Suppression des fichiers de cache et d'historique FireAMP sous Windows

Table des matières

- Introduction
- Fichiers de base de données pour le cache et l'historique
  - Objectif
  - Motifs du renvoi
  - Identifier les fichiers de base de données
- Procédure de suppression des fichiers de base de données
  - Étape 1 : Arrêter le service Connecteur FireAMP
    - Interface utilisateur
    - Console de services
    - Invite de commandes
  - Étape 2 : Supprimer les fichiers de base de données requis
    - Fichiers de base de données cache
    - Fichiers de base de données historique
  - Étape 3 : Démarrez le service Connecteur FireAMP

Introduction

Ce document présente certains scénarios qui nécessitent la suppression de fichiers de base de données dans FireAMP for Endpoints et décrit une procédure appropriée pour les supprimer si nécessaire. FireAMP for Endpoints conserve un enregistrement de ses détections et dispositions de fichiers récentes dans les fichiers de base de données. Dans certains cas, un ingénieur d'assistance Cisco peut vous demander de supprimer certains fichiers de la base de données afin de résoudre un problème.

> Avertissement : Vous ne pouvez supprimer un fichier de base de données que si le support technique Cisco vous y invite.

Fichiers de base de données pour le cache et l'historique

Objectif

Les fichiers de la base de données de cache conservent les dispositions connues des fichiers. Les fichiers de la base de données d'historique suivent toutes les détections de fichiers FireAMP, ainsi que les noms de fichiers source et les valeurs SHA256.

Lorsque vous ajoutez une liste de blocage à une stratégie et que vous mettez à jour le connecteur, le comportement d'un fichier donné ne change pas immédiatement. En effet, le cache

a déjà identifié que le fichier n'est pas malveillant. En tant que tel, il ne sera pas modifié ou remplacé par votre liste de blocage. La disposition change lorsque le cache expire en fonction de la durée de votre stratégie et qu'une nouvelle recherche est effectuée, d'abord sur vos listes, puis sur le cloud.

Motifs du renvoi

Si la base de données d'historique et les fichiers de la base de données cache sont supprimés d'un répertoire, ils sont recréés à nouveau au redémarrage du service FireAMP. Dans certains cas, il peut être nécessaire de supprimer ces fichiers du répertoire FireAMP. Par exemple, si vous souhaitez tester une détection personnalisée simple ou une liste de blocage d'application pour un fichier donné.

Il est possible qu'une base de données soit corrompue, ce qui vous empêche d'ouvrir ou d'afficher les détections dans une base de données. Si la base de données est corrompue sur un système, elle peut également entraîner des erreurs au sein du service Connecteur FireAMP, telles que l'impossibilité de démarrer le connecteur ou la dégradation des performances globales du système. Dans ces cas, vous pouvez effacer les fichiers d'historique du connecteur afin d'éviter les problèmes de performances dus à la corruption et de pouvoir capturer de nouveaux journaux à des fins de diagnostic.

Identifier les fichiers de base de données

Sous Microsoft Windows, ces fichiers se trouvent généralement à l'adresse C:\Program Files\Sourcefire\fireAMP ou C:\Program Files\Cisco\AMP.

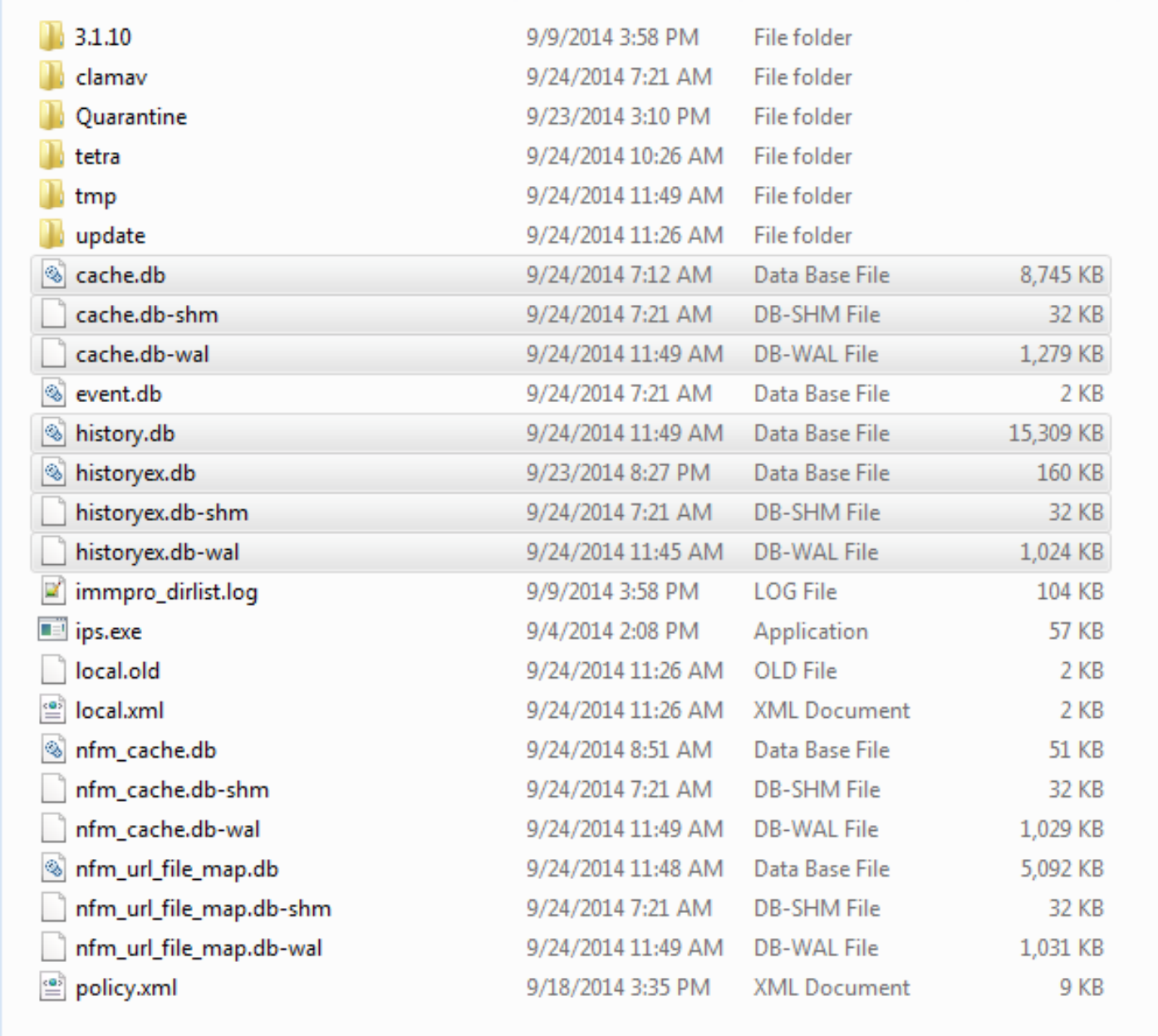
Les noms des fichiers de la base de données cache sont les suivants :

```
cache.db
cache.db-shm
cache.db-wal
```

Les noms des fichiers de base de données d'historique sont :

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

Cette capture d'écran présente les fichiers de l'Explorateur de fichiers Windows :



3.1.10	9/9/2014 3:58 PM	File folder	
clamav	9/24/2014 7:21 AM	File folder	
Quarantine	9/23/2014 3:10 PM	File folder	
tetra	9/24/2014 10:26 AM	File folder	
tmp	9/24/2014 11:49 AM	File folder	
update	9/24/2014 11:26 AM	File folder	
cache.db	9/24/2014 7:12 AM	Data Base File	8,745 KB
cache.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
cache.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,279 KB
event.db	9/24/2014 7:21 AM	Data Base File	2 KB
history.db	9/24/2014 11:49 AM	Data Base File	15,309 KB
historyex.db	9/23/2014 8:27 PM	Data Base File	160 KB
historyex.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
historyex.db-wal	9/24/2014 11:45 AM	DB-WAL File	1,024 KB
immpro_dirlist.log	9/9/2014 3:58 PM	LOG File	104 KB
ips.exe	9/4/2014 2:08 PM	Application	57 KB
local.old	9/24/2014 11:26 AM	OLD File	2 KB
local.xml	9/24/2014 11:26 AM	XML Document	2 KB
nfm_cache.db	9/24/2014 8:51 AM	Data Base File	51 KB
nfm_cache.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
nfm_cache.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,029 KB
nfm_url_file_map.db	9/24/2014 11:48 AM	Data Base File	5,092 KB
nfm_url_file_map.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
nfm_url_file_map.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,031 KB
policy.xml	9/18/2014 3:35 PM	XML Document	9 KB

Procédure de suppression des fichiers de base de données

Étape 1 : Arrêter le service Connecteur FireAMP

Vous pouvez arrêter le service FireAMP Connector de plusieurs manières :

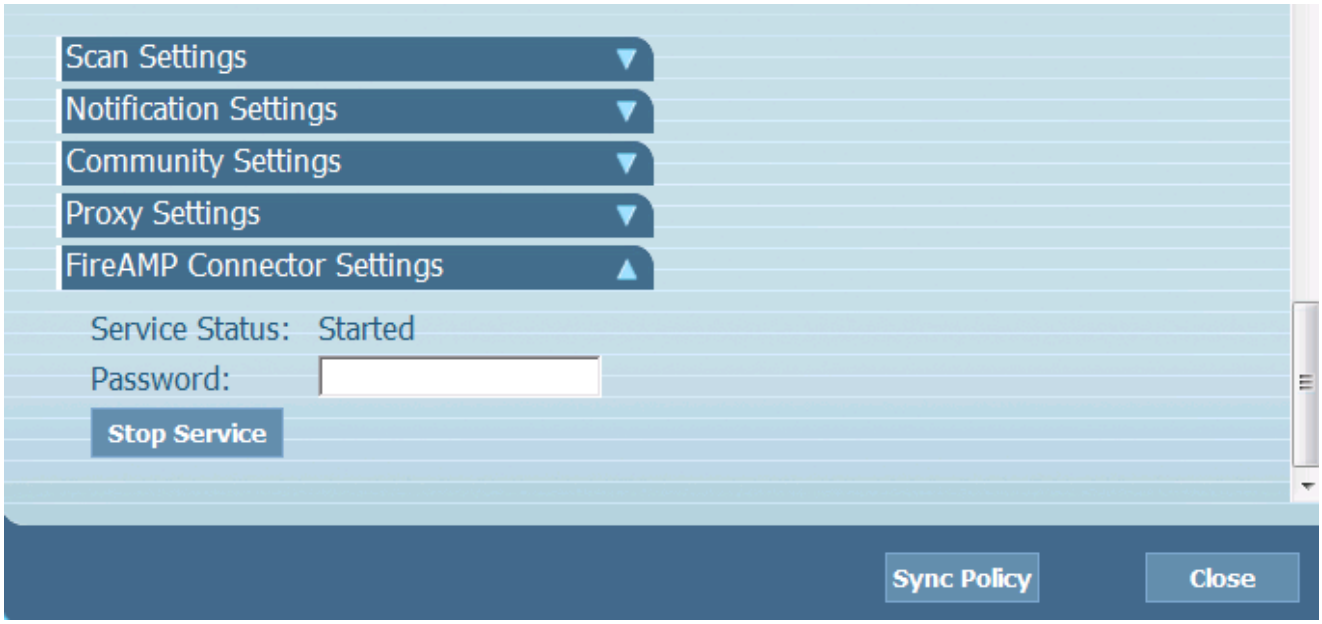
- Interface utilisateur (UI) du service Connecteur FireAMP
- Console des services Windows
- Invite de commandes de l'administrateur

Interface utilisateur

Remarque : Si la protection des connecteurs est activée, vous devez utiliser l'interface utilisateur pour arrêter le service Connecteur FireAMP.

---

a. Ouvrez l'interface utilisateur à partir de la barre d'état système et cliquez sur Settings.
b. Faites défiler la page vers le bas et développez Paramètres du connecteur FireAMP.
c. Dans le champ Mot de passe, saisissez le mot de passe de protection du connecteur. Cliquez sur Arrêter le service.

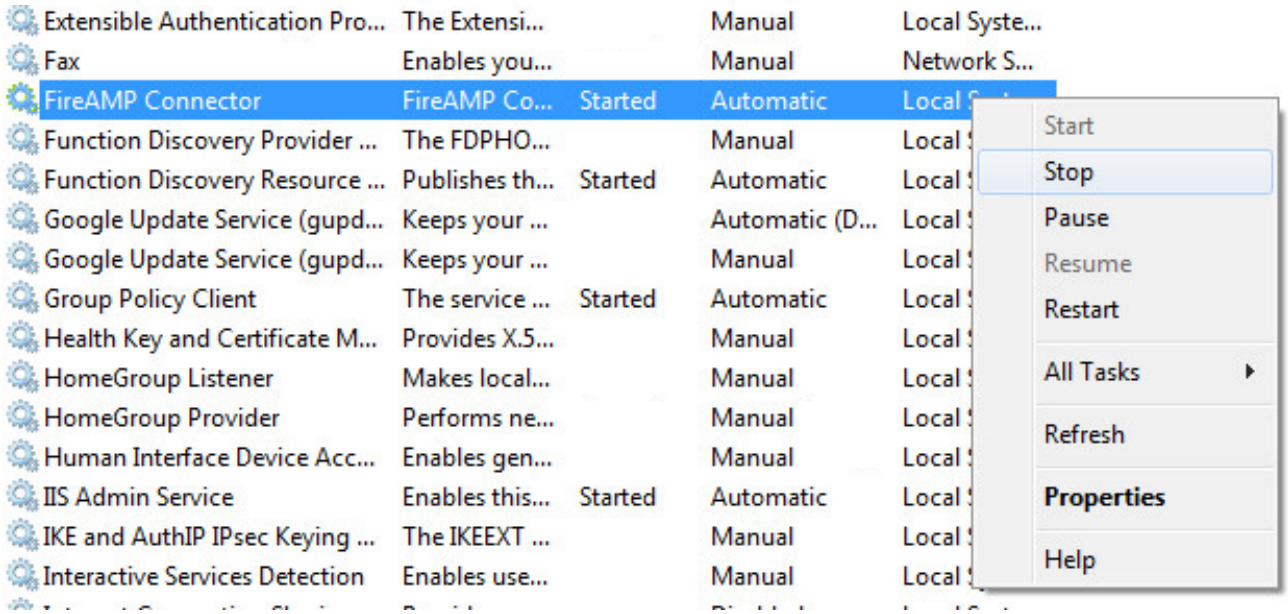


Console de services

Remarque : Pour arrêter et démarrer des services dans la console Services, vous devez disposer de privilèges d'administrateur.

Pour arrêter le service Connecteur FireAMP à partir de la console de services, procédez comme suit :

a. Accédez au menu Démarrer.
b. Saisissez services.msc et appuyez sur Entrée. La console Services s'ouvre.
c. Sélectionnez le service Connecteur FireAMP et cliquez avec le bouton droit sur le nom du service.
d. Choisissez Stop afin d'arrêter le service.

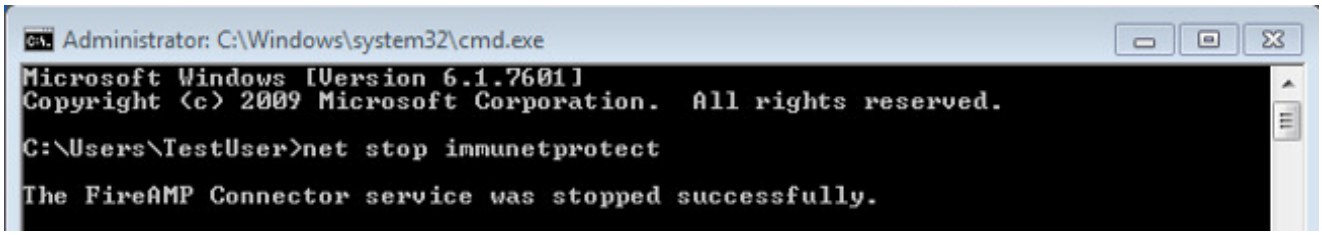


Invite de commandes

Pour arrêter le service Connecteur FireAMP à partir de l'invite de commandes d'un administrateur, procédez comme suit :

a. Accédez au menu Démarrer.
b. Entrez cmd.exe et appuyez sur Entrée. Une fenêtre d'invite de commandes s'ouvre.
c. Entrez la commande net stop immunetprotect. Si vous disposez de la version 5.0.1 ou ultérieure, entrez la commande wmic service où « name like 'immunetprotect%' » call startservice.

   Cette capture d'écran illustre un exemple d'arrêt réussi du service :



Étape 2 : Supprimer les fichiers de base de données requis

Fichiers de base de données cache

Une fois le service arrêté, vous pouvez supprimer ces trois fichiers cache :

> Avertissement : Si vous ne supprimez pas tous les fichiers de la base de données de cache associée, cela peut créer des problèmes de mise en cache avec la base de données recréée. Par conséquent, le service peut ne pas démarrer ou ses performances peuvent être dégradées.

```
cache.db
cache.db-shm
cache.db-wal
```

Fichiers de base de données historique

Une fois le service arrêté, supprimez ces fichiers de base de données d'historique :

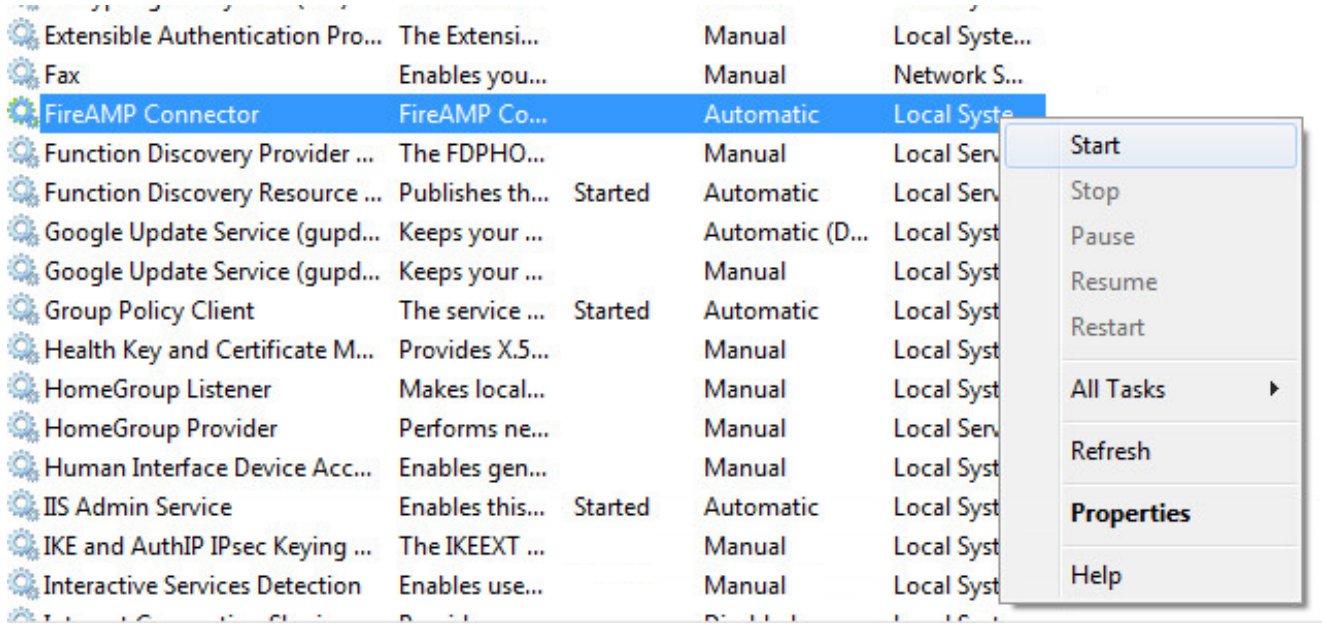
> Avertissement : Si vous ne supprimez pas tous les fichiers de base de données d'historique associés, cela peut créer des problèmes de mise en cache avec la base de données recréée. Par conséquent, le service peut ne pas démarrer ou ses performances peuvent être dégradées.

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

Étape 3 : Démarrez le service Connecteur FireAMP

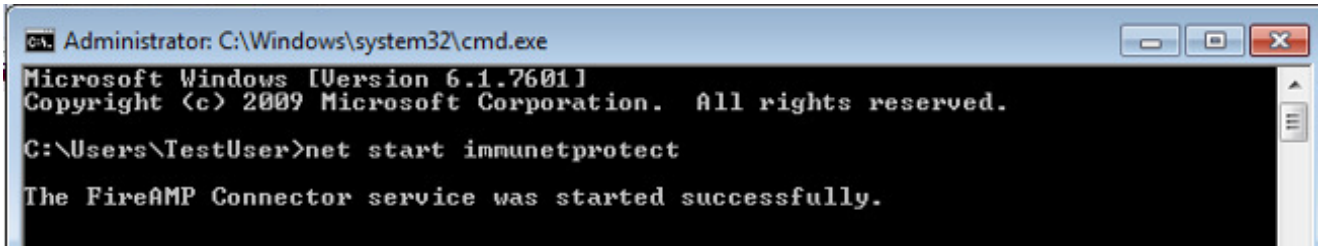
Pour démarrer le service FireAMP Connector, procédez comme suit :

a. Accédez au menu Démarrer.
b. Saisissez services.msc et appuyez sur Entrée. La console Services s'ouvre.
c. Choisissez le service Connecteur FireAMP et cliquez avec le bouton droit sur le nom du service.
d. Choisissez Start afin de démarrer le service.



Vous pouvez également saisir la commande net start immunetprotect à l'invite de commandes de l'administrateur. Si vous disposez de la version 5.0.1 ou ultérieure, entrez la commande wmic service où « name like 'immunetprotect%' » call startservice.

Cette capture d'écran présente un exemple de démarrage réussi du service :



Après le redémarrage des services, un nouvel ensemble de fichiers de base de données est créé. Vous devriez maintenant disposer d'une nouvelle instance du connecteur FireAMP avec les listes blanches, les listes de blocage, les exclusions, etc.

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.

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.