Erreur de vérification de préconnexion CSD Hostscan dans le client sécurisé

Table des matières

Problème

Un utilisateur rencontre le message d'erreur « Echec de la vérification de préconnexion du CSD de Hostscan » lorsqu'il tente de se connecter à un VPN à l'aide de Cisco Secure Client sur un périphérique Windows 11. L'erreur se produit avant l'affichage de l'invite de connexion, empêchant l'utilisateur d'accéder à la connexion VPN. Le même utilisateur peut se connecter au VPN à partir d'un autre périphérique en utilisant des informations d'identification et un profil VPN identiques, ce qui indique que le problème est spécifique au périphérique et non lié aux informations d'identification.

Autres entrées du journal d'erreurs observées :

- CONNECTIFC_ERROR_FILE_OPEN_FAILED (Code de retour : -30015466 / 0xFE360016)
- Échec du traitement HostScan
- La tentative de connexion a échoué en raison d'un problème réseau ou PC

L'utilisateur a pu se connecter à d'autres profils VPN où l'affichage n'était pas activé, mais n'a pas pu se connecter à des profils où l'affichage était activé. La configuration fonctionnait auparavant sans qu'aucune modification connue n'ait été apportée à la configuration.

Environnement

- Client sécurisé Cisco version 5.1.7.80
- Système d'exploitation : Windows 11
- Profil VPN avec positionnement activé

- Le problème est spécifique au périphérique, affectant un seul utilisateur sur un périphérique particulier
- Lié à l'ID de bogue Cisco : CSCwk54713

Résolution

La résolution implique la désinstallation complète et sans problème du client sécurisé Cisco et la réinstallation du logiciel. Les méthodes de désinstallation et de réinstallation standard ne résolvent pas toujours le problème en raison d'entrées de registre ou de fichiers résiduels corrompus.

Étape 1: Désactiver les services tiers

Désactivez tous les services tiers dans Msconfig, y compris les services proxy s'ils sont disponibles, et ne gardez actifs que les modules Cisco Secure Client.

Étape 2: Nettoyer la désinstallation avec l'outil Microsoft

Utilisez l'outil de dépannage d'installation et de désinstallation de programme Microsoft pour supprimer tous les modules Cisco du périphérique concerné. Cet outil permet une désinstallation plus complète que les méthodes de désinstallation Windows standard.

Corriger les problèmes qui empêchent l'installation ou la suppression de programmes.

Étape 3: Nettoyage manuel des fichiers

Après la désinstallation, vérifiez et supprimez manuellement tous les dossiers, fichiers, exécutables et fichiers DLL Cisco restants de ces répertoires :

```
C:\Program Files (x86)\Cisco
C:\ProgramData\Cisco\
C:\Users\<current user>\AppData\Local\Cisco
```

Supprimez tous les fichiers et dossiers résiduels trouvés dans ces emplacements, car ils ne restent pas toujours même après le processus de désinstallation.

Étape 4: Nettoyage du Registre

Vérifiez les chemins d'accès au Registre pour les entrées anciennes du client sécurisé Cisco et supprimez-les si elles sont présentes :

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco
HKEY_LOCAL_MACHINE\Software\WOW6432node\Cisco
```

Étape 5: Activer la consignation du débogage (facultatif)

Si un dépannage supplémentaire est nécessaire, activez la journalisation Curl en copiant le fichier debuglogconfig.json :

```
{
"web_helper" : 3,
"vpn_ipsec_ikev2" : 3,
"vpn_curl" : 3,
"vpn_state" : 3
}
```

dans ce répertoire :

```
C:\ProgramData\Cisco\Cisco Secure Client
```

Étape 6: Redémarrage du système

Redémarrez le point de terminaison pour vous assurer que toutes les modifications prennent effet et effacez les processus restants ou les verrous du Registre.

Étape 7: Réinstaller le client sécurisé Cisco

Installez le package de prédéploiement de Cisco Secure Client ou autorisez l'installation automatique via des outils de gestion tels qu'Intune. Vérifiez que l'installation a réussi avant de continuer.

Étape 8: Tester la connexion VPN

Tentative de connexion au profil VPN qui échouait précédemment. Si le problème persiste, générez un nouveau bundle DART pour une analyse plus approfondie.

⚠ Mise en garde : Possible. Les détails mentionnés ici semblent contenir des procédures ou des commandes qui pourraient avoir un impact significatif si elles étaient exécutées. Veuillez vous assurer que ces procédures ou commandes ont été évaluées par un expert ou une unité commerciale avant d'être exécutées ou recommandées.

Motif

Le problème est causé par des entrées de registre corrompues ou une interférence de logiciels tiers qui empêche les bibliothèques et les exécutions Hostscan de démarrer ou de mettre à jour correctement. Cette corruption affecte le processus de vérification de pré-connexion CSD (Cisco Security Desktop), qui est requis pour les profils VPN avec posturisation activée. La corruption se produit généralement au niveau du périphérique, expliquant pourquoi le même utilisateur peut se connecter correctement à partir d'autres périphériques. Les méthodes de désinstallation standard ne suppriment pas toujours tous les composants endommagés, ce qui nécessite un nettoyage manuel des fichiers et des entrées de registre.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

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.