Journaux des événements du fichier d'accès sécurisé manquants dans SIEM après modification de la licence

Table des matières

Problème

Les journaux d'événements de fichiers ont cessé d'être reçus par le SIEM à partir du stockage AWS S3 tandis que les journaux DNS continuaient d'être remis avec succès. Les connecteurs de données d'événement de fichier affichaient une icône « déconnecté » dans l'interface SIEM. Les journaux qui ont cessé d'apparaître ont été identifiés comme des enregistrements d'événements de fichiers liés à DLP/IPS. Les journaux de la couche DNS sont restés opérationnels pendant toute la période du problème.

L'environnement utilisait à la fois Umbrella et Secure Access pendant la migration, avec des journaux envoyés au même compartiment AWS. Les clés avaient été permutées et leur bon fonctionnement a été confirmé. La version du schéma était à la version 10 alors que la version 16 était disponible.

Environnement

- Organisation Cisco Secure Access avec configurations Umbrella et Secure Access
- Intégration du stockage AWS S3 pour l'exportation des journaux
- Plate-forme Microsoft Sentinel SIEM
- Schéma version 10 utilisé (version 16 disponible)
- La licence Secure Access est passée d'Advantage à Essentials le 23 juin 2026
- Dernière observation des journaux d'événements de fichiers le 24 juin 2026

Résolution

L'enquête a révélé que les journaux d'événements de fichiers étaient liés à la fonctionnalité DLP/IPS, qui nécessite des fonctionnalités de licence spécifiques. La cause première a été identifiée lors de l'analyse suivante.

Étape 1: Analyse du trafic

Vérifiez la Recherche d'activité dans Accès sécurisé pour confirmer les modèles de trafic :

1.- Accédez à Recherche d'activité et filtrez le trafic Web ou les événements de disposition malveillante. L'analyse a montré que le trafic DNS était présent mais qu'aucun événement de trafic Web n'était visible au cours des 30 derniers jours et qu'aucune règle avec l'inspection des fichiers activée n'a été identifiée.
2.- Traffic Flow > Logs on the CSA report > S3 bucket - SIEM.

Étape 2: Historique des licences

1.- Consultez l'historique des licences dans Secure Access pour identifier les modifications qui correspondent au moment de l'arrêt du journal des événements de fichiers.

2.- Accédez à Secure Access > Admin > Subscription pour afficher le niveau de licence actuel et le résumé des fonctionnalités.

L'enquête a montré que la licence Secure Access est passée de Secure Access Advantage à Secure Access Essentials le 23 juin 2026, ce qui correspond au moment où les journaux d'événements de fichiers ont cessé d'apparaître.

Étape 3: Vérification des fonctionnalités

Vérifiez quelles fonctionnalités sont incluses dans le niveau de licence actuel. La fonctionnalité DLP et IPS, qui génère des journaux d'événements de fichiers, n'est pas incluse dans le niveau de

licence Secure Access Essentials.

Étape 4: Confirmation et cause première

La date du changement de licence correspond parfaitement à l'arrêt de l'affichage des journaux d'événements de fichiers. Étant donné que la journalisation de la couche DNS est restée fonctionnelle et constituait la principale exigence, le cas a été résolu en tenant compte du fait que les journaux d'événements de fichiers ne seraient pas disponibles sous la licence Essentials actuelle.

Motif

Les journaux d'événements de fichiers ont cessé d'être générés suite à un changement de licence de Secure Access Advantage à Secure Access Essentials le 23 juin 2026. Les journaux d'événements de fichiers sont associés aux fonctionnalités DLP et IPS, qui ne sont pas incluses dans le niveau de licence Essentials. La rétrogradation de licence a supprimé l'accès aux fonctionnalités d'inspection de fichiers qui génèrent ces types de journaux 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.