Dépannage de Visited-Network-Identifier AVP manquant sous Notify Request

Table des matières

Introduction

Ce document décrit comment dépanner le VNI manquant sous le message 'Notify request' entre MME et HSS sur l'interface S6a.

Conditions préalables

Spécifications techniques 3GPP - 29.272, 29.229

RFC (Request For Comments) - 6733

Exigences

Cisco recommande que vous connaissiez le guide d'administration de StarOS-Mobility Management Entity (MME).

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Notification Request and Answer (NOR/NOA) est l'un des messages les plus simples sur l'interface S6a/S6d. L'idée de base de ce message est d'informer le serveur HSS (Home Subscriber Server) de la modification des informations relatives au réseau et à l'équipement utilisateur.

La procédure de notification est utilisée entre le MME et le HSS, ainsi qu'entre le SGSN (Serving GPRS Support Node) et le HSS afin de notifier le HSS :

- Attribution/modification/suppression d'une passerelle PDN (Packet Data Network) pour un nom de point d'accès (APN)
- Lorsqu'une mise à jour d'emplacement entre MME n'a pas lieu, mais que le HSS doit être averti de la nécessité d'envoyer un emplacement d'annulation au SGSN actuel.
- L'entité utilisateur (UE) dispose d'une capacité de mémoire disponible pour recevoir un ou plusieurs messages courts
- L'UE est à nouveau accessible

Format de message de NOR-NOA

```
< Notify-Request> ::= < Diameter Header: 323, REQ, PXY, 16777251 >
                       < Session-Id >
                       [ Vendor-Specific-Application-Id ]
                       { Auth-Session-State }
                       { Origin-Host }
                       { Origin-Realm }
                        [ Destination-Host ]
                                                { Destination-Realm }

                       { User-Name }
                      * [ Supported-Features ]
                       [ Terminal-Information ]
                       [ MIP6-Agent-Info ]
                       [ Visited-Network-Identifier ]
                       [ Context-Identifier ]
                       [Service-Selection]
                       [ Alert-Reason ]
                       [ UE-SRVCC-Capability ]
                       [ NOR-Flags ]
                     [Homogeneous-Support-of-IMS-Voice-Over-PS-Sessions ]
                      *[ AVP ]


< Notify-Answer> ::= < Diameter Header: 323, PXY, 16777251 >
                      < Session-Id >
                      [ Vendor-Specific-Application-Id ]
                      [ Result-Code ]
                      [ Experimental-Result ]
                      { Auth-Session-State }
                      { Origin-Host }
                      { Origin-Realm }
                      [ OC-Supported-Features ]
                      [ OC-OLR ]
```

```
*[ Supported-Features ]
*[ AVP ]
*[ Failed-AVP ]
```

Process

1. Initiation : Le processus est généralement lancé par le MME lorsqu'un événement pertinent lié à l'UE se produit.
2. Message NOR : Le MME envoie un message NOR au HSS. Ce message inclut les identifiants nécessaires tels que l'identité internationale de l'abonné mobile (IMSI) et les détails de l'événement ou du changement.
3. Traitement par HSS : Le HSS traite la demande, met à jour ses enregistrements et peut effectuer d'autres actions si nécessaire en fonction des informations reçues.
4. Notifier la réponse : Le HSS renvoie une réponse de notification au MME, confirmant la mise à jour et incluant toutes les données ou instructions supplémentaires nécessaires.

Quel est le rôle de Visited Network Identifier AVP ?

La paire de valeurs d'attribut (AVP) VNI (Visited-Network-Identifier) est de type Octet-String. Ce protocole AVP contient un identificateur qui aide le réseau domestique à identifier le réseau visité (par exemple, le nom de domaine du réseau visité).

Le protocole VNI AVP sert à identifier le réseau où se trouve actuellement l'utilisateur, ou « visiteur », et est principalement utilisé dans les scénarios d'itinérance. Ces informations sont essentielles pour :

- Décisions de routage : S'assurer que les demandes et les réponses sont correctement acheminées entre le réseau domestique et le réseau visité.
- Application des politiques : Application de politiques de réseau et de règles de facturation appropriées en fonction de l'emplacement de l'utilisateur et des accords du réseau visité avec le réseau domestique.

7.3.105 Visited-Network-Identifier

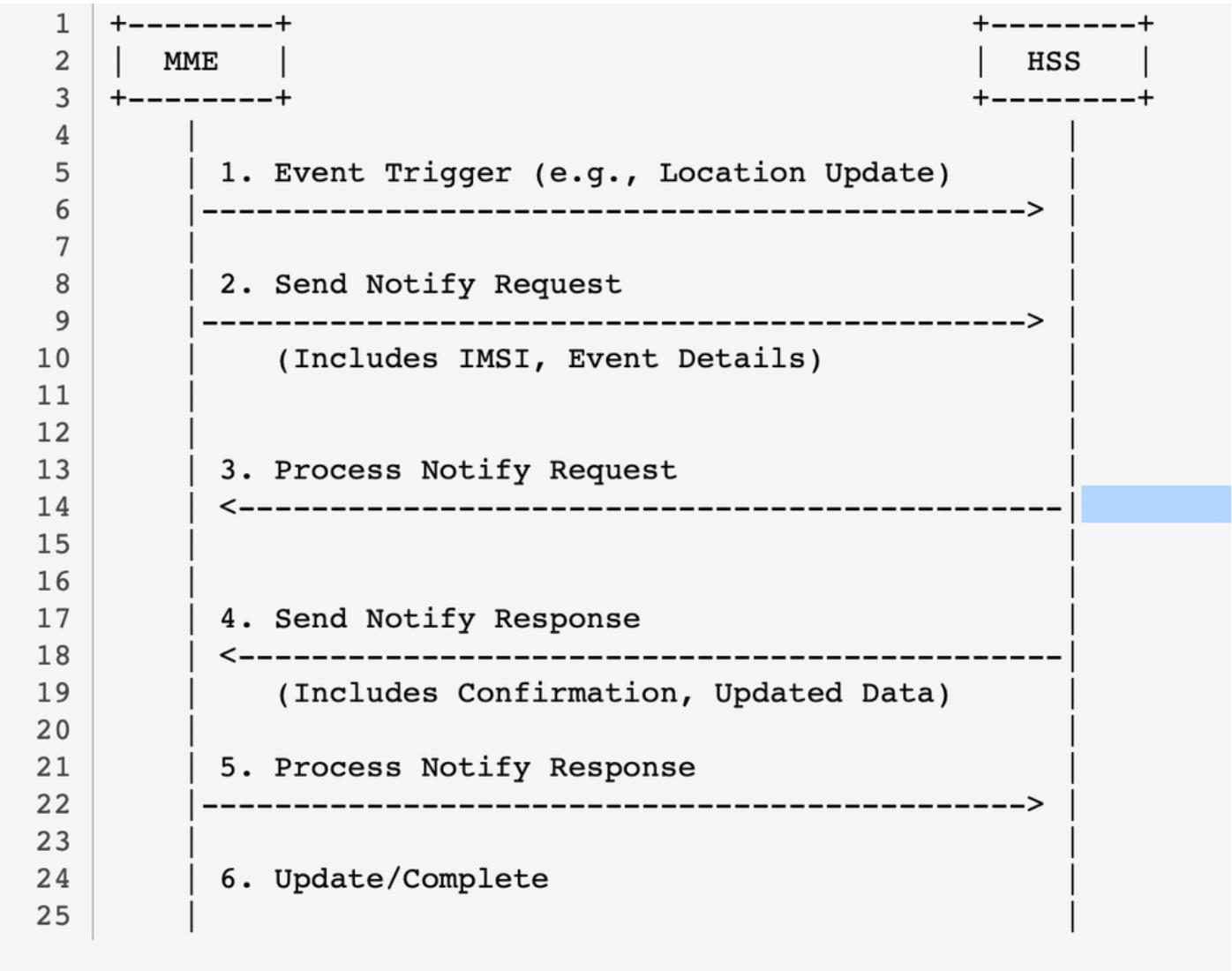
The Visited-Network-Identifier AVP contains the identity of the network where the PDN-GW was allocated, in the case of dynamic PDN-GW assignment.

The AVP shall be encoded as:

mnc<MNC>.mcc<MCC>.3gppnetwork.org

Référence 3gpp pour Visited-Network-Identifier AVP

Flux d’appels



flux d'appels NON-OU

Flux d'appels Notify-Request/Answer

1. Déclencheur d'événement dans MME

- Un événement d'abonné se produit dans le MME qui nécessite la notification du HSS. Exemples :
  - Une mise à jour d'emplacement
  - Un changement dans le réseau visité (par exemple, l'itinérance)
  - Une mise à jour de l'état de l'abonnement (par exemple, actif ou inactif)
- Le MME prépare un message NOR

2. MME envoie une requête de notification

- Le MME construit le message NOR avec ces AVP clés :
  - Contient le nom de domaine de l'ID du réseau mobile terrestre public (PLMN) du réseau visité où se trouve actuellement l'abonné.
  - ID de session : Identificateur unique de la session Diameter
  - Origin-Host et Origin-Realm : Identifie le MME en tant qu'expéditeur
  - Destination-Host et Destination-Realm : Identifie le HSS comme destinataire

- IMSI (User-Identifier) : Identificateur unique de l'abonné
- VNI
- Auth-Session-State : Indique si la session est avec ou sans état

3. HSS reçoit et traite la demande de notification

- Le HSS traite le NOR et valide ses AVP :
  - Cochez la case IMSI pour localiser l'enregistrement de l'abonné.
  - Valide le VNI afin de s'assurer qu'il correspond à un réseau connu et pris en charge.
  - Met à jour les données de l'abonné pour refléter le nouveau réseau ou état visité.
- Si la validation réussit, le HSS prépare une réponse positive.
- S'il y a des problèmes (par exemple, VNI manquant), le HSS prépare une réponse d'erreur.

4. HSS envoie une notification-réponse (NOA)

- Le HSS envoie un message NOA au MME :
  - DIAMETER_SUCCESS (2001) : Indique un traitement réussi
  - DIAMETER_INVALID_AVP_VALUE (5004) : Si le VNI est incorrect
  - DIAMETER_MISSING_AVP (5005) : Si le VNI est manquant mais requis
  - Contient le VNI AVP s'il est à l'origine de la panne
  - Code-Résultat
  - Échec du protocole AVP (le cas échéant)

5. MME gère la fonction Notify-Answer

- À la réception de l'avis :
  - Si Result-Code réussit, le MME continue ses opérations
  - Si une erreur est signalée, le MME analyse l'AVP défaillant (le cas échéant) afin d'identifier le problème

Dépannage

- L'aspect principal est de vérifier si la 'demande de notification' est 'activée' sur tous les 'services HSS'. Vous pouvez faire la même chose en exécutant cette interface de ligne de commande :

```
******** show hss-peer-service service all *******

Service name                    : hss<>
Notify Request Message          : Enable
Service name                    : hss<>
Notify Request Message          : Enable
```

- Une fois cette case cochée, vous pouvez demander ces journaux afin de résoudre le problème plus en détail :

1. Request “config verbose”

2. Monitor Subscriber with all the required options:
   monitor subscriber <imsi>, along with 19,33,34,35,A,S,X,Y,+++

3. Debug logs:

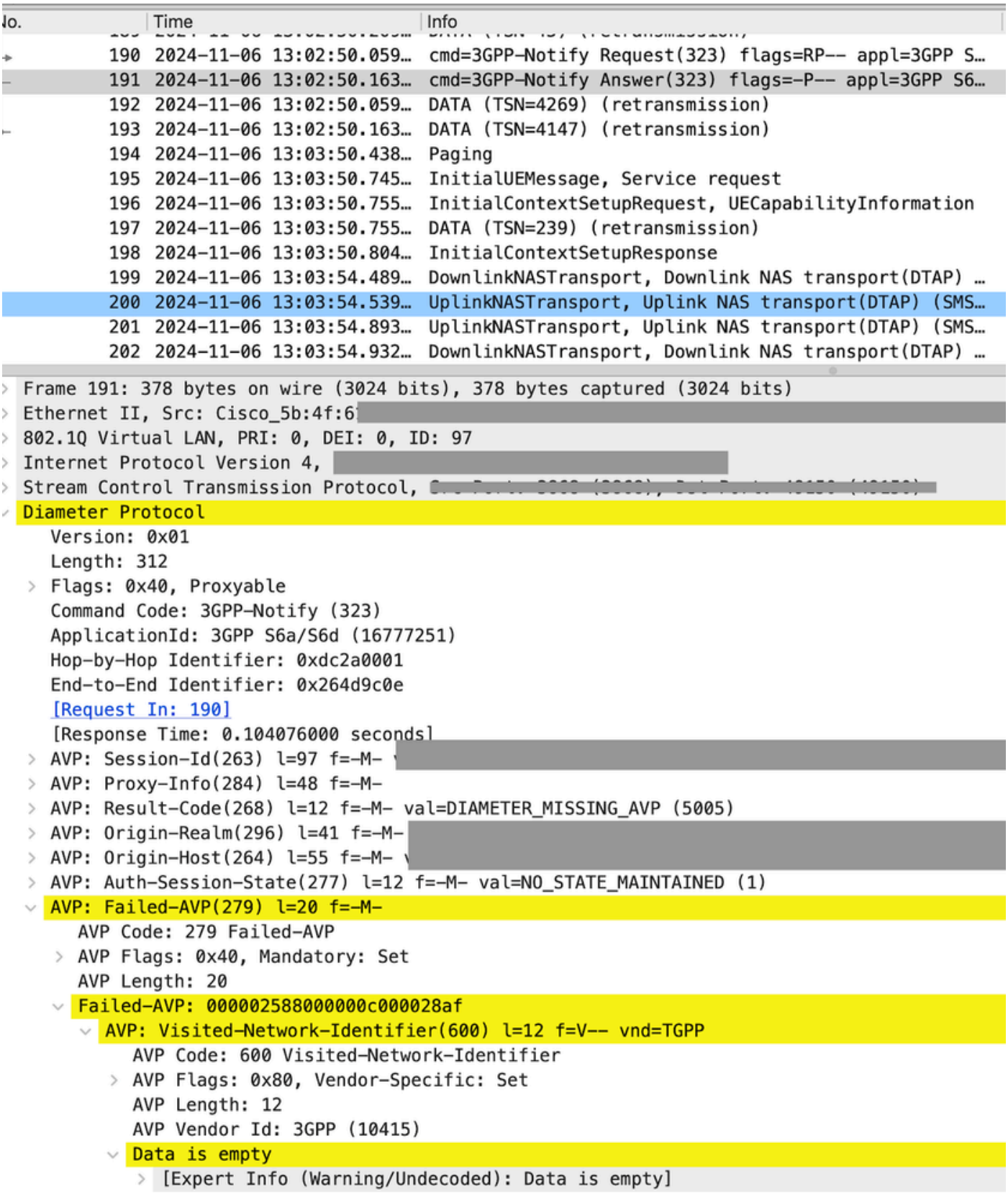
   logging filter active facility diameter level debug
   logging filter active facility sessmgr level debug
   logging filter active facility mme-app level debug
   logging active
    no logging active // to deactivate

4. Logging monitor:

   configure
    logging monitor msid <imsi>
   exit

5. Request syslogs which captures the issue.

Scénario problématique

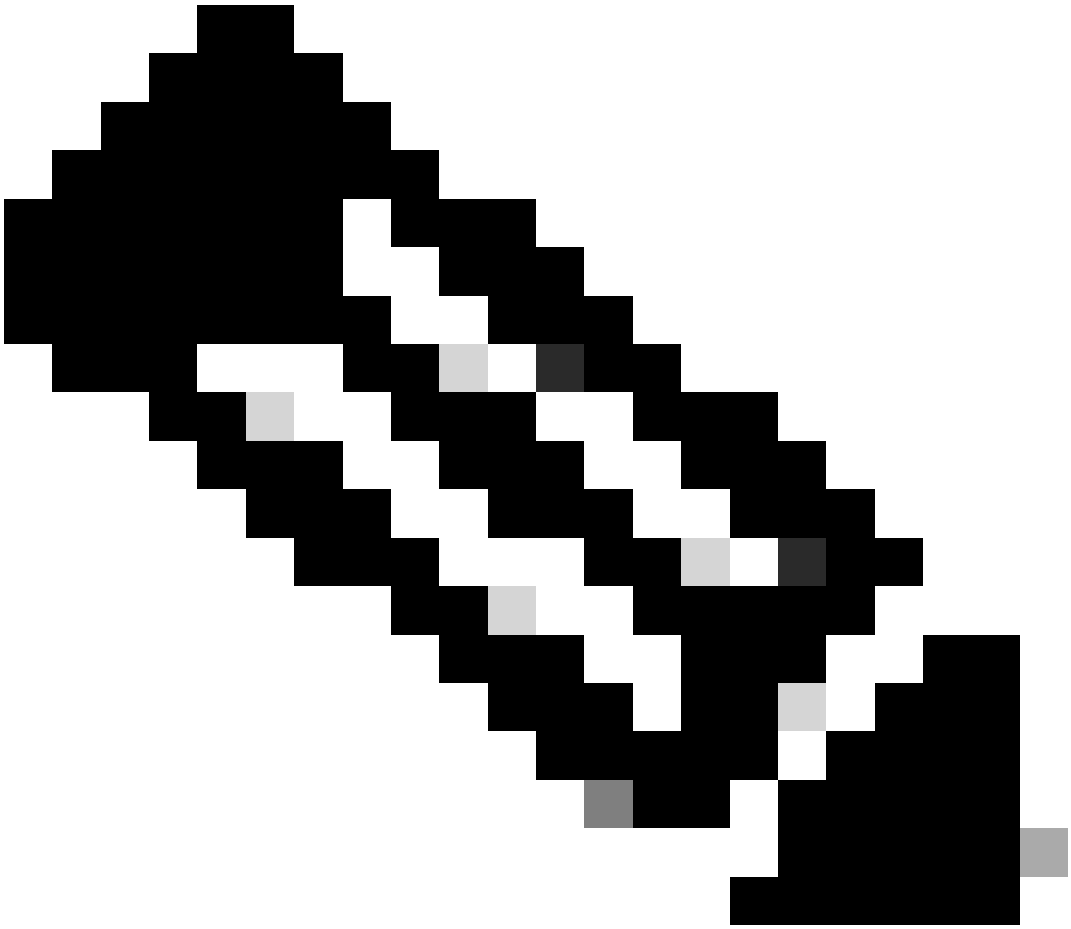


Pcap problématique

Dans cette référence Packet Capture (PCAP), vous pouvez voir l'identifiant de réseau visité manquant sous « notify-answer ».

Le paquet 190 correspond à la « demande de notification » et 191 à la « réponse de notification ».

Le code de résultat du diamètre dans ce scénario est 'Diameter_Missing_AVP', post que vous pouvez également voir le 'Failed AVP' qui pointe vers 'Visited-Network-Identifier' qui à son tour affiche 'data empty'.



Remarque : Le protocole AVP en échec est un protocole AVP groupé qui fournit des informations de débogage lorsqu'une demande est rejetée ou n'est pas entièrement traitée en raison d'une erreur dans un protocole AVP spécifique.

Voici quelques-unes des raisons d'un échec de l'AVP :

· Un AVP qui n'est pas construit correctement

· Un AVP non reconnu ou non pris en charge

· Valeur AVP non valide.

· Un AVP requis qui est manquant

· Un AVP qui est explicitement exclu

· Un AVP limité à 0, 1 ou 0-1 occurrences, mais comportant au moins deux occurrences

Afin de poursuivre le dépannage du problème, vous devez vous assurer que vous continuez à parcourir tous les journaux demandés.

Comme nous l'avons souligné précédemment, vous devez d'abord vérifier la configuration hss-peer-service du noeud problématique.

Configuration de référence :

```
hss-peer-service <>
      diameter hss-endpoint <>
      no diameter update-dictionary-avps
      --- more lines ---
    exit
```

Dans cette configuration, vous pouvez voir qu'il n'y avait pas de diamètre update-dictionary-avps. Le problème était évident lorsqu'il n'y avait aucun dictionnaire de mise à jour mappé à une version 3gpp. En outre, vous pouvez rencontrer quelques scénarios où l'interface de ligne de commande « diameter update-dictionary-avps 3gpp-r9/10 » est présente et où le problème est toujours évident.

Par conséquent, il a été mis à jour à la dernière version selon le guide d'administration de StarOS afin de corriger le problème, qui est la version 11.

Voici la configuration de référence :

<#root>

Mode

Exec > Global Configuration > Context Configuration > HSS Peer Service Configuration

configure > context

context_name

> hss-peer-service

service_name

Entering the above command sequence results in the following prompt:

[*context_name*]*host_name*(config-hss-peer-service)#

Syntax

diameter update-dictionary-avps { 3gpp-r10 | 3gpp-r11 | 3gpp-r9 }

no diameter update-dictionary-avps

no

Sets the command to the default value where Release 8 ('standard') dictionary is used for backward compa

3gpp-r10

Configures the MME /SGSN to signal additional AVPs to HSS in support of Release 10 of 3GPP 29.272.

3gpp-r11

Configures the MME /SGSN to signal additional AVPs to HSS in support of Release 11 of 3GPP 29.272.

Using this keyword is necessary to enable the MME to fully support inclusion of the Additional Mobile S

a-msisdn

command in the Call-Control Profile configuration mode.

3gpp-r9

Configures the MME/SGSN to signal Release 9 AVPs to HSS.

Usage Guidelines

Use this command to configure the 3GPP release that should be supported for this HSS peer service.

This command is only applicable for the 'standard' diameter dictionary as defined in the

diameter hss-dictionary

command.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.