

ChromeOS SWG Web Protection non funziona e di conseguenza nessun registro Web Mostra in Activity Search

Sommario

Problema

I log Web non sono stati generati per gli utenti ChromeOS nonostante la protezione di Secure Web Gateway (SWG) fosse abilitata per l'organizzazione. Gli endpoint ChromeOS interessati mostravano solo la protezione a livello DNS senza alcuna attività di registrazione SWG/Web visibile nell'interfaccia Activity Search. Gli utenti riscontravano un'assenza totale di registri del traffico Web mentre lo stato di protezione SWG indicava che era abilitato.

Durante l'analisi, i log di diagnostica hanno rilevato ripetuti errori di sincronizzazione nell'endpoint <http://407.checkumbrella.com> con risposte di errore HTTP 407 (autenticazione proxy richiesta). Il client/estensione ChromeOS non è stato in grado di autenticarsi correttamente con il servizio proxy, impedendo la corretta attivazione della protezione SWG e la successiva generazione del registro Web.

Ambiente

- Cisco Secure Access
- Endpoint ChromeOS con estensione/client Cisco Secure Access
- Console di amministrazione Google per la gestione di ChromeOS

Risoluzione

Il problema è stato risolto abilitando lo schema di autenticazione di base per l'unità organizzativa

Google Admin (OU) che contiene gli utenti ChromeOS interessati ed eseguendo un ricaricamento della policy per attivare la protezione SWG.

Passaggio 1: Raccolta e analisi log

Acquisizione HAR raccolta (esaminare i registri di rete e della console) per identificare la causa principale dell'errore di sincronizzazione. Nei registri sono stati rilevati errori di autenticazione ripetuti durante il tentativo di sincronizzazione con il servizio Cisco Secure Access.

Passaggio 2: Abilita autenticazione di base per unità organizzativa amministrazione Google

Nella console di Google Admin, passare all'unità organizzativa contenente gli utenti ChromeOS interessati e abilitare lo schema di autenticazione Basic Auth. Ciò consente al client/estensione ChromeOS di autenticarsi correttamente con il servizio proxy Cisco Secure Access.

Passaggio 3: Ricaricamento e verifica delle policy

Dopo aver abilitato l'autenticazione di base, eseguire un ricaricamento delle policy sui dispositivi ChromeOS interessati. Verificate che la protezione SWG diventi attiva controllando lo stato della protezione. La protezione SWG deve ora essere visualizzata come attiva anziché come unica protezione a livello DNS.

Passaggio 4: Convalida

Testare l'attività di navigazione Web dagli utenti ChromeOS interessati e confermare che i log Web sono ora generati e visibili nell'interfaccia di ricerca attività. I registri devono indicare un'ispezione adeguata del traffico Web e la registrazione attraverso il servizio SWG.

Causa

Lo schema di autenticazione Basic Auth del client/estensione ChromeOS era disabilitato per l'unità organizzativa Google Admin contenente gli utenti interessati. Senza l'autenticazione di base abilitata, i dispositivi ChromeOS non possono autenticarsi correttamente con il servizio proxy Cisco Secure Access, causando errori HTTP 407 (autenticazione proxy richiesta) durante i tentativi di sincronizzazione. Ciò ha impedito alla protezione SWG di attivarsi correttamente, causando il fallback dei dispositivi alla protezione solo DNS e impedendo la generazione di log Web.

Contenuto correlato

- [Risoluzione dei problemi e raccolta di informazioni di base per Cisco Secure Access](#)
- [Cisco Secure Access Chromebook Client](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).