Configuration et dépannage de la synchronisation d'état de posture

Table des matières

Introduction

Ce document décrit la configuration et l'utilisation de la synchronisation d'état de posture introduite dans la version 3.1 de Cisco Identity Service Engine(ISE).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Flux de posture sur Cisco ISE
- Configuration des composants de posture sur Cisco ISE

Il est supposé que vous avez une configuration Posture à la place de n'importe quel type.

Pour mieux comprendre les concepts décrits plus loin, il est recommandé de passer en revue les

points suivants :

- Guide de l'administrateur de Cisco Identity Services Engine, version 3.1
- Comparaison des versions antérieures d'ISE avec le flux de posture ISE dans ISE 2.2
- Gestion et positionnement des sessions ISE

Composants utilisés

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

- Cisco ISE version 3.1
- Cisco Secure Client 5.0.00556

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

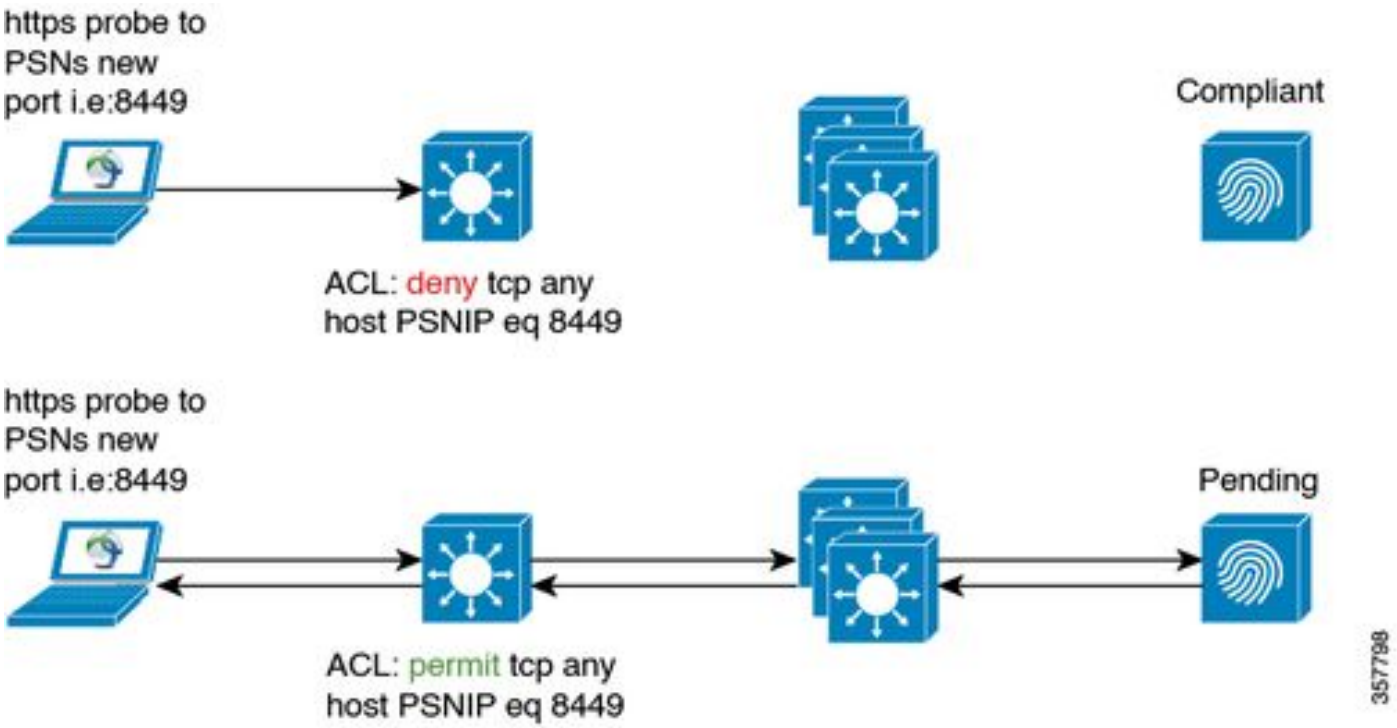
Le flux de posture ISE ne permet généralement pas de mettre à jour l'état de posture sur le client à partir de l'ISE. Le module Cisco Secure Client Posture permet d'évaluer l'état de la position du terminal et de le conserver jusqu'à la modification du réseau, la réévaluation périodique ou d'autres déclencheurs côté client. Si l'état de la position du terminal change sur ISE en raison d'une fermeture de session ou d'autres raisons, le module Secure Client Posture Module peut ne pas être au courant de ce changement, de sorte que le terminal reste dans l'état Posture inconnue avec un accès réseau limité jusqu'à ce que l'un des déclencheurs côté client se produise.

Ce document se concentre sur une nouvelle fonctionnalité - Synchronisation de l'état de la position, qui a été développée pour résoudre ce type de problème et permettre à ISE de fournir des commentaires au module Secure Client Posture sur l'état actuel de la position du terminal.

Configurer

Le port de sonde d'état de position a été introduit sur chaque noeud PSN ISE lorsque la synchronisation d'état de position est activée - TCP 8449 par défaut. Il est censé être accessible à partir du point de terminaison si l'état de la position du point de terminaison est Inconnu ou En attente et inaccessible si l'état du point de terminaison est Conforme.

Diagramme du réseau



Configurations

La configuration de la fonction de synchronisation d'état de posture se compose de deux parties :

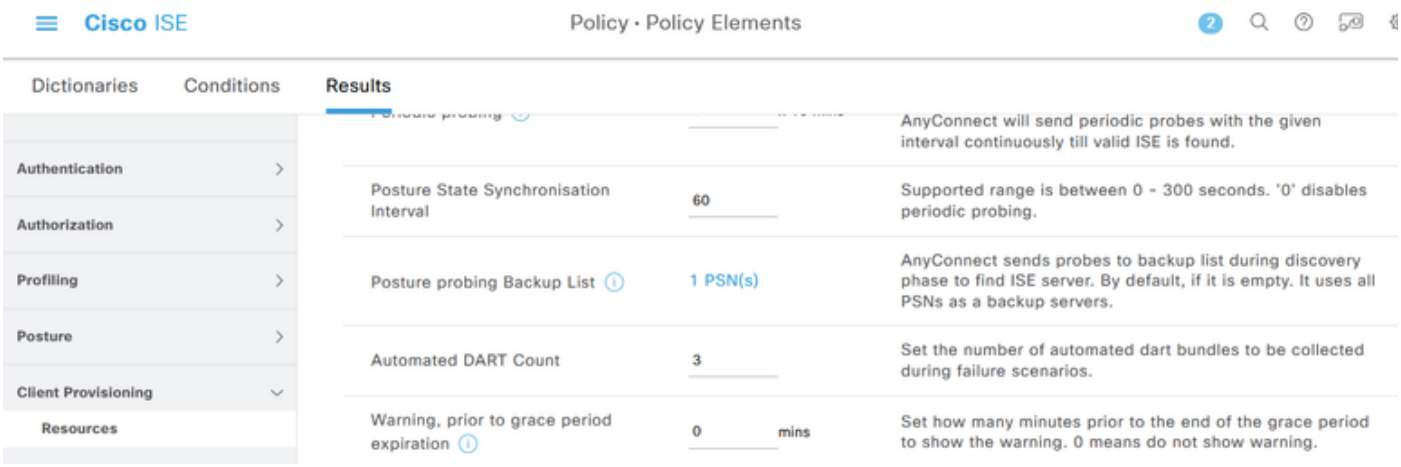
1. Configuration du profil de posture AnyConnect

   1.1 Dans l'interface utilisateur graphique de Cisco ISE, accédez à Policy > Policy Elements > Results > Client Provisioning > Resources.

   1.2 Sélectionnez le profil de posture AnyConnect que vous utilisez déjà ou créez-en un nouveau.

   1.3 Dans la zone Comportement de l'agent, configurez l'intervalle de synchronisation d'état de posture sur une valeur comprise entre 1 et 300 secondes, 0 - désactive la synchronisation d'état de posture

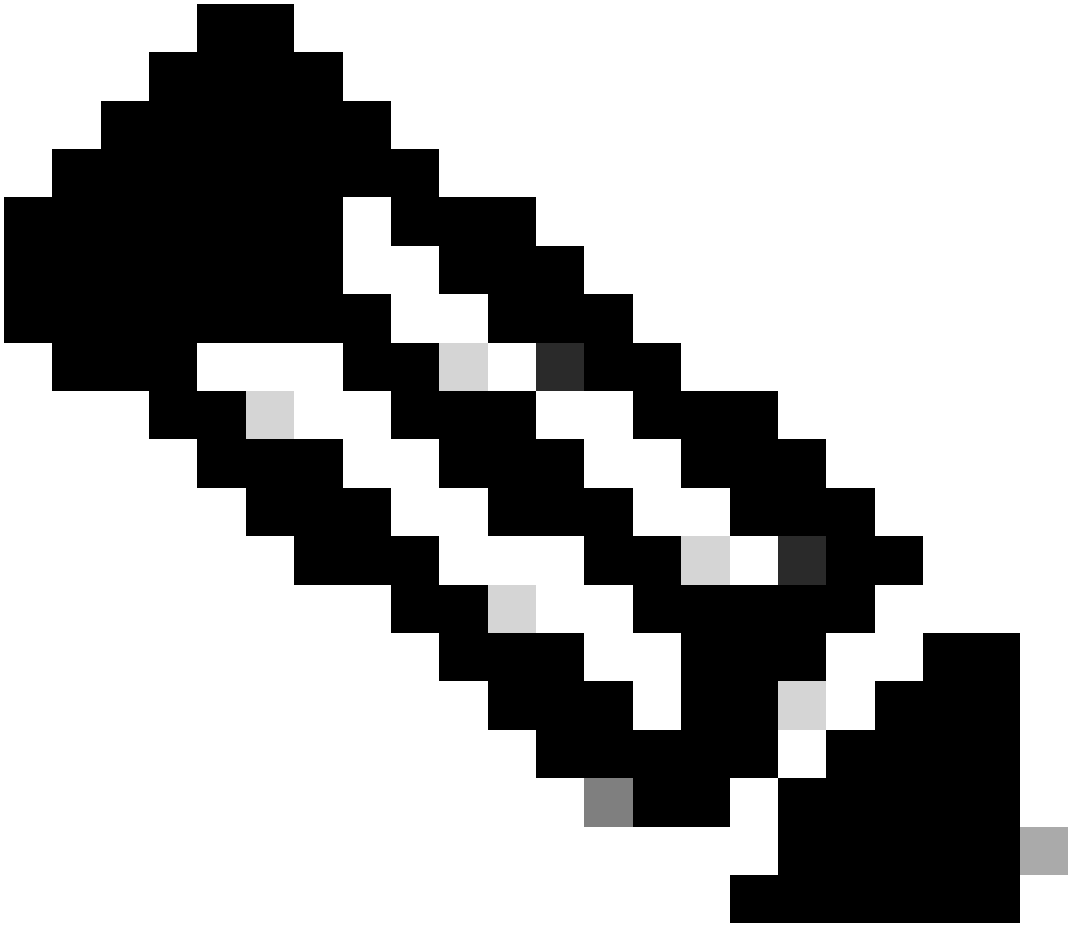
   1.4 Vous pouvez configurer la liste de sauvegarde de l'analyse de position - Secure Client utilise cette liste pour vérifier l'état de position sur les PSN sélectionnés. Si vous ne choisissez aucun PSN, le PSN connecté et deux serveurs de sauvegarde sont utilisés comme sauvegardes pour la synchronisation d'état.



2. Configuration d'une liste de contrôle d'accès téléchargeable (dACL) pour bloquer l'accès au port de synchronisation d'état de position sur Cisco ISE lorsque l'état de position du client est Conforme ou Non conforme. Vous devez ajouter une entrée de refus de contrôle d'accès avec le port de synchronisation d'état de position pour chaque PSN en haut des ACL utilisées pour les points d'extrémité conformes pour restreindre l'accès au port de synchronisation d'état de position si l'état du point d'extrémité est connu, par exemple :

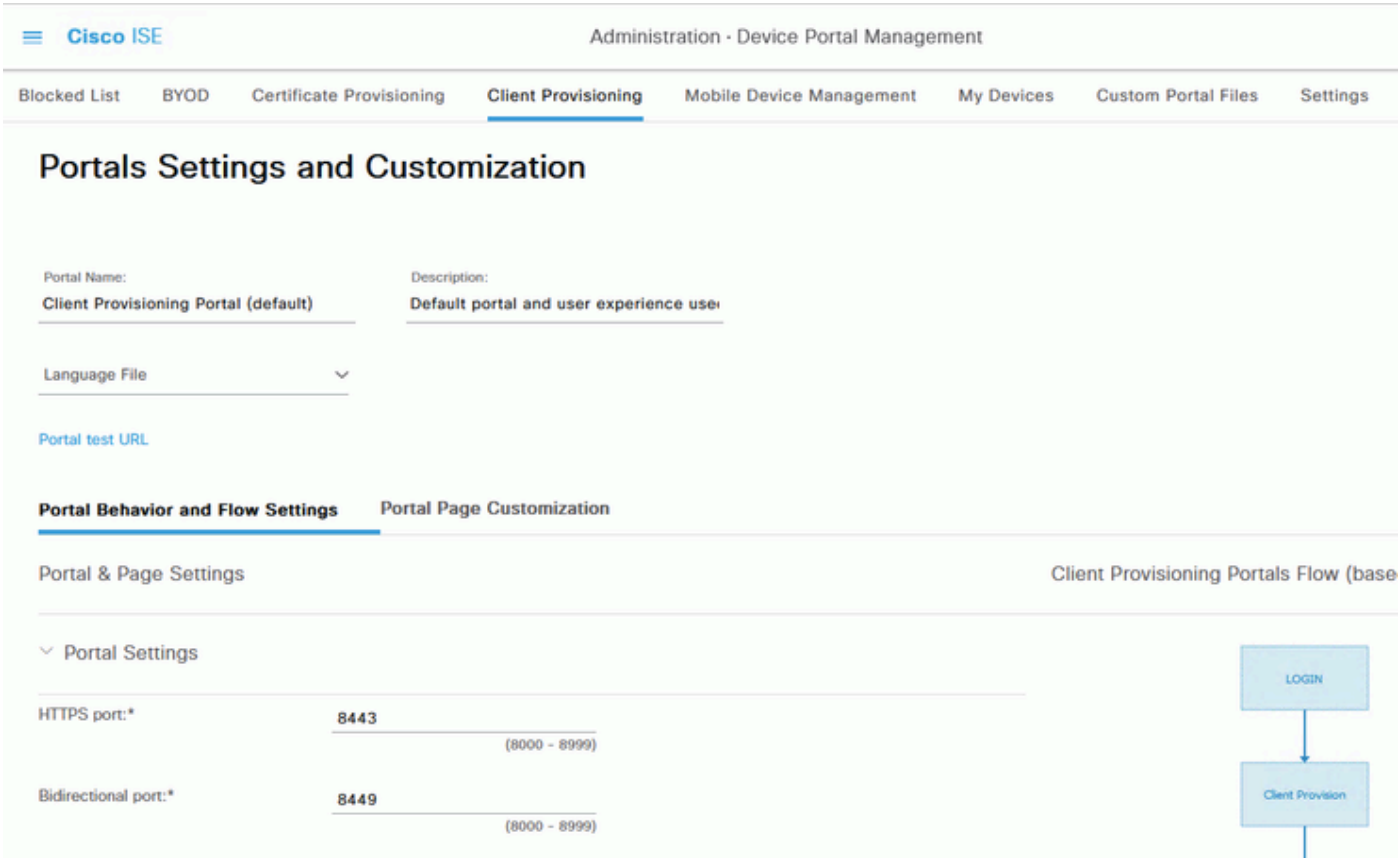
```
deny tcp any host PSN1-IP-ADDRESS eq 8449
deny tcp any host PSN2-IP-ADDRESS eq 8449
permit ip any any
```

permit ip any any n'est pas obligatoire, vous pouvez le remplacer par n'importe quel ensemble de règles selon vos besoins.



Remarque : si l'entrée deny dans dACL n'est pas configurée, l'alarme de détection de configuration de posture est déclenchée sur le tableau de bord Cisco ISE et la synchronisation d'état de posture est désactivée sur le terminal jusqu'à ce que le client sécurisé Cisco soit redémarré.

Le port de synchronisation d'état de posture (port bidirectionnel) peut être modifié sur la page de configuration du portail d'approvisionnement du client. Accédez à Administration > Device Portal Management > Client Provisioning > Select desirable portal > Portal Behavior and Flow Settings et ouvrez Portal Settings. Impossible de modifier le port de synchronisation d'état de posture pour le portail d'approvisionnement du client par défaut.



Vérifier

De l'offre DART

La synchronisation de l'état de la position peut être vérifiée du côté client en consultant les journaux du module Cisco Secure Client Posture (AnyConnect_ISEPosture.txt) du bundle DART :

1. L'évaluation de la posture est terminée, l'état de la posture est Conforme.

```
2022/11/09 12:22:47 [Information] aciseagent Function: Authenticator::sendUIStatus Thread Id: 0xC60 Fil
```

2. État de la position La recherche de synchronisation a démarré.

```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

3. La connexion HTTPS au PSN ISE sur le port de synchronisation d'état de posture (8449) est initiée.

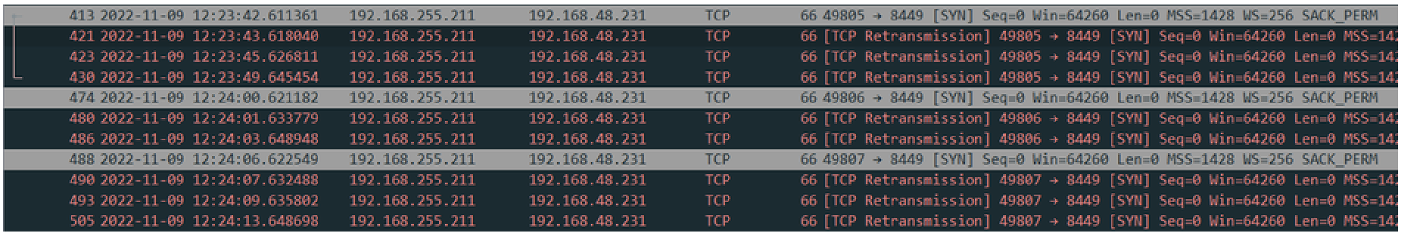
```
2022/11/09 12:22:47 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:22:47 [Information] aciseagent Function: HttpConnection::MakeRequest Thread Id: 0x296C Fi
```

4. Délai d'attente pour l'analyse de synchronisation Posture Status.

```
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_winhttp_post Thread Id: 0x296C File
2022/11/09 12:22:54 [Information] aciseagent Function: hs_transport_post Thread Id: 0x296C File: hs_tra
2022/11/09 12:22:54 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

À partir de la capture de paquets sur le client

La capture de paquets effectuée sur le client montre les paquets SYN envoyés vers le noeud PSN ISE sur le port de synchronisation d'état de posture (8449) sans réponse SYN-ACK d'ISE PSN :



413	2022-11-09 12:23:42.611361	192.168.255.211	192.168.48.231	TCP	66 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
421	2022-11-09 12:23:43.618040	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
423	2022-11-09 12:23:45.626811	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
430	2022-11-09 12:23:49.645454	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49805 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
474	2022-11-09 12:24:00.621182	192.168.255.211	192.168.48.231	TCP	66 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
480	2022-11-09 12:24:01.633779	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
486	2022-11-09 12:24:03.648948	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49806 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
488	2022-11-09 12:24:06.622549	192.168.255.211	192.168.48.231	TCP	66 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
490	2022-11-09 12:24:07.632488	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
493	2022-11-09 12:24:09.635802	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14
505	2022-11-09 12:24:13.648698	192.168.255.211	192.168.48.231	TCP	66 [TCP Retransmission] 49807 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=14

À partir de ISE

La configuration correcte de la synchronisation d'état de posture ne peut pas être vérifiée du côté ISE, car la connexion sur le port de synchronisation d'état de posture (8449) est supposée échouer.

Redémarrage de posture lors du changement d'état de posture

1) Des informations d'état de session ont été reçues d'ISE avec l'état de position « Inconnu » alors que le client sécurisé Cisco est dans un état « Conforme ».

```
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_htt
```

```
2022/11/09 12:26:24 [Information] aciseagent Function: dump_http_headers Thread Id: 0x296C File: hs_http
```

2) Cisco Secure Client accuse réception du changement d'état de la position et redémarre la détection de position :

```
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
```

3) Cisco Secure Client arrête la synchronisation d'état de posture jusqu'à l'évaluation de la posture :

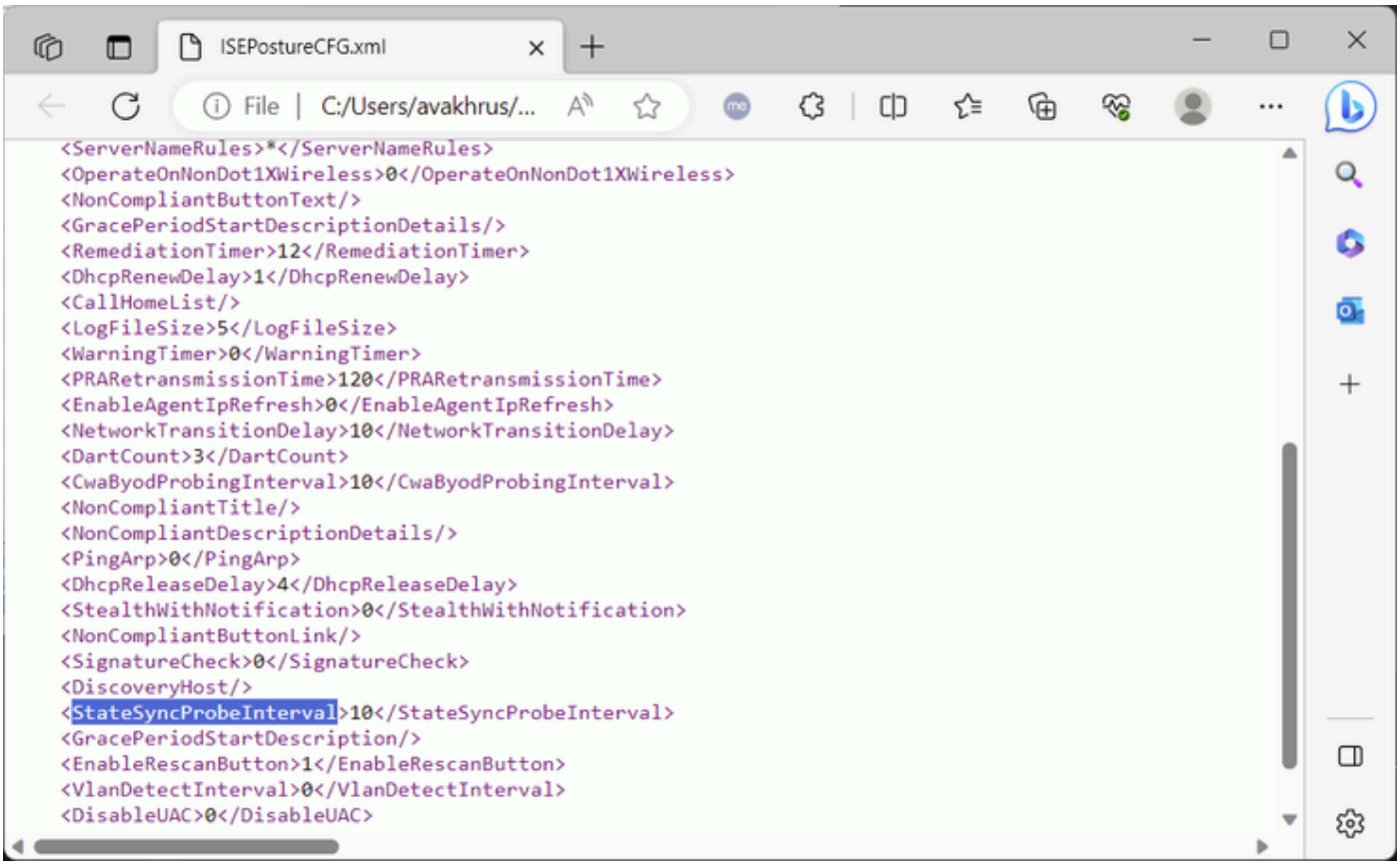
```
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::processMessage Thread Id: 0xC60
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: SwiftHttpRunner::restartDiscovery Thread Id: 0xC
2022/11/09 12:26:24 [Information] aciseagent Function: hs_transport_free Thread Id: 0xC60 File: hs_trans
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:24 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x296
```

Dépannage

La synchronisation d'état de posture ne démarre pas

S'il n'y a aucune indication de démarrage de la synchronisation d'état de posture dans le fichier journal AnyConnect_ISEPosture.txt et que le client n'essaie pas d'établir une connexion avec le noeud PSN ISE sur le port de synchronisation d'état de posture (8449), vérifiez le fichier de configuration de posture ISEPostureCFG.xml à partir du bundle DART ou directement sur l'ordinateur client : « %ProgramData%\Cisco\Cisco Secure Client\ISE Posture\ » pour un PC Windows.

Le paramètre responsable de la synchronisation d'état de posture est "StateSyncProbeInterval", il est supposé être défini avec une valeur supérieure à 0 :



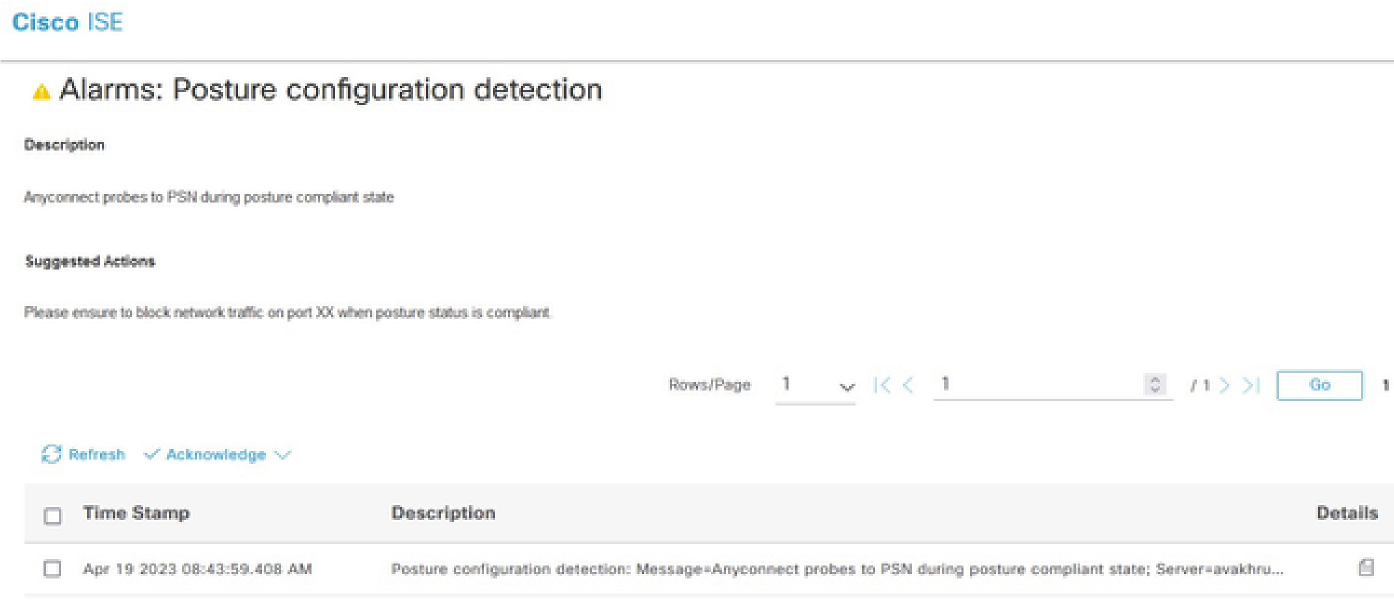
L'absence de "StateSyncProbeInterval" ou une valeur de "0" signifie que la synchronisation d'état de position est désactivée.

Si "Intervalle de synchronisation d'état de posture" est défini dans le profil de posture sur ISE mais n'est pas reflété dans un fichier de configuration sur le client, alors le provisionnement de posture doit être examiné.

Échec de la synchronisation d'état de posture avec alarme sur le tableau de bord ISE

Si la synchronisation d'état de posture échoue avec l'alarme sur ISE, cela signifie que le client sécurisé Cisco a pu atteindre ISE sur le port de synchronisation d'état de posture (8449) et a demandé un état pour la session avec l'état « Conforme ».

- Alarme dans l'interface utilisateur ISE :



- Valider à partir de la capture de paquets

La connexion TCP sur le port de synchronisation d'état de posture (8449) est établie :

No.	Time	Source	Destination	Protocol	Length	Info
988	2022-11-09 12:26:24.690977	192.168.255.211	192.168.48.231	TCP	66	49819 → 8449 [SYN] Seq=0 Win=64260 Len=0 MSS=1428 WS=256 SACK_PERM
989	2022-11-09 12:26:24.744041	192.168.48.231	192.168.255.211	TCP	66	8449 → 49819 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1300 SACK_PERM WS=128
990	2022-11-09 12:26:24.744102	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=1 Ack=1 Win=262400 Len=0
991	2022-11-09 12:26:24.744548	192.168.255.211	192.168.48.231	TLSv1…	268	Client Hello
992	2022-11-09 12:26:24.796877	192.168.48.231	192.168.255.211	TCP	60	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=0
993	2022-11-09 12:26:24.813236	192.168.48.231	192.168.255.211	TCP	1354	8449 → 49819 [ACK] Seq=1 Ack=215 Win=30336 Len=1300 [TCP segment of a reassembl
994	2022-11-09 12:26:24.813335	192.168.48.231	192.168.255.211	TLSv1…	824	Server Hello, Certificate, Server Key Exchange, Server Hello Done
995	2022-11-09 12:26:24.813396	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=215 Ack=2071 Win=262400 Len=0
996	2022-11-09 12:26:24.815274	192.168.255.211	192.168.48.231	TLSv1…	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
997	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	60	Change Cipher Spec
998	2022-11-09 12:26:24.881656	192.168.48.231	192.168.255.211	TLSv1…	99	Encrypted Handshake Message
999	2022-11-09 12:26:24.881755	192.168.255.211	192.168.48.231	TCP	54	49819 → 8449 [ACK] Seq=341 Ack=2122 Win=262400 Len=0

- Validation à partir du journal du module Cisco Secure Client Posture

Vérifiez AnyConnect_ISEPosture.txt dans l'offre groupée DART :

1) La connexion HTTPS au PSN ISE sur le port de synchronisation d'état de posture (8449) est initiée.

```
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
```

2) Des informations sur l'état de la session ont été reçues d'ISE avec l'état de posture « Conforme ».

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

```
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
2022/11/09 12:26:34 [Information] aciseagent Function: dump_http_headers Thread Id: 0x2750 File: hs_htt
```

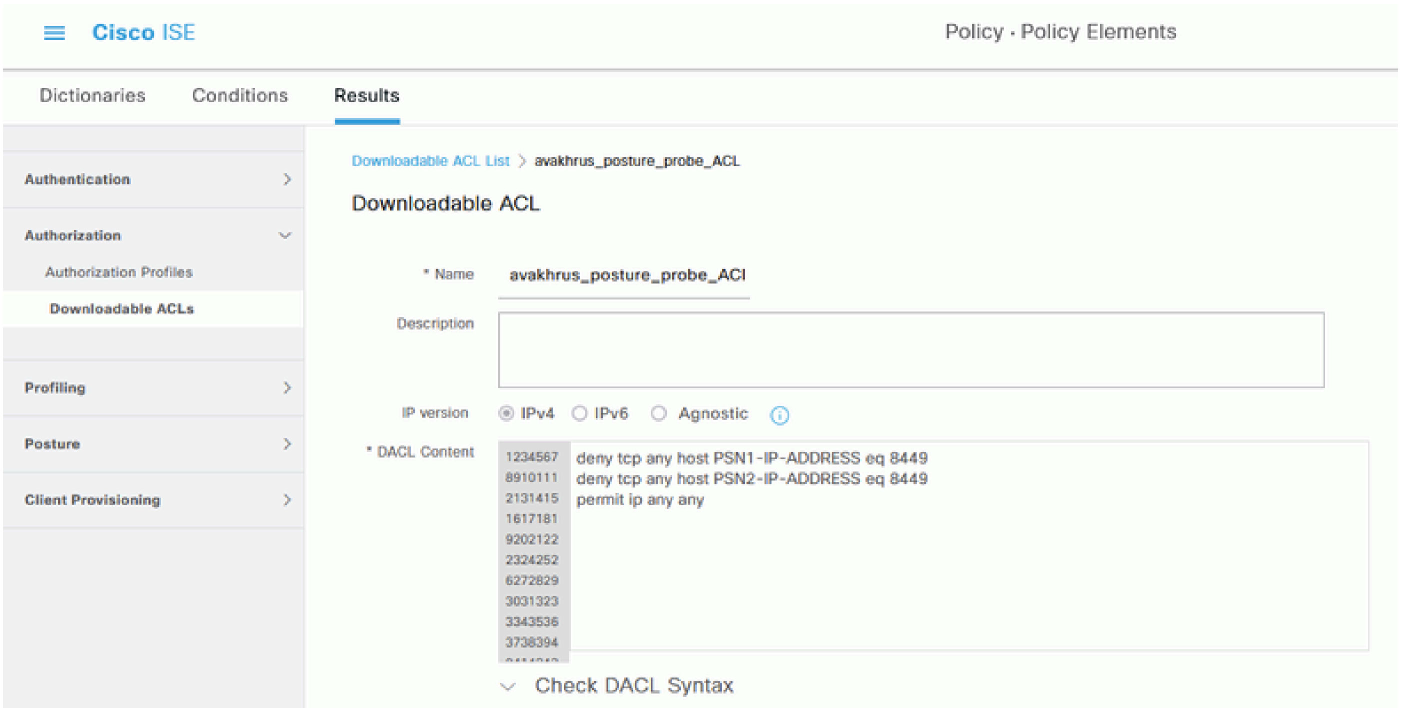
3) La synchronisation d'état de posture s'arrête en raison de la détection d'une configuration incorrecte :

```
2022/11/09 12:26:34 [Error] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x2750 File
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::sessionSyncProbe Thread Id: 0x275
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
2022/11/09 12:26:34 [Information] aciseagent Function: PeriodicProbe::ProcessMessage Thread Id: 0xC60 F
```

La synchronisation d'état de posture ne peut pas être redémarrée à partir de l'interface utilisateur graphique du client sécurisé Cisco en redémarrant l'évaluation de la posture ou une modification du réseau. Au lieu de cela, le client sécurisé Cisco doit être redémarré pour que la synchronisation d'état de posture fonctionne à nouveau.

Vérifier la dACL configurée pour le profil d'autorisation Posture "Compliant"

1. Validez que la dACL appropriée est configurée pour le profil d'autorisation Posture « Compliant » :



2. Validez que la dACL du rapport d'authentification détaillé a été envoyée correctement suite à

l'authentification du point d'extrémité « Conforme ».

CPMSessionID	c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0
CiscoAVPair	aaa:service=ip_admission,aaa:event=acl-download

Result

Class	CACS:c0a830e7lFjmLTxwC_6BfWNqU3RwKrGfaDTw5krqr1QOzEm/ej0:ISE-PSN-FQDN/482174459/480
cisco-av-pair	ip:inacl#1=deny tcp any host PSN1-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#2=deny tcp any host PSN2-IP-ADDRESS eq 8449
cisco-av-pair	ip:inacl#3=permit ip any any

3. Vérifiez que la dACL est correctement appliquée sur un périphérique d’accès réseau :

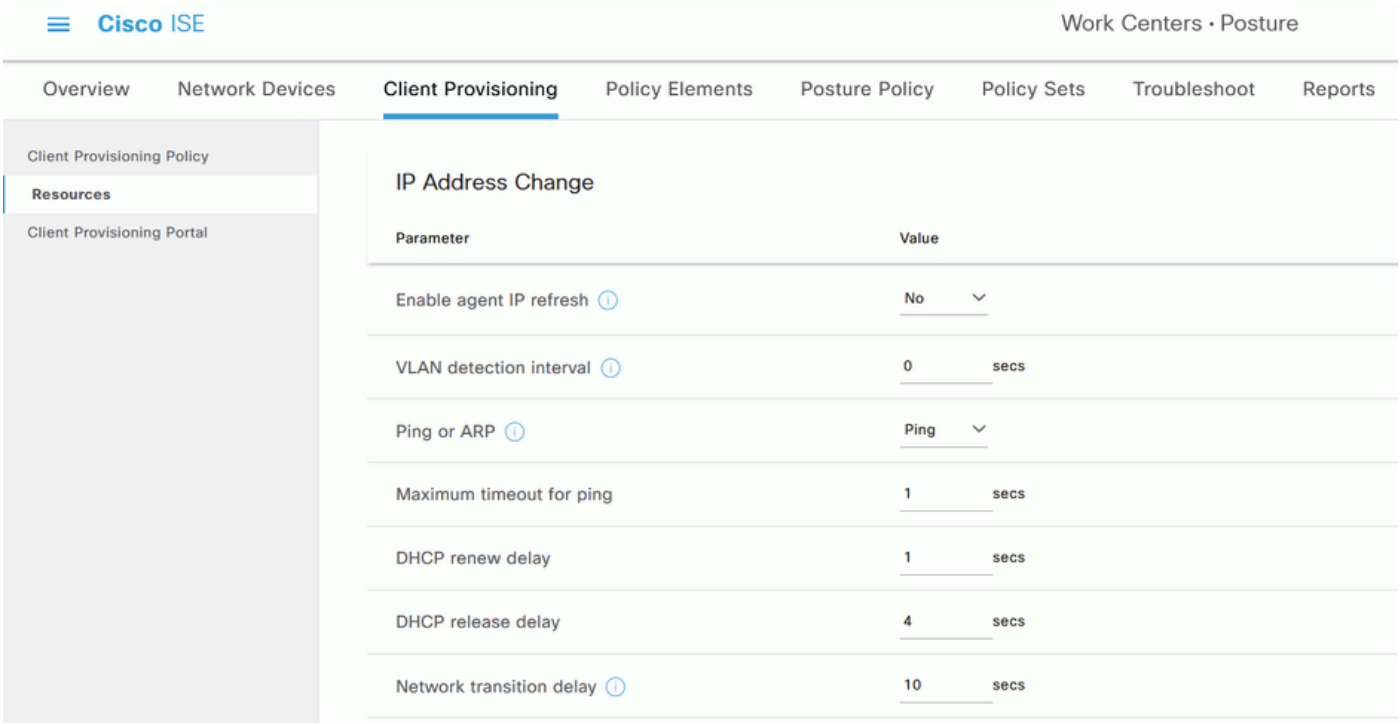
```
avakhrus_3560C#sh authe sess int fa0/12 det
            Interface:  FastEthernet0/12
          MAC Address:  0050.56a8.be02
         IPv6 Address:  Unknown
         IPv4 Address:  192.168.255.193
            User-Name:  TRAINING\bob
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
      Restart timeout:  N/A
Periodic Acct timeout:  172800s (local), Remaining: 92111s
       Session Uptime:  1515s
    Common Session ID:  C0A8FF0C00000012679EAF14
      Acct Session ID:  0x00000012
               Handle:  0x5D000005
       Current Policy:  POLICY_Fa0/12

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:
             ACS ACL:  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac

Method status list:
       Method           State

       mab              Stopped
       dot1x            Authc Success
```

```
avakhrus_3560C#sh access-lists | s  xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac
Extended IP access list xACSACLx-IP-avakhrus_posture_probe_ACL-636b75ac (per-user)
    1 deny tcp any host PSN1-IP-ADDRESS eq 8449
    2 deny tcp any host PSN2-IP-ADDRESS eq 8449
    3 permit ip any any
```

Problèmes identifiés

Échec de la synchronisation d'état de posture avec alarme sur ISE

La synchronisation d'état de posture peut échouer avec l'alarme sur ISE même si la dACL appropriée est appliquée sur un périphérique d'accès réseau au point d'extrémité client. Cela se produit si la sonde de synchronisation d'état de posture est exécutée plus rapidement que l'application de la dACL ou si la sonde de synchronisation d'état de posture est déjà en cours lorsque la dACL est appliquée. Le problème a été étudié dans l'ID de bogue Cisco CSCwd58316 . Pour contourner ce problème, vous devez définir le « délai de transition réseau » sur 10 secondes dans le profil de posture Anyconnect (Paramètres du profil d'agent de posture ISE).



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.