Configurer la sauvegarde et la restauration à partir de l'interface utilisateur graphique dans CUCM

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Sauvegarde
- Restaurer

Dépannage

Informations connexes

Introduction

Ce document décrit la configuration requise pour les fonctions de sauvegarde et de restauration dans CUCM à partir de l'interface graphique utilisateur (GUI).

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Cisco Unified Communications Manager (CUCM)
- Secure File Transfer Protocol (SFTP)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

- Cisco Unified Communications Manager version 10.5.2.15900-8

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.

Informations générales

Le Disaster Recovery System (DRS),qui peut être appelé à partir de CUCM Administration, fournit des capacités complètes de sauvegarde et de restauration des données pour tous les serveurs du cluster. Le DRS permet de planifier régulièrement des sauvegardes de données automatiques ou appelées par l'utilisateur.

DRS restaure ses propres paramètres (périphérique de sauvegarde et paramètres de planification) dans le cadre de la sauvegarde/restauration de la plateforme. DRS sauvegarde et restaure les fichiers et drfDevice.xml les drfSchedule.xml fichiers. Lorsque le serveur est restauré avec ces fichiers, il n'est pas nécessaire de reconfigurer le périphérique de sauvegarde et la planification DRS.

Le système de reprise après sinistre comprend les fonctionnalités suivantes :

- Interface utilisateur permettant d'effectuer des tâches de sauvegarde et de restauration.
- Architecture de système distribué avec fonctions de sauvegarde et de restauration.
- Sauvegardes planifiées
- Archivez les sauvegardes sur un lecteur de bande physique ou un serveur SFTP distant.

Le système de reprise après sinistre comporte deux fonctions clés : Agent maître (MA) et Agent local (LA).

L'agent maître coordonne les activités de sauvegarde et de restauration avec les agents locaux. Le système active automatiquement l'agent maître et l'agent local sur tous les noeuds du cluster.

Le cluster CUCM (qui implique les noeuds CUCM et les Cisco Instant Messaging & Presence (IM&P) serveurs) doit répondre aux exigences suivantes :

- **Port 22** afin d'établir la communication avec le serveur SFTP
- Vérifiez que les certificats **IPsec** et **Tomcat** n'ont pas expiré - effectué.

  Afin de vérifier la validité des certificats, accédez à

Remarque : Afin de régénérer les certificats ipsec et Tomcat, utilisez la Procédure pour régénérer les certificats dans CUCM

- Assurez-vous que la configuration de la réplication de base de données est terminée et qu'elle n'affiche aucune erreur ou incohérence provenant du serveur de publication CUCM et des serveurs de publication IM&P.

Les paramètres du serveur SFTP doivent couvrir les exigences suivantes :

- Les informations de connexion sont disponibles.
- Il doit être accessible à partir du serveur CUCM.
- Les fichiers sont inclus dans le chemin sélectionné lors d'une restauration.

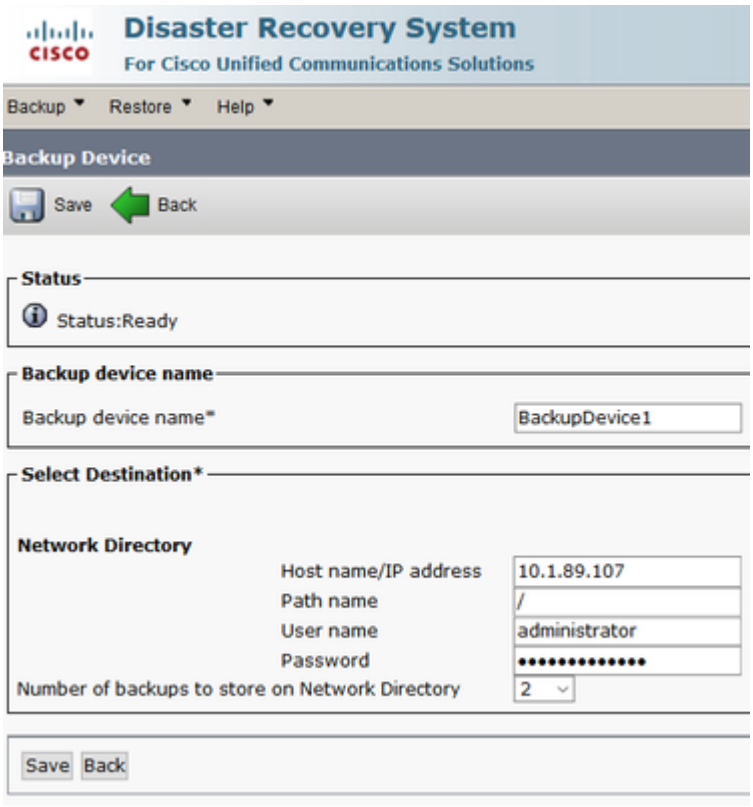
Configurer

Sauvegarde

Le Disaster Recovery System effectue une sauvegarde au niveau du cluster, ce qui signifie qu'il collecte les sauvegardes pour tous les serveurs d'un cluster CUCM vers un emplacement central et archive les données de sauvegarde sur un périphérique de stockage physique.

Étape 1 : création de périphériques de sauvegarde sur lesquels les données sont enregistrées accéder à **Disaster Recovery System** > **Backup** > **Backup Device**.

Étape 2. Sélectionnez **Add New**;définir un **Backup Device Name** serveur et entrez les valeurs SFTP. Enregistrer.

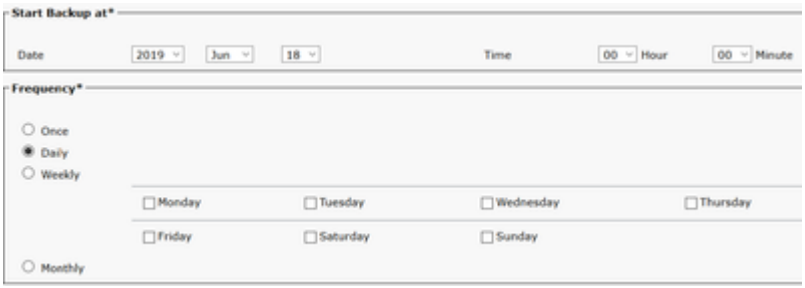


Étape 3 : création et modification des plannings de sauvegarde afin de sauvegarder les données
Naviguez jusqu'à **Backup** > **Scheduler**.

Étape 4. Définissez un **Schedule Name**.Sélectionnez le **Device Name** , puis vérifiez le **Features** en fonction de votre scénario.



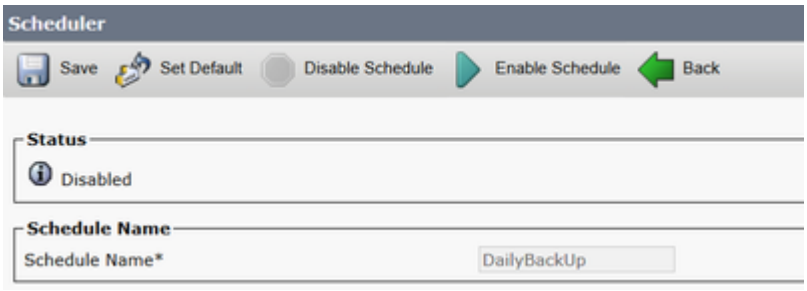
Étape 5 : configuration d’une sauvegarde planifiée en fonction de votre scénario



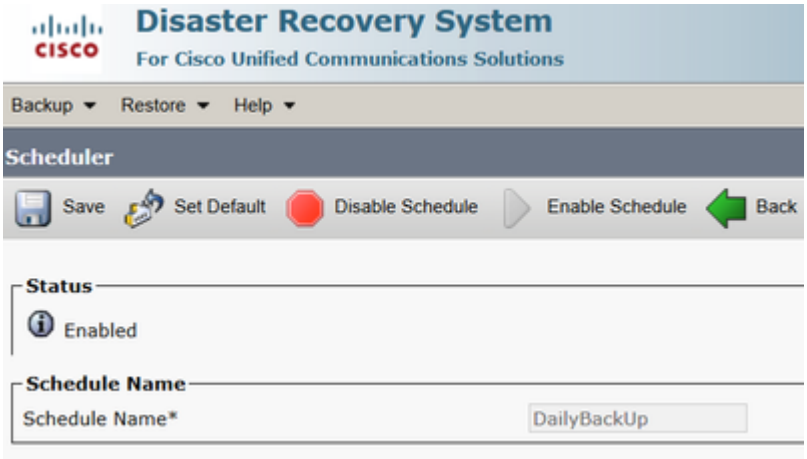
Étape 6. Sélectionnez **Save** et notez l'avertissement comme indiqué dans l'image. Sélectionnez **OK** afin d'avancer.



Étape 7. Une fois que vous avez créé ce **Backup Schedule** fichier, sélectionnez **Enable Schedule**.



Étape 8. Attendez que l'état passe à **Enabled**.

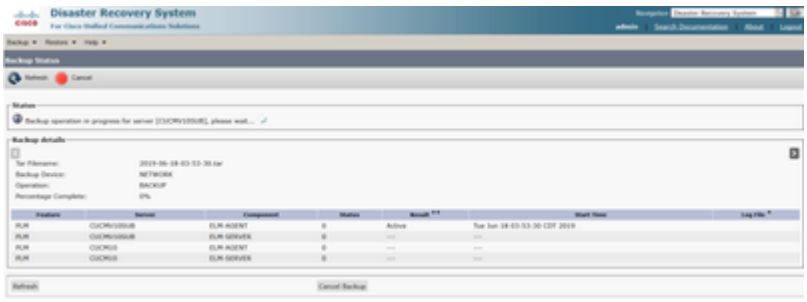


Étape 9. Si une sauvegarde manuelle est requise, accédez à **Backup** > **Manual Backup**.

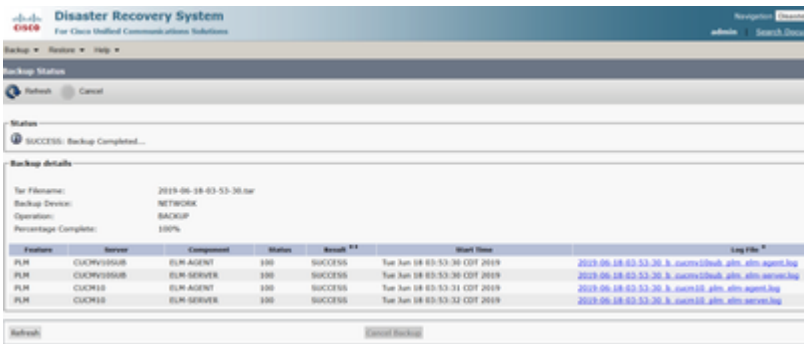
Étape 10. Sélectionnez le **Device Name** et vérifiez le **Features** en fonction de votre scénario.



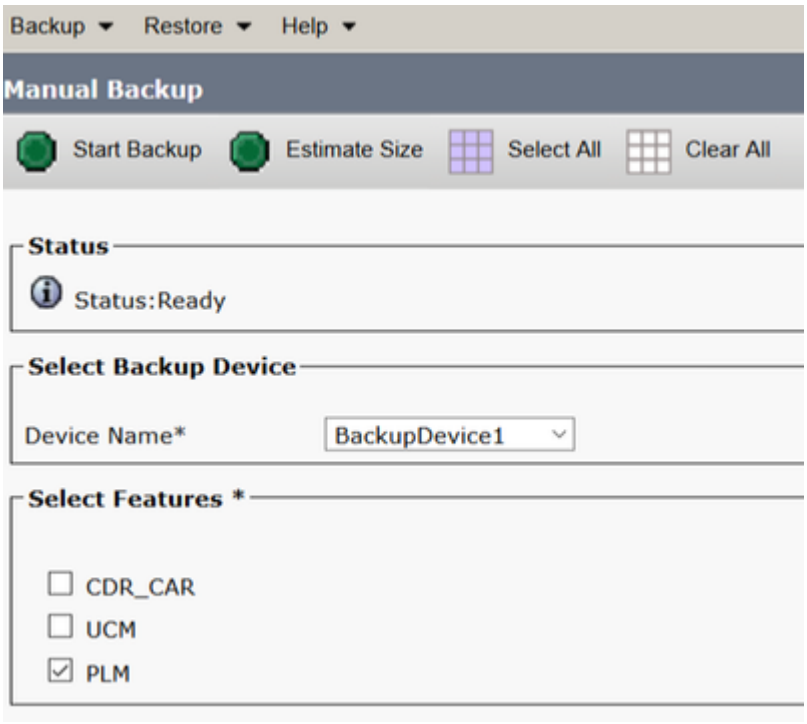
Étape 11. Sélectionnez **Start Backup** et l'opération est affichée en cours.



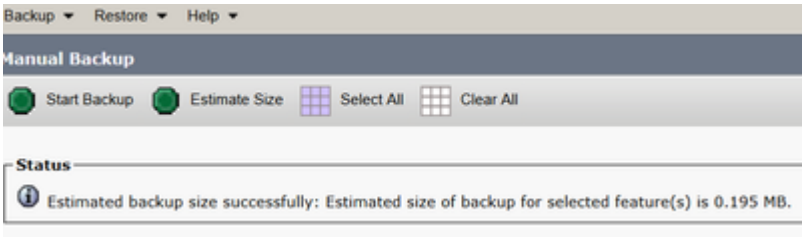
Étape 12. Lorsque la sauvegarde manuelle est terminée, le message de fin s'affiche.



Étape 13. Pour estimer la taille du fichier tar de sauvegarde utilisé par le périphérique SFTP, sélectionnez **Estimate Size**.

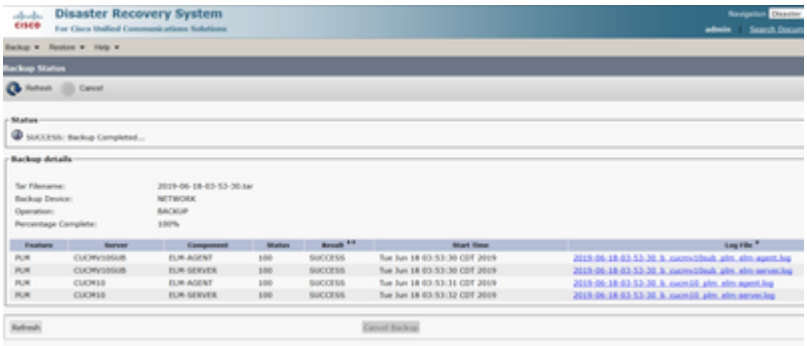


Étape 14. La taille de l’estimation s’affiche comme illustré dans l’image

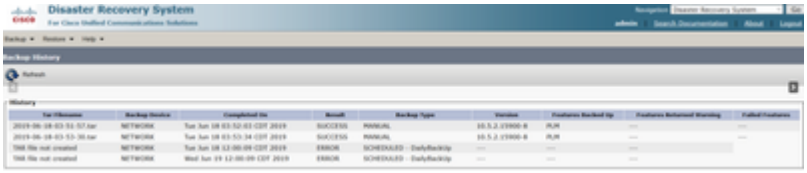


Remarque : La fonction Taille estimée est calculée en fonction des sauvegardes précédentes réussies et peut varier au cas où la configuration aurait été modifiée depuis la dernière sauvegarde.

Étape 15. Pour vérifier l’état de la sauvegarde pendant son exécution, accédez à **Backup** > **Backup Status**.



Étape 16. Pour consulter les procédures de sauvegarde effectuées dans le système, accédez à **Backup** > **History**.



Restaurer

DRS restaure principalement drfDevice.xml et les drfSchedule.xml fichiers. Cependant, lorsqu'une restauration des données système est effectuée, vous pouvez choisir les noeuds du cluster qui doivent être restaurés.

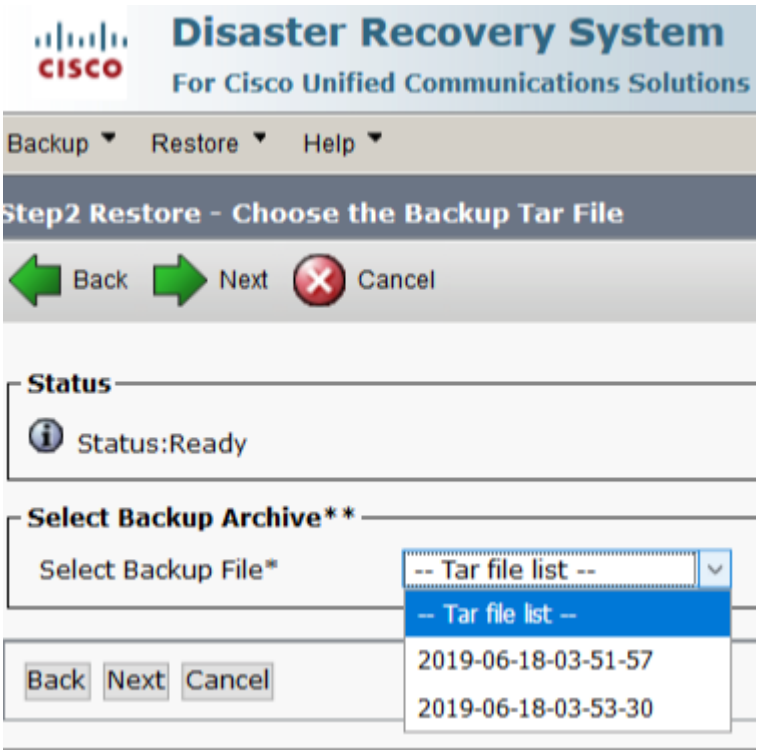
Remarque : Le périphérique de sauvegarde (serveur SFTP) doit déjà être configuré afin de récupérer les fichiers tar de celui-ci et de restaurer le système avec ces fichiers.

Étape 1. Accédez à **Disaster Recovery System** > **Restore** > **Restore Wizard**.

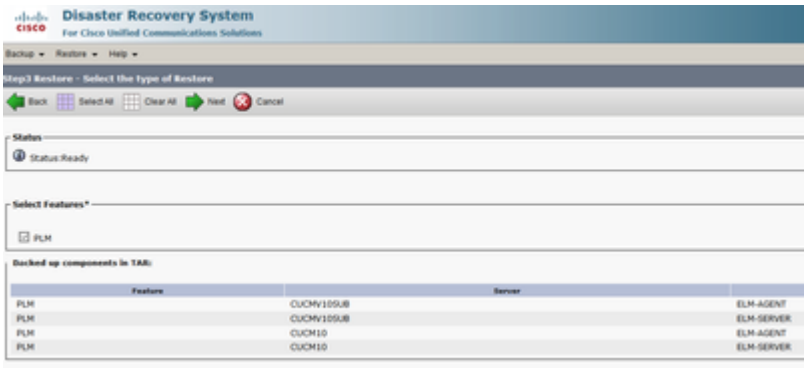
Étape 2. Sélectionnez le **Device Name** qui stocke le fichier de sauvegarde à utiliser pour la restauration. Sélectionner **Next**.



Étape 3. Sélectionnez le fichier **Backup File** dans la liste affichée des fichiers disponibles, comme illustré dans l'image. Le fichier de sauvegarde sélectionné doit inclure les informations à restaurer.



Étape 4. Dans la liste des fonctionnalités disponibles, sélectionnez la fonctionnalité à restaurer.



Étape 5. Sélectionnez les noeuds dans lesquels appliquer la restauration.

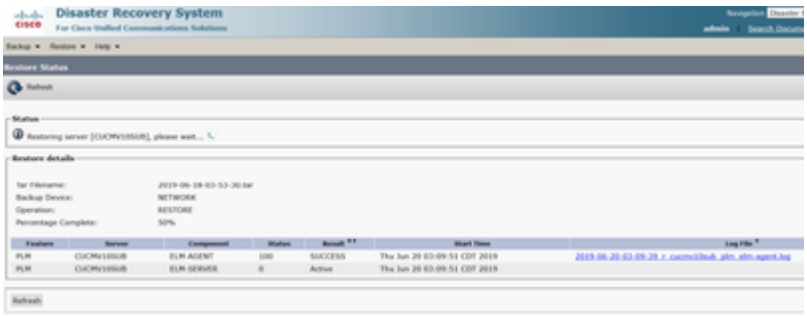


Remarque : La restauration en une étape permet la restauration de l'ensemble du cluster si le serveur de publication a déjà été reconstruit ou installé à nouveau. Cette option n'est visible QUE si le fichier de sauvegarde sélectionné pour la restauration est le fichier de sauvegarde du cluster et que les fonctionnalités choisies pour la restauration incluent la ou les fonctionnalités enregistrées auprès des noeuds d'éditeur et d'abonné.

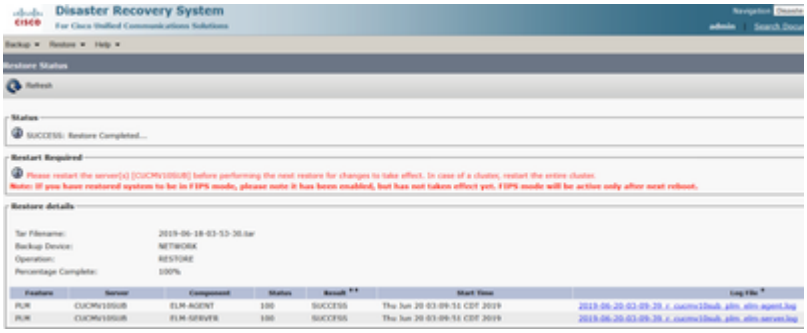
Étape 6. Sélectionnez **Restore** pour démarrer le processus et l'état de restauration est mis à jour.



Étape 7. Pour vérifier l'état de la restauration, accédez à **Restore** > **Current Status**.



Étape 8. La **Restore Status** modification SUCCESS s'effectue une fois l'opération terminée.



Étape 9. Pour que les modifications prennent effet, le système doit être redémarré.

```
admin:utils system restart

Do you really want to restart ?

Enter (yes/no)? yes


 Appliance is being Restarted ...
Warning: Restart could take up to 5 minutes.
Stopping Service Manager...
-  Service Manager shutting down services... Please Wait
Restart operation appears to be stuck

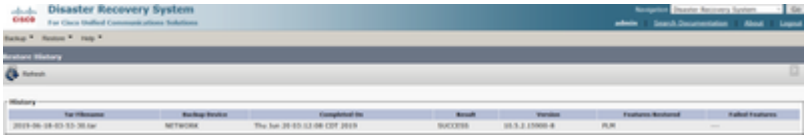
Would you like to force the Restart?

continue Restart (yes/no)?
Broadcast message from admin@CUCMv10SUB
        (unknown) at 3:19 ...

The system is going down for reboot NOW!
```

Conseil : Utilisez une procédure prise en charge afin de redémarrer le système Arrêter ou redémarrer le système

Étape 10. Pour consulter les procédures de restauration effectuées dans le système, accédez à **Restore** > **History**.



Dépannage

Cette section fournit des informations pour dépanner votre configuration.

Le cluster CUCM (qui implique les noeuds CUCM et les serveurs Cisco Instant Messaging & Presence) doit répondre aux exigences suivantes :

- Port 22 afin d'établir la communication avec le serveur SFTP.
- Vérifiez que les certificats IPsec et Tomcat n'ont pas expiré - effectué.

  Afin de vérifier la validité des certificats, accédez à

Remarque : Pour régénérer les certificats ipsec et Tomcat, utilisez la Procédure de régénération des certificats dans CUCM

- Assurez-vous que la configuration de la réplication de base de données est terminée et qu'elle n'affiche aucune erreur ou incohérence provenant du serveur de publication CUCM et des serveurs de publication IM&P.
- Validez l'accessibilité entre les serveurs et le serveur SFTP.
- Vérifiez que tous les serveurs du cluster sont authentifiés à l'aide de la commande **show network cluster**.

Lorsque des échecs de sauvegarde ou de restauration sont signalés et qu'une assistance supplémentaire est requise, cet ensemble de journaux doit être collecté et partagé avec le centre d'assistance technique (TAC) :

- Journaux principaux Cisco DRF
- Journaux locaux Cisco DRF
- Journaux d'échec de la page État actuel de DRF
- Horodatage de l'émission

Informations connexes

- Serveurs SFTP pris en charge

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.