Exemple de configuration des modes d'opération des points d'accès H-REAP

Table des matières

Introduction

Ce document présente le concept du point d'accès Hybrid Remote Edge Access Point (H-REAP) et explique ses différents modes de fonctionnement avec un exemple de configuration.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Connaissance des contrôleurs LAN sans fil (WLC) et de la configuration des paramètres de base du WLC

- Connaissance de REAP

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- WLC de la gamme Cisco 4400 qui exécute la version de microprogramme 7.0.116.0
- Point d'accès léger (LAP) Cisco 1131AG
- Routeurs de la gamme Cisco 2800 exécutant la version 12.4(11)T.
- Adaptateur client Cisco Aironet 802.11a/b/g qui exécute la version 4.0 du microprogramme
- Utilitaire de bureau Cisco Aironet version 4.0
- Cisco Secure ACS exécutant la version 4.0

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

H-REAP est une solution sans fil pour les déploiements de filiales et de bureaux distants. H-REAP permet aux clients de configurer et de contrôler des points d'accès (AP) dans une filiale ou un bureau distant à partir du bureau de l'entreprise via une liaison WAN sans déployer de contrôleur dans chaque bureau.

Le H-REAP peut commuter le trafic de données de clients localement et exécuter l'authentification de clients localement lorsque la connexion au contrôleur est perdue. Une fois connecté au contrôleur, le H-REAP peut également effectuer une transmission tunnel du trafic de retour au contrôleur. En mode connecté, le point d'accès REAP hybride peut également effectuer une authentification locale.

H-REAP est pris en charge uniquement sur :

- AP 1130AG, 1140, 1240, 1250, 1260, AP801, AP 802, 1040 et AP3550
- Contrôleurs Cisco 5500, 4400, 2100, 2500 et Flex 7500
- Commutateur de contrôleur intégré Catalyst 3750G

- Module de services sans fil (WiSM) Catalyst 6500
- Module de contrôleur LAN sans fil (WLCM) pour routeurs à services intégrés (ISR)

Le trafic client sur les H-REAP peut soit être commuté localement au niveau du point d'accès, soit retourné à un contrôleur par tunneling. Cela dépend de la configuration par WLAN. En outre, le trafic client commuté localement sur le H-REAP peut être étiqueté 802.1Q pour permettre la séparation côté câblé. Pendant une panne de réseau étendu, le service sur tous les réseaux locaux sans fil commutés localement et authentifiés localement persiste.

Remarque : si les AP sont en mode H-REAP et commutés localement sur le site distant, l'affectation dynamique des utilisateurs à un VLAN spécifique basé sur la configuration du serveur RADIUS n'est pas prise en charge. Cependant, vous devriez pouvoir attribuer des utilisateurs à des VLAN spécifiques en fonction du mappage VLAN statique/SSID (Service Set Identifier) effectué localement au niveau du point d'accès. Par conséquent, un utilisateur qui appartient à un SSID particulier peut être assigné à un VLAN spécifique auquel le SSID est mappé localement au niveau du point d'accès.

Remarque : si la voix sur WLAN est importante, les points d'accès doivent être exécutés en mode local afin d'obtenir la prise en charge de CCKM et de Connection Admission Control (CAC), qui ne sont pas pris en charge en mode H-REAP.

H-REAP sur REAP

Référez-vous à Exemple de configuration de point d'accès de périphérie distante (REAP) avec des points d'accès légers et des contrôleurs de réseau local sans fil (WLC) pour plus d'informations pour aider à comprendre REAP.

H-REAP a été introduit à la suite de ces lacunes de REAP :

- Le protocole REAP ne dispose pas de séparation côté câblé. Cela est dû à l'absence de prise en charge de la norme 802.1Q. Les données des réseaux locaux sans fil atterrissent sur le même sous-réseau câblé.
- Lors d'une défaillance WAN, un point d'accès REAP cesse le service offert sur tous les WLAN, à l'exception du premier spécifié dans le contrôleur.

C'est ainsi que H-REAP surmonte ces deux lacunes :

- Prend en charge dot1Q et le mappage VLAN vers SSID. Ce mappage VLAN/SSID doit être effectué au niveau de H-REAP. Pendant ce temps, assurez-vous que les VLAN configurés sont correctement autorisés via les ports des commutateurs et routeurs intermédiaires.
- Fournit un service continu à tous les WLAN configurés pour la commutation locale.

Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce

document.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configuration

Cet exemple suppose que le contrôleur est déjà configuré avec des configurations de base. Le contrôleur utilise ces configurations :

- Adresse IP de l'interface de gestion : 172.16.1.10/16
- Adresse IP de l'interface AP-Manager : 172.16.1.11/16
- Adresse IP du routeur de passerelle par défaut : 172.16.1.25/16
- Adresse IP de la passerelle virtuelle : 1.1.1.1

Remarque : ce document ne présente pas les configurations WAN et la configuration des routeurs et des commutateurs disponibles entre le H-REAP et le contrôleur. Cela suppose que vous connaissez l'encapsulation WAN et les protocoles de routage utilisés. En outre, ce document suppose que vous comprenez comment les configurer afin de maintenir la connectivité entre le H-REAP et le contrôleur via la liaison WAN. Dans cet exemple, l'encapsulation HDLC est utilisée sur la liaison WAN.

Amorçage du point d'accès avec un contrôleur et configuration de H-REAP

Si vous voulez que le point d'accès découvre un contrôleur à partir d'un réseau distant où les mécanismes de découverte CAPWAP ne sont pas disponibles, vous pouvez utiliser l'amorçage. Cette méthode vous permet de spécifier le contrôleur auquel le point d'accès doit se connecter.

Afin d'amorcer un AP compatible H-REAP, connectez l'AP au réseau câblé au bureau central. Lors de son démarrage, le point d'accès H-REAP recherche d'abord une adresse IP pour lui-même. Une fois qu'il obtient une adresse IP via un serveur DHCP, il démarre et recherche un contrôleur pour effectuer le processus d'enregistrement.

Un point d'accès H-REAP peut apprendre l'adresse IP du contrôleur de n'importe quelle manière expliquée dans Enregistrement d'un point d'accès léger (LAP) à un contrôleur de réseau local sans fil (WLC).

Remarque : vous pouvez également configurer le LAP pour détecter le contrôleur à l'aide des commandes CLI au niveau du point d'accès. Référez-vous à Découverte du contrôleur H-REAP à l'aide des commandes CLI pour plus d'informations.

L'exemple de ce document utilise la procédure DHCP option 43 pour que H-REAP apprenne l'adresse IP du contrôleur. Il se connecte ensuite au contrôleur, télécharge l'image logicielle et la configuration les plus récentes à partir du contrôleur, et initialise la liaison radio. Il enregistre la

configuration téléchargée dans la mémoire non volatile pour une utilisation en mode autonome.

Une fois que le LAP est enregistré auprès du contrôleur, procédez comme suit :

1. Dans l'interface graphique du contrôleur, sélectionnez Wireless>Access Points.

   Ceci affiche le LAP enregistré avec ce contrôleur.

2. Cliquez sur l'AP que vous souhaitez configurer.

3. Dans la fenêtre APs>Details, cliquez sur l'onglet High Availability, et définissez les noms de contrôleurs que les AP utiliseront pour s'enregistrer, puis cliquez sur Apply.

   Vous pouvez définir jusqu'à trois noms de contrôleurs (principal, secondaire et tertiaire). Les AP recherchent le contrôleur dans le même ordre que celui que vous fournissez dans cette fenêtre. Comme cet exemple n'utilise qu'un contrôleur, il définit le contrôleur comme contrôleur principal.

4. Configurez LAP pour H-REAP.

   Afin de configurer le LAP pour fonctionner en mode H-REAP, dans la fenêtre APs>Details, sous l'onglet General, choisissez AP mode as H-REAP dans le menu déroulant correspondant.

   Ceci configure le LAP pour fonctionner en mode H-REAP.

   Remarque : dans cet exemple, vous pouvez voir que l'adresse IP du point d'accès est changée en mode statique et que l'adresse IP statique 172.18.1.10 a été attribuée. Cette affectation se produit car il s'agit du sous-réseau à utiliser au bureau distant. Par conséquent, vous utilisez l'adresse IP du serveur DHCP, mais uniquement au cours de la première phase d'enregistrement. Une fois que le point d'accès est enregistré sur le contrôleur, vous changez l'adresse en une adresse IP statique.

Maintenant que votre LAP est amorcé avec le contrôleur et configuré pour le mode H-REAP, l'étape suivante consiste à configurer H-REAP côté contrôleur et à discuter des états de commutation H-REAP.

Théorie des opérations H-REAP

Le LAP compatible H-REAP fonctionne dans les deux modes suivants :

- Mode connecté :

  Un H-REAP est dit en mode connecté lorsque sa liaison de plan de contrôle CAPWAP au WLC est active et opérationnelle. Cela signifie que la liaison WAN entre le LAP et le WLC n'est pas inactive.

- Mode autonome :

  Un H-REAP est dit être en mode autonome lorsque sa liaison WAN au WLC est en panne.

Par exemple, lorsque ce H-REAP n'a plus de connectivité au WLC connecté via la liaison WAN.

Le mécanisme d'authentification utilisé pour authentifier un client peut être défini comme Central ou Local.

- Central Authentication : fait référence au type d'authentification qui implique le processus du WLC à partir du site distant.
- Authentification locale : désigne les types d'authentification qui n'impliquent aucun traitement du WLC pour l'authentification.

Remarque : tous les traitements d'authentification et d'association 802.11 se produisent au niveau du H-REAP, quel que soit le mode utilisé par le LAP. En mode connecté, H-REAP proxie ensuite ces associations et authentifications au WLC. En mode autonome, le LAP ne peut pas informer le WLC de tels événements.

Lorsqu'un client se connecte à un AP H-REAP, l'AP transfère tous les messages d'authentification au contrôleur. Une fois l'authentification réussie, ses paquets de données sont soit commutés localement, soit renvoyés au contrôleur par tunneling. Cela dépend de la configuration du réseau local sans fil auquel il est connecté.

Avec H-REAP, les WLAN configurés sur un contrôleur peuvent fonctionner dans deux modes différents :

- Commutation centrale :

  Un WLAN sur H-REAP est dit fonctionner en mode de commutation centrale si le trafic de données de ce WLAN est configuré pour être tunnelisé vers le WLC.

- Commutation locale :

  Un WLAN sur H-REAP est dit fonctionner en mode de commutation locale si le trafic de données de ce WLAN se termine localement au niveau de l'interface filaire du LAP lui-même, sans être tunnellisé vers le WLC.

  Remarque : seuls les WLAN 1 à 8 peuvent être configurés pour la commutation locale H-REAP, car seuls ces WLAN peuvent être appliqués aux AP des gammes 1130, 1240 et 1250 qui prennent en charge la fonctionnalité H-REAP.

États de commutation H-REAP

Combiné aux modes d'authentification et de commutation mentionnés dans la section précédente, un H-REAP peut fonctionner dans l'un de ces états :

- Authentification centrale, Commutation centrale
- Authentification désactivée, Commutation désactivée

- Authentification centrale, Commutation locale
- Authentification désactivée, Commutation locale
- Authentification locale, Commutation locale

Authentification centrale, Commutation centrale

Dans cet état, pour le WLAN donné, le point d'accès transfère toutes les demandes d'authentification du client au contrôleur et transfère toutes les données du client au WLC par tunnel. Cet état n'est valide que lorsque le H-REAP est en mode connecté. Tout réseau local sans fil configuré pour fonctionner dans ce mode est perdu en cas de panne du réseau étendu, quelle que soit la méthode d'authentification.

Cet exemple utilise les paramètres de configuration suivants :

- Nom WLAN/SSID : Central
- Sécurité de couche 2 : WPA2
- Commutation locale H-REAP : désactivée

Complétez ces étapes afin de configurer le WLC pour l'authentification centrale, la commutation centrale à l'aide de l'interface graphique utilisateur :

1. Cliquez sur WLANs afin de créer un nouveau WLAN nommé Central, puis cliquez sur Apply.
2. Comme ce WLAN utilise l'authentification centrale, nous utilisons l'authentification WPA2 dans le champ Layer 2 Security. WPA2 est la sécurité de couche 2 par défaut pour un WLAN.
3. Sélectionnez l'onglet AAA Servers, puis le serveur approprié configuré pour l'authentification.
4. Comme ce WLAN utilise la commutation centrale, vous devez vous assurer que la case H-REAP Local Switching est désactivée (c'est-à-dire que la case Local Switching n'est pas cochée). Cliquez ensuite sur Apply.

Vérification de l'authentification centrale, Commutation centrale

Procédez comme suit :

1. Configurez le client sans fil avec les mêmes SSID et configurations de sécurité.

   Dans cet exemple, le SSID est Central et la méthode de sécurité est WPA2.

2. Entrez le nom d'utilisateur et le mot de passe configurés dans le serveur RADIUS>User Setup afin d'activer le SSID central dans le client.

   Cet exemple utilise User1 comme nom d'utilisateur et mot de passe.

Le client est authentifié de manière centralisée par le serveur RADIUS et est associé au point d'accès H-REAP. Le H-REAP est maintenant dans l'authentification centrale, la commutation centrale.

Authentification désactivée, Commutation désactivée

Avec la même configuration expliquée dans la section Authentification centrale, Commutation centrale, désactivez la liaison WAN qui connecte le contrôleur. Maintenant, le contrôleur attend une réponse de pulsation du point d'accès. Une réponse de pulsation est similaire aux messages de test d'activité. Le contrôleur essaie cinq pulsations consécutives, chaque seconde.

Comme il n'est pas reçu avec une réponse de pulsation du H-REAP, le WLC annule l'enregistrement du LAP.

Émettez la commande debug capwap events enable à partir de l'interface de ligne de commande du WLC afin de vérifier le processus de désinscription. Voici l'exemple de sortie de cette commande debug :

<#root>

```
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90

Did not receive heartbeat reply from
AP 00:15:c7:ab:55:90

Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Down capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 apfSpamProcessStateChangeInSpamConte
xt: Deregister capwap event for AP 00:15:c7:ab:55:90 slot 1
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 0!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90

Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 0
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Received capwap Down event for AP 00:
15:c7:ab:55:90 slot 1!
Thu Jan 18 03:19:32 2007: 00:15:c7:ab:55:90 Deregister capwap event for AP 00:15:
c7:ab:55:90 slot 1
```

Le H-REAP passe en mode autonome.

Comme ce WLAN était précédemment authentifié et commuté de manière centralisée, le trafic de contrôle et de données a été renvoyé au contrôleur par une tunnellisation. Par conséquent, sans le contrôleur, le client ne peut pas maintenir l'association avec le H-REAP et il est déconnecté. Cet état de H-REAP avec l'association du client et l'authentification étant désactivée est appelé Authentication Down, Switching Down.

Authentification centrale, Commutation locale

Dans cet état, pour le WLAN donné, le WLC gère toutes les authentifications client, et le LAP H-REAP commute les paquets de données localement. Une fois que le client s'est authentifié avec succès, le contrôleur envoie des commandes de contrôle capwap au H-REAP et demande au LAP de commuter localement les paquets de données du client donné. Ce message est envoyé par client lors d'une authentification réussie. Cet état s'applique uniquement en mode connecté.

Cet exemple utilise les paramètres de configuration suivants :

- Nom WLAN/SSID : Central-Local
- Sécurité de couche 2 : WPA2.
- Commutation locale H-REAP : activée

À partir de l'interface graphique du contrôleur, procédez comme suit :

1. Cliquez sur WLANs afin de créer un nouveau WLAN nommé Central-Local, puis cliquez sur Apply.
2. Comme ce WLAN utilise l'authentification centrale, choisissez l'authentification WPA2 dans le champ Layer 2 Security.
3. Dans la section Radius Servers, sélectionnez le serveur approprié configuré pour l'authentification.
4. Cochez la case H-REAP Local Switching afin de commuter le trafic client qui appartient à ce WLAN localement au niveau de H-REAP.

Vérification de l'authentification centrale, commutation locale

Procédez comme suit :

1. Configurez le client sans fil avec les mêmes SSID et configurations de sécurité.

   Dans cet exemple, le SSID est Central-Local et la méthode de sécurité est WPA2.

2. Entrez le nom d'utilisateur et le mot de passe configurés dans le serveur RADIUS>User Setup afin d'activer le SSID central-local dans le client.

   Cet exemple utilise User1 comme nom d'utilisateur et mot de passe.

3. Click OK.

   Le client est authentifié de manière centralisée par le serveur RADIUS et est associé au point d'accès H-REAP. Le H-REAP est maintenant dans l'authentification centrale, la commutation locale.

Authentification désactivée, Commutation locale

Si un WLAN commuté localement est configuré pour un type d'authentification qui doit être traité sur le WLC (comme l'authentification EAP [dynamic WEP/WPA/WPA2/802.11i], WebAuth ou NAC), en cas de défaillance du WAN, il entre l'authentification down, l'état de commutation local. Dans cet état, pour le WLAN donné, le H-REAP rejette tous les nouveaux clients qui essaient de s'authentifier. Cependant, il continue d'envoyer des balises et des réponses d'analyse pour maintenir les clients existants correctement connectés. Cet état n'est valide qu'en mode autonome.

Afin de vérifier cet état, utilisez la même configuration expliquée dans la section Authentification centrale, Commutation locale.

Si la liaison WAN qui connecte le WLC est en panne, le WLC passe par le processus de désinscription du H-REAP.

Une fois radié, H-REAP passe en mode autonome.

Le client associé via ce WLAN conserve sa connectivité. Cependant, comme le contrôleur, l'authentificateur n'est pas disponible, H-REAP n'autorise aucune nouvelle connexion à partir de ce WLAN.

Ceci peut être vérifié par l'activation d'un autre client sans fil dans le même WLAN. Vous pouvez constater que l'authentification de ce client échoue et que ce client n'est pas autorisé à s'associer.

Remarque : lorsqu'un nombre de clients WLAN est égal à zéro, le H-REAP cesse toutes les fonctions 802.11 associées et n'émet plus de balises pour le SSID donné. Le WLAN passe ainsi à l'état H-REAP suivant : authentification désactivée, mise hors tension.

Authentification locale, Commutation locale

Dans cet état, le LAP H-REAP gère les authentifications client et commute localement les paquets de données client. Cet état n'est valide qu'en mode autonome et seulement pour les types d'authentification qui peuvent être gérés localement au niveau du point d'accès et qui n'impliquent pas le traitement du contrôleur

Le H-REAP qui était précédemment dans l'état de commutation locale de l'authentification centrale, passe dans cet état, à condition que le type d'authentification configuré puisse être géré localement au niveau du point d'accès. Si l'authentification configurée ne peut pas être gérée localement, telle que l'authentification 802.1x, alors en mode autonome, le H-REAP passe à l'authentification down, en mode de commutation locale.

Voici quelques-uns des mécanismes d'authentification courants qui peuvent être gérés localement au niveau du point d'accès en mode autonome :

- Open (ouvert)
- Partagé

- WPA-PSK
- WPA2-PSK

Remarque : tous les processus d'authentification sont gérés par le WLC lorsque le point d'accès est en mode connecté. Pendant que le H-REAP est en mode autonome, les authentifications ouvertes, partagées et WPA/WPA2-PSK sont transférées aux LAP où se produit l'authentification de tous les clients.

Remarque : l'authentification Web externe n'est pas prise en charge lors de l'utilisation de REAP hybride avec la commutation locale activée sur le WLAN.

Cet exemple utilise les paramètres de configuration suivants :

- Nom WLAN/SSID : Local
- Sécurité de couche 2 : WPA-PSK
- Commutation locale H-REAP : activée

À partir de l'interface graphique du contrôleur, procédez comme suit :

1. Cliquez sur WLANs afin de créer un nouveau WLAN nommé Local, puis cliquez sur Apply.
2. Comme ce WLAN utilise l'authentification locale, choisissez WPA-PSK ou l'un des mécanismes de sécurité mentionnés qui peuvent être gérés localement dans le champ Layer 2 Security.

   Cet exemple utilise WPA-PSK.
3. Une fois choisi, vous devez configurer la clé pré-partagée/phrase de passe à utiliser.

   Ce doit être le même côté client pour que l'authentification réussisse.
4. Cochez la case H-REAP Local Switching afin de commuter le trafic client qui appartient à ce WLAN localement au niveau de H-REAP.

Vérification de l'authentification locale, commutation locale

Procédez comme suit :

1. Configurez le client avec les mêmes SSID et configurations de sécurité.

   Ici, le SSID est Local et la méthode de sécurité est WPA-PSK.
2. Activez le SSID local dans le client.

   Le client est authentifié centralement au niveau du contrôleur et s'associe au H-REAP. Le trafic client est configuré pour commuter localement. Maintenant, le H-REAP est dans l'état Authentification centrale, Commutation locale.

3. Désactivez la liaison WAN qui se connecte au contrôleur.

   Comme d'habitude, le contrôleur passe par le processus de radiation. H-REAP est radié du contrôleur.

   Une fois radié, H-REAP passe en mode autonome.

   Cependant, le client qui appartient à ce WLAN conserve son association avec H-REAP.

   En outre, étant donné que le type d'authentification ici peut être géré localement au niveau du point d'accès sans le contrôleur, H-REAP autorise les associations à partir de tout nouveau client sans fil via ce WLAN.

4. Afin de vérifier cela, activez tout autre client sans fil sur le même WLAN.

   Vous pouvez voir que le client est authentifié et associé avec succès.

Dépannage

- Afin de dépanner davantage les problèmes de connectivité du client au port de console du H-REAP, entrez cette commande :

  <#root>

  AP_CLI#

  show capwap reap association

- Afin de dépanner davantage les problèmes de connectivité du client au niveau du contrôleur et de limiter la sortie de débogage supplémentaire, utilisez cette commande :

  <#root>

  AP_CLI#

  debug mac addr

- Afin de déboguer les problèmes de connectivité 802.11 d'un client, utilisez cette commande :

  <#root>

  AP_CLI#

```
debug dot11 state enable
```

- Déboguez le processus d'authentification 802.1X d'un client et les échecs avec cette commande :

```
<#root>

AP_CLI#

debug dot1x events enable
```

- Les messages du contrôleur principal/RADIUS peuvent être débogués à l'aide de cette commande :

```
<#root>

AP_CLI#

debug aaa events enable
```

- Vous pouvez également utiliser cette commande pour activer une suite complète de commandes debug du client :

```
<#root>

AP_CLI#

debug client
```

Informations connexes

- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Exemple de configuration de réseaux VLAN sur des contrôleurs de réseau local sans fil
- Guide de configuration du contrôleur de réseau local sans fil Cisco, version 7.0
- Guide de conception et de déploiement REAP hybride
- Dépannage de base d'un point d'accès de périphérie distant hybride (H-REAP)
- Exemple de configuration du basculement du contrôleur de réseau local sans fil pour les points d'accès légers
- Assistance produit sans fil

- Assistance et documentation techniques - Cisco Systems

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.