Registros de eventos de archivos de Secure Access que faltan en SIEM después del cambio de licencia

Contenido

Problema

Los registros de eventos de archivo dejaron de ser recibidos por SIEM desde el almacenamiento AWS S3 mientras que los registros DNS continuaron siendo entregados correctamente. Los conectores de datos de Evento de archivo mostraban un icono de "desconexión" en la interfaz SIEM. Los registros que dejaron de aparecer se identificaron como registros de eventos de archivo relacionados con DLP/IPS. Los registros de la capa DNS siguieron funcionando durante todo el período del problema.

El entorno utilizaba Umbrella y Secure Access durante la migración, con registros enviados a la misma cubeta de AWS. Las llaves se habían girado y se confirmó que funcionaban correctamente. Se observó que la versión del esquema estaba en la versión 10, mientras que la versión 16 estaba disponible.

Entorno

- Organización Cisco Secure Access con configuraciones Umbrella y Secure Access
- Integración de almacenamiento AWS S3 para la exportación de registros
- plataforma Microsoft Sentinel SIEM
- Versión de esquema 10 en uso (versión 16 disponible)
- La licencia de Secure Access cambió de Advantage a Essentials el 23 de junio de 2026
- Registros de eventos de archivos observados por última vez el 24 de junio de 2026

Resolución

La investigación reveló que los registros de eventos de archivos estaban relacionados con la funcionalidad de DLP/IPS, que requiere funciones de licencias específicas. La causa principal se identificó en el siguiente análisis.

Paso 1: Análisis del tráfico

Verifique la Búsqueda de actividad en Acceso seguro para confirmar los patrones de tráfico:

1.- Navegue hasta Búsqueda de actividad y filtre el tráfico web o los eventos de disposición maliciosos. El análisis mostró que el tráfico DNS estaba presente, pero que no había eventos de tráfico web visibles durante los últimos 30 días y no se identificaron reglas con la inspección de archivos habilitada.
2.- Flujo de tráfico > Registros en el informe CSA > S3 bucket - SIEM.

Paso 2: Revisión del historial de licencias

1.- Revise el historial de licencias en Secure Access para identificar cualquier cambio que se alinee con el tiempo de la detención del registro de eventos de archivo.

2.- Navegue hasta Secure Access > Admin > Subscription para ver el nivel de licencia actual y el resumen de funciones.

La investigación mostró que la licencia de Secure Access cambió de Secure Access Advantage a Secure Access Essentials el 23 de junio de 2026, lo que coincidió con el momento en que dejaron de aparecer los registros de eventos de archivos.

Paso 3: Verificación de funciones

Verifique qué funciones se incluyen en el nivel de licencia actual. La funcionalidad DLP e IPS, que genera registros de eventos de archivos, no se incluye en el nivel de licencia de Secure Access

Essentials.

Paso 4: Confirmación y causa raíz

El tiempo del cambio de licencia coincidió perfectamente cuando los registros de eventos de archivo dejaron de aparecer. Dado que el registro de la capa DNS seguía funcionando y era el requisito principal, el caso se resolvió con el entendimiento de que los registros de eventos de archivo no estarían disponibles bajo la licencia Essentials actual.

Causa

Los registros de eventos de archivos dejaron de generarse debido a un cambio de licencia de Secure Access Advantage a Secure Access Essentials el 23 de junio de 2026. Los registros de eventos de archivos están asociados a la funcionalidad DLP e IPS, que no se incluyen en el nivel de licencia Essentials. La reversión de licencia eliminó el acceso a las capacidades de inspección de archivos que generan estos tipos de registro específicos.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).