool disponible lorsque :

- Un UE se désenregistre (envoie REGISTER avec Expires: 0)
- Un enregistrement expire sans être rafraîchi
- Un tunnel IPsec est détruit manuellement via l'interface Web
- L'administrateur système nettoie les tunnels obsolètes

Planification de capacité :

Pour la planification de déploiement :

- Chaque tunnel actif utilise environ 1 Ko de mémoire
- Un déploiement de production typique prend en charge 10000-50000 tunnels simultanés
- Surveillez les tendances d'utilisation pour prédire quand une expansion de capacité est nécessaire
- Si vous dépassez régulièrement 80 % d'utilisation, coordonnez-vous avec les administrateurs système pour augmenter les plages SPI/port

Configuration de l'association de sécurité (SA) :

1. L'UE envoie REGISTER avec l'en-tête `Security-Client` :

   ```
   Security-Client: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                    spi-c=12345; spi-s=67890; port-c=5100; port-
   s=6100
   ```

2. Le P-CSCF répond avec `Security-Server` :

   ```
   Security-Server: ipsec-3gpp; alg=hmac-sha-1-96; ealg=null;
                    spi-c=11111; spi-s=22222; port-c=5100; port-
   s=6100
   ```

3. Le P-CSCF crée des politiques IPsec en utilisant `setkey` :

   ```
   # Client vers Serveur
   spdadd <ue-ip>[5100] <pcscf-ip>[6100] any -P out ipsec esp/
   transport//require;

   # Serveur vers Client
   spdadd <pcscf-ip>[6100] <ue-ip>[5100] any -P in ipsec esp/
   transport//require;
   ```

4. Tous les messages SIP suivants utilisent le tunnel IPsec

Algorithmes pris en charge :

- **Authentification** : hmac-md5-96, hmac-sha-1-96
- **Chiffrement** : null, des-ede3-cbc, aes-cbc (préféré : null pour LTE)

3. Gestion des médias

Note importante : Dans nos déploiements, **le P-CSCF ne relaie PAS les médias par défaut**. Les médias (RTP/SRTP) circulent directement de l'UE à **OmniTAS** (Telephony Application Server) ou d'autres points de terminaison multimédias. Le P-CSCF ne gère que la signalisation SIP.

Les médias circulent directement entre les UE et l'OmniTAS (Telephony Application Server), contournant complètement le P-CSCF pour le trafic RTP/SRTP :

```
UE <------ SIP ------> P-CSCF <------ SIP ------> S-CSCF <------ SIP
------> OmniTAS
    <---------------------- RTP/SRTP (direct vers TAS)
---------------------->
```

Le P-CSCF ne gère que la signalisation SIP. Tous les médias (voix, vidéo) sont établis directement entre l'UE et OmniTAS.

4. Application de la QoS et des politiques (Interface Rx)

Intégration Diameter Rx

Objectif : Coordonner la QoS avec PCRF pour l'établissement de porteurs

Configuration Diameter :

Le P-CSCF se connecte au PCRF via Diameter sur le port 3868 en utilisant l'application Rx (ID d'application 16777236, ID de fournisseur 3GPP 10415).

Opérations Rx :

1. **AAR (Demande d'authentification d'autorisation)** : Demande QoS pour le flux multimédia
2. **AAA (Réponse d'authentification d'autorisation)** : Le PCRF accorde/refuse
3. **STR (Demande de terminaison de session)** : Libérer la QoS à la fin de l'appel

Flux de message AAR

Informations multimédias envoyées au PCRF :

- Description du flux (IP, port, protocole)
- Exigences de bande passante (montant/descendant)
- Type de média (audio, vidéo)
- État du flux (activé, désactivé)

5. Protection anti-inondation

Configuration du module Pike (Limitation de taux) : Le module pike fournit une protection contre les inondations avec ces paramètres :

- **Unité de temps d'échantillonnage** : 2 secondes - fenêtre de temps pour mesurer le taux de demande
- **Densité des demandes par unité** : 16 demandes autorisées par fenêtre de 2 secondes d'une seule IP
- **Latence de suppression** : 300 secondes (5 minutes) - durée pendant laquelle une IP est bloquée après avoir dépassé la limite

Suivi des échecs d'authentification : Le P-CSCF suit les tentatives d'authentification échouées pour prévenir les attaques par force brute :

- Maintient un compteur de table de hachage pour les tentatives d'authentification échouées par IP source
- Incrémente le compteur en cas d'échec d'authentification avec une expiration de 120 secondes
- Si une IP dépasse 10 tentatives échouées dans les 120 secondes, bloque l'IP avec 403 Trop de tentatives échouées
- Empêche les attaquants de deviner les identifiants des utilisateurs

Fonctions E-CSCF

Le P-CSCF inclut la fonctionnalité E-CSCF pour la gestion des appels d'urgence.

Détection des appels d'urgence

URI SIP reconnues :

- `urn:service:sos` (urgence générale)
- `urn:service:sos.police`
- `urn:service:sos.ambulance`
- `urn:service:sos.fire`
- `urn:service:sos.marine`
- `urn:service:sos.mountain`

Logique de détection : Les appels d'urgence sont détectés en examinant le Request-URI :

- Vérifie si la méthode est INVITE (demande de configuration d'appel)
- Vérifie si le Request-URI correspond aux modèles d'urgence :

    - Format URN : urn:service:sos* (URNs SOS définis dans la RFC 5031)
    - Urgence nord-américaine : 911
    - Urgence européenne/internationale : 112
- Si un appel d'urgence est détecté, il est routé vers le bloc de gestion des URGENCES pour un traitement spécial

Mappage IMEI vers MSISDN pour les appels d'urgence

Pourquoi cela est nécessaire : Lorsque les utilisateurs passent des appels d'urgence (par exemple, 911, 112, urn:service:sos), l'UE ne **fournit souvent pas le MSISDN (numéro de téléphone)** dans le message SIP. Les services d'urgence (PSAP - Public Safety Answering Point) ont besoin de connaître le numéro de téléphone de l'appelant à des fins de rappel. Pour résoudre ce problème, le P-CSCF/E-CSCF maintient un mappage de l'IMEI (identifiant de l'appareil) vers le MSISDN.

Comment cela fonctionne :

1. **Lors de l'enregistrement** (lorsque le MSISDN est connu) :
    - Extrait l'IMEI de l'en-tête Contact avec le paramètre +sip.instance (format : urn:gsma:imei:123456-78-901234-5)
    - Extrait le MSISDN de l'identité publique de l'utilisateur (IMPU) dans le nom d'utilisateur de l'en-tête From
    - Stocke le mappage IMEI → MSISDN dans une table de hachage avec un TTL de 24 heures (86400 secondes)
    - Exemple : imei_msisdn["urn:gsma:imei:123456789012345"] = "12015551234"
    - **Dans les déploiements en cluster** : Réplique automatiquement le mappage à tous les autres nœuds P-CSCF dans le cluster
2. **Lors de l'appel d'urgence** (lorsque le MSISDN peut manquer) :
    - Extrait l'IMEI de l'en-tête Contact de l'appel d'urgence avec le paramètre +sip.instance
    - Effectue une recherche dans la table de hachage pour récupérer le MSISDN associé à cet IMEI
    - Si le MSISDN est trouvé dans le mappage :
        - Ajoute l'en-tête P-Asserted-Identity avec le MSISDN complet (sip:+12015551234@domain)
        - Cela fournit au PSAP le numéro de rappel pour l'appelant d'urgence

Haute disponibilité - Synchronisation multi-nœuds :

Dans les déploiements de production avec plusieurs nœuds P-CSCF pour la redondance, les mappages IMEI→MSISDN sont automatiquement synchronisés entre tous les nœuds :

Comportement de réplication en cluster :

Lorsqu'un UE s'enregistre sur **P-CSCF Node 1** :

1. Le nœud 1 crée le mappage IMEI→MSISDN localement
2. Le nœud 1 diffuse immédiatement le mappage à tous les autres nœuds P-CSCF dans le cluster
3. **P-CSCF Node 2**, **Node 3**, etc. reçoivent la mise à jour et créent des copies locales identiques
4. Tous les nœuds ont maintenant le même mappage IMEI→MSISDN

Pourquoi cela importe :

Si un UE s'est enregistré via P-CSCF Node 1 mais passe un appel d'urgence qui est routé vers P-CSCF Node 2 (en raison de l'équilibrage de charge ou de la bascule), le nœud 2 a déjà le mappage IMEI→MSISDN et peut fournir le numéro de rappel au PSAP.

Mécanisme de synchronisation :

La synchronisation se fait via des messages basés sur SIP entre les nœuds P-CSCF :

- Utilise des messages SIP personnalisés pour propager les mises à jour de la table de hachage
- Les messages sont envoyés au format JSON contenant l'IMEI, le MSISDN et le TTL
- La transmission est automatique et transparente - aucune intervention de l'opérateur n'est nécessaire
- Les mises à jour sont diffusées à tous les membres du cluster en quelques millisecondes

Impact sur les opérations :

- **Résilience** : Les appels d'urgence fonctionnent correctement, quel que soit le nœud P-CSCF qui gère l'appel
- **Pas de point de défaillance unique** : Tout nœud P-CSCF peut fournir le numéro de rappel pour tout UE enregistré
- **Automatique** : La synchronisation est intégrée et ne nécessite aucune configuration ou intervention manuelle
- **Surveillance** : Via l'interface Web, accédez à P-CSCF → Tables de hachage → imei_msisdn pour voir les mappages sur chaque nœud

Exigences de configuration en cluster :

Pour que la synchronisation de la table de hachage fonctionne :

- Tous les nœuds P-CSCF doivent être configurés avec les adresses des autres

- Les nœuds se découvrent automatiquement via des notifications de disponibilité
- La connectivité réseau doit permettre le trafic SIP entre tous les nœuds P-CSCF
- Si la synchronisation échoue, vérifiez que les règles de pare-feu permettent la communication entre nœuds

Scénario d'exemple :

```
1. L'utilisateur s'enregistre : IMEI=123456789012345,
MSISDN=12015551234
   → Stocké : imei_msisdn[123456789012345] = 12015551234

2. L'utilisateur compose le 911 : INVITE urn:service:sos (MSISDN non
dans l'en-tête From)
   → P-CSCF extrait l'IMEI de Contact : 123456789012345
   → P-CSCF recherche : imei_msisdn[123456789012345] → 12015551234
   → P-CSCF ajoute l'en-tête : P-Asserted-Identity:
<sip:+12015551234@...>
   → PSAP reçoit l'appel avec le numéro de rappel : +12015551234
```

Routage d'urgence

Fonctionnalités des appels d'urgence :

- Contourne la vérification d'enregistrement
- Ajoute PIDF-LO (Format de données de présence - Objet de localisation)
- Route vers le serveur d'application d'urgence ou PSAP
- Gestion prioritaire (prévient les appels normaux)
- Informations de localisation provenant de LRF ou de l'UE

Opérations de l'interface Web

Accéder à la page P-CSCF

Accédez à : `https://<control-panel>/pcscf`

Mise en page de la page

La page P-CSCF a trois onglets principaux :

1. **Contacts enregistrés** - Enregistrements actifs
2. **Localisation de l'utilisateur** - Recherche par IMSI/IP
3. **Tables de hachage** - Tables de mémoire partagée

Affichage des contacts enregistrés

Colonnes d'affichage :

- **AoR** (Adresse d'enregistrement) : Identité SIP de l'utilisateur
- **Contact** : URI de contact de l'appareil
- **Expires** : Horodatage d'expiration de l'enregistrement
- **IP publique** : Adresse IP publique de l'UE
- **Reçu** : IP réellement reçue (si différente de Contact)
- **Path** : En-tête Path pour le routage
- **ID de session Rx** : ID de session Diameter Rx (si QoS active)

Fonctionnalités :

- Actualisation automatique toutes les 5 secondes
- Recherche par AoR ou Contact partiel
- Tri par colonne (cliquer sur l'en-tête)
- Lignes extensibles pour des détails complets

Exemple de sortie :

```
AoR: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Contact: sip:12015551234@10.4.12.100:5060;transport=udp
Expires: 2025-11-29 14:30:15
IP publique: 10.4.12.100
Reçu: 10.4.12.100:52341
Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
ID de session Rx: rx-pcscf-session-12345
```

Recherche de la localisation de l'utilisateur

Options de recherche :

- Par IMSI : `imsi:310150123456789`
- Par IP : `10.4.12.100`

Cas d'utilisation :

1. Trouver quel utilisateur utilise une IP spécifique
2. Vérifier si l'IMSI est enregistré
3. Vérifier l'état du tunnel IPsec
4. Vérifier les routes de service

Gestion des tables de hachage

Tables communes :

Table	Objectif	Taille typique
`imei_msisdn`	Mappage d'urgence IMEI→MSISDN	100-1000 entrées
`service_routes`	Routes de service mises en cache	Par enregistrement
`dialog_out`	Suivi des dialogues sortants	Par appel

Opérations :

- **Lister les tables** : Cliquez sur l'onglet "Tables de hachage"
- **Dumper la table** : Cliquez sur le nom de la table pour voir le contenu
- **Supprimer une entrée** : Cliquez sur "Supprimer" à côté de l'entrée
- **Vider la table** : Cliquez sur "Vider" pour effacer toute la table (utilisez avec prudence !)

Exemple d'entrée :

```
Clé:   urn:gsma:imei:123456-78-901234-5
Valeur: 310150123456789
TTL:   86400 secondes (24 heures)
```

Flux d'appels

Appel d'origine mobile (MO)

Tous les appels d'origine sont routés via le TAS (OmniTAS) pour la logique de service et la facturation :

Appel de terminaison mobile (MT)

Les appels de terminaison passent également par le TAS pour la logique de service :

Flux d'appel d'urgence

Dépannage

Problèmes d'enregistrement

UE ne peut pas s'enregistrer

Symptômes : L'UE reçoit 408 Timeout ou aucune réponse

Étapes de diagnostic :

1. Vérifiez l'état de l'enregistrement via le panneau de contrôle :
    - Accédez à la page P-CSCF

    - Vérifiez l'onglet "Contacts enregistrés"
    - Vérifiez que l'utilisateur apparaît dans la liste

2. Examinez les journaux système via la page des journaux du panneau de contrôle pour des erreurs

3. Vérifiez la connectivité réseau entre l'UE et le P-CSCF

4. Vérifiez que les règles de pare-feu permettent le trafic SIP (port 5060 UDP/TCP)

5. Coordonnez-vous avec les administrateurs système si le service P-CSCF semble être hors service

Tunnel IPsec non établi

Symptômes : Défi 401 envoyé mais le re-REGISTER échoue

Étapes de diagnostic :

1. Examinez les journaux système via la page des journaux du panneau de contrôle pour des erreurs liées à IPsec

2. Vérifiez que l'UE envoie l'en-tête Security-Client dans le REGISTER initial

3. Vérifiez que l'UE utilise les ports IPsec (5100 client, 6100 serveur) dans le re-REGISTER

4. Vérifiez que l'adresse reçue correspond au point de terminaison IPsec attendu

5. Coordonnez-vous avec les administrateurs système pour vérifier que les modules du noyau IPsec sont chargés et qu'aucun conflit de port n'existe

Problèmes d'appels

Les appels ne sont pas routés vers l'UE

Symptômes : INVITE vers P-CSCF mais l'UE ne sonne pas

Étapes de diagnostic :

1. Vérifiez que l'enregistrement existe via le panneau de contrôle :

    - Accédez à la page P-CSCF
    - Vérifiez l'onglet "Contacts enregistrés"
    - Recherchez l'utilisateur et vérifiez que l'enregistrement est actif

2. Vérifiez que l'en-tête Path a été stocké dans l'enregistrement
3. Vérifiez que les appels sont envoyés à la bonne adresse de contact
4. Examinez les journaux système pour des erreurs de routage
5. Vérifiez que le chemin réseau du P-CSCF vers l'UE est accessible

Audio unidirectionnel

Symptômes : Une partie ne peut pas entendre l'autre

Note : Dans nos déploiements, **le P-CSCF ne relaie pas les médias**. Les médias circulent directement entre l'UE et OmniTAS. Si vous rencontrez un audio unidirectionnel, le problème est probablement aux points de terminaison ou dans le routage réseau, et non au P-CSCF.

Étapes de diagnostic :

1. Vérifiez que le SDP dans INVITE/200 OK contient les bonnes adresses IP et ports (examinez via les journaux système ou la capture de paquets si disponible pour les administrateurs)
2. Vérifiez que les règles de pare-feu permettent le trafic RTP/SRTP entre l'UE et OmniTAS
3. Vérifiez la configuration NAT si l'UE est derrière un NAT
4. Vérifiez que le point de terminaison multimédia OmniTAS est accessible depuis l'UE (connectivité réseau)
5. Coordonnez-vous avec les administrateurs système pour une analyse de capture de paquets si nécessaire

Les appels d'urgence échouent

Symptômes : Les appels urn:service:sos sont rejetés

Étapes de diagnostic :

1. Vérifiez la table de hachage IMEI→MSISDN via le panneau de contrôle :
    - Accédez à P-CSCF → Onglet Tables de hachage
    - Vérifiez que la table `imei_msisdn` contient des entrées
    - Vérifiez que l'IMEI de l'appelant a un mappage
2. Testez d'abord avec un utilisateur enregistré effectuant un appel d'urgence (pour isoler les problèmes d'enregistrement par rapport aux problèmes de

routage d'urgence)

3. Examinez les journaux système via la page des journaux du panneau de contrôle pour des erreurs de routage d'urgence

4. Vérifiez la configuration du serveur d'application d'urgence

5. Coordonnez-vous avec les administrateurs système pour examiner la configuration de la route d'urgence si nécessaire

Problèmes de performance

Utilisation élevée du CPU

Causes possibles :

- Trop d'enregistrements
- Déclenchement de l'anti-inondation Pike
- Requêtes lentes de la base de données

Solutions :

1. Vérifiez le nombre d'enregistrements via le panneau de contrôle :
    - Accédez à P-CSCF → Onglet Contacts enregistrés
    - Examinez le nombre total d'enregistrements actifs

2. Examinez les journaux système pour des blocages anti-inondation Pike

3. Coordonnez-vous avec les administrateurs système pour une mise à l'échelle horizontale (ajouter plus d'instances P-CSCF) si nécessaire

Utilisation élevée de la mémoire

Causes possibles :

- Croissance de la table de hachage
- Table de dialogue non nettoyée
- Fuite de mémoire

Solutions :

1. Examinez les tables de hachage via le panneau de contrôle :
    - Accédez à P-CSCF → Onglet Tables de hachage
    - Vérifiez les tailles de table et les comptes d'entrées

2. Effacez les anciennes entrées via le panneau de contrôle :

    - Sélectionnez la table de hachage problématique
    - Utilisez l'opération "Vider" si nécessaire (utilisez avec prudence - efface toute la table)

3. Coordonnez-vous avec les administrateurs système pour redémarrer le service P-CSCF si une fuite de mémoire est suspectée

Problèmes Diameter/Rx

Pair PCRF fermé

Symptômes : Le pair Diameter montre un état "Fermé" dans l'interface Web

Étapes de diagnostic :

1. Vérifiez l'état du pair Diameter via le panneau de contrôle :
    - Accédez à la page Diameter
    - Sélectionnez le nœud P-CSCF
    - Vérifiez l'état du pair PCRF (devrait être "I_Open" lorsqu'il est connecté)
2. Vérifiez la connectivité réseau vers le PCRF (coordonnez-vous avec l'équipe réseau si nécessaire)
3. Essayez d'activer le pair via le panneau de contrôle :
    - Accédez à la page Diameter
    - Trouvez le pair PCRF
    - Cliquez sur le bouton "Activer"
4. Examinez les journaux système via la page des journaux du panneau de contrôle pour des erreurs de connexion Diameter
5. Coordonnez-vous avec les administrateurs système pour vérifier la configuration Diameter si nécessaire

La QoS ne fonctionne pas

Symptômes : Les appels se connectent mais aucun porteur QoS n'est établi

Étapes de diagnostic :

1. Examinez les journaux système via le panneau de contrôle pour les messages AAR (Demande d'authentification d'autorisation) et AAA (Réponse d'authentification d'autorisation)
2. Vérifiez le code de résultat de la réponse PCRF (devrait être 2001 pour le

succès)

3. Vérifiez que le pair PCRF est connecté (voir section précédente)

4. Vérifiez que les informations multimédias dans le SDP sont correctement envoyées au PCRF

5. Coordonnez-vous avec les administrateurs système pour vérifier la configuration QoS si nécessaire

Meilleures pratiques

Sécurité

1. **Utilisez toujours IPsec** pour les appareils mobiles (LTE/5G)
2. **Activez TLS** pour les clients fixes/entreprises
3. **Configurez l'anti-inondation** (Pike) pour la protection contre les DoS
4. **Limitez les tentatives d'authentification échouées** pour prévenir la force brute
5. **Utilisez des chiffrements forts** pour TLS (désactivez SSLv2/v3)
6. **Faites régulièrement tourner** les clés IPsec (via le re-enregistrement)

Performance

1. **Ajustez hash_size** en fonction des enregistrements attendus :

    - 1000 utilisateurs : hash_size=10 (crée 2^10 = 1024 seaux de hachage)
    - 10000 utilisateurs : hash_size=13 (crée 2^13 = 8192 seaux de hachage)
    - 100000 utilisateurs : hash_size=16 (crée 2^16 = 65536 seaux de hachage)

2. **Ajustez les processus de travail** en fonction des cœurs CPU :

    - Réglez les enfants pour correspondre au nombre de cœurs CPU pour le traitement SIP
    - Réglez tcp_children à 2× cœurs CPU pour la gestion des connexions TCP

3. **Utilisez mlock_pages** pour prévenir l'échange :

    - Activez mlock_pages=yes pour verrouiller les pages de mémoire partagée dans la RAM
    - Empêche la dégradation des performances due à l'échange de mémoire sur disque

4. **Désactivez le cache DNS** pour les environnements IMS :

- Réglez dns_cache_init=off pour utiliser des recherches DNS fraîches
- Nécessaire pour l'équilibrage de charge dynamique basé sur DNS SRV

5. **Activez l'équilibrage de charge SRV** :
   - Réglez dns_srv_lb=yes pour distribuer le trafic sur plusieurs serveurs
   - Utilise les enregistrements DNS SRV pour la distribution automatique de la charge

Surveillance

1. **Activez les métriques Prometheus** (port 9090 dans la config) - Voir Référence des métriques pour toutes les métriques P-CSCF disponibles
2. **Surveillez les tendances du nombre d'enregistrements**
3. **Suivez la santé des pairs Diameter** (Rx vers PCRF)
4. **Alertez sur les taux d'erreur élevés** dans les journaux
5. **Surveillez le nombre de dialogues** (sessions actives)
6. **Vérifiez régulièrement l'utilisation de la mémoire**

Haute disponibilité

1. **Déployez plusieurs instances P-CSCF**

2. **Utilisez DNS SRV** pour l'équilibrage de charge :

```
_sip._udp.pcscf.example.com. SRV 10 50 5060 pcscf01.example.com.
_sip._udp.pcscf.example.com. SRV 10 50 5060 pcscf02.example.com.
```

3. **Évitez l'état** lorsque cela est possible (proxy sans état)

4. **Utilisez une base de données partagée** pour les données persistantes (si nécessaire)

5. **Surveillez via l'interface Web** en utilisant les vérifications de santé du panneau de contrôle

Services d'urgence

1. **Toujours autoriser** les appels d'urgence même s'ils ne sont pas enregistrés
2. **Stockez le mappage IMEI→MSISDN** lors de l'enregistrement
3. **Définissez le TTL** pour la table de hachage d'urgence (86400 = 24 heures)
4. **Testez régulièrement** avec le PSAP de test
5. **Assurez-vous de la connectivité LRF** pour la localisation
6. **Gestion prioritaire** pour les appels d'urgence

Référence

Ressources techniques supplémentaires

Pour les administrateurs système et les développeurs, la documentation technique des modules est disponible en ligne pour les composants logiciels sous-jacents.

Spécifications 3GPP

- **TS 23.228** : Architecture IMS
- **TS 24.229** : Profil SIP IMS
- **TS 33.203** : Sécurité d'accès
- **TS 23.167** : Services d'urgence
- **TS 29.214** : Interface Rx (PCRF)

RFCs

- **RFC 3261** : SIP
- **RFC 3327** : En-tête Path
- **RFC 3608** : En-tête Service-Route
- **RFC 3GPP-IMS** : P-En-têtes (P-Asserted-Identity, etc.)
- **RFC 5626** : Sortant (gestion de connexion)

Guide des opérations S-CSCF

Table des matières

1. Aperçu
2. Rôle dans l'architecture IMS
3. Fonctions S-CSCF
4. Opérations de l'interface Web
5. Flux d'appels
6. Dépannage

Aperçu

Le **S-CSCF** (Serving Call Session Control Function) est le serveur de contrôle de session central dans le cœur IMS. Il effectue l'enregistrement, l'authentification, le routage des sessions et le déclenchement des services. Le S-CSCF est le registraire autoritaire pour les utilisateurs dans son réseau domestique et maintient un état de session complet pour tous les appels.

Spécifications 3GPP

- **3GPP TS 23.228** : Système multimédia IP (IMS) Étape 2
- **3GPP TS 24.229** : Protocole de contrôle d'appel IMS
- **3GPP TS 29.228** : Interface Cx (S-CSCF vers HSS)
- **3GPP TS 29.229** : Protocoles Cx et Dx
- **3GPP TS 23.218** : Interface ISC (S-CSCF vers AS)
- **3GPP TS 32.260** : Facturation IMS

Responsabilités clés

1. **Autorité d'enregistrement** : Registraire SIP autoritaire pour les utilisateurs du réseau domestique
2. **Authentification** : Valide les informations d'identification de l'utilisateur via le HSS
3. **Routage des sessions** : Route les appels entrants et sortants
4. **Déclenchement de services** : Invoque les serveurs d'applications en fonction des iFC (critères de filtrage initiaux)
5. **Gestion des profils utilisateurs** : Stocke et applique les profils de service du HSS
6. **Présence** : Gère les SUBSCRIBE/PUBLISH/NOTIFY pour les services de présence
7. **Interconnexion PSTN** : Route vers/depuis les réseaux PSTN hérités

Remarque sur la facturation : Bien que le S-CSCF ait la capacité d'effectuer une facturation en ligne via l'interface Ro vers un OCS (Système de facturation en ligne), **dans nos déploiements, cette fonctionnalité est généralement désactivée**. La facturation est plutôt gérée par le **TAS (Serveur d'applications de téléphonie)** où elle peut correctement tenir compte de scénarios complexes tels que le renvoi d'appels, le transfert d'appels, l'itinérance sur les réseaux 2G/3G et d'autres services supplémentaires que le S-CSCF seul ne peut pas suivre avec précision.

Caractéristiques clés

- **Avec état** : Maintient l'état complet du dialogue
- **Logique de service** : Exécute des règles de routage complexes et des déclencheurs de service
- **Intégration HSS** : Synchronisation continue avec la base de données des utilisateurs
- **Interface de serveur d'applications** : ISC (Contrôle de service IMS)
- **CSCF le plus complexe** : Configuration la plus importante et le plus de fonctionnalités

Rôle dans l'architecture IMS

Position dans le réseau

Points de référence 3GPP

Interface	Protocole	Objectif	Connecté à
Mw	SIP	I-CSCF/P-CSCF vers S-CSCF	I-CSCF, P-CSCF
ISC	SIP	S-CSCF vers Serveur d'application	AS, TAS
Cx	Diameter	Données utilisateur, authentification, enregistrement	HSS
Ro	Diameter	Facturation en ligne (temps réel)	OCS
Rf	Diameter	Facturation hors ligne (CDR)	CDF/CGF
Mi	SIP	S-CSCF vers BGCF	BGCF (routage PSTN)

Fonctions S-CSCF

1. Enregistrement et authentification

Le S-CSCF est le registraire autoritaire qui valide les informations d'identification des utilisateurs et stocke les liaisons d'enregistrement.

Flux d'enregistrement avec authentification

Algorithmes d'authentification pris en charge

Configuration : Le S-CSCF est configuré avec les paramètres d'authentification suivants :

- Délai d'expiration des vecteurs d'authentification : 599 secondes
- Taille du hachage des données d'authentification : 1024 seaux
- Vérifie uniquement l'IMPU pour l'authentification (pas d'IMPI)

Algorithmes pris en charge :

- **AKAv1-MD5** : 3GPP AKA avec MD5 (le plus courant pour LTE/5G)
- **AKAv2-MD5** : AKA amélioré
- **MD5** : Digest HTTP
- **CableLabs-Digest** : PacketCable/IMS pour les réseaux câblés
- **3GPP-Digest** : Variante Digest-MD5
- **TISPAN-HTTP_DIGEST_MD5** : ETSI TISPAN
- **HSS-Selected** : Laisser le HSS choisir l'algorithme

Flux AKA :

1. **RAND** : Défi aléatoire (128 bits)
2. **AUTN** : Jeton d'authentification pour prouver l'identité du HSS
3. **XRES** : Réponse attendue de l'UE
4. **CK/IK** : Clé de chiffrement / Clé d'intégrité pour IPsec

Génération de nonce :

```
nonce = base64(RAND) + ":" + algorithm_indicator
```

Validation de la réponse :

```
UE_response = base64(RES)
Expected = base64(XRES)

if (UE_response == Expected) {
    # Succès de l'authentification
} else {
    # Échec de l'authentification
}
```

Re-synchronisation AKA

Si le numéro de séquence (SQN) de l'UE est désynchronisé avec le HSS :

Processus :

1. L'UE envoie AUTS (jeton de synchronisation d'authentification) dans l'en-tête d'autorisation
2. Le S-CSCF extrait AUTS de l'en-tête
3. Le S-CSCF envoie MAR (Demande d'authentification multimédia) avec AUTS au HSS
4. Le HSS resynchronise son numéro de séquence et envoie de nouveaux vecteurs d'authentification
5. Le S-CSCF reçoit de nouveaux vecteurs et continue le flux d'authentification

Paramètres d'enregistrement

Le S-CSCF est configuré avec les paramètres d'enregistrement suivants :

Temps d'expiration d'enregistrement :

- Expiration par défaut/min/max : 599 secondes (environ 10 minutes)
- Expiration par défaut/min/max d'abonnement : 599 secondes

Gestion des contacts :

- Contacts maximum par IMPU : 1 (enregistrement d'un seul appareil)
- Comportement de contact maximum : Écraser le plus ancien (lorsque la limite est dépassée, supprimer le contact le plus ancien)

2. Base de données de localisation utilisateur (USRLOC)

Le S-CSCF maintient une base de données des utilisateurs enregistrés et de leurs liaisons de contact.

Structure de la base de données

Le S-CSCF maintient plusieurs tables de base de données pour stocker les informations d'enregistrement et d'utilisateur :

Table IMPU : Stocke les identités publiques multimédias IP (les URI SIP avec lesquelles les utilisateurs s'enregistrent). Chaque IMPU a des attributs comme :

- Identité publique (sip:user@domain.com)
- Type (identité publique utilisateur vs. identité publique de service)
- Statut de restriction
- État d'enregistrement (enregistré/non enregistré)
- Adresses de fonction de facturation (CCF1, CCF2, ECF1, ECF2)

Table de contact IMPU : Stocke les liaisons de contact réelles pour chaque IMPU, y compris :

- URI de contact (où atteindre l'appareil)

- Temps d'expiration
- En-tête de chemin (route de retour via P-CSCF)
- Chaîne User-Agent
- Adresse reçue (IP réelle d'où provient l'enregistrement)

Table des abonnés : Mappe les IMPIs (Identités privées) à leurs IMPUs associés. Une identité privée peut avoir plusieurs identités publiques.

Table de profil de service : Stocke le profil utilisateur XML reçu du HSS lors de l'enregistrement, y compris les critères de filtrage initiaux (iFC) pour le déclenchement de services.

Configuration de la table de hachage

Le S-CSCF utilise une table de hachage en mémoire pour des recherches d'enregistrement rapides. Pour les déploiements avec plus de 20 000 utilisateurs, la taille du hachage doit être ajustée en conséquence (par exemple, 8 192 seaux pour ~50 000 utilisateurs) afin de maintenir les performances de recherche.

Gestion des enregistrements via l'interface Web

Toutes les opérations de localisation utilisateur peuvent être effectuées via l'**interface web du panneau de contrôle** à `/scscf` :

- **Onglet Liste d'enregistrement** : Voir tous les utilisateurs enregistrés avec pagination et recherche
- **Onglet Localisation utilisateur** : Interroger des détails spécifiques sur l'IMPU, y compris toutes les liaisons de contact
- **Actions rapides** : Recherche, désenregistrement, vidage IFC et test des opérations IFC

L'interface web fournit une vue en temps réel de l'état d'enregistrement, des liaisons de contact et permet des actions administratives telles que la désinscription forcée lorsque cela est nécessaire pour le dépannage.

3. Critères de filtrage initiaux (iFC) et déclenchement de services

Le S-CSCF évalue les **iFC** (critères de filtrage initiaux) du profil de service de l'utilisateur pour déterminer quand invoquer les serveurs d'applications.

Structure iFC (XML)

Exemple du profil utilisateur HSS :

```
<IMSSubscription>
  <PrivateID>user@ims.mnc001.mcc001.3gppnetwork.org</PrivateID>
```

```
  <ServiceProfile>
    <PublicIdentity>
      <Identity>sip:user@ims.mnc001.mcc001.3gppnetwork.org</Identity>
      <IdentityType>0</IdentityType>  <!-- 0=identité publique
utilisateur -->
    </PublicIdentity>

    <InitialFilterCriteria>
      <Priority>0</Priority>  <!-- Plus bas = plus haute priorité -->
      <TriggerPoint>
        <ConditionTypeCNF>1</ConditionTypeCNF>  <!-- 0=DNF, 1=CNF -->
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <Method>INVITE</Method>
        </SPT>
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <SessionCase>0</SessionCase>  <!-- 0=originaire -->
        </SPT>
      </TriggerPoint>
      <ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
        <DefaultHandling>0</DefaultHandling>  <!--
0=SESSION_CONTINUED, 1=SESSION_TERMINATED -->
      </ApplicationServer>
    </InitialFilterCriteria>

    <InitialFilterCriteria>
      <Priority>1</Priority>
      <TriggerPoint>
        <ConditionTypeCNF>0</ConditionTypeCNF>  <!-- DNF -->
        <SPT>
          <ConditionNegated>0</ConditionNegated>
          <Group>0</Group>
          <RequestURI>^sip:\+1800.*</RequestURI>  <!-- Numéro gratuit
-->
        </SPT>
      </TriggerPoint>
      <ApplicationServer>
        <ServerName>sip:tollfree-as.example.com</ServerName>
        <DefaultHandling>0</DefaultHandling>
      </ApplicationServer>
    </InitialFilterCriteria>
  </ServiceProfile>
</IMSSubscription>
```

Déclencheurs de point de service (SPT)

Types de SPT :

1. **Méthode** : Méthode SIP (INVITE, MESSAGE, SUBSCRIBE, etc.)
2. **RequestURI** : Regex sur Request-URI
3. **SIPHeader** : Vérifier la présence/valeur de l'en-tête SIP
4. **SessionCase** : Originaire (0), Terminant (1), Terminant non enregistré (2)
5. **SessionDescription** : Contenu SDP (type de média, codec, etc.)

Logique :

- **CNF** (Forme normale conjonctive) : ET d'OU - `(A OU B) ET (C OU D)`
- **DNF** (Forme normale disjonctive) : OU d'ET - `(A ET B) OU (C ET D)`

Groupe : Les SPT avec le même numéro de groupe sont combinés par OR, puis les groupes sont combinés par AND (pour CNF).

Flux de correspondance iFC

Test des iFC via l'interface Web

Le panneau de contrôle fournit deux opérations via l'interface web :

1. **Dump iFC** : Afficher tous les iFC pour un utilisateur - affiche la structure XML complète des points de déclenchement et du routage du serveur d'application

2. **Test iFC** : Simuler un appel pour voir quel AS serait déclenché - teste un scénario d'appel hypothétique avec un IMPU spécifié, une URI d'origine et une URI de destination pour déterminer quel iFC correspondrait

Flux de travail de l'interface Web :

1. Naviguer vers la page S-CSCF
2. Cliquer sur l'onglet "IFC"
3. Entrer l'IMPU
4. Choisir "Dump IFC" ou "Test IFC"
5. Voir la structure détaillée des iFC avec les points de déclenchement et le routage AS

4. Gestion des dialogues

Le S-CSCF maintient l'état complet du dialogue SIP pour tous les appels actifs.

Base de données de dialogue

Le S-CSCF maintient une table de dialogue qui suit les appels actifs avec les

informations suivantes :

- Call-ID (identifiant unique pour le dialogue SIP)
- URIs et tags From/To
- Numéros de séquence de l'appelant et du destinataire (CSeq)
- Ensembles de routes pour les deux parties
- Adresses de contact
- Informations sur les sockets
- État du dialogue et horodatages
- Valeurs de délai d'expiration

États de dialogue

Les dialogues passent par trois états :

- **Précoce** : Réponse provisionnelle reçue (par exemple, 180 Ringing)
- **Confirmé** : 200 OK reçu et ACK envoyé/reçu (appel actif)
- **Supprimé** : BYE envoyé/reçu (appel terminé)

Configuration du dialogue

Le module de dialogue est configuré pour :

- Détecter le routage en spirale (même demande passant plusieurs fois)
- Maintenir des profils séparés pour les côtés d'origine et de terminaison
- Persister les dialogues dans la base de données (mode d'écriture avec mises à jour périodiques)
- Définir des délais d'expiration spécifiques au dialogue
- Suivre les ensembles de routes pour un routage correct dans le dialogue

Opérations de l'interface Web :

1. Naviguer vers S-CSCF → Onglet Dialogues
2. Voir les appels actifs avec :
    - Call-ID
    - URIs From/To
    - État (Précoce/Confirmé)
    - Heure de début
    - Délai d'expiration
3. Cliquer sur "Fin de dialogue" pour terminer un appel spécifique
4. Cliquer sur "Fin de tous les dialogues actifs" pour une terminaison de masse d'urgence

5. Gestion des appels sortants

Lorsqu'un utilisateur enregistré initie un appel, le S-CSCF le traite comme une session **sortante**.

Flux d'appel sortant

Configuration de la route sortante

Traitement des appels sortants : Le S-CSCF effectue plusieurs étapes de validation et de routage lors du traitement des appels sortants :

1. **Vérification de l'enregistrement** : Vérifie que l'utilisateur appelant est actuellement enregistré. Si ce n'est pas le cas, l'appel est rejeté avec une réponse 403 Interdit.

2. **Gestion de l'en-tête d'identité** :

    - Supprime tous les en-têtes P-Asserted-Identity existants de la demande
    - Ajoute un nouvel en-tête P-Asserted-Identity contenant l'identité de l'appelant authentifié

3. **Corrélation de facturation** : Crée et ajoute un en-tête P-Charging-Vector contenant :

    - Identifiant de facturation IMS (icid) généré à partir du Call-ID et de l'horodatage
    - Identifiant inter-opérateur d'origine (orig-ioi) pour la facturation multi-opérateur

4. **Déclenchement de services** : Évalue les critères de filtrage initiaux (iFC) pour les déclencheurs de session sortante afin de déterminer si des serveurs d'applications doivent être invoqués

5. **Facturation en ligne** (si activée) : Initie une demande de contrôle de crédit Diameter Ro (CCR) avec le type d'événement "0" (demande initiale) pour les appels sortants

6. **Suivi du dialogue** : Assigne l'appel au profil de dialogue "orig" (sortant) à des fins de suivi

7. **Décision de routage** : Route l'appel soit vers le traitement PSTN (si la destination est un numéro de téléphone) soit vers l'ICSCF de terminaison pour le routage IMS

6. Gestion des appels entrants

Lorsqu'un appel est destiné à un utilisateur enregistré, le S-CSCF le traite comme **entrant**.

Flux d'appel entrant

Configuration de la route de terminaison

Traitement des appels entrants : Le S-CSCF gère les appels entrants en tentant d'abord de localiser l'utilisateur appelé, puis en appliquant la logique de service appropriée :

1. **Recherche de localisation utilisateur** : Interroge la base de données d'enregistrement pour déterminer si l'utilisateur appelé est actuellement enregistré
    - Utilise le nom d'utilisateur et le domaine de la Request-URI pour construire l'IMPU
    - Récupère les liaisons de contact et les informations de routage si enregistré
2. **Si l'utilisateur n'est PAS enregistré** :
    - Tente de récupérer le profil de service non enregistré du HSS via une demande d'attribution de serveur (SAR)
    - Si réussi, évalue les iFC pour les déclencheurs de session "terminant non enregistré" (par exemple, messagerie vocale, services hors ligne)
    - Si aucun service non enregistré n'est disponible, répond avec 480 Temporarily Unavailable
3. **Si l'utilisateur EST enregistré** :
    - Évalue les iFC pour les déclencheurs de session "terminant" afin de déterminer l'invocation du serveur d'application
    - Initie la facturation en ligne (si activée) en envoyant un CCR Diameter Ro avec le type d'événement "0" pour les appels entrants
    - Assigne l'appel au profil de dialogue "term" (terminant) pour le suivi
    - Transmet l'INVITE au P-CSCF enregistré en utilisant l'en-tête Path stocké lors de l'enregistrement

7. Interconnexion PSTN via OmniTAS

Le S-CSCF route les appels vers/depuis le PSTN via l'**interface Mi** vers le **BGCF (Fonction de contrôle de passerelle de sortie)**, qui est intégré dans OmniTAS dans notre déploiement.

Interface Mi - S-CSCF vers BGCF

Point de référence 3GPP : Mi (interface SIP entre S-CSCF et BGCF)

L'interface Mi est utilisée lorsque le S-CSCF détermine qu'un appel doit sortir

vers le PSTN. Dans notre architecture, la fonctionnalité BGCF est intégrée directement dans OmniTAS, donc tous les appels d'origine mobile (MO) destinés à des numéros PSTN sont routés vers OmniTAS.

Flux de routage PSTN

Comment fonctionne le routage PSTN :

1. **Détection du numéro de destination** : Le S-CSCF examine la Request-URI pour déterminer si la destination est un numéro de téléphone (format E.164 comme +12015551234)

2. **Routage vers OmniTAS** : Pour les destinations PSTN, le S-CSCF route l'appel via l'interface Mi vers OmniTAS, qui inclut une fonctionnalité BGCF intégrée

3. **Traitement BGCF dans OmniTAS** : OmniTAS détermine le point de sortie PSTN approprié en fonction de :

    - Analyse du numéro de destination (code pays, code régional)
    - Règles de routage à coût minimal
    - Groupes de troncs disponibles
    - Sélection du transporteur

4. **Sortie PSTN** : OmniTAS gère l'interaction réelle de la passerelle multimédia pour compléter l'appel vers le réseau PSTN

Détails de l'interface Mi :

- **Protocole** : SIP
- **Objectif** : Routage des appels destinés au PSTN du S-CSCF vers le BGCF
- **Direction** : S-CSCF → OmniTAS (avec BGCF)
- **Types d'appels** : Appels d'origine mobile (MO) vers des numéros PSTN

Configuration : Le S-CSCF est configuré pour reconnaître les destinations PSTN (numéros de téléphone) et les router vers OmniTAS. Lorsque OmniTAS est utilisé comme TAS (Serveur d'applications de téléphonie), il inclut intrinsèquement des capacités BGCF, éliminant ainsi le besoin d'un composant BGCF séparé.

8. Architecture de facturation

Le S-CSCF a la capacité intégrée d'interfacer avec un OCS (Système de facturation en ligne) via l'interface Diameter Ro pour le contrôle de crédit en temps réel. Cependant, **dans nos déploiements, la facturation S-CSCF est généralement désactivée** au profit de la facturation au niveau du **TAS (Serveur d'applications de téléphonie)**.

Pourquoi la facturation est-elle effectuée au niveau du TAS plutôt qu'au S-CSCF

Avantages de la facturation basée sur le TAS :

1. **Scénarios de renvoi d'appels** : Lorsque un appel est transféré, le S-CSCF ne voit que l'INVITE initial vers la destination d'origine. Il n'a pas de visibilité sur la logique de renvoi ou la destination finale. Le TAS, cependant, gère le service de renvoi et sait :
    - Qui a initié l'appel
    - Pour qui l'appel était à l'origine
    - Où l'appel a été transféré
    - Durée de l'appel transféré
    - Partie appropriée à facturer (appelant, transféré, ou les deux)
2. **Itinérance 2G/3G** : Lorsque les abonnés itinèrent sur des réseaux hérités 2G/3G, les appels peuvent contourner complètement le cœur IMS et passer par l'infrastructure à commutation de circuits. Le TAS s'intègre à la fois dans les domaines IMS et CS (commutation de circuits) et peut :
    - Détecter quand un abonné est en itinérance sur 2G/3G
    - Appliquer des frais d'itinérance appropriés
    - Suivre la durée des appels à travers les types de réseau
    - Gérer les transferts entre les domaines IMS et CS
3. **Transfert d'appels** : Semblable au renvoi d'appels, les transferts d'appels impliquent des changements en cours d'appel que le S-CSCF ne suit pas :
    - Transferts à l'aveugle (transfert immédiat)
    - Transferts assistés (consultation puis transfert)
    - Transfert vers la messagerie vocale
    - Transferts multi-parties
4. **Appels de conférence** : Les conférences multi-parties nécessitent une logique de facturation spéciale :
    - Qui a initié la conférence
    - Combien de participants
    - Durée pendant laquelle chaque participant était en ligne
    - Taux différents pour l'initiateur de la conférence par rapport aux participants
5. **Services supplémentaires** : Des services tels que la mise en attente d'appels, la mise en attente et l'appel à trois nécessitent que le TAS comprenne l'état du service :
    - Plusieurs appels simultanés par utilisateur
    - Événements de mise en attente/reprise

    - Appels fusionnés

6. **Logique prépayée vs. postpayée** : Le TAS peut appliquer différentes stratégies de facturation :
    - Prépayé : Vérifications de crédit en temps réel et coupure d'appel
    - Postpayé : Génération de CDR pour la facturation mensuelle
    - Hybride : Taux différents pour différentes fonctionnalités de service
7. **Flexibilité de tarification** : Le TAS a tout le contexte pour appliquer des règles de tarification complexes :
    - Tarification selon l'heure de la journée
    - Tarification basée sur la destination (locale, longue distance, internationale)
    - Remises sur volume
    - Taux promotionnels
    - Minutes groupées contre frais de dépassement

Limitations de la facturation S-CSCF :

- Ne voit que le dialogue SIP de base (INVITE → 200 OK → BYE)
- Pas de connaissance des services supplémentaires
- Ne peut pas suivre les changements d'état d'appel en cours d'appel
- Contexte limité pour les décisions de tarification
- Ne comprend pas l'activité du domaine CS

Interface Ro du S-CSCF (Disponible mais désactivée par défaut)

Bien que non utilisée en production, le S-CSCF prend en charge la facturation en ligne via Diameter Ro. Cette capacité reste dans la configuration mais est désactivée.

Comment la facturation S-CSCF fonctionnerait (si activée)

Si la facturation S-CSCF était activée, le système utiliserait l'interface Diameter Ro (ID d'application 4) pour communiquer avec un OCS. Le S-CSCF serait configuré avec les informations de pair OCS (FQDN, domaine, port 3868) et enverrait des demandes de contrôle de crédit (CCR) à trois points clés dans le cycle de vie de l'appel :

Flux CCR (si activé) :

Quand la facturation serait-elle déclenchée :

1. **CCR-Initial** : Envoyé lorsque l'INVITE est reçu, avant de permettre à l'appel de se poursuivre. Le OCS vérifie le solde du compte et accorde ou refuse le crédit (appel rejeté avec 402 Paiement requis).

2. **CCR-Update** : Envoyé périodiquement pendant l'appel en fonction du temps Granted-Service-Unit du OCS (par exemple, toutes les 300 secondes). Cela garantit que les longs appels ne dépassent pas le crédit disponible.

3. **CCR-Terminate** : Envoyé lorsque l'appel se termine (BYE reçu ou délai d'expiration du dialogue), rapportant l'utilisation finale au OCS pour déduction de compte.

Déploiement réel : Étant donné que cette fonctionnalité de facturation est désactivée dans nos déploiements, le S-CSCF route simplement les appels sans vérifications de contrôle de crédit. Toute la logique de facturation est gérée en aval par le TAS, qui a une visibilité complète sur l'ensemble du flux d'appel et le contexte de service.

9. Présence et SUBSCRIBE/PUBLISH

Le S-CSCF gère la présence SIP pour le statut de disponibilité des utilisateurs.

Architecture de présence

Configuration de la présence

La fonctionnalité de présence du S-CSCF est configurée avec :

- **Expiration maximum** : 3600 secondes (1 heure) - durée maximale d'abonnement
- **État par défaut** : "actif" - l'état de présence par défaut est actif
- **Support PIDF** : Activé - permet la modification des documents PIDF (Format de données d'information de présence)

Gestion de PUBLISH

Traitement de la publication de présence : Lorsque le S-CSCF reçoit une demande PUBLISH (utilisée pour mettre à jour l'état de présence) :

1. **Détection de méthode** : Vérifie si la demande entrante est une méthode PUBLISH
2. **Vérification d'autorisation** : Vérifie que l'utilisateur est actuellement enregistré dans la base de données de localisation. Si non enregistré, répond avec 403 Interdit
3. **Mise à jour de présence** : Traite la demande PUBLISH pour mettre à jour les informations de présence de l'utilisateur dans la base de données de présence
4. **Gestion des erreurs** : Si le traitement de la présence échoue (par exemple, erreur de base de données, document de présence mal formé), répond avec 500 Erreur serveur

Gestion de SUBSCRIBE

Traitement de l'abonnement à la présence : Lorsque le S-CSCF reçoit une demande SUBSCRIBE (utilisée pour surveiller la présence d'un autre utilisateur) :

1. **Détection de méthode** : Vérifie si la demande entrante est une méthode SUBSCRIBE
2. **Vérification du type d'événement** : Examine l'en-tête Event pour déterminer le type d'abonnement
    - Si l'événement est "reg" (paquet d'événement d'enregistrement), il s'agit d'un abonnement aux changements d'état d'enregistrement
    - Pour les abonnements d'événements d'enregistrement, effectue une demande d'attribution de serveur (SAR) au HSS si l'utilisateur n'est pas enregistré, pour obtenir le profil de service
    - Évalue les iFC pour les déclencheurs "subscribe" afin de déterminer si des serveurs d'applications doivent gérer l'abonnement
3. **Traitement de l'abonnement à la présence** : Gère la demande SUBSCRIBE pour créer ou actualiser un abonnement de surveillance de présence
4. **Gestion des erreurs** : Si le traitement de l'abonnement échoue, répond avec 500 Erreur serveur

Opérations de l'interface Web

Accéder à la page S-CSCF

Naviguer vers : `https://<panneau-de-contrôle>/scscf`

Disposition de la page

La page S-CSCF a cinq onglets principaux :

1. **Liste d'enregistrement** - Liste paginée des utilisateurs enregistrés
2. **Localisation utilisateur** - Interroger des détails spécifiques sur l'IMPU
3. **Dialogues** - Sessions d'appel actives
4. **IFC** - Gestion et test des critères de filtrage initiaux
5. **Tables de hachage** - Tables de mémoire partagée

Onglet Liste d'enregistrement

Objectif : Voir tous les utilisateurs enregistrés avec pagination

Colonnes d'affichage :

- **IMPU** : Identité publique multimédia IP (URI SIP)
- **Contacts** : Nombre de liaisons de contact enregistrées
- **État** : État d'enregistrement (Enregistré/Non enregistré)

- **Expire** : Horodatage d'expiration de l'enregistrement

Fonctionnalités :

- Pagination (50 utilisateurs par page)
- Recherche par IMPU ou contact
- Tri par colonne
- Cliquer sur la ligne pour développer et voir les détails du contact

Exemple :

```
IMPU: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
Contacts: 1
État: Enregistré
Expire: 2025-11-29 15:45:30

[Développer pour voir :]
  Contact: sip:12015551234@10.4.12.100:5060;transport=tcp
  Path: <sip:term@pcscf.ims.mnc001.mcc001.3gppnetwork.org:5060;lr>
  User-Agent: Client IMS Android v1.0
  Reçu: 10.4.12.100:52341
```

Actions rapides :

- **Recherche** : Recherche rapide pour un IMPU spécifique
- **Dump IFC** : Voir les critères de filtrage initiaux pour l'utilisateur
- **Test IFC** : Simuler un appel pour tester le déclenchement de l'AS
- **Désinscrire** : Forcer le désenregistrement (à utiliser avec précaution !)

Onglet Localisation utilisateur

Objectif : Interrogation détaillée d'un IMPU spécifique

Opérations :

1. Entrer l'IMPU (par exemple, `sip:user@domain.com`)
2. Cliquer sur "Lookup"
3. Voir des informations détaillées :
    - Tous les contacts enregistrés
    - En-tête Service-Route
    - Horodatages d'enregistrement
    - En-têtes de chemin
    - IMPIs associés (Identités privées)

Cas d'utilisation :

- Dépanner pourquoi l'utilisateur ne peut pas recevoir d'appels
- Vérifier les détails d'enregistrement
- Vérifier les liaisons de contact

- Vérifier les routes de service

Onglet Dialogues

Objectif : Surveiller et gérer les sessions d'appel actives

Colonnes d'affichage :

- **Call-ID** : Call-ID SIP
- **From URI** : Identité de l'appelant
- **To URI** : Identité appelée
- **État** : Précoce (sonnerie) ou Confirmé (répondu)
- **Heure de début** : Quand le dialogue a été créé
- **Délai d'expiration** : Valeur de délai d'expiration du dialogue

Opérations :

- **Rafraîchir** : Rafraîchissement manuel (rafraîchissement automatique toutes les 5s)
- **Fin de dialogue** : Terminer un appel spécifique (envoie BYE)
- **Fin de tous les dialogues actifs** : Terminaison de masse d'urgence

Exemple :

```
Call-ID: 3c26700857a87f84@10.4.12.165
From: sip:12015551234@ims.mnc001.mcc001.3gppnetwork.org
To: sip:+12015555678@ims.mnc001.mcc001.3gppnetwork.org
État: Confirmé
Heure de début: 2025-11-29 15:30:15
Délai d'expiration: 360000 secondes

[Bouton Fin de dialogue]
```

Avertissement : Mettre fin aux dialogues terminera immédiatement les appels actifs. Utiliser uniquement pour le dépannage ou les situations d'urgence.

Onglet IFC

Objectif : Voir et tester les critères de filtrage initiaux pour le déclenchement de services

L'onglet IFC fournit deux opérations principales : Dump IFC (récupérer et afficher un iFC d'un utilisateur depuis le HSS) et Test IFC (simuler un scénario d'appel pour voir quels serveurs d'applications seraient déclenchés).

Opération Dump IFC

1. Entrer l'IMPU : `sip:user@domain.com`

2. Cliquer sur "Dump IFC"
3. Voir la structure détaillée des iFC :
    - Ordre de priorité
    - Points de déclenchement (conditions SPT)
    - URIs des serveurs d'application
    - Gestion par défaut

Exemple de sortie :

```
<InitialFilterCriteria>
  <Priority>0</Priority>
  <TriggerPoint>
    <ConditionTypeCNF>1</ConditionTypeCNF>
    <SPT>
      <Group>0</Group>
      <Method>INVITE</Method>
    </SPT>
    <SPT>
      <Group>0</Group>
      <SessionCase>0</SessionCase>  <!-- Originaire -->
    </SPT>
  </TriggerPoint>
  <ApplicationServer>

<ServerName>sip:tas.ims.mnc001.mcc001.3gppnetwork.org</ServerName>
    <DefaultHandling>0</DefaultHandling>
  </ApplicationServer>
</InitialFilterCriteria>
```

Opération Test IFC

1. Entrer l'IMPU : `sip:user@domain.com`
2. Entrer l'URI d'origine : `sip:user@domain.com` (partie appelante)
3. Entrer l'URI de destination : `sip:+12015555678@domain.com` (partie appelée)
4. Cliquer sur "Test IFC"
5. Voir les résultats :
    - Quel iFC a correspondu
    - Quels serveurs d'applications seraient invoqués
    - Dans quel ordre (priorité)

Cas d'utilisation :

- Vérifier la configuration du déclenchement de services
- Dépanner pourquoi l'AS n'est pas invoqué
- Tester un nouvel iFC avant le déploiement en production
- Comprendre le flux d'appel pour des scénarios spécifiques

Onglet Tables de hachage

Semblable au P-CSCF et à l'ICSCF, gérer les tables de hachage de mémoire partagée.

Tables de hachage S-CSCF courantes :

- `auth` : Cache des vecteurs d'authentification
- `profile` : Profils utilisateurs mis en cache (si utilisé)
- Tables personnalisées pour la logique de service

Flux d'appels

Flux d'enregistrement complet

Voir la section "1. Enregistrement et authentification" ci-dessus pour le diagramme de séquence détaillé.

Flux d'appel sortant complet

Voir la section "5. Gestion des appels sortants" ci-dessus pour le diagramme de séquence détaillé.

Flux d'appel entrant complet

Voir la section "6. Gestion des appels entrants" ci-dessus pour le diagramme de séquence détaillé.

Dépannage

Problèmes d'enregistrement

L'utilisateur ne peut pas s'enregistrer - 403 Interdit

Causes possibles :

- Utilisateur non provisionné dans le HSS
- HSS injoignable
- Échec de l'authentification
- Restriction appliquée

Étapes de diagnostic :

1. Vérifier la connectivité HSS via le panneau de contrôle :
    - Naviguer vers la page Diameter

    - Sélectionner le nœud S-CSCF
    - Vérifier que le pair HSS est affiché comme "I_Open" (connecté)

2. Examiner les journaux S-CSCF pour le flux de messages MAR/MAA (Demande/Réponse d'authentification multimédia)

3. Vérifier que l'utilisateur existe dans le HSS (si accessible)

4. Vérifier les journaux S-CSCF pour les vecteurs d'authentification reçus du HSS

5. Tester avec un algorithme d'authentification différent si pris en charge

L'utilisateur ne peut pas s'enregistrer - 500 Erreur serveur

Causes possibles :

- Connexion à la base de données perdue
- Échec de SAR/SAA
- Erreur de module

Solutions :

1. Vérifier la connectivité de la base de données depuis le serveur S-CSCF (vérifier que la base de données est accessible et que les informations d'identification sont correctes)

2. Examiner les journaux S-CSCF pour le flux de messages SAR/SAA (Demande/Réponse d'attribution de serveur) Diameter

3. Redémarrer le service S-CSCF si nécessaire pour récupérer des erreurs de module

Problèmes de routage des appels

Les appels ne sont pas routés vers l'utilisateur

Symptômes : L'INVITE atteint le S-CSCF mais n'est pas transféré au P-CSCF

Étapes de diagnostic :

1. Vérifier que l'utilisateur est enregistré via l'interface web du panneau de contrôle :

    - Naviguer vers S-CSCF → Onglet Localisation utilisateur
    - Entrer l'IMPU et cliquer sur "Lookup"
    - Vérifier que l'utilisateur est affiché comme enregistré avec des liaisons de contact

2. Vérifier que des liaisons de contact existent et que l'en-tête Path est présent

3. Examiner les journaux S-CSCF pour le traitement de la route de terminaison

4. Tester avec une destination différente pour isoler le problème

Serveur d'application non déclenché

Symptômes : iFC devrait correspondre mais AS non invoqué

Étapes de diagnostic :

1. Dump iFC via l'interface web du panneau de contrôle :
    - Naviguer vers S-CSCF → Onglet IFC
    - Entrer l'IMPU
    - Cliquer sur "Dump IFC"
    - Examiner les points de déclenchement et les URIs des serveurs d'application

2. Tester la correspondance iFC via l'interface web :
    - Naviguer vers S-CSCF → Onglet IFC
    - Entrer l'IMPU, l'URI d'origine et l'URI de destination
    - Cliquer sur "Test IFC"
    - Vérifier quel iFC aurait dû correspondre

3. Vérifier si le profil utilisateur a été chargé depuis le HSS en examinant les journaux

4. Vérifier que SAA (Réponse d'attribution de serveur) du HSS contenait le XML du profil utilisateur

5. Examiner les journaux S-CSCF pour les erreurs d'analyse iFC

Problèmes de dialogue

Les dialogues ne se terminent pas après BYE

Symptômes : Le dialogue reste dans la base de données après la fin de l'appel

Solutions :

1. Vérifier les dialogues actifs via le panneau de contrôle :
    - Naviguer vers S-CSCF → Onglet Dialogues

    - Examiner le nombre de dialogues et les états

2. Vérifier la détection BYE dans les journaux du module de dialogue

3. Vérifier les paramètres de délai d'expiration du dialogue dans la configuration

4. Mettre fin manuellement au dialogue via le panneau de contrôle :

    - Naviguer vers S-CSCF → Onglet Dialogues
    - Trouver le dialogue bloqué
    - Cliquer sur "Fin de dialogue"

5. Examiner la base de données pour les entrées de dialogue orphelines et nettoyer si nécessaire

Problèmes de facturation

Délai d'attente CCR

Remarque : Dans nos déploiements, la facturation S-CSCF est généralement désactivée. La facturation est gérée par le TAS. Si vous voyez des erreurs liées à la facturation, vérifiez que la facturation S-CSCF Ro n'a pas été accidentellement activée.

Symptômes : Les appels échouent avec des erreurs de facturation (si la facturation est activée)

Causes possibles :

- OCS injoignable
- Pair Diameter Ro hors ligne
- Délai de transaction trop court

Solutions :

1. Vérifier l'état du pair OCS via le panneau de contrôle :

    - Naviguer vers la page Diameter
    - Sélectionner le nœud S-CSCF
    - Vérifier si le pair OCS est affiché comme "I_Open" (connecté)

2. Tester la connectivité réseau OCS depuis le serveur S-CSCF

3. Examiner la configuration du délai d'attente de transaction Diameter

4. Vérifier les journaux S-CSCF pour le flux de messages CCR/CCA et les erreurs

Crédit insuffisant - Tous les appels échouent

Remarque : Ce problème ne s'applique que si la facturation S-CSCF est activée (ce qui n'est généralement pas le cas dans nos déploiements).

Symptômes : Les utilisateurs reçoivent 402 Paiement requis pour tous les appels

Solutions :

1. Vérifier que la facturation S-CSCF doit réellement être activée (généralement elle doit être désactivée)

2. Vérifier le solde OCS pour les comptes de test si la facturation est intentionnellement activée

3. Examiner les codes de résultat CCA (Réponse de contrôle de crédit) dans les journaux S-CSCF

4. Envisager de désactiver la facturation S-CSCF et d'utiliser la facturation basée sur le TAS à la place

Problèmes PSTN

Les appels vers le PSTN échouent - 503 Pas de passerelle disponible

Causes possibles :

- Pas de MGCF/passerelle configurée
- Toutes les passerelles hors ligne
- Dispatcher non chargé

Solutions :

1. Coordonner avec les administrateurs système pour vérifier que les passerelles PSTN sont configurées

2. Tester la connectivité de la passerelle depuis le serveur S-CSCF (accessibilité réseau, réponse SIP)

3. Examiner la configuration de la passerelle avec les administrateurs système

4. Ajouter des passerelles manquantes si nécessaire via les administrateurs système

Problèmes de performance

Utilisation élevée du CPU

Causes possibles :

- Trop de dialogues
- Requêtes lentes de la base de données
- Surcharge d'évaluation iFC

Solutions :

1. Vérifier le nombre de dialogues via le panneau de contrôle :
    - Naviguer vers S-CSCF → Onglet Dialogues
    - Examiner le nombre de dialogues actifs
2. Optimiser les tables de base de données (dialogue, impu, impu_contact) si les requêtes de base de données sont lentes
3. Ajouter des index de base de données si nécessaire (sur impu.impu, dialog.callid, etc.)
4. Ajuster le nombre de processus de travail dans la configuration si nécessaire (augmenter de 4 par défaut à 8 pour une charge élevée)

Meilleures pratiques

Haute disponibilité

1. **Déployer plusieurs S-CSCF** avec une base de données partagée
2. **Utiliser des capacités** pour la sélection S-CSCF à l'I-CSCF
3. **Réplication de base de données** : Master-master ou master-esclave
4. **Persistance de session** : Mode dialogue en écriture
5. **Vérifications de santé** : Surveiller les enregistrements et les comptes de dialogue

Sécurité

1. **Toujours authentifier** les utilisateurs via le HSS
2. **Valider P-Asserted-Identity** uniquement à partir de sources de confiance
3. **Limiter le taux** d'enregistrements et d'appels par utilisateur
4. **Assainir les en-têtes** des réseaux non fiables
5. **Utiliser TLS** pour Diameter (Cx, Ro)

Performance

1. **Ajuster la taille du hachage pour la localisation utilisateur** : La taille du hachage doit être définie en fonction du nombre d'utilisateurs attendus. Par exemple, hash_size=13 (ce qui équivaut à 2^13 = 8192 seaux) est approprié pour environ 50 000 utilisateurs

2. **Mettre en cache les profils utilisateurs** : Si le HSS le prend en charge, activer la mise en cache des profils pour réduire les demandes SAR Diameter

3. **Optimiser iFC** : Garder les conditions de point de déclenchement (SPT) simples et minimiser le nombre de règles iFC par utilisateur pour réduire la surcharge d'évaluation

4. **Utiliser des opérations asynchrones pour Diameter** : Configurer le traitement asynchrone pour MAR (authentification), SAR (enregistrement) et CCR (facturation) afin d'éviter de bloquer les processus de travail

5. **Surveiller régulièrement les performances de la base de données** : Suivre les temps d'exécution des requêtes, optimiser les index et s'assurer que le pool de connexions fonctionne efficacement

Surveillance

Pour une liste complète de toutes les métriques S-CSCF, voir la **Référence des métriques**.

Métriques clés à suivre :

- Taux de réussite d'enregistrement
- Taux de succès MAR/SAR/LIR
- Nombre de dialogues (appels actifs)
- Temps d'évaluation iFC
- Latence des requêtes de base de données
- Temps de disponibilité des pairs Diameter
- Temps de configuration des appels

Référence

Spécifications 3GPP

- **TS 23.228** : Architecture IMS
- **TS 24.229** : Protocole SIP IMS
- **TS 29.228** : Interface Cx
- **TS 23.218** : Interface ISC
- **TS 32.260** : Facturation IMS

Guide des opérations de l'interface utilisateur Web

Table des matières

1. Aperçu
2. Accéder au panneau de contrôle
3. Gestion du P-CSCF
4. Gestion de l'I-CSCF
5. Gestion du S-CSCF
6. Gestion des pairs Diameter
7. Opérations sur les tables de hachage
8. Visualisation des journaux
9. Surveillance et métriques

Aperçu

L'interface utilisateur Web OmniCall CSCF fournit un panneau de contrôle complet pour la surveillance et la gestion en temps réel de tous les composants CSCF (P-CSCF, I-CSCF, S-CSCF). L'interface est construite sur Phoenix LiveView et offre :

- **Visibilité en temps réel** sur les enregistrements, les appels actifs et l'état du système
- **Gestion des tables de hachage** pour les structures de données en mémoire critiques pour la performance
- **Surveillance et contrôle des pairs Diameter**
- **Métriques Prometheus** pour la surveillance du système
- **Visualisation des journaux en direct** pour le dépannage

Architecture

Le panneau de contrôle communique avec les instances backend CSCF pour :

- Interroger les enregistrements d'utilisateurs et les données de localisation
- Inspecter les dialogues actifs (appels)
- Gérer les pairs Diameter
- Voir et manipuler les tables de hachage
- Accéder à la configuration des critères de filtrage initiaux (IFC)

Accéder au panneau de contrôle

Accès par défaut

Le panneau de contrôle est accessible via HTTP sur le serveur CSCF :

```
http://<cscf-server>:4000/
```

Port par défaut : 4000 (configurable dans `ControlPanel.Supervisor`)

Configuration

Le panneau de contrôle nécessite la configuration de l'hôte CSCF dans `config/config.exs` ou `config/runtime.exs` :

```
config :cscf, :cscf_hosts,
  pcscf: [
    {host: "10.4.12.165", port: 9060, label: "P-CSCF 1"}
  ],
  icscf: [
    {host: "10.4.12.166", port: 9060, label: "I-CSCF 1"}
  ],
  scscf: [
    {host: "10.4.12.167", port: 9060, label: "S-CSCF 1"}
  ]
```

Navigation

Le panneau de contrôle fournit des onglets de navigation pour chaque composant CSCF :

- **P-CSCF** - `/pcscf` - Contacts d'enregistrement et tables de hachage
- **I-CSCF** - `/icscf` - Liste S-CSCF, domaines NDS, sessions
- **S-CSCF** - `/scscf` - Enregistrements, dialogues, gestion IFC
- **Diameter** - `/diameter` - État et contrôle des pairs Diameter
- **Journaux** - `/logs` - Visualisation des journaux en direct

Gestion du P-CSCF

URL : `/pcscf`

Fonctionnalités

Le panneau P-CSCF affiche les contacts enregistrés et les informations sur les tables de hachage des instances P-CSCF.

Onglet Contacts enregistrés

Affiche tous les enregistrements IMS actuels visibles par le P-CSCF :

Colonne	Description
IMSI	IMSI de l'abonné ou identifiant de contact
État	État de l'enregistrement (enregistré, non enregistré)
Expire	Temps jusqu'à l'expiration de l'enregistrement
Chemin	En-tête SIP Path pour le routage

Opérations :

- **Cliquez sur la ligne** pour développer et voir les informations détaillées sur le contact, y compris :
  - AoR complet (Adresse d'enregistrement)
  - Adresse IP de l'UE
  - Détails du chemin
  - Statistiques (slots max, enregistrements)

Onglet Tables de hachage

Gérez les tables de hachage P-CSCF. Voir Opérations sur les tables de hachage ci-dessous.

Mises à jour en temps réel

La vue P-CSCF se rafraîchit automatiquement toutes les 5 secondes pour montrer l'état actuel des enregistrements.

Gestion de l'I-CSCF

URL : `/icscf`

Fonctionnalités

Le panneau I-CSCF fournit une surveillance des opérations I-CSCF, y compris la sélection S-CSCF et le suivi des sessions.

Onglet Liste S-CSCF

Affiche tous les serveurs S-CSCF configurés connus de l'I-CSCF :

- **ID** : Identifiant S-CSCF
- **Nom** : FQDN S-CSCF
- **Capacités** : Nombre de capacités prises en charge

Onglet Domaines NDS

Affiche les domaines NDS (Network Domain Security) de confiance configurés sur l'I-CSCF.

Onglet Sessions

Affiche les sessions I-CSCF actives, y compris :

- **Call-ID** : SIP Call-ID
- **Candidats S-CSCF** : Liste des serveurs S-CSCF considérés pour l'attribution
    - Nom S-CSCF
    - Score de sélection
    - Âge (temps écoulé depuis l'ajout du candidat)

Onglet Tables de hachage

Gérez les tables de hachage I-CSCF. Voir Opérations sur les tables de hachage ci-dessous.

Gestion du S-CSCF

URL : `/scscf`

Le panneau S-CSCF est le plus riche en fonctionnalités, offrant une gestion complète des enregistrements, des dialogues et des IFC.

Onglet Liste des enregistrements

Parcourez tous les enregistrements actifs avec pagination :

Fonctionnalités :

- **Contrôles de pagination** : Décalage et limite pour de grandes bases de données d'enregistrement
- **Détails de l'enregistrement** pour chaque IMPU :
    - Identité publique de l'utilisateur (IMPU)
    - État de l'enregistrement
    - Numéro de slot
    - Détails du contact avec User-Agent et expiration
    - Call-ID

Actions rapides pour chaque enregistrement :

- **Recherche** : Voir les informations détaillées de l'IMPU
- **Dump IFC** : Voir les critères de filtrage initiaux pour l'utilisateur

- **Test IFC** : Tester la correspondance des IFC pour des appels simulés
- **Désenregistrer** : Supprimer administrativement l'enregistrement

Onglet Localisation de l'utilisateur

Interrogez et inspectez les données de localisation des utilisateurs :

- Voir l'état brut de la localisation de l'utilisateur depuis le S-CSCF
- **Formulaire de recherche IMPU** : Interroger une identité publique spécifique
- Affiche les détails complets de l'enregistrement, y compris les contacts, l'état et les métadonnées

Onglet Dialogues

Gérez les sessions d'appel actives (dialogues) :

Colonne	Description
Dialog ID	Identifiant h_entry:h_id
Call-ID	SIP Call-ID
From	URI de la partie appelante
To	URI de la partie appel��e
État	État du dialogue

Opérations :

- **Terminer le dialogue** : Terminer un appel spécifique (envoie BYE)
- **Terminer tous** : Terminer tous les appels actifs (avec confirmation)

Onglet IFC

Outils de critères de filtrage initiaux pour la gestion du déclenchement de services :

Dump IFC

Récupérer et afficher toutes les règles IFC pour un IMPU donné :

- Identité publique
- Identité privée
- Nombre de profils de service
- **Critères de filtrage** pour chaque profil de service :
  - Priorité (ordre d'exécution)
  - Gestion par défaut (SESSION_CONTINUED vs SESSION_TERMINATED)
  - Nom du serveur d'application
  - Drapeaux d'inclusion REGISTER

    - **Détails du point de déclenchement** :
        - Type de condition (DNF ou CNF)
        - Déclencheurs de points de service (SPTs) :
            - METHOD, HEADER, SESSION_CASE, REQUEST_URI, etc.
            - Drapeaux de négation

L'affichage des IFC comprend :

- Badges de priorité codés par couleur
- Explications logiques des points de déclenchement extensibles
- DNF (Forme normale disjointe) = OU de ET
- CNF (Forme normale conjointe) = ET de OU

Test IFC

Tester quels serveurs d'application seraient déclenchés pour une session simulée :

Entrée :

- URI (identité publique de l'abonné)
- Direction (originaire ou terminante)
- Méthode (INVITE, REGISTER, MESSAGE, SUBSCRIBE)
- URI de la requête (destination)

Sortie :

- État d'enregistrement
- Nombre d'IFC correspondants
- Liste des serveurs d'application déclenchés avec l'index IFC

Onglet Tables de hachage

Gérez les tables de hachage S-CSCF. Voir Opérations sur les tables de hachage ci-dessous.

Gestion des pairs Diameter

URL : `/diameter`

Fonctionnalités

Surveillez et contrôlez les connexions des pairs Diameter (interfaces Cx, Rx, Ro).

Informations de résumé

Le tableau de bord affiche :

- **Royaume** : Royaume Diameter
- **Identité** : Origin-Host Diameter
- **Nombre de pairs** : Nombre de pairs configurés
- **Travailleurs** : Nombre de travailleurs CDP
- **Longueur de la file d'attente** : Transactions en attente
- **Délai de connexion** : Délai de connexion (secondes)
- **Délai de transaction** : Délai de transaction (secondes)
- **Accepter les pairs inconnus** : Drapeau de politique

Liste des pairs

Tableau de tous les pairs Diameter :

Colonne	Description
FQDN	Nom de domaine pleinement qualifié du pair
État	État de la connexion (I_Open, Closed, etc.)
Statut	Activé ou Désactivé
Dernière utilisation	Temps écoulé depuis la dernière transaction
Applications	Nombre d'applications Diameter prises en charge

Opérations :

- **Activer le pair** : Activer un pair désactivé
- **Désactiver le pair** : Désactiver le pair (avec confirmation)
- **Cliquez sur la ligne** : Développez pour voir les applications prises en charge

Mappage des applications

Le panneau de contrôle mappe automatiquement les ID d'application Diameter aux noms d'interface 3GPP :

- **Cx/Dx** (16777216:10415) - Abonnement/Autorisation IMS
- **Sh/Dh** (16777217:10415) - Accès aux données utilisateur
- **Rx** (16777236:10415) - Contrôle du plan média IMS
- **Ro** (16777238:10415/0) - Facturation en ligne
- **Gx** (16777224:10415) - Contrôle de la politique
- **S6a/S6d** (16777251:10415) - LTE/EPC MME-HSS
- Et bien d'autres (voir source : `diameter_live.ex`)

Mises à jour en temps réel

L'état des pairs Diameter se rafraîchit automatiquement toutes les 5 secondes.

Opérations sur les tables de hachage

Aperçu

Les composants CSCF utilisent des tables de hachage en mémoire pour des données critiques pour la performance. Le panneau de contrôle fournit une visibilité et une gestion de ces tables.

Tables de hachage disponibles

Les tables varient selon le type de CSCF. Exemples courants :

Table de hachage	CSCF	Objectif
`imei_msisdn`	P-CSCF	Mappage des rappels d'urgence
`service_routes`	P-CSCF	Routes de service mises en cache
`auth`	S-CSCF	Vecteurs d'authentification
Divers	Tous	Mise en cache spécifique au composant

Les tables de hachage sont des structures de données en mémoire utilisées pour des opérations critiques pour la performance.

Visualisation des tables de hachage

Accès : Naviguez vers n'importe quel panneau CSCF → Onglet Tables de hachage

1. Voir la liste de toutes les tables de hachage avec des statistiques :
    - Nom de la table
    - Nombre d'éléments
    - Taille
2. **Sélectionnez la table** pour voir les entrées
3. **Trier** par nom, éléments ou taille

Visualisation du contenu des tables de hachage

Cliquez sur une table pour inspecter toutes les entrées :

- **Clé** : Clé de la table de hachage
- **Valeur** : Valeur stockée
- **Actions** : Bouton de suppression

Gestion des entrées de hachage

Supprimer une entrée unique

1. Sélectionnez la table de hachage
2. Localisez l'entrée
3. Cliquez sur le bouton **Supprimer** (icône de poubelle)
4. Confirmez l'action

Résultat : L'entrée est supprimée de la table de hachage

Vider toute la table

1. Sélectionnez la table de hachage
2. Cliquez sur le bouton **Vider la table**
3. **AVERTISSEMENT** : Confirme avant de vider TOUTES les entrées
4. Confirmez l'action

Résultat : Toutes les entrées sont supprimées de la table

Précaution : Vider les tables peut provoquer une interruption temporaire du service :

- Vidage `imei_msisdn` : Les rappels d'urgence peuvent échouer jusqu'à la nouvelle inscription
- Vidage `auth` : Les défis d'authentification en cours échoueront
- Vidage `service_routes` : La prochaine requête sera routée via la découverte I-CSCF

Visualisation des journaux

URL : `/logs`

Fonctionnalités

Voir les journaux d'application en temps réel depuis le panneau de contrôle.

Fonctionnalités (implémentation dans la dépendance ControlPanel) :

- Diffusion en direct des journaux
- Filtrage par niveau de journal
- Capacités de recherche et de filtrage

Surveillance et métriques

Intégration Prometheus

OmniCall CSCF expose des métriques Prometheus pour la surveillance et l'alerte.

Point de terminaison des métriques :

```
http://<host>:9090/metrics
```

Chaque hôte CSCF (P-CSCF, I-CSCF, S-CSCF) expose des métriques sur le port 9090. Configurez Prometheus pour extraire tous les hôtes pour une visibilité complète.

Pour une référence complète de toutes les métriques P-CSCF, I-CSCF et S-CSCF, voir la **Référence des métriques**.

Métriques disponibles

Les métriques suivantes sont exposées par l'application du panneau de contrôle OmniCall CSCF. Pour les métriques des composants CSCF (SIP, Diameter, IMS, etc.), voir la **Référence des métriques**.

Métriques VM

- `vm_memory_total` - Mémoire totale de la VM Erlang (octets)
- `vm_memory_processes_used` - Mémoire utilisée par les processus (octets)
- `vm_memory_binary` - Mémoire binaire (octets)
- `vm_memory_ets` - Mémoire de la table ETS (octets)
- `vm_total_run_queue_lengths_total` - Longueur totale de la file d'attente d'exécution
- `vm_system_counts_process_count` - Nombre de processus
- `vm_system_counts_atom_count` - Nombre d'atomes
- `vm_system_counts_port_count` - Nombre de ports

Métriques HTTP Phoenix

- `phoenix_endpoint_stop_duration` - Durée de la requête HTTP (millisecondes)
- `phoenix_router_dispatch_stop_duration` - Durée de dispatch du routeur (millisecondes)

Métriques LiveView

- `phoenix_live_view_mount_stop_duration` - Durée de montage LiveView (millisecondes)

Métriques d'intégration du backend CSCF

- `cscf_backend_request_count` - Nombre de requêtes RPC backend
  - Tags : `host`, `command`, `result`
- `cscf_backend_request_duration` - Durée RPC backend (millisecondes)
  - Tags : `host`, `command`
- `cscf_backend_error_count` - Nombre d'erreurs RPC backend
  - Tags : `host`, `error_type`

Tableaux de bord Grafana

État actuel : Les métriques sont exposées via le point de terminaison Prometheus. Des tableaux de bord Grafana pré-construits ne sont pas actuellement inclus, mais peuvent être créés en utilisant les métriques disponibles.

Panneaux de tableau de bord recommandés :

- Latence RPC backend par commande
- Tendances du nombre d'enregistrements
- Tendances du nombre de dialogues
- Taux d'erreurs backend
- Utilisation de la mémoire de la VM Erlang
- Performance de montage LiveView

Intégration

Configurez Prometheus pour extraire des métriques de tous les hôtes CSCF :

```
scrape_configs:
  - job_name: 'cscf_pcscf'
    static_configs:
      - targets: ['pcscf1.example.com:9090',
'pcscf2.example.com:9090']

  - job_name: 'cscf_icscf'
    static_configs:
      - targets: ['icscf1.example.com:9090',
'icscf2.example.com:9090']

  - job_name: 'cscf_scscf'
    static_configs:
      - targets: ['scscf1.example.com:9090',
'scscf2.example.com:9090']
```

Meilleures pratiques

Directives opérationnelles

Surveillance :

- Surveillez les métriques Prometheus pour la santé du système
- Surveillez les erreurs RPC backend
- Suivez la croissance de la mémoire de la VM Erlang

Gestion des tables de hachage :

- Évitez de vider les tables en production à moins que cela ne soit absolument nécessaire
- Surveillez la croissance de la taille des tables pour des problèmes de mémoire potentiels
- Utilisez la suppression sélective au lieu du vidage complet de la table

Dépannage :

- Utilisez les journaux en direct pour le débogage en temps réel
- Vérifiez l'état des pairs Diameter avant d'enquêter sur les échecs d'enregistrement
- Vérifiez la connectivité du backend CSCF si le panneau de contrôle affiche des erreurs

Performance :

- Le rafraîchissement automatique du panneau de contrôle est de 5 secondes par défaut
- Les grandes listes d'enregistrements utilisent la pagination pour éviter les problèmes de performance
- Les opérations sur les tables de hachage sont lourdes en lecture ; minimisez les opérations d'écriture pendant les heures de pointe

Documentation connexe

- **Guide des opérations P-CSCF** - Opérations spécifiques au P-CSCF
- **Guide des opérations I-CSCF** - Opérations spécifiques à l'I-CSCF
- **Guide des opérations S-CSCF** - Opérations spécifiques au S-CSCF
- **Guide des opérations Diameter** - Gestion des pairs Diameter
- **Guide des opérations CSCF** - Opérations générales CSCF et dépannage

Documentation de conformité à l'interception ANSSI R226

Objet du document : Ce document fournit les spécifications techniques requises pour l'autorisation ANSSI R226 en vertu des articles R226-3 et R226-7 du Code pénal français pour le réseau de cœur IMS OmniCSCF (Fonctions de contrôle de session d'appel).

Classification : Documentation de conformité réglementaire

Autorité cible : Agence nationale de la sécurité des systèmes d'information (ANSSI)

Réglementation : R226 - Protection de la vie privée des correspondances et interception légale

---

1. SPÉCIFICATIONS TECHNIQUES DÉTAILLÉES

1.1 Identification du système

Nom du produit : OmniCSCF IMS Core Network
Type de produit : Réseau de cœur IP Multimedia Subsystem (IMS)
Fonction principale : Contrôle de session d'appel VoIP/VoLTE et livraison de services multimédias
Modèle de déploiement : Infrastructure de télécommunications sur site

Composants du réseau :

- P-CSCF (Proxy Call Session Control Function)
- E-CSCF (Emergency Call Session Control Function)
- I-CSCF (Interrogating Call Session Control Function)
- S-CSCF (Serving Call Session Control Function)

Ce système gère l'enregistrement, l'authentification, le routage de session et le contrôle des appels pour les réseaux IP Multimedia Subsystem (IMS). Les capacités d'interception détaillées et les caractéristiques de cryptage sont décrites dans les sections ci-dessous.

1.2 Capacités d'interception

1.2.1 Capture d'enregistrement et d'acquisition de session

Capture d'enregistrement SIP :

Le système CSCF traite tous les enregistrements SIP et maintient un état d'enregistrement complet :

- **Identifiants d'utilisateur :**
  - IMPU (IP Multimedia Public Identity) - URI SIP (par exemple, sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org)
  - IMPI (IP Multimedia Private Identity) - Nom d'utilisateur d'authentification (par

exemple, user@ims.mnc001.mcc001.3gppnetwork.org)
    - IMSI (International Mobile Subscriber Identity) - À partir des en-têtes P ou HSS
    - MSISDN (Numéro de téléphone mobile) - À partir de l'IMPU ou du profil utilisateur HSS

- **Métadonnées d'enregistrement :**
    - URI de contact (adresse réseau UE actuelle)
    - En-tête de chemin (route de retour via P-CSCF)
    - En-tête Service-Route (route vers S-CSCF)
    - Chaîne User-Agent (identification du type d'appareil)
    - Horodatage d'expiration de l'enregistrement
    - Adresse IP source et port
    - Protocole de transport (TCP/UDP/TLS)
    - Vecteurs d'authentification (RAND, AUTN, XRES, CK, IK du HSS)

- **Informations de localisation du réseau :**
    - En-tête P-Access-Network-Info (antenne relais, zone de localisation)
    - P-Visited-Network-ID (identification du réseau en itinérance)
    - Adresse IP reçue (source réelle)
    - Adresse P-CSCF (point d'entrée réseau)

Capture de session d'appel :

Le S-CSCF maintient un état de dialogue SIP complet pour tous les appels actifs :

- **Identifiants de session :**
    - Call-ID (identifiant de session unique)
    - URIs et tags From/To
    - Ensembles de routes pour les deux parties
    - Original-Dialog-ID (pour le suivi des interactions avec le serveur d'application)

- **Métadonnées de session :**
    - Identité de l'appelant (en-tête From, P-Asserted-Identity)
    - Partie appelée (en-tête To, Request-URI)
    - Horodatage d'établissement de session
    - Horodatage de terminaison de session
    - État du dialogue (Précoce/Confirmé/Supprimé)
    - Numéros CSeq (séquençage des transactions)

- **Informations multimédias :**
    - SDP (Session Description Protocol) dans les corps de message SIP
    - Adresses des serveurs multimédias (OmniTAS)
    - Informations sur les codecs (formats audio/vidéo)
    - Points de terminaison de flux multimédia
    - Allocations de ports RTP/RTCP

Identification des appels d'urgence :

Le composant E-CSCF identifie et route les appels d'urgence :

- Détection de numéro d'urgence (112, 911, etc.)

- Capture de l'IMEI (International Mobile Equipment Identity)
- Mapping IMEI vers MSISDN (pour rappel)
- Informations de localisation de l'UE ou du réseau
- Support du protocole HELD (HTTP-Enabled Location Delivery)
- Destination de routage d'urgence (PSAP/AS d'urgence)

1.2.2 Stockage et traitement des données

IMPORTANT : État en mémoire uniquement

Les composants CSCF (P-CSCF, E-CSCF, I-CSCF, S-CSCF) maintiennent **toutes les données d'état en mémoire uniquement**. Il n'y a **aucun stockage de base de données persistant** des données d'enregistrement ou de session d'appel. Tous les liaisons d'enregistrement, l'état de dialogue et les associations de sécurité IPsec sont stockés en mémoire et sont perdus lors du redémarrage du système.

Données d'enregistrement actives (en mémoire) :

Le système CSCF maintient un état en temps réel uniquement :

État d'enregistrement P-CSCF :

- Données d'association de sécurité IPsec (paires SPI, ports, paramètres de cryptage)
- Liaisons de contact UE et adresses réseau
- Points de terminaison et état de tunnel IPsec
- Périodes de validité d'enregistrement

État d'enregistrement S-CSCF :

- Identités publiques (IMPU) et état d'enregistrement actuel
- Liaisons de contact avec en-têtes de chemin, User-Agent, adresses reçues
- Mappings d'identité privée (IMPI) vers identité publique
- Profils utilisateur du HSS (mis en cache lors de l'enregistrement)

État de session active (en mémoire) :

Le S-CSCF maintient un état d'appel actif uniquement :

- Identifiants d'appel (Call-ID), identités des participants (tags From/To)
- Ensembles de routes et adresses de contact
- État de session (Précoce/Confirmé/Terminé)
- Informations de timing de session

Aucun CDR ou suivi historique :

Les composants CSCF ne génèrent ni ne stockent :

- Enregistrements de détails d'appel (CDRs)
- Enregistrements d'appels historiques
- Enregistrements d'enregistrement historiques
- Suivi d'événements à long terme

Génération de CDR et suivi historique : Tous les enregistrements de détails d'appel, données de facturation et suivi d'appels historiques sont gérés par le **TAS (Telephony Application Server - OmniTAS)**, et non par les composants CSCF.

Journalisation des messages SIP/Diameter :

Les CSCF peuvent générer des journaux d'événements en temps réel à des fins opérationnelles :

- **Journalisation des messages SIP :** Journalisation optionnelle des messages SIP (INVITE, REGISTER, etc.)
- **Journalisation des messages Diameter :** Journalisation optionnelle des transactions Diameter (Cx, Rx, Ro)
- **Événements système :** Changements de configuration, erreurs, pannes

Ces journaux sont des journaux opérationnels transitoires, pas des enregistrements d'appels persistants. La conservation des journaux est configurable et généralement à court terme (heures à jours) uniquement à des fins de débogage.

1.2.3 Capacités d'analyse

Surveillance en temps réel :

Le panneau de contrôle web Phoenix LiveView fournit :

- **Surveillance des enregistrements :**
  - Voir tous les utilisateurs enregistrés avec pagination
  - Recherche par IMPU, contact, IMPI
  - Détails d'enregistrement (contact, chemin, user-agent, expiration)
  - Capacité de désenregistrement forcé
- **Surveillance des dialogues :**
  - Vue des sessions d'appel actives
  - Call-ID, URIs From/To, état, durée
  - Capacité de terminaison d'appel (envoyer BYE)
  - Actualisation automatique toutes les 5 secondes
- **État du système :**
  - État des pairs Diameter (HSS, PCRF, connectivité OCS)
  - État de la passerelle frontend
  - Métriques de capacité du système
  - Capacité de tunnel IPsec (P-CSCF)

Remarque sur les données historiques :

Les composants CSCF ne maintiennent pas de données historiques. Pour les enregistrements d'appels historiques, CDRs et analyse des modèles de communication, les autorités d'interception légale doivent coordonner avec **OmniTAS (Telephony Application Server)**, qui gère toute la génération de CDR et le suivi d'appels à long terme.

Visibilité de déclenchement de service en temps réel :

Le S-CSCF traite les Critères de Filtrage Initiaux (iFC) en temps réel :

- L'évaluation des iFC détermine quels serveurs d'application sont déclenchés pour chaque appel
- Visibilité en temps réel sur les services invoqués

- Décisions de routage du serveur d'application visibles dans le flux de messages SIP

État du réseau :

- État de connectivité HSS (interface Diameter Cx)
- Distribution de sélection S-CSCF (I-CSCF)
- Modèles de routage d'appels
- Temps de réponse du serveur d'application
- Performance des transactions Diameter

1.3 Capacités de contre-mesures

1.3.1 Mécanismes de protection de la vie privée

Confidentialité des communications :

- **Tunnels IPsec :** Tunnels ESP (Encapsulating Security Payload) entre l'UE et le P-CSCF
    - Cryptage : AES-CBC, AES-GCM
    - Authentification : HMAC-SHA1, HMAC-SHA256
    - Dérivation de clé à partir de l'IMS AKA (CK/IK du HSS)
    - Associations de sécurité par UE
- **Support TLS/TLS :**
    - Support SIP sur TLS (SIPS)
    - Diameter sur TLS (connexions HSS, PCRF, OCS)
    - Authentification basée sur des certificats
    - Confidentialité parfaite à l'avance (PFS) via ECDHE/DHE
- **En-têtes de confidentialité SIP :**
    - P-Asserted-Identity (ID d'appelant authentifié)
    - En-tête de confidentialité (demande de suppression de l'ID d'appelant)
    - Support de session anonyme

Contrôle d'accès :

- Authentification et contrôle d'accès de l'interface Web
- Interface BINRPC pour le panneau de contrôle (port 2046)
- Contrôles d'accès au registre et séparation des rôles
- Authentification SIP (AKA via HSS)
- Authentification des pairs Diameter

Journalisation d'audit :

- Journalisation complète des messages SIP et Diameter
- Événements d'enregistrement/désenregistrement
- Événements d'établissement et de terminaison d'appel
- Actions administratives via l'interface Web
- Changements de configuration
- Succès/échec de l'authentification

1.3.2 Fonctionnalités de protection des données

Sécurité d'accès :

- Contrôle d'accès basé sur les rôles (RBAC)
- Comptes de surveillance en lecture seule
- Contrôles d'authentification et d'autorisation

Durcissement du système :

- Ports réseau exposés minimaux (5060 SIP, 3868 Diameter, 8086 Web UI)
- Vérification de la validité des messages SIP
- Prévention des boucles Max-Forwards
- Limitation de débit et protection anti-inondation
- Limites de taille de message
- Isolation des processus de travail

1.4 Points d'intégration pour l'interception légale

1.5.1 Architecture d'interception légale ETSI

Le système CSCF fournit une base pour l'interception légale conforme à l'ETSI. Bien que les interfaces X1/X2/X3 natives ne soient pas intégrées, tous les points d'accès aux données nécessaires existent pour l'intégration avec des systèmes externes de Fonction de Médiation d'Interception Légale (LIMF).

Interfaces LI ETSI standard :

Interface X1 - Fonction d'administration :

- **Objet :** Provisionnement de mandat et de cible par les forces de l'ordre
- **Direction :** LEMF → LIMF (bidirectionnel)
- **Fonctions :**
  - Activer/désactiver l'interception pour les cibles (IMPUs, IMSIs, MSISDNs)
  - Définir la durée et la période de validité de l'interception
  - Configurer les critères de filtrage (identités, fenêtres temporelles)
  - Récupérer l'état de l'interception
- **Intégration avec CSCF :**
  - LIMF maintient une base de données de mandats (liste de cibles - externe au CSCF)
  - LIMF surveille l'état en temps réel du CSCF et les journaux de messages pour les sessions correspondantes
  - LIMF filtre en fonction des critères fournis par X1

Interface X2 - Livraison d'IRI (Informations liées à l'interception) :

- **Objet :** Livrer des métadonnées de session aux forces de l'ordre
- **Direction :** LIMF → LEMF (unidirectionnel)
- **Format de données :** XML/ASN.1 conforme à ETSI TS 102 232
- **Contenu du CSCF :**
  - Identifiants de session (Call-ID, tags de dialogue)
  - Partie appelante (URI From, P-Asserted-Identity, IMPU, IMSI, MSISDN)
  - Partie appelée (URI To, Request-URI, IMPU, IMSI, MSISDN)
  - Horodatages d'enregistrement
  - Horodatages de configuration/démontage de session
  - Localisation réseau (P-Access-Network-Info, antenne relais, zone de localisation)
  - Adresses P-CSCF/S-CSCF (identification des éléments réseau)
  - User-Agent (type d'appareil)
  - Informations d'itinérance (P-Visited-Network-ID)

Interface X3 - Livraison CC (Contenu de la communication) :

- **Objet :** Livrer le contenu réel de la communication
- **Direction :** LIMF → LEMF (unidirectionnel)
- **Format de données :** Conforme à ETSI TS 102 232
- **Contenu du CSCF :**
  - Corps de messages SIP (descriptions de session SDP)
  - Adresses des serveurs multimédias (pour interception RTP)
  - Informations sur les codecs
  - Messages instantanés SIP MESSAGE (contenu du corps)
  - Données d'application (si routées via CSCF)

Remarque : Pour les flux RTP audio/vidéo, le LIMF doit également s'intégrer avec les serveurs multimédias (OmniTAS) pour capturer le contenu multimédia réel. Le CSCF fournit des informations de configuration de session (SDP) montrant où les flux multimédias circulent.

1.5.2 Sources de données CSCF pour l'interception légale

1. Accès aux données d'enregistrement :

Données d'enregistrement P-CSCF :

- IMPU (identité publique)
- URI de contact (adresse réseau UE)
- IP et port reçus
- En-tête de chemin
- Expiration de l'enregistrement
- Informations SPI et port IPsec
- Chaîne User-Agent

Données d'enregistrement S-CSCF :

- Identités publiques (IMPU), état de barring, état d'enregistrement
- Liaisons de contact avec en-têtes de chemin, User-Agent, adresses reçues
- Mappings d'identité privée (IMPI) vers identité publique
- Profils utilisateur du HSS (format XML incluant les détails de l'abonné)

Méthodes d'accès :

- Interfaces d'accès aux données en lecture seule
- Interface de surveillance Web UI
- Journalisation d'événements en temps réel

2. Données de session active :

Données de dialogue S-CSCF :

- Call-ID (identifiant de session unique)
- URIs et tags From/To
- Numéros CSeq de l'appelant et du destinataire
- Ensembles de routes pour les deux parties
- Adresses de contact
- État du dialogue (Précoce, Confirmé, Supprimé)
- Horodatage de début
- Valeurs de délai d'expiration

Méthodes d'accès :

- Surveillance de l'état de dialogue en temps réel
- Requête par identifiants de session ou identifiants de partie
- Capacités d'exportation pour analyse judiciaire

3. Journalisation des messages SIP :

Capture des journaux :

- Tous les messages SIP peuvent être enregistrés (REGISTER, INVITE, MESSAGE, etc.)
- Niveaux de journalisation configurables
- Journalisation structurée avec horodatages
- Journalisation Syslog ou basée sur des fichiers

Analyse des journaux :

- Analyser les en-têtes SIP pour l'extraction d'identité
- Extraire le SDP pour les informations multimédias
- Suivre les séquences de messages (CSeq)
- Corréler les requêtes et les réponses

Exemple d'entrée de journal :

```
INFO: INVITE sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org SIP/2.0
From: <sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>;tag=abc123
To: <sip:+33687654321@ims.mnc001.mcc001.3gppnetwork.org>
Call-ID: f81d4fae-7dec-11d0-a765-00a0c91e6bf6@ims.mnc001.mcc001.3gppnetwork.org
P-Asserted-Identity: <sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org>
P-Access-Network-Info: 3GPP-E-UTRAN-FDD; utran-cell-id-3gpp=208011234567890
Content-Type: application/sdp

v=0
o=- 1234567890 1234567890 IN IP4 192.168.1.100
s=-
c=IN IP4 10.20.30.40
t=0 0
m=audio 49170 RTP/AVP 0 8
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
```

4. Journalisation des messages Diameter :

Messages Cx (Communication HSS) :

- UAR/UAA : Autorisation utilisateur (contient IMPU, IMPI)
- LIR/LIA : Informations de localisation (contient IMPU, S-CSCF de service)
- MAR/MAA : Authentification (contient IMPI, vecteurs d'authentification)
- SAR/SAA : Attribution de serveur (contient IMPU, IMPI, profil utilisateur XML)

Données Diameter disponibles :

- IMSI (à partir du profil utilisateur)
- MSISDN (à partir du profil utilisateur)
- IMPUs associés (plusieurs identités par abonné)
- Profil utilisateur (services, barring, état d'itinérance)

Exemple de journal :

```
Diameter Cx SAA reçu du HSS :
User-Name: user@ims.mnc001.mcc001.3gppnetwork.org
Public-Identity: sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org
Server-Name: sip:scscf.ims.mnc001.mcc001.3gppnetwork.org
Result-Code: 2001 (Succès)
User-Data: <XML profil utilisateur avec IMSI, MSISDN, iFC>
```

5. Données d'appel d'urgence (E-CSCF) :

Mapping IMEI vers MSISDN :

- Le P-CSCF crée un mapping lorsque l'UE s'enregistre avec l'IMEI
- TTL de 24 heures (Time-To-Live)
- Utilisé pour le rappel d'urgence
- Synchronisé entre les nœuds de cluster P-CSCF

Conservation des données :

- Les mappings IMEI vers MSISDN sont conservés pendant 24 heures
- Disponibles pour la corrélation de rappel d'urgence
- Accessibles via des interfaces de surveillance

Journaux d'appels d'urgence :

- Détection de numéro d'urgence (112, 911, etc.)
- Extraction de l'IMEI à partir des contacts ou des en-têtes P
- Informations de localisation (à partir de HELD ou P-Access-Network-Info)
- Routage PSAP (Public Safety Answering Point)
- Routage E-CSCF vers AS d'urgence

1.5.3 Capacités d'intégration pour LIMF

Le système fournit plusieurs méthodes d'intégration pour les systèmes de Fonction de Médiation d'Interception Légale (LIMF) :

1. **Accès aux données d'enregistrement et de session :**
    - Accès en temps réel aux données d'enregistrement (identités, emplacements, informations sur les appareils)
    - Surveillance des sessions actives (état des appels, participants, timing)
    - Capacités de requête historique
2. **Journalisation des événements :**
    - Journalisation des messages SIP avec niveaux de détail configurables
    - Journalisation des messages Diameter pour les interactions HSS
    - Journaux d'événements structurés avec horodatages
3. **Surveillance en temps réel :**
    - Surveillance de l'état d'enregistrement en direct
    - Suivi des sessions d'appel actives
    - Détection d'appels d'urgence et informations de routage

Les méthodes d'intégration prennent en charge à la fois les architectures basées sur le polling et celles basées sur les événements pour la connectivité LIMF.

1.5.4 Mapping des données CSCF aux interfaces LI

Mapping des données CSCF à l'IRI (X2) :

Source de données CSCF	Champ IRI	Exemple de données
IMPU (en-têtes SIP/état en mémoire)	Partie A	sip:+33612345678@ims.mnc001.mcc001.3gppnetwork.org
IMPI (en-têtes SIP/état en mémoire)	ID d'authentification	user@ims.mnc001.mcc001.3gppnetwork.org
IMSI (profil utilisateur HSS)	ID d'abonné	208011234567890
MSISDN (profil utilisateur HSS)	Numéro de téléphone	+33612345678
Call-ID (en-têtes SIP/état de dialogue)	ID de session	f81d4fae-7dec-11d0-a765-00a0c91e6bf6@...
From/To (en-têtes SIP)	Partie A/Partie B	sip:+33612345678@... / sip:+33687654321@...
Horodatage d'enregistrement (en mémoire)	Heure de l'événement	2025-11-29T10:30:00Z
P-Access-Network-Info (en-tête SIP)	Localisation	3GPP-E-UTRAN-FDD;utran-cell-id-3gpp=208011234567890
IP reçue (contact SIP)	Adresse IP UE	10.20.30.40:5060
Adresse P-CSCF (routage SIP)	Élément réseau	10.4.12.165:5060
Adresse S-CSCF (routage SIP)	Élément réseau	10.4.11.45:5060

Mapping des données CSCF au CC (X3) :

Source de données CSCF	Champ CC	Exemple de données
Corps de MESSAGE SIP	Contenu du message instantané	"Bonjour, comment ça va ?"
SDP dans INVITE	Informations sur la session multimédia	Points de terminaison RTP, codecs
Adresse du serveur multimédia	Cible d'interception RTP	10.50.60.70:49170

Remarque : Pour le contenu audio/vidéo réel (RTP), le LIMF doit coordonner avec les serveurs multimédias (OmniTAS) pour capturer les flux RTP. Le CSCF fournit uniquement des informations de configuration de session.

1.5 Interface de surveillance basée sur le Web

Le système comprend un panneau de contrôle basé sur le Web pour la surveillance en temps réel et l'accès administratif :

Capacités de surveillance :

- État d'enregistrement en temps réel (abonnés actifs, emplacements, informations sur les appareils)
- Surveillance des sessions d'appel actives (participants, état des appels, timing)
- Recherche et filtrage par identité (IMPU, IMPI, IMSI, MSISDN)
- État et capacité du tunnel IPsec
- Capacités d'exportation pour analyse judiciaire

Sécurité :

- Accès chiffré HTTPS/TLS
- Authentification requise
- Journalisation d'audit de toutes les actions administratives
- Modes d'accès en lecture seule pour le personnel de surveillance

---

2. CAPACITÉS DE CRYPTAGE ET DE CRYPTANALYSE

2.1 Aperçu des capacités cryptographiques

L'OmniCSCF met en œuvre plusieurs couches de protection cryptographique pour le signalement et les données des abonnés. Cette section documente toutes les capacités cryptographiques requises par l'ANSSI.

2.2 Cryptage de tunnel IPsec ESP (UE vers P-CSCF)

2.2.1 Mise en œuvre du protocole IPsec

Mode IPsec pris en charge :

- ESP (Encapsulating Security Payload) - Protocole IP 50
- Mode transport (pas de mode tunnel)
- Protège le signalement SIP entre l'UE et le P-CSCF

Algorithmes de cryptage pris en charge :

Le système avec IPsec du noyau prend en charge :

- **AES-CBC (Advanced Encryption Standard - Cipher Block Chaining) :**
  - AES-128-CBC (clé de 128 bits)
  - AES-192-CBC (clé de 192 bits)
  - AES-256-CBC (clé de 256 bits) - Recommandé
- **AES-GCM (Advanced Encryption Standard - Galois/Counter Mode) :**
  - AES-128-GCM (clé de 128 bits avec AEAD)
  - AES-256-GCM (clé de 256 bits avec AEAD) - Recommandé
- **3DES-CBC (Triple DES - Cipher Block Chaining) :**
  - Clé effective de 168 bits (dépréciée, compatibilité héritée)
- **Cryptage NULL :**

    - Pas de confidentialité (authentification uniquement)
    - Utilisé uniquement pour le débogage ou des scénarios de conformité sp��cifiques

Algorithmes d'authentification pris en charge :

- **HMAC-SHA1 (Hash-based Message Authentication Code - SHA-1) :**
    - Sortie de 160 bits
    - Compatibilité héritée
- **HMAC-SHA256 (HMAC - SHA-256) :**
    - Sortie de 256 bits
    - Recommandé
- **HMAC-SHA384 (HMAC - SHA-384) :**
    - Sortie de 384 bits
- **HMAC-SHA512 (HMAC - SHA-512) :**
    - Sortie de 512 bits
- **HMAC-MD5 :**
    - Sortie de 128 bits
    - Déprécié, uniquement pour compatibilité héritée

Dérivation de clé :

Les clés IPsec (CK - Cipher Key, IK - Integrity Key) sont dérivées de l'authentification IMS AKA :

1. L'UE effectue l'authentification AKA avec S-CSCF/HSS
2. Le HSS génère CK (128 bits) et IK (128 bits)
3. Le S-CSCF livre CK/IK au P-CSCF via une interface interne
4. Le P-CSCF utilise CK/IK pour établir des associations de sécurité IPsec avec l'UE
5. CK utilisé pour le cryptage ESP
6. IK utilisé pour l'authentification ESP

Paramètres d'association de sécurité :

- **Durée de vie :** Liée à l'expiration de l'enregistrement SIP (généralement 599 secondes)
- **Protection contre la répétition :** Activée (fenêtre anti-replay)
- **Numéros de séquence :** 32 bits ou 64 bits (ESN - Numéros de séquence étendus)
- **Confidentialité parfaite à l'avance :** Non applicable (clés issues de AKA, pas de Diffie-Hellman)

Mise en œuvre :

La capacité IPsec du P-CSCF :

- Interfaces avec la pile IPsec du noyau Linux (cadre XFRM)
- Configure les politiques de sécurité et les associations via l'API du noyau
- Allocation et gestion de SPI (Security Parameter Index)
- Allocation de ports pour le trafic protégé

2.2.2 Capacités de configuration IPsec

Sélection de suite de chiffrement :

Le P-CSCF peut être configuré pour préférer des suites de chiffrement spécifiques :

Préférées (sécurité forte) :

- ESP avec AES-256-GCM et HMAC-SHA256
- ESP avec AES-256-CBC et HMAC-SHA256

Supportées (compatibilité) :

- ESP avec AES-128-CBC et HMAC-SHA1
- ESP avec 3DES-CBC et HMAC-SHA1 (héritage)

Gestion des clés :

- IKE (Internet Key Exchange) n'est PAS utilisé
- Clés fournies via IMS AKA (CK/IK du HSS)
- Configuration manuelle des associations de sécurité via XFRM du noyau
- Destruction automatique des SA à l'expiration de l'enregistrement

Cycle de vie du tunnel :

1. L'UE s'enregistre → Authentification AKA → CK/IK générés
2. Le P-CSCF reçoit CK/IK du S-CSCF
3. Le P-CSCF alloue une paire de SPI (SPI client, SPI serveur)
4. Le P-CSCF alloue une paire de ports (port client, port serveur)
5. Le P-CSCF configure les SA IPsec du noyau en utilisant CK/IK
6. Le P-CSCF envoie les paramètres IPsec à l'UE dans 200 OK (en-tête Security-Server)
7. L'UE configure les SA IPsec avec les mêmes paramètres
8. Tout le trafic SIP ultérieur passe par les tunnels ESP
9. À l'expiration de l'enregistrement ou au désenregistrement : SA supprimées, ressources libérées

2.3 Cryptage TLS (SIP et Diameter)

2.3.1 TLS pour SIP (SIPS)

Versions TLS prises en charge :

- **TLS 1.2** (RFC 5246) - Pris en charge
- **TLS 1.3** (RFC 8446) - Pris en charge (si support du noyau/bibliothèque)
- **TLS 1.0/1.1** - Déprécié (désactivé par défaut)
- **SSL 2.0/3.0** - NON SOUTENU (vulnérabilités connues)

Mise en œuvre TLS :

le système utilise OpenSSL ou LibreSSL :

- Bibliothèques TLS standard de l'industrie
- Implémentations validées cryptographiquement
- Mises à jour de sécurité régulières

Suites de chiffrement prises en charge :

TLS 1.3 (Préférée) :

- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

TLS 1.2 (Pris en charge) :

- ECDHE-RSA-AES256-GCM-SHA384 (Confidentialité parfaite à l'avance)
- ECDHE-RSA-AES128-GCM-SHA256 (Confidentialité parfaite à l'avance)
- ECDHE-ECDSA-AES256-GCM-SHA384 (Confidentialité parfaite à l'avance)
- DHE-RSA-AES256-GCM-SHA384 (Confidentialité parfaite à l'avance)
- DHE-RSA-AES128-GCM-SHA256 (Confidentialité parfaite à l'avance)

Chiffres faibles désactivés :

- Pas de RC4
- Pas de MD5
- Pas de cryptage NULL
- Pas de chiffres de grade EXPORT
- Pas de DES/3DES (déprécié)

Support des certificats :

- **Certificats X.509** (format standard)
- **Clés RSA :** minimum 2048 bits, recommandé 4096 bits
- **Clés ECDSA :** courbes P-256, P-384, P-521 prises en charge
- **Validation de chaîne de certificats**
- **Vérification de la CRL (Certificate Revocation List)** (optionnelle)
- **OCSP (Online Certificate Status Protocol)** (optionnel)

Fonctionnalités TLS :

- **Confidentialité parfaite à l'avance (PFS) :** Via échange de clés ECDHE/DHE
- **Indication de nom de serveur (SNI) :** Prise en charge
- **Reprise de session TLS :** Prise en charge (optimisation des performances)
- **Authentification par certificat client :** Prise en charge (TLS mutuel)

SIP sur TLS (SIPS) :

- Transport : TCP avec cryptage TLS
- Port : 5061 (port SIPS standard)
- Utilisé pour la communication inter-CSCF (optionnel)
- Utilisé pour les connexions de réseau de confiance

2.3.2 TLS pour Diameter

Capacités Diameter :

Le système prend en charge :

- **Diameter sur SCTP** (préféré pour la fiabilité)
- **Diameter sur TCP avec TLS**
- **Port :** 3868 (port Diameter standard)

Cas d'utilisation :

- **Interface Cx :** S-CSCF/I-CSCF vers HSS (données d'abonné, authentification)
- **Interface Rx :** P-CSCF vers PCRF (politique QoS)
- **Interface Ro :** S-CSCF vers OCS (facturation en ligne - si activée)

Configuration TLS pour Diameter :

Les mêmes suites de chiffrement que SIP

- TLS 1.2/1.3
- Échange de clés ECDHE/DHE (PFS)
- Cryptage AES-GCM
- Authentification SHA256/SHA384

Authentification par certificat :

- Les pairs Diameter s'authentifient via des certificats TLS
- TLS mutuel (certificats client et serveur)
- Validation FQDN (Fully Qualified Domain Name) dans les certificats
- Validation de la chaîne CA de confiance

2.4 Cryptographie d'authentification

2.4.1 Fonctions cryptographiques IMS AKA

Algorithme 3GPP AKA (MILENAGE) :

Utilisé pour générer des vecteurs d'authentification (RAND, AUTN, XRES, CK, IK) :

Fonctions cryptographiques :

- **f1 :** Fonction d'authentification de message (calculer MAC-A et MAC-S)
- **f2 :** Fonction de réponse (calculer RES à partir de RAND et K)
- **f3 :** Dérivation de clé de chiffrement (calculer CK)
- **f4 :** Dérivation de clé d'intégrité (calculer IK)
- **f5 :** Fonction de clé d'anonymat (calculer AK pour la confidentialité de l'IMSI)

Matériel de clé :

- **K :** Clé d'abonné permanente de 128 bits (stockée dans ISIM et HSS)
- **OPc :** Clé variante d'opérateur (dérivée de K et OP)
- **RAND :** Défi aléatoire de 128 bits
- **SQN :** Numéro de séquence de 48 bits (protection contre la répétition)

Séquence AKA :

1. Le HSS génère RAND (aléatoire cryptographiquement)
2. Le HSS calcule MAC-A = f1(K, RAND, SQN, AMF)
3. Le HSS calcule AUTN = (SQN ⊕ AK) || AMF || MAC-A
4. Le HSS calcule XRES = f2(K, RAND)
5. Le HSS calcule CK = f3(K, RAND)
6. Le HSS calcule IK = f4(K, RAND)
7. Le HSS envoie {RAND, AUTN, XRES, CK, IK} au S-CSCF
8. Le S-CSCF défie l'UE avec RAND et AUTN
9. L'UE calcule RES = f2(K, RAND) en utilisant ISIM
10. L'UE envoie RES au S-CSCF
11. Le S-CSCF compare RES avec XRES (validation d'authentification)

Propriétés de sécurité :

- **Authentification mutuelle :** L'UE vérifie le HSS via AUTN, le HSS vérifie l'UE via RES
- **Frais de clé :** RAND est aléatoire, SQN empêche la répétition
- **Dérivation de clé :** CK et IK dérivés du secret partagé K

2.4.2 Authentification par hachage HTTP

Pour l'authentification non-IMS (si utilisée) :

Algorithme : MD5 (RFC 2617)

- **Fonction de hachage :** MD5 (sortie de 128 bits)
- **Challenge-Réponse :** Basé sur nonce
- **Protection contre la répétition :** Nonce avec horodatage

Remarque : L'authentification HTTP Digest avec MD5 est considérée comme faible. L'IMS AKA est fortement préférée.

2.5 Hachage et intégrité

2.5.1 Fonctions de hachage disponibles

le système peut utiliser (via OpenSSL/crypto du noyau) :

- **SHA-256 :** Sortie de 256 bits, recommandé
- **SHA-384 :** Sortie de 384 bits
- **SHA-512 :** Sortie de 512 bits
- **SHA-1 :** Sortie de 160 bits, déprécié pour un usage de sécurité
- **MD5 :** Sortie de 128 bits, déprécié pour un usage de sécurité

Utilisation :

- Constructions HMAC pour IPsec/TLS
- Vérification de l'intégrité des données
- Génération de nonce
- Détection de doublons (hachage Call-ID)

2.5.2 Intégrité des messages

Intégrité des messages SIP :

- **IPsec ESP :** HMAC-SHA256 pour SIP authentifié sur IPsec
- **TLS :** Authentification des messages via MAC TLS
- **Digest SIP :** Intégrité de l'en-tête d'authentification

Intégrité des messages Diameter :

- **TLS :** Diameter sur TLS fournit une authentification des messages
- **HMAC :** Les messages Diameter peuvent inclure des AVPs HMAC pour l'intégrité

2.6 Génération de nombres aléatoires

Génération de nombres aléatoires cryptographiquement sécurisée :

le système s'appuie sur :

- **Linux kernel /dev/urandom :** PRNG (Générateur de nombres pseudo-aléatoires cryptographiquement sécurisé)
- **OpenSSL RAND_bytes() :** CSPRNG (Générateur de nombres pseudo-aléatoires cryptographiquement sécurisé)

Utilisation :

- Allocation de SPI (valeur de départ aléatoire)
- Génération de Call-ID
- Génération de paramètres de branche
- Génération de nonce pour l'authentification
- Génération d'ID de session

2.7 Gestion des clés

2.7.1 Gestion des certificats TLS

Stockage des certificats :

- Stockage dans le système de fichiers avec des permissions restreintes (0600)
- Situé dans : `/etc/system/tls/`
- Format PEM pour les certificats et les clés

Génération de certificats :

```
# Générer une clé privée RSA de 4096 bits
openssl genrsa -out system-key.pem 4096

# Générer une CSR (demande de signature de certificat)
openssl req -new -key system-key.pem -out system.csr \
  -subj "/C=FR/ST=IDF/L=Paris/O=Omnitouch/
CN=scscf.ims.mnc001.mcc001.3gppnetwork.org"

# Certificat auto-signé (développement/test)
openssl x509 -req -days 365 -in system.csr \
  -signkey system-key.pem -out system-cert.pem

# Production : Soumettre la CSR à une CA de confiance
```

Rotation des certificats :

- Renouvellement annuel des certificats recommandé
- Redémarrage du service en douceur pour charger de nouveaux certificats
- Aucun temps d'arrêt requis

2.7.2 Gestion des clés IPsec

Dérivation de clé :

- CK (Cipher Key) et IK (Integrity Key) à partir de l'IMS AKA
- Clés de 128 bits du HSS
- Livrées en toute sécurité via Diameter Cx (sur TLS)

Durée de vie des clés :

- Liée à l'expiration de l'enregistrement SIP (généralement 599 secondes)
- Re-dérivation lors du rafraîchissement de l'enregistrement
- Destruction automatique des clés lors du désenregistrement

Stockage des clés :

- Éphémère (en mémoire uniquement pendant l'enregistrement actif)
- Installé dans la pile IPsec du noyau
- Pas de stockage persistant des clés
- Clés supprimées lorsque SA supprimée

2.8 Résistance à la cryptanalyse

2.8.1 Sélection d'algorithmes

Défense contre la cryptanalyse :

- **Pas d'algorithmes personnalisés :** Uniquement des algorithmes standard de l'industrie, examinés par des pairs
- **Taille de clé forte :** AES-256, RSA-4096, SHA-256
- **Chiffrement authentifié :** AES-GCM (AEAD - Chiffrement authentifié avec données associées)
- **Confidentialité parfaite à l'avance :** ECDHE/DHE dans TLS
- **Mises à jour régulières :** Patches de sécurité OpenSSL/LibreSSL appliqués

Algorithmes dépréciés désactivés :

- MD5 (collisions de hachage)
- RC4 (faiblesses du chiffre de flux)
- DES/3DES (petite taille de bloc, longueur de clé)
- SSL 2.0/3.0 (vulnérabilités de protocole)
- TLS 1.0/1.1 (attaques BEAST, POODLE)

2.8.2 Atténuation des attaques par canaux auxiliaires

Résistance aux attaques par temporisation :

- Comparaison en temps constant pour les réponses d'authentification
- Pas de fuites de temporisation dans les opérations cryptographiques (via OpenSSL)

Protection de la mémoire :

- Isolation de la pile IPsec du noyau
- Isolation de la mémoire des processus
- Pas de swap pour les données sensibles (si configuré)

2.9 Conformité et normes

Conformité aux normes cryptographiques :

- **NIST SP 800-52 :** Directives TLS
- **NIST SP 800-131A :** Transitions d'algorithmes cryptographiques
- **RFC 7525 :** Recommandations TLS

- **ETSI TS 133 203 :** Sécurité d'accès 3GPP (IMS AKA)
- **ETSI TS 133 210 :** Sécurité de couche réseau IP (IPsec)
- **3GPP TS 33.203 :** Sécurité d'accès pour IMS
- **3GPP TS 33.210 :** Sécurité de domaine réseau

Réglementations françaises en matière de cryptographie :

- Pas de cryptographie restreinte à l'exportation (tous les algorithmes standard)
- Moyens cryptographiques standard (pas de portes dérobées gouvernementales)
- Certification de produit cryptographique ANSSI (si requise)

Référence des métriques IMS CSCF

Ce document fournit une référence complète pour toutes les métriques exportées par les composants P-CSCF, I-CSCF et S-CSCF.

Accès aux métriques

Tous les composants CSCF exposent des métriques Prometheus sur le port 9090 :

```
http://<host>:9090/metrics
```

Chaque hôte CSCF (P-CSCF, I-CSCF, S-CSCF) exporte ses propres métriques. Configurez votre serveur Prometheus pour extraire toutes les hôtes pour une couverture de surveillance complète.

Exemple de configuration Prometheus :

```
scrape_configs:
  - job_name: 'cscf_pcscf'
    static_configs:
      - targets: ['pcscf1.example.com:9090',
'pcscf2.example.com:9090']

  - job_name: 'cscf_icscf'
    static_configs:
      - targets: ['icscf1.example.com:9090']

  - job_name: 'cscf_scscf'
    static_configs:
      - targets: ['scscf1.example.com:9090',
'scscf2.example.com:9090']
```

Pour des conseils opérationnels sur la surveillance et l'alerte, voir :

- Guide des opérations de l'interface Web
- Guide de capacité et de dimensionnement

Surveillance via le panneau de contrôle

Le panneau de contrôle OmniCall CSCF fournit une visibilité en temps réel sur l'état opérationnel qui génère ces métriques. Alors que les métriques sont exportées via Prometheus pour une analyse historique et des alertes, le panneau de contrôle montre l'état actuel des enregistrements, des dialogues et des pairs

Diameter.

Gestion S-CSCF

Voir les enregistrements actifs et les données de localisation des utilisateurs :

Le nombre d'enregistrements visible dans l'interface utilisateur correspond à des métriques telles que `ims_usrloc_scscf_active_impus` et `ims_usrloc_scscf_active_contacts`.

Surveillance des pairs Diameter

Surveillez l'état des pairs Diameter et les longueurs de file d'attente :

La longueur de la file d'attente affichée ici correspond à la métrique `cdp_queuelength`. L'état du pair "I_Open" indique des connexions saines.

Chaque pair montre les applications Diameter prises en charge. Par exemple :

- **16777216:10415 (Cx/Dx)** - Utilisé par I-CSCF et S-CSCF pour la communication HSS (UAR, LIR, MAR, SAR)
- **16777236:10415 (Rx)** - Utilisé par P-CSCF pour la politique QoS PCRF
- **4 (Ro)** - Utilisé par S-CSCF pour le chargement en ligne

Ceci correspond à des métriques telles que `ims_icscf_uar_*`, `ims_icscf_lir_*`, `ims_auth_mar_*`, `ims_registrar_scscf_sar_*`, et `ims_qos_*`.

Métriques P-CSCF

Métriques CDP (Diameter)

Nom de la métrique	Signification
`cdp_average_response_time`	Temps de réponse moyen pour les requêtes Diameter en millisecondes (calculé comme replies_response_time / replies_received)
`cdp_queuelength`	Longueur actuelle de la file d'attente des tâches de travail Diameter
`cdp_replies_received`	Nombre total de réponses Diameter reçues
`cdp_replies_response_time`	Temps total passé à attendre les réponses Diameter en millisecondes
`cdp_timeout`	Nombre d'événements de timeout sur les requêtes Diameter

Statistiques SIP de base

Compteurs de requêtes

Nom de la métrique	Signification
core_rcv_requests	Nombre total de requêtes SIP reçues
core_rcv_requests_ack	Nombre de requêtes ACK reçues
core_rcv_requests_bye	Nombre de requêtes BYE reçues
core_rcv_requests_cancel	Nombre de requêtes CANCEL reçues
core_rcv_requests_info	Nombre de requêtes INFO reçues
core_rcv_requests_invite	Nombre de requêtes INVITE reçues
core_rcv_requests_message	Nombre de requêtes MESSAGE reçues
core_rcv_requests_notify	Nombre de requêtes NOTIFY reçues
core_rcv_requests_options	Nombre de requêtes OPTIONS reçues
core_rcv_requests_prack	Nombre de requêtes PRACK reçues
core_rcv_requests_publish	Nombre de requêtes PUBLISH reçues
core_rcv_requests_refer	Nombre de requêtes REFER reçues
core_rcv_requests_register	Nombre de requêtes REGISTER reçues
core_rcv_requests_subscribe	Nombre de requêtes SUBSCRIBE reçues
core_rcv_requests_update	Nombre de requêtes UPDATE reçues

Compteurs de réponses (Général)

Nom de la métrique	Signification
core_rcv_replies	Nombre total de réponses SIP reçues
core_rcv_replies_18x	Nombre de réponses provisoires 180/181/183/186/187/189 reçues
core_rcv_replies_1xx	Nombre de réponses 1xx (provisoires) reçues
core_rcv_replies_2xx	Nombre de réponses 2xx (succès) reçues
core_rcv_replies_3xx	Nombre de réponses 3xx (redirection) reçues
core_rcv_replies_4xx	Nombre de réponses 4xx (erreur client) reçues
core_rcv_replies_5xx	Nombre de réponses 5xx (erreur serveur) reçues
core_rcv_replies_6xx	Nombre de réponses 6xx (échec global) reçues

Compteurs de réponses par méthode (1xx)

Nom de la métrique	Signification
core_rcv_replies_1xx_bye	Nombre de réponses 1xx aux requêtes BYE
core_rcv_replies_1xx_cancel	Nombre de réponses 1xx aux requêtes CANCEL
core_rcv_replies_1xx_invite	Nombre de réponses 1xx aux requêtes INVITE
core_rcv_replies_1xx_message	Nombre de réponses 1xx aux requêtes MESSAGE
core_rcv_replies_1xx_prack	Nombre de réponses 1xx aux requêtes PRACK
core_rcv_replies_1xx_refer	Nombre de réponses 1xx aux requêtes REFER

Nom de la métrique	Signification
core_rcv_replies_1xx_reg	Nombre de réponses 1xx aux requêtes REGISTER
core_rcv_replies_1xx_update	Nombre de réponses 1xx aux requêtes UPDATE

Compteurs de réponses par méthode (2xx)

Nom de la métrique	Signification
core_rcv_replies_2xx_bye	Nombre de réponses 2xx (succès) aux requêtes BYE
core_rcv_replies_2xx_cancel	Nombre de réponses 2xx (succès) aux requêtes CANCEL
core_rcv_replies_2xx_invite	Nombre de réponses 2xx (succès) aux requêtes INVITE
core_rcv_replies_2xx_message	Nombre de réponses 2xx (succès) aux requêtes MESSAGE
core_rcv_replies_2xx_prack	Nombre de réponses 2xx (succès) aux requêtes PRACK
core_rcv_replies_2xx_refer	Nombre de réponses 2xx (succès) aux requêtes REFER
core_rcv_replies_2xx_reg	Nombre de réponses 2xx (succès) aux requêtes REGISTER
core_rcv_replies_2xx_update	Nombre de réponses 2xx (succès) aux requêtes UPDATE

Compteurs de réponses par méthode (3xx)

Nom de la métrique	Signification
core_rcv_replies_3xx_bye	Nombre de réponses 3xx (redirection) aux requêtes BYE
core_rcv_replies_3xx_cancel	Nombre de réponses 3xx (redirection) aux requêtes CANCEL
core_rcv_replies_3xx_invite	Nombre de réponses 3xx (redirection) aux requêtes INVITE
core_rcv_replies_3xx_message	Nombre de réponses 3xx (redirection) aux requêtes MESSAGE
core_rcv_replies_3xx_prack	Nombre de réponses 3xx (redirection) aux requêtes PRACK
core_rcv_replies_3xx_refer	Nombre de réponses 3xx (redirection) aux requêtes REFER
core_rcv_replies_3xx_reg	Nombre de réponses 3xx (redirection) aux requêtes REGISTER
core_rcv_replies_3xx_update	Nombre de réponses 3xx (redirection) aux requêtes UPDATE

Compteurs de réponses par méthode (4xx)

Nom de la métrique	Signification
core_rcv_replies_4xx_bye	Nombre de réponses 4xx (erreur client) aux requêtes BYE
core_rcv_replies_4xx_cancel	Nombre de réponses 4xx (erreur client) aux requêtes CANCEL
core_rcv_replies_4xx_invite	Nombre de réponses 4xx (erreur client) aux requêtes INVITE
core_rcv_replies_4xx_message	Nombre de réponses 4xx (erreur client) aux requêtes MESSAGE
core_rcv_replies_4xx_prack	Nombre de réponses 4xx (erreur client) aux requêtes PRACK
core_rcv_replies_4xx_refer	Nombre de réponses 4xx (erreur client) aux requêtes REFER
core_rcv_replies_4xx_reg	Nombre de réponses 4xx (erreur client) aux requêtes REGISTER
core_rcv_replies_4xx_update	Nombre de réponses 4xx (erreur client) aux requêtes UPDATE

Compteurs de réponses par méthode (5xx)

Nom de la métrique	Signification
core_rcv_replies_5xx_bye	Nombre de réponses 5xx (erreur serveur) aux requêtes BYE
core_rcv_replies_5xx_cancel	Nombre de réponses 5xx (erreur serveur) aux requêtes CANCEL
core_rcv_replies_5xx_invite	Nombre de réponses 5xx (erreur serveur) aux requêtes INVITE
core_rcv_replies_5xx_message	Nombre de réponses 5xx (erreur serveur) aux requêtes MESSAGE
core_rcv_replies_5xx_prack	Nombre de réponses 5xx (erreur serveur) aux requêtes PRACK
core_rcv_replies_5xx_refer	Nombre de réponses 5xx (erreur serveur) aux requêtes REFER
core_rcv_replies_5xx_reg	Nombre de réponses 5xx (erreur serveur) aux requêtes REGISTER
core_rcv_replies_5xx_update	Nombre de réponses 5xx (erreur serveur) aux requêtes UPDATE

Compteurs de réponses par méthode (6xx)

Nom de la métrique	Signification
core_rcv_replies_6xx_bye	Nombre de réponses 6xx (échec global) aux requêtes BYE

Nom de la métrique	Signification
core_rcv_replies_6xx_cancel	Nombre de réponses 6xx (échec global) aux requêtes CANCEL
core_rcv_replies_6xx_invite	Nombre de réponses 6xx (échec global) aux requêtes INVITE
core_rcv_replies_6xx_message	Nombre de réponses 6xx (échec global) aux requêtes MESSAGE
core_rcv_replies_6xx_prack	Nombre de réponses 6xx (échec global) aux requêtes PRACK
core_rcv_replies_6xx_refer	Nombre de réponses 6xx (échec global) aux requêtes REFER
core_rcv_replies_6xx_reg	Nombre de réponses 6xx (échec global) aux requêtes REGISTER
core_rcv_replies_6xx_update	Nombre de réponses 6xx (échec global) aux requêtes UPDATE

Compteurs de codes d'état spécifiques

Nom de la métrique	Signification
core_rcv_replies_400	Nombre de réponses 400 Bad Request reçues
core_rcv_replies_401	Nombre de réponses 401 Unauthorized reçues
core_rcv_replies_402	Nombre de réponses 402 Payment Required reçues
core_rcv_replies_403	Nombre de réponses 403 Forbidden reçues
core_rcv_replies_404	Nombre de réponses 404 Not Found reçues
core_rcv_replies_405	Nombre de réponses 405 Method Not Allowed reçues
core_rcv_replies_406	Nombre de réponses 406 Not Acceptable reçues
core_rcv_replies_407	Nombre de réponses 407 Proxy Authentication Required reçues
core_rcv_replies_408	Nombre de réponses 408 Request Timeout reçues
core_rcv_replies_409	Nombre de réponses 409 Conflict reçues
core_rcv_replies_410	Nombre de réponses 410 Gone reçues
core_rcv_replies_411	Nombre de réponses 411 Length Required reçues
core_rcv_replies_413	Nombre de réponses 413 Request Entity Too Large reçues
core_rcv_replies_414	Nombre de réponses 414 Request-URI Too Long reçues
core_rcv_replies_415	Nombre de réponses 415 Unsupported Media Type reçues
core_rcv_replies_420	Nombre de réponses 420 Bad Extension reçues
core_rcv_replies_480	Nombre de réponses 480 Temporarily Unavailable reçues
core_rcv_replies_481	Nombre de réponses 481 Call/Transaction Does Not Exist reçues
core_rcv_replies_482	Nombre de réponses 482 Loop Detected reçues
core_rcv_replies_483	Nombre de réponses 483 Too Many Hops reçues
core_rcv_replies_484	Nombre de réponses 484 Address Incomplete reçues
core_rcv_replies_485	Nombre de réponses 485 Ambiguous reçues

Nom de la métrique	Signification
core_rcv_replies_486	Nombre de réponses 486 Busy Here reçues
core_rcv_replies_487	Nombre de réponses 487 Request Terminated reçues
core_rcv_replies_488	Nombre de réponses 488 Not Acceptable Here reçues
core_rcv_replies_489	Nombre de réponses 489 Bad Event reçues
core_rcv_replies_491	Nombre de réponses 491 Request Pending reçues
core_rcv_replies_493	Nombre de réponses 493 Undecipherable reçues

Statistiques de transfert et d'erreur

Nom de la métrique	Signification
core_fwd_replies	Nombre de réponses SIP transférées
core_fwd_requests	Nombre de requêtes SIP transférées
core_drop_replies	Nombre de réponses SIP abandonnées
core_drop_requests	Nombre de requêtes SIP abandonnées
core_err_replies	Nombre de réponses d'erreur
core_err_requests	Nombre de requêtes d'erreur
core_bad_URIs_rcvd	Nombre de messages avec des URI malformés reçus
core_bad_msg_hdr	Nombre de messages avec des en-têtes mauvais/ malformés
core_unsupported_methods	Nombre de requêtes avec des méthodes SIP non prises en charge

Suivi des dialogues

Nom de la métrique	Signification
dialog_ng_active	Nombre de dialogues actuellement actifs (répondu/ confirmé)
dialog_ng_early	Nombre de dialogues précoces (sonnant/état provisoire)
dialog_ng_expired	Nombre de dialogues qui ont expiré ou ont été forcés à se terminer
dialog_ng_processed	Nombre total de dialogues traités depuis le démarrage

Statistiques DNS

Nom de la métrique	Signification
dns_failed_dns_request	Nombre de requêtes DNS échouées
dns_slow_dns_request	Nombre de requêtes DNS lentes (dépassant le seuil)

IMS IPSec P-CSCF

Nom de la métrique	Signification
ims_ipsec_pcscf_spi_free	Nombre de valeurs SPI (Security Parameter Index) libres disponibles

Nom de la métrique	Signification
	pour allocation
ims_ipsec_pcscf_spi_total	Capacité totale SPI configurée pour le système
ims_ipsec_pcscf_spi_used	Nombre de valeurs SPI actuellement allouées/utilisées
ims_ipsec_pcscf_spi_utilization_pct	Pourcentage d'utilisation du pool SPI
ims_ipsec_pcscf_worker_cache_size	Taille du cache IPSec du processus de travail

IMS QoS (Interface Rx)

Métriques AAR d'enregistrement

Nom de la métrique	Signification
ims_qos_active_registration_rx_sessions	Nombre de sessions d'enregistrement Rx actuellement actives
ims_qos_registration_aars	Nombre total de messages AAR (Authorization-Authentication Request) d'enregistrement envoyés
ims_qos_successful_registration_aars	Nombre de transactions AAR d'enregistrement réussies
ims_qos_failed_registration_aars	Nombre de transactions AAR d'enregistrement échouées
ims_qos_registration_aar_avg_response_time	Temps de réponse moyen pour les messages AAR d'enregistrement en millisecondes
ims_qos_registration_aar_response_time	Temps total de réponse pour tous les messages AAR d'enregistrement en millisecondes
ims_qos_registration_aar_replies_received	Nombre total de réponses AAR d'enregistrement reçues
ims_qos_registration_aar_timeouts	Nombre de timeouts de requêtes AAR d'enregistrement

Métriques AAR de média

Nom de la métrique	Signification
ims_qos_active_media_rx_sessions	Nombre de sessions Rx de média actuellement actives
ims_qos_media_rx_sessions	Nombre total de sessions Rx de média

Nom de la métrique	Signification
	créées
ims_qos_media_aars	Nombre total de messages AAR de média envoyés
ims_qos_successful_media_aars	Nombre de transactions AAR de média réussies
ims_qos_failed_media_aars	Nombre de transactions AAR de média échouées
ims_qos_media_aar_avg_response_time	Temps de réponse moyen pour les messages AAR de média en millisecondes
ims_qos_media_aar_response_time	Temps total de réponse pour tous les messages AAR de média en millisecondes
ims_qos_media_aar_replies_received	Nombre total de réponses AAR de média reçues
ims_qos_media_aar_timeouts	Nombre de timeouts de requêtes AAR de média

Métriques ASR

Nom de la métrique	Signification
ims_qos_asrs	Nombre total de messages ASR (Abort-Session-Request) reçus de PCRF

IMS USRLOC P-CSCF

Nom de la métrique	Signification
ims_usrloc_pcscf_expired_contacts	Nombre de liaisons de contact expirées
ims_usrloc_pcscf_registered_contacts	Nombre de liaisons de contact actuellement enregistrées
ims_usrloc_pcscf_registered_impus	Nombre d'IMPUs (IMS Public User Identities) actuellement enregistrés

Base de données MySQL

Nom de la métrique	Signification
mysql_driver_errors	Nombre d'erreurs de connexion/driver MySQL

Module Pike (Blocage IP)

Nom de la métrique	Signification
pike_blocked_ips	Nombre d'adresses IP actuellement bloquées (détection d'inondation)

Module Registrar

Nom de la métrique	Signification
registrar_accepted_regs	Nombre de requêtes REGISTER acceptées (module de registraire hérité)
registrar_rejected_regs	Nombre de requêtes REGISTER rejetées (module de registraire hérité)
registrar_default_expire	Temps d'expiration par défaut pour les enregistrements en secondes
registrar_default_expires_range	Plage d'expiration par défaut configurée
registrar_expires_range	Plage d'expiration configurée
registrar_max_contacts	Nombre maximum de contacts autorisés par AOR
registrar_max_expires	Temps d'expiration maximum autorisé en secondes

Statistiques de script

Nom de la métrique	Signification
script_register_failed	Nombre de tentatives d'enregistrement échouées dans la logique de script de routage
script_register_success	Nombre d'enregistrements réussis traités par le script de routage
script_register_time	Temps total passé à traiter les enregistrements dans le script de routage (millisecondes)

Transport SCTP

Nom de la métrique	Signification
sctp_assoc_shutdown	Nombre de fermetures d'associations SCTP initiées localement
sctp_comm_lost	Nombre d'associations SCTP perdues en raison d'une défaillance de communication
sctp_connect_failed	Nombre de tentatives de connexion SCTP sortantes échouées
sctp_current_opened_connections	Nombre d'associations SCTP actuellement ouvertes
sctp_current_tracked_connections	Nombre d'associations SCTP actuellement

Nom de la métrique	Signification
	suivies
sctp_established	Nombre total d'associations SCTP établies
sctp_local_reject	Nombre d'associations SCTP entrantes rejetées localement
sctp_remote_shutdown	Nombre de fermetures d'associations SCTP initiées par le pair
sctp_send_failed	Nombre d'opérations d'envoi SCTP échouées
sctp_send_force_retry	Nombre de nouvelles tentatives forcées sur les envois SCTP échoués
sctp_sendq_full	Nombre de tentatives d'envoi échouées en raison d'une file d'envoi pleine

Mémoire partagée

Nom de la métrique	Signification
shmem_fragments	Nombre de fragments dans le pool de mémoire partagée (indique la fragmentation)
shmem_free_size	Montant de mémoire partagée libre en octets
shmem_max_used_size	Taille maximale de mémoire partagée utilisée depuis le démarrage en octets
shmem_real_used_size	Mémoire partagée réellement utilisée, y compris la surcharge de l'allocateur en octets
shmem_total_size	Taille totale du pool de mémoire partagée en octets
shmem_used_size	Mémoire partagée actuellement utilisée (données utilisateur uniquement) en octets

Module SL (sans état)

Compteurs de réponses sans état par classe

Nom de la métrique	Signification
sl_1xx_replies	Nombre de réponses sans état 1xx envoyées
sl_2xx_replies	Nombre de réponses sans état 2xx envoyées
sl_3xx_replies	Nombre de réponses sans état 3xx envoyées
sl_4xx_replies	Nombre de réponses sans état 4xx envoyées
sl_5xx_replies	Nombre de réponses sans état 5xx envoyées
sl_6xx_replies	Nombre de réponses sans état 6xx envoyées
sl_xxx_replies	Nombre d'autres réponses sans état envoyées

Compteurs de réponses sans état spécifiques

Nom de la métrique	Signification
sl_200_replies	Nombre de réponses sans état 200 OK envoyées
sl_202_replies	Nombre de réponses sans état 202 Accepted envoyées
sl_300_replies	Nombre de réponses sans état 300 Multiple Choices envoyées
sl_301_replies	Nombre de réponses sans état 301 Moved Permanently envoyées
sl_302_replies	Nombre de réponses sans état 302 Moved Temporarily envoyées
sl_400_replies	Nombre de réponses sans état 400 Bad Request envoyées
sl_401_replies	Nombre de réponses sans état 401 Unauthorized envoyées
sl_403_replies	Nombre de réponses sans état 403 Forbidden envoyées
sl_404_replies	Nombre de réponses sans état 404 Not Found envoyées
sl_407_replies	Nombre de réponses sans état 407 Proxy Authentication Required envoyées
sl_408_replies	Nombre de réponses sans état 408 Request Timeout envoyées
sl_483_replies	Nombre de réponses sans état 483 Too Many Hops envoyées
sl_500_replies	Nombre de réponses sans état 500 Server Internal Error envoyées

Statistiques générales sans état

Nom de la métrique	Signification
sl_sent_replies	Nombre total de réponses sans état envoyées
sl_sent_err_replies	Nombre de réponses d'erreur sans état envoyées
sl_received_ACKs	Nombre de messages ACK reçus pour des transactions sans état
sl_failures	Nombre d'échecs d'envoi de réponses sans état

Transport TCP

Nom de la métrique	Signification
tcp_con_reset	Nombre de connexions TCP réinitialisées (RST reçues sur une connexion établie)
tcp_con_timeout	Nombre de connexions TCP fermées en raison d'un timeout d'inactivité
tcp_connect_failed	Nombre de tentatives de connexion TCP sortantes échouées
tcp_connect_success	Nombre de connexions TCP sortantes réussies
tcp_current_opened_connections	Nombre de connexions TCP actuellement ouvertes
tcp_current_write_queue_size	Taille totale actuelle des files d'écriture TCP

Nom de la métrique	Signification
	sur toutes les connexions
tcp_established	Nombre total de connexions TCP établies (entrantes et sortantes)
tcp_local_reject	Nombre de connexions TCP entrantes rejetées localement
tcp_passive_open	Nombre de connexions TCP entrantes acceptées
tcp_send_timeout	Nombre d'opérations d'envoi TCP qui ont expiré (mode asynchrone)
tcp_sendq_full	Nombre de tentatives d'envoi échouées parce que la file d'envoi était pleine

Module TM/TMX (Transaction)

Compteurs de type de transaction

Nom de la métrique	Signification
tmx_UAC_transactions	Nombre de transactions UAC (client) créées
tmx_UAS_transactions	Nombre de transactions UAS (serveur) créées
tmx_active_transactions	Nombre de transactions actuellement actives
tmx_inuse_transactions	Nombre de transactions actuellement en cours d'utilisation

Achèvement de transaction par statut

Nom de la métrique	Signification
tmx_2xx_transactions	Nombre de transactions complétées avec une réponse 2xx
tmx_3xx_transactions	Nombre de transactions complétées avec une réponse 3xx
tmx_4xx_transactions	Nombre de transactions complétées avec une réponse 4xx
tmx_5xx_transactions	Nombre de transactions complétées avec une réponse 5xx
tmx_6xx_transactions	Nombre de transactions complétées avec une réponse 6xx

Statistiques de réponse de transaction

Nom de la métrique	Signification
tmx_rpl_absorbed	Nombre de réponses absorbées par la couche de transaction (doublons)
tmx_rpl_generated	Nombre de réponses générées localement par le module de

Nom de la métrique	Signification
	transaction
tmx_rpl_received	Nombre de réponses reçues pour des transactions
tmx_rpl_relayed	Nombre de réponses relayées par le module de transaction
tmx_rpl_sent	Nombre de réponses envoyées par le module de transaction

USRLOC (Localisation de l'utilisateur)

Nom de la métrique	Signification
usrloc_location_contacts	Nombre de contacts dans le domaine 'location' (module usrloc standard)
usrloc_location_expires	Nombre de contacts expirés dans le domaine 'location'
usrloc_registered_users	Nombre d'utilisateurs/AORs (Address of Records) enregistrés

---

Métriques I-CSCF

L'I-CSCF partage la plupart des statistiques SIP de base avec le P-CSCF (voir la section Statistiques SIP de base P-CSCF ci-dessus). Les métriques suivantes sont spécifiques à la fonctionnalité I-CSCF.

Contexte opérationnel I-CSCF

L'I-CSCF maintient une liste d'instances S-CSCF disponibles pour l'équilibrage de charge :

L'I-CSCF interroge le HSS pour sélectionner les instances S-CSCF appropriées pour les nouveaux enregistrements. Le succès de ces opérations est suivi dans les métriques UAR et LIR ci-dessous.

IMS I-CSCF (Interface Cx - Communication HSS)

L'I-CSCF utilise l'interface Diameter Cx pour communiquer avec le HSS (Home Subscriber Server) pour les requêtes de localisation et d'autorisation des utilisateurs.

Métriques UAR (User-Authorization-Request)

Nom de la métrique	Signification
ims_icscf_uar_avg_response_time	Temps de réponse moyen pour les messages UAR en millisecondes (calculé comme uar_replies_response_time /

Nom de la métrique	Signification
	uar_replies_received)
ims_icscf_uar_replies_received	Nombre total de réponses UAA (User-Authorization-Answer) reçues du HSS
ims_icscf_uar_replies_response_time	Temps total de réponse pour tous les messages UAR en millisecondes
ims_icscf_uar_timeouts	Nombre de timeouts de requêtes UAR

Métriques LIR (Location-Info-Request)

Nom de la métrique	Signification
ims_icscf_lir_avg_response_time	Temps de réponse moyen pour les messages LIR en millisecondes (calculé comme lir_replies_response_time / lir_replies_received)
ims_icscf_lir_replies_received	Nombre total de réponses LIA (Location-Info-Answer) reçues du HSS
ims_icscf_lir_replies_response_time	Temps total de réponse pour tous les messages LIR en millisecondes
ims_icscf_lir_timeouts	Nombre de timeouts de requêtes LIR

Métriques communes

L'I-CSCF exporte également les métriques communes suivantes (documentées dans la section P-CSCF ci-dessus) :

- **Métriques CDP (Diameter)** - Statistiques du protocole Diameter
- **Statistiques SIP de base** - Compteurs de requêtes/réponses par méthode et code d'état
- **Statistiques DNS** - Métriques de requêtes DNS
- **Base de données MySQL** - Erreurs de connexion à la base de données
- **Module Pike** - Statistiques de blocage IP
- **Mémoire partagée** - Statistiques d'utilisation de la mémoire
- **Module SL (sans état)** - Compteurs de réponses sans état
- **Transport TCP** - Statistiques de connexion TCP
- **Module TM/TMX (Transaction)** - Suivi de l'état des transactions

---

Métriques S-CSCF

Le S-CSCF partage la plupart des statistiques SIP de base avec le P-CSCF et l'I-CSCF (voir la section Statistiques SIP de base P-CSCF ci-dessus). Les métriques suivantes sont spécifiques à la fonctionnalité S-CSCF.

Contexte opérationnel S-CSCF

Le S-CSCF fournit des informations détaillées sur la localisation des utilisateurs et la gestion des IFC (Critères de Filtrage Initiaux) :

La recherche de localisation des utilisateurs montre les IMPUs enregistrés avec des liaisons de contact et des profils de service. Le nombre de contacts et d'IMPUs actifs est suivi par les métriques `ims_usrloc_scscf_active_contacts` et `ims_usrloc_scscf_active_impus`.

L'IFC (Critères de Filtrage Initiaux) détermine quels serveurs d'application traitent les sessions SIP. Le panneau de contrôle permet de décharger et de tester les règles IFC. La performance de l'évaluation des IFC peut impacter les temps de configuration des appels suivis dans les métriques de transaction (`tmx_*`).

Authentification IMS (Interface Cx - MAR)

Le S-CSCF utilise l'interface Diameter Cx pour authentifier les utilisateurs avec le HSS via MAR (Multimedia-Auth-Request).

Nom de la métrique	Signification
`ims_auth_mar_avg_response_time`	Temps de réponse moyen pour les messages MAR en millisecondes (calculé comme mar_replies_response_time / mar_replies_received)
`ims_auth_mar_replies_received`	Nombre total de réponses MAA (Multimedia-Auth-Answer) reçues du HSS
`ims_auth_mar_replies_response_time`	Temps total de réponse pour tous les messages MAR en millisecondes
`ims_auth_mar_timeouts`	Nombre de timeouts de requêtes MAR

Registraire IMS S-CSCF

Statistiques d'enregistrement

Nom de la métrique	Signification
`ims_registrar_scscf_accepted_regs`	Nombre de requêtes REGISTER acceptées avec succès
`ims_registrar_scscf_rejected_regs`	Nombre de requêtes REGISTER rejetées
`ims_registrar_scscf_default_expire`	Temps d'expiration par défaut pour les enregistrements en secondes
`ims_registrar_scscf_default_expires_range`	Configuration de la plage d'expiration par défaut

Nom de la métrique	Signification
ims_registrar_scscf_max_contacts	Nombre maximum de contacts autorisés par enregistrement
ims_registrar_scscf_max_expires	Temps d'expiration maximum autorisé en secondes
ims_registrar_scscf_notifies_in_q	Nombre de messages NOTIFY en attente dans la file d'attente

Métriques SAR (Server-Assignment-Request)

Nom de la métrique	Signification
ims_registrar_scscf_sar_avg_response_time	Temps de réponse moyen pour les messages SAR en millisecondes (calculé comme sar_replies_response_time / sar_replies_received)
ims_registrar_scscf_sar_replies_received	Nombre total de réponses SAA (Server-Assignment-Answer) reçues du HSS
ims_registrar_scscf_sar_replies_response_time	Temps total de réponse pour tous les messages SAR en millisecondes
ims_registrar_scscf_sar_timeouts	Nombre de timeouts de requêtes SAR

IMS USRLOC S-CSCF

Nom de la métrique	Signification
ims_usrloc_scscf_active_contacts	Nombre de liaisons de contact actuellement actives enregistrées
ims_usrloc_scscf_active_impus	Nombre d'IMPUs (IMS Public User Identities) actuellement actifs enregistrés
ims_usrloc_scscf_active_subscriptions	Nombre de souscriptions actuellement actives
ims_usrloc_scscf_contact_collisions	Nombre de collisions de hachage dans la table de hachage des contacts
ims_usrloc_scscf_impu_collisions	Nombre de collisions de hachage dans la table de hachage des IMPU
ims_usrloc_scscf_subscription_collisions	Nombre de collisions de hachage dans la table de hachage des souscriptions

Suivi des dialogues

Le S-CSCF suit l'état des dialogues pour les appels actifs :

Nom de la métrique	Signification
`dialog_ng_active`	Nombre de dialogues actuellement actifs (répondu/confirmé)
`dialog_ng_early`	Nombre de dialogues précoces (sonnant/état provisoire)
`dialog_ng_expired`	Nombre de dialogues qui ont expiré ou ont été forcés à se terminer
`dialog_ng_processed`	Nombre total de dialogues traités depuis le démarrage

Métriques communes

Le S-CSCF exporte également les métriques communes suivantes (documentées dans la section P-CSCF ci-dessus) :

- **Métriques CDP (Diameter)** - Statistiques du protocole Diameter
- **Statistiques SIP de base** - Compteurs de requêtes/réponses par méthode et code d'état (note : le S-CSCF a généralement un nombre plus élevé de fwd_requests et fwd_replies car il route entre les points de terminaison)
- **Statistiques DNS** - Métriques de requêtes DNS
- **Base de données MySQL** - Erreurs de connexion à la base de données
- **Module Pike** - Statistiques de blocage IP
- **Mémoire partagée** - Statistiques d'utilisation de la mémoire
- **Module SL (sans état)** - Compteurs de réponses sans état
- **Transport TCP** - Statistiques de connexion TCP
- **Module TM/TMX (Transaction)** - Suivi de l'état des transactions (note : le S-CSCF a généralement à la fois des transactions UAC et UAS car il agit à la fois comme client et serveur)