

Position du périphérique d'accès sécurisé Intermittent " ; Obsolète" ; Erreur

Table des matières

Problème

La position du périphérique dans Cisco Secure Access affiche par intermittence l'état « obsolète » pour les périphériques inscrits, ce qui empêche la validation de la position Zero Trust Access.

Les utilisateurs rencontrent les messages d'erreur suivants pendant des périodes spécifiques :

- "La position de votre appareil est obsolète"
- "Impossible d'exécuter automatiquement un contrôle de sécurité pour votre périphérique"

Le problème se produit malgré le fait que Duo Desktop indique une conformité totale avec toutes les exigences de sécurité, y compris les mises à jour Windows, la configuration du mot de passe système, le chiffrement BitLocker et l'activation du pare-feu. Pendant les périodes problématiques, les tentatives de désinscription et de réinscription des périphériques concernés échouent avec des erreurs internes. La seule solution de contournement temporaire qui restaure le fonctionnement normal consiste à effectuer un redémarrage complet du système, ce qui perturbe l'accès utilisateur et la productivité.

D'autres symptômes incluent le maintien de la connectivité du VPN AnyConnect pendant toute la période du problème, tandis que les processus d'inscription et de validation de position Zero Trust Access échouent par intermittence pendant les périodes prévisibles.

Environnement

- Cisco Secure Access avec fonctionnalité Device Posture activée
- Client Duo Desktop pour la vérification de la conformité des périphériques

- Terminals Windows avec chiffrement BitLocker, mots de passe système et pare-feu Windows activés
- Déploiement Zero Trust Access nécessitant une validation de posture
- Les profils de position configurés dans Cisco Secure Access correspondent à l'état de conformité des périphériques

Résolution

Le problème a été résolu en mettant à niveau le client Cisco Secure Access vers la dernière version 5.1.15.287. Cette version corrige le défaut sous-jacent qui a provoqué des échecs intermittents de validation de la position du périphérique.

Processus de mise à niveau client

Étape 1: Identifiez la version actuelle du client sur les terminaux affectés.

Vérifiez la version existante du client Cisco Secure Access via l'interface d'application ou les enregistrements d'installation du système.

Étape 2: Téléchargez et déployez la version 5.1.15.287 du client.

Procurez-vous le logiciel client mis à jour auprès du canal de distribution Cisco approprié et déployez-le sur tous les terminaux concernés qui rencontrent des problèmes de validation de la position du périphérique.

Étape 3: Vérifiez la résolution.

Une fois la mise à niveau du client terminée, surveillez l'état du périphérique pendant les fenêtres de temps précédemment problématiques pour confirmer le fonctionnement stable sans nécessiter de redémarrage du système.



Remarque : Il est recommandé d'installer la dernière version du client Secure.

Étapes de validation

Après la mise à niveau du client, vérifiez que :

- La validation de la position du périphérique s'effectue correctement pendant les périodes précédemment problématiques.
- L'inscription Zero Trust Access fonctionne sans erreurs internes.
- Les opérations de désinscription et de réinscription se terminent correctement si nécessaire.
- Aucun redémarrage du système n'est nécessaire pour maintenir la conformité de la position du périphérique.
- L'état des postes de travail Duo Desktop et Cisco Secure Access reste synchronisé.

Motif

Les échecs intermittents de validation de position de périphérique ont été provoqués par le bogue Cisco ayant l'ID CSCws68569. Ce défaut a affecté la communication entre le client Cisco Secure Access et les services de validation de position, ce qui a entraîné des problèmes de synchronisation temporaires qui ont empêché la création de rapports d'état de conformité de périphérique précis pendant des fenêtres opérationnelles spécifiques.

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.