

ChromeOS SWG Web Protection ne fonctionne pas et, par conséquent, aucun journal Web apparaît dans la recherche d'activité

Table des matières

Problème

Les journaux Web n'ont pas été générés pour les utilisateurs de ChromeOS malgré la protection Secure Web Gateway (SWG) qui semble être activée pour l'organisation. Les terminaux ChromeOS affectés affichaient uniquement une protection de niveau DNS sans aucune activité de journalisation SWG/Web visible dans l'interface de recherche d'activité. Les utilisateurs ne disposaient d'aucun journal de trafic Web alors que l'état de protection SWG indiquait qu'il était activé.

Au cours de l'enquête, les journaux de diagnostic ont révélé des échecs de synchronisation répétés au point d'extrémité <http://407.checkumbrella.com> avec des réponses d'erreur HTTP 407 (authentification proxy requise). Le client/poste ChromeOS n'a pas pu s'authentifier correctement auprès du service proxy, ce qui a empêché l'activation correcte de la protection SWG et la génération ultérieure du journal Web.

Environnement

- Accès sécurisé Cisco
- Terminaux ChromeOS avec client/extension Cisco Secure Access
- Console d'administration Google pour la gestion ChromeOS

Résolution

Le problème a été résolu en activant le schéma d'authentification d'authentification de base pour l'unité d'organisation d'administration de Google (OU) contenant les utilisateurs de ChromeOS affectés et en effectuant un rechargement de stratégie pour activer la protection SWG.

Étape 1: Collecte et analyse des journaux

Capture HAR collectée (examen des journaux du réseau et de la console) pour identifier la cause première de l'échec de synchronisation. Les journaux indiquaient des échecs d'authentification répétés lors de la tentative de synchronisation avec le service Cisco Secure Access.

Étape 2: Activer l'authentification de base pour Google Admin OU

Dans la console Google Admin, naviguez jusqu'à l'unité d'organisation contenant les utilisateurs ChromeOS affectés et activez le schéma d'authentification Basic Auth. Cela permet au client/poste ChromeOS de s'authentifier correctement auprès du service proxy d'accès sécurisé Cisco.

Étape 3: Rechargement et vérification des stratégies

Après avoir activé l'authentification de base, effectuez un rechargement de stratégie sur les périphériques ChromeOS affectés. Vérifiez que la protection SWG devient active en vérifiant l'état de protection. La protection SWG doit désormais apparaître comme active et non plus uniquement au niveau DNS.

Étape 4: Validation

Testez l'activité de navigation Web des utilisateurs ChromeOS affectés et vérifiez que les journaux Web sont maintenant générés et visibles dans l'interface de recherche d'activité. Les journaux doivent présenter une inspection du trafic Web et une journalisation correctes via le service SWG.

Motif

Le client/poste ChromeOS avait le schéma d'authentification d'authentification de base désactivé pour l'unité d'organisation d'administration de Google contenant les utilisateurs affectés. Si l'authentification de base n'est pas activée, les périphériques ChromeOS ne peuvent pas s'authentifier correctement auprès du service proxy d'accès sécurisé Cisco, ce qui entraîne des erreurs HTTP 407 (authentification proxy requise) lors des tentatives de synchronisation. Cela empêchait la protection SWG de s'activer correctement, ce qui entraînait le retour des périphériques à la protection DNS uniquement et empêchait la génération de journaux Web.

Autres informations utiles

- [Dépannage et collecte des informations de base pour Cisco Secure Access](#)
- [Client Cisco Secure Access Chromebook](#)
- [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.