Défaillance de la connexion VPN du client sécurisé Cisco avec authentification SAML et erreurs de dictionnaire Bencode

Table des matières

Problème

Les connexions VPN utilisant Cisco Secure Client ne peuvent pas être établies lors de l'utilisation de l'authentification SAML avec Google IdP. Bien que l'authentification SAML réussisse du côté IdP, le client échoue pendant le traitement post-authentification et passe à un état déconnecté, empêchant la création du tunnel VPN.

Environnement

- Client sécurisé Cisco version 5.1.13.17
- Authentification SAML configurée avec Google IdP
- Accès sécurisé : accès à distance sécurisé pour le client (VPN, position, ressource privée)
- Les journaux d'authentification Google IdP affichent une authentification SAML réussie

Résolution

Le problème a été résolu en réinstallant le client sécurisé Cisco. L'approche de dépannage suivante a été documentée :

Étapes de diagnostic initiales

Étape 1: Collecter les journaux DART à partir du point d'extrémité affecté - https://www.cisco.com/c/en/us/support/docs/security/secure-client/221919-collect-dart-bundle-for-secure-client.html

Extract Dart Bundle > Cisco Secure client > Anyconnect VPN > Logs > Under VPN Folder > AnyConnectVPN.txt - affiche les erreurs suivantes lors de la lecture des paramètres internes, les erreurs suivantes apparaissant continuellement :

- Échec d'internalisation du dictionnaire Bencode
- Impossible de créer le dictionnaire Bencode
- PHONEHOMEVPN_ERROR_UNATTENTED
- GLOBAL_ERROR_UNEXPECTED

Étape 2: Vérifier l'état de l'authentification SAML côté IdP

Vérifiez que les journaux Google IdP affichent une authentification SAML réussie pour isoler le problème dans le traitement post-authentification côté client.

application des résolutions

Étape 1: Réinstaller le client sécurisé Cisco

Désinstallez l'installation existante de Cisco Secure Client et effectuez une nouvelle installation du logiciel client.

Étape 2: Vérifier la restauration de la connectivité VPN

Après la réinstallation, testez la connexion VPN avec l'authentification SAML pour confirmer que la connexion s'établit correctement et que le tunnel est créé correctement.

La réinstallation de Cisco Secure Client a restauré la fonctionnalité VPN, permettant une authentification SAML réussie et l'établissement d'un tunnel.

Motif

La cause principale semble être liée à des données de configuration internes corrompues dans l'installation du client sécurisé Cisco, affectant spécifiquement la capacité du composant CPhoneHomeVpn/PhoneHomeAgent à traiter les données du dictionnaire Bencode pendant le traitement post-authentification. Les erreurs répétées « Bencode dictionary internalize failed » et « Failed to create Bencode dictionary » indiquent que le client n'a pas pu analyser ou traiter correctement les données de configuration interne requises pour établir le tunnel VPN après une authentification SAML réussie.

Le problème a été résolu par la réinstallation du client, ce qui suggère que le problème était lié à des données côté client corrompues plutôt qu'à des problèmes de configuration côté serveur ou d'intégration IdP.

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.