

Utiliser le guide de configuration pour l'intégration DRA multifournisseur

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Étapes de configuration et meilleures pratiques](#)

[Étape 1: Déterminer le mode de connectivité DRA \(homologues entrants et sortants\)](#)

[Étape 2: Configurer l'homologue entrant dans Policy Builder](#)

[Étape 3: Configuration de l'adresse IP hôte AVP](#)

[Étape 4: Valider l'échange de capacités homologues](#)

[Étape 5: Assurez-vous que le nom d'hôte source unique du diamètre est défini à chaque noeud homologue de diamètre](#)

[Étape 6 :Configurez la table de routage de tronçon suivant pour les homologues DRA](#)

Introduction

Ce document décrit les étapes de configuration ainsi que les meilleures pratiques pour l'intégration DRA multifournisseur avec le cluster PCRF Cisco Policy Suite (CPS).

Conditions préalables

Exigences

Cisco recommande aux ingénieurs travaillant avec cette solution de se familiariser avec les sujets suivants :

- système d'exploitation Linux
- Plate-forme et architecture de cluster Cisco Policy Suite (CPS)
- Fonction PCRF (Policy and Charging Rules Function)
- Utilisation de l'éditeur Vi
- Outil d'analyse réseau Wireshark

Composants utilisés

Les informations contenues dans ce document sont basées sur la version CPS 25.1 et la version 8.10 d'AlmaLinux.

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.

Étapes de configuration et meilleures pratiques

Étape 1: Déterminer le mode de connectivité DRA (homologues entrants et sortants)

- Homologues entrants : Le PCRF est configuré pour accepter les demandes de connexion des homologues Diameter désignés. Le noeud homologue initie la requête d'échange de capacités de diamètre (CER) au PCRF.
- Homologues sortants : Le PCRF est configuré pour initier le CER vers ses homologues.

Meilleure pratique :

Pour la plupart des intégrations DRA multifournisseurs, configurez le DRA en tant qu'homologue entrant, où le DRA initie le CER vers le PCRF.

Étape 2: Configurer l'homologue entrant dans Policy Builder

Dans l'interface utilisateur graphique du générateur de politiques, configurez le nom d'homologue entrant et le domaine homologue, en faisant référence aux tables Homologues entrants et Domaines.



Remarque : Pour obtenir une description détaillée des paramètres, reportez-vous au Guide de configuration mobile CPS, version 25.1.0, dans la section Configuration de la pile de diamètres.

Ces paramètres peuvent être configurés sous Homologues entrants :

Table des homologues

Paramètre	Description
Pairs	Définit les noms d'homologues autorisés à établir des connexions vers PCRF.
Nom d'hôte local	Identifie le nom d'hôte local du Policy Director (équilibreur de charge) qui identifie et autorise une connexion entrante de l'homologue.
Numéro d'instance	Indique le numéro attribué au processus Policy Server (QNS) qui établit une connexion avec l'homologue sortant.  Remarque : Le nom d'hôte local et le numéro d'instance doivent être spécifiés si l'intention est qu'un seul processus Policy Server (QNS) sur Policy Builder (équilibreur de charge) autorise/lance une connexion avec ledit homologue. Sinon, le numéro d'instance peut être maintenu à 0. Dans ce cas, tous les processus Policy Server (QNS) sur Policy Director (équilibreur de charge) tentent/autorisent la connexion avec l'homologue. La valeur par défaut est 0.
Classement	Priorité attribuée à cet homologue pour la transmission d'une requête initiée par PCRF. Les plus la valeur d'évaluation est élevée, plus la priorité attribuée à l'homologue est élevée. La valeur par défaut est 1.
Plage de ports	Doit être spécifié uniquement lorsque la connexion de transport sous-jacente est SCTP et non obligatoire lorsque le même protocole est TCP .

Délai de réponse	Cisco recommande de ne pas utiliser ce paramètre.
Modèle de nom	La valeur VP d'origine-hôte A dans CER doit être validée par rapport à ce modèle dans ordre d'établissement de la connexion. Si ce n'est pas le cas, le CER est silencieusement ignorée et la connexion TCP est réinitialisée par PCRF. La vérification du modèle de nom n'a pas lieu si l'option Accepter un homologue non défini décrit dans Configuration de la pile de diamètres. Le modèle de nom doit être l'expression régulière Java standard syntaxe décrite ici.

Tableau des domaines

Paramètre	Description
Domaines	Définit les domaines homologues autorisés à établir des connexions vers PCRF.
Type de pair	Non utilisé avec les domaines entrants.
Protocole de traitement	Mappage entre le nom du domaine et la logique PCRF spécifique qui peut être appliqué pour le message, pour plus d'informations sur le protocole de traitement. Lorsqu'une pile de diamètre avec un domaine de diamètre est importée sans protocole attribué, il prend la valeur par défaut GX_TGPP .
Classement	Priorité attribuée à ce domaine pour la transmission d'une requête initiée par PCRF. Ceci

	est uniquement utilisé avec le protocole de traitement SY_PRIME. La valeur par défaut est 0. Plus la valeur d'évaluation est faible, plus la priorité attribuée au domaine est élevée. Par exemple, un domaine ayant Rating=10 est utilisé après un domaine ayant Note = 1.
Alias de statistiques	Quelles que soient les statistiques qui sont générées pour le royaume respectif obtient le nom configuré dans l'alias de statistiques ajouté à ces statistiques. Ceci s'applique uniquement aux statistiques mbean com.broadhop.message.
Modèle de nom	Domaine d'origine Une valeur VP dans CER doit être validée par rapport à ce modèle dans ordre de traitement du message entrant. Si cela ne se produit pas, le message est ignoré en silence et la connexion TCP est réinitialisée par PCRF. Le modèle de nom doit être l'expression régulière Java standard syntaxe décrite ici.

Meilleure pratique :

Pour un contrôle plus granulaire, configurez des entrées spécifiques d'homologue et de domaine de gestion des identités selon les besoins, et pour autoriser la création d'homologue uniquement à partir d'homologues spécifiques, décochez la case Accepter l'homologue non défini.

Exemple :

Figure 1 : Table des homologues entrants

REFERENCE DATA

File Tools

Systems

- Summary
- system-1
 - Plugin Configurations
 - cluster-1
 - Plugin Configurations
 - Diameter Configuration
 - Lab-PCRF
 - USuM Configuration

- Account Balance Templates
- Custom Reference Data Tables
- Diameter Agents
- Diameter Clients
- Diameter Defaults
- Fault List
- Notifications
- Policy Enforcement Points
- Rule Retry Profiles
- Subscriber Data Sources
- Tariff Times

Diameter Stack

***Name**
Lab-PCRF

***Realm**
pcrf.mnc[redacted].mcc[redacted].3gppnetwork

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
	0	1		[redacted]	*[redacted]*

Add
Remove
↑
↓

Realms

Peer Type	*Processing Protocol	Rating	Stats Alias	*Name Pattern
	GX_TGPP	0		.*
	RX_TGPP	0		.*

Figure 1 : Table des homologues entrants

Étape 3: Configuration de l'adresse IP hôte AVP

Le protocole AVP Diameter Host-IP-Address communique l'adresse IP du noeud lors des échanges CER/CEA (RFC 3588) pour les connexions SCTP. Dans Cisco CPS PCRF, cette adresse est par défaut l'adresse IP de l'interface interne, qui est différente de l'adresse IP du service Diameter attendue pour certains fournisseurs DRA.

Dans Cisco CPS PCRF, vous pouvez utiliser l'adresse IP virtuelle de l'équilibreur de charge (LbVIP) ou l'adresse IP physique des machines virtuelles de l'équilibreur de charge comme adresse IP de point d'extrémité source-diamètre.

Par défaut, l'adresse IP de l'interface interne est communiquée en tant qu'adresse IP d'hôte dans les messages CER/CEA de diamètre, comme indiqué dans l'image, où l'on peut voir que l'adresse IP source dans la capture est différente de l'adresse IP vue dans l'adresse IP d'hôte AVP.

Figure 2 : Message CEA avec IP interne comme adresse IP d'hôte

No.	Time	Source	Destination	Protocol	Length	Info
28	11.542641	DRA IP	PCRF Service IP	DIAME...	264	cmd=Capabilities-Exchange Request(257) flags=R--- appl=Diameter Common Message
30	11.794483	PCRF Service IP	DRA IP	DIAME...	592	cmd=Capabilities-Exchange Answer(257) flags=---- appl=Diameter Common Messages

Frame 30: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)						
Linux cooked capture v1						
Internet Protocol Version 4, Src: PCRF Service IP (10.130.130.130), Dst: DRA IP (10.18.18.18)						
Transmission Control Protocol, Src Port: 3868, Dst Port: 49151, Seq: 1, Ack: 197, Len: 524						
Diameter Protocol						
Version: 0x01						
Length: 524						
Flags: 0x00						
Command Code: Capabilities-Exchange (257)						
ApplicationId: Diameter Common Messages (0)						
Hop-by-Hop Identifier: 0x5992d592						
End-to-End Identifier: 0x071fbd73						
[Request In: 28]						
[Response Time: 0.251842000 seconds]						
AVP: Origin-Host(264) l=63 f=M- val=pcrf.mnc.mcc.3gppnetwork.org						
AVP: Origin-Realm(296) l=42 f=M- val=pcrf.mnc046.mcc404.3gppnetwork.org						
AVP: Host-IP-Address(257) l=14 f=M- val=192.12 (192.12)						
AVP: Vendor-Id(266) l=12 f=M- val=26878						
AVP: Supported-Vendor-Id(265) l=12 f=M- val=10415						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Gx (16777238)						
AVP: Supported-Vendor-Id(265) l=12 f=M- val=8164						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Supported-Vendor-Id(265) l=12 f=M- val=9						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Supported-Vendor-Id(265) l=12 f=M- val=7898						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Supported-Vendor-Id(265) l=12 f=M- val=5535						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Rx (16777236)						
AVP: Supported-Vendor-Id(265) l=12 f=M- val=13019						
AVP: Vendor-Specific-Application-Id(260) l=32 f=M-						
AVP: Product-Name(269) l=21 f= val=Cisco Quantum						
AVP: Result-Code(268) l=12 f=M- val=DIAMETER_SUCCESS (2001)						

Figure 2 : Message CEA avec IP interne comme adresse IP d'hôte

Bien que ce protocole AVP ne soit pas obligatoire lorsque le protocole TCP est utilisé comme protocole de transport (reportez-vous à la RFC 3588), certains fournisseurs de DRA se réfèrent à ce protocole AVP lors de l'établissement de la connexion Diameter et s'attendent à ce que le service Diameter IP de PCRF soit utilisé à la place du protocole IP interne. Si cette attente n'est pas satisfaite, les pairs ne parviendront pas à établir.

Meilleure pratique :

Pour annoncer l'adresse IP du service Diameter dans l'AVP d'adresse IP d'hôte à partir de PCRF, mettez à jour le fichier /etc/hosts avec une entrée mappant le nom de domaine complet (FQDN) source PCRF (tel que défini dans les points d'extrémité locaux de la pile Diameter) à l'adresse IP souhaitée.



Remarque : Reportez-vous aux tableaux des points d'extrémité locaux dans le Guide de configuration mobile CPS, version 25.1.0, sous la section Configuration de la pile de diamètres pour plus de détails.

Pour mettre à jour des entrées d'hôtes supplémentaires dans le PCRF CPS basé sur Openstack :

- Vérifiez que le cluster CPS est à l'état déployé.

curl -X GET [installer le système API](#).

- Récupérez et mettez à jour le fichier additional-hosts.yaml via l'API REST.

```
curl -X GET http://<IP Cluster Manager>:8458/api/system/config/additional-hosts >> additional-hosts.yaml
```

- Appliquez les modifications à l'aide des commandes curl comme décrit dans la documentation du produit.

```
curl -X PUT système API hôtes supplémentaires -H "Content-Type : application/yaml" --data-binary @additional-hosts.yaml
```

À la fin de cet appel d'API, Cluster Manager est configuré avec le nouveau fichier /etc/hostsfile et toutes les autres machines virtuelles déployées sont alors mises à jour de manière asynchrone.



Remarque : Pour obtenir des instructions détaillées, reportez-vous au Guide d'installation de CPS pour OpenStack, section API d'orchestration.

Pour mettre à jour les entrées d'hôtes supplémentaires dans CPS PCRF basé sur Vmware :

- Ajoutez l'entrée dans le fichier AdditionalHosts.csv situé dans le chemin /var/qps/config/deploy/csv/
- Pour importer des modifications dans la machine virtuelle Cluster Manager :

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

- Appliquer les modifications à partir du Gestionnaire de cluster :

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```



Remarque : Pour obtenir des instructions détaillées, reportez-vous au Guide d'installation

de CPS pour VMware, section Configuration d'hôtes supplémentaires.

Exemple :

Figure 3 : Diamètre de l'interface utilisateur graphique Points d'extrémité locaux

*Local End Points						
*Local Host Name	Instance Number	*Advertised Diameter F Q D N	*Listening Port	Local Bind Ip	*Transport Protocol	Multi Homing Hosts
HOSTNAME-lb01	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	
HOSTNAME-lb02	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	

Add Remove ↕ ↕

Figure 3 : Diamètre de l'interface utilisateur graphique Points d'extrémité locaux

Exemple d'entrée /etc/hosts :

<#root>

10.x.x.130 HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org

```
192.x.x.16 HOSTNAME-cluman installer
#END_QPS_OTHER_HOSTS
[root@Hostname-cluman ~]#
```

Étape 4: Valider l'échange de capacités homologues

L'autorité de régulation de domaine doit annoncer explicitement la prise en charge des applications Diameter telles que Gx (16777238) et Rx (16777236) dans les messages de demande d'échange de capacités (CER) et d'échange de capacités (CEA).

L'application Relay, avec l'identificateur d'application 0xffffffff, n'est pas prise en charge par Cisco PCRF. Si seule l'application Relay (4294967295) est échangée et non Gx/Rx, la connexion homologue est établie en mode relais uniquement et PCRF ne répond pas aux messages CCR-I.

Référez-vous à la section Routage de tronçon suivant dans le Guide de configuration mobile CPS pour plus de détails.

Meilleure pratique :

Pendant la phase d'établissement de la connexion homologue, capturez toujours le pcap sur PCRF pour vous assurer que DRA envoie un message de demande d'échange de capacités (CER) de diamètre avec un jeu de valeurs d'ID d'application d'authentification AVP Diamètre des applications telles que Gx (16777238) ou Rx (16777236) ou les deux et PCRF répond avec des valeurs similaires dans le message de réponse d'échange de capacités (CEA).

Figure 4 : Message CER avec une valeur incorrecte dans Auth-Application-Id en tant que relais

```

Diameter Protocol
  Version: 0x01
  Length: 196
  > Flags: 0x80, Request
  Command Code: Capabilities-Exchange (257)
  ApplicationId: Diameter Common Messages (0)
  Hop-by-Hop Identifier: 0x5b2c55d3
  End-to-End Identifier: 0x171b0936
  [Answer In: 409]
  > AVP: Origin-Host(264) l=59 f=-M- val=[REDACTED]01ors.mnc[REDACTED].mcc[REDACTED].3gppnetwork.org
  > AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
  > AVP: Host-IP-Address(257) l=14 f=-M- val=10.[REDACTED].[REDACTED].146
  > AVP: Vendor-Id(266) l=12 f=-M- val=323
  > AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
  > AVP: Auth-Application-Id(258) l=12 f=-M- val=Relay (4294967295)
    AVP Code: 258 Auth-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 12
    Auth-Application-Id: Relay (4294967295)
  > AVP: Firmware-Revision(267) l=12 f=--- val=6491648
```

Figure 4 : Message CER avec une valeur incorrecte dans Auth-Application-Id as Relay

Figure 5 : Message CER avec les valeurs correctes dans Auth-Application-Id : Gx et Rx

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x38370427

End-to-End Identifier: 0x0d3fbc01

[Answer In: 30]

```
> AVP: Origin-Host(264) l=60 f=-M- val=[redacted]drax01c[redacted].mnc084.mcc404.3gppnetwork.org
> AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
> AVP: Host-IP-Address(257) l=14 f=-M- val=10.[redacted].[redacted].151
> AVP: Vendor-Id(266) l=12 f=-M- val=323
> AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
✓ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  AVP Code: 260 Vendor-Specific-Application-Id
  > AVP Flags: 0x40, Mandatory: Set
  AVP Length: 32
  ✓ Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000014
    > AVP: Vendor-Id(266) l=12 f=-M- val=10415
    ✓ AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Rx (16777236)
      AVP Code: 258 Auth-Application-Id
      > AVP Flags: 0x40, Mandatory: Set
      AVP Length: 12
      Auth-Application-Id: 3GPP Rx (16777236)
  ✓ AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
    AVP Code: 260 Vendor-Specific-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 32
    ✓ Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000016
      > AVP: Vendor-Id(266) l=12 f=-M- val=10415
      > AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Gx (16777238)
> AVP: Firmware-Revision(267) l=12 f=--- val=6557952
```

Figure 5 : Message CER avec les valeurs correctes dans Auth-Application-Id : Gx et Rx

Étape 5: Assurez-vous que le nom d'hôte source unique du diamètre est défini à chaque noeud homologue de diamètre

Cisco CPS PCRF prend en charge un environnement dans lequel chaque noeud homologue connecté requiert un nom d'hôte source de diamètre unique.

Si la migration doit être effectuée pour des connexions homologues de diamètre à partir d'une connectivité Gx ou Rx directe existante vers des liaisons à médiation DRA, la liaison DRA pour chaque interface de diamètre (Gx ou Rx) entre PCEF ou P-CSCF et DRA doit idéalement utiliser un nom d'hôte source unique pour l'application de diamètre (la valeur de l'origine-hôte AVP) qui serait différente de celle utilisée pour la connectivité PCRF directe avec le même noeud homologue.

Cela garantit que les requêtes des noeuds homologues sont acheminées via la liaison homologue DRA correcte et ne sont pas abandonnées si d'anciennes entrées de liaison directe désactivée sont présentes dans la liste PCRF show_peers.py.

Meilleure pratique :

S'il n'est pas possible de modifier le nom d'hôte pour les liaisons DRA sur l'homologue, effectuez un redémarrage complet des quatre services QNS séquentiellement sur chaque machine virtuelle d'équilibrage de charge après avoir supprimé les liaisons homologues directes.

Cela permettrait de s'assurer que les anciennes entrées obsolètes (hôte d'origine :) des homologues utilisées précédemment pour l'interface de diamètre direct (Gx/Rx) entre PCEF/P-CSCF et PCRF ne sont plus présentes dans la liste de connexion d'homologue de diamètre PCRF, et que la sortie de `show_peers.py` aurait uniquement des connexions d'homologue DRA et donc un routage correct des messages d'application de diamètre (par exemple : Gx_CCA-I, Gx_CCA-T) à partir des liaisons de diamètre nouvellement créées entre DRA et PCRF.



Remarque : Le redémarrage des services QNS sur les machines virtuelles LB affecte le trafic et réinitialise toutes les connexions d'homologue de diamètre sur ces instances QNS. Effectuez cette étape au cours d'une fenêtre de maintenance planifiée.

Étape 6 : configurez la table de routage de tronçon suivant pour les homologues DRA

Cette fonctionnalité permet l'interfonctionnement avec un DRA qui n'est pas en mode de masquage de topologie. Lorsqu'un DRA établit une connexion, il annonce ses propres valeurs Origin-Host et Realm. Cependant, les messages d'application Diameter utilisent l'hôte d'origine et le domaine (par exemple, PCEF, TDF, AF) de l'hôte d'application réel, de sorte que PCRF doit déterminer quelle connexion DRA utiliser pour remettre les messages à l'hôte correct.



Remarque : La table Routes du tronçon suivant est uniquement utilisée pour les requêtes initiées par PCRF. Les réponses aux requêtes entrantes sont toujours envoyées via la même connexion que celle sur laquelle elles ont été reçues, afin d'éviter le routage asymétrique.

Ces paramètres peuvent être configurés dans la table de routage de tronçon suivant :

Paramètre	Description
Domaine du saut suivant	Nom de domaine DRA tel que reçu dans Origin-Realm AVP dans CER ou CEA

	message.  Remarque : Tous les domaines de saut suivant (domaine de saut suivant) doivent correspondre à la valeur VP du domaine origine A dans le message CER/CEA entrant.
Hôtes du saut suivant	Liste de noms d'hôtes DRA telle que reçue dans Origin-Host AVP dans CER ou CEA message.  Remarque : Tous les noms d'hôtes de tronçon suivant (hôtes de tronçon suivant) doivent correspondre à la valeur VP d'origine-hôte A dans le message CER/CEA entrant.
ID d'application	ID d'application de diamètre annoncé comme étant pris en charge par le DRA. Il contient des informations qui identifient le service particulier que le service session appartient à.
Modèle des domaines de destination	Modèle de nom de domaine de destination réel reçu dans le protocole AVP du domaine d'origine dans le message AAR. Le modèle doit être le standard Java régulier syntaxe d'expression.
Modèle hôte de destination	Modèle de nom d'hôte de destination réel tel que reçu dans Origin-Host AVP dans message AAR. Le modèle doit être un modèle Java standard les conventions. Le modèle doit être le standard Java régulier syntaxe d'expression.

Meilleure pratique :

Essayez toujours d'utiliser le modèle d'expression régulière correct (correspondance de

caractères génériques) lors de l'écriture des entrées dans la colonne Modèle de domaines de destination et Modèle d'hôte de destination dans

Table de routage de tronçon suivant pour réduire les entrées de configuration pour les homologues Gx et Rx et plusieurs connexions et empêcher les erreurs de configuration.



Remarque : Reportez-vous au Guide de configuration mobile CPS, version 25.1.0, sous la section Routage de tronçon suivant pour obtenir des instructions de configuration détaillées.

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.