Logs de eventos do arquivo de acesso seguro ausentes do SIEM após a alteração da licença

Contents

Problema

Os logs de eventos de arquivo pararam de ser recebidos pelo SIEM do armazenamento AWS S3, enquanto os logs DNS continuaram a ser entregues com êxito. Os conectores de dados do evento de arquivo exibiram um ícone "desconectado" na interface SIEM. Os logs que pararam de aparecer foram identificados como registros de Evento de Arquivo relacionados a DLP/IPS. Os registros da camada DNS permaneceram funcionais durante todo o período do problema.

O ambiente estava usando o Umbrella e o Secure Access durante a migração, com logs enviados ao mesmo bucket do AWS. As chaves foram giradas e confirmadas como funcionando corretamente. Observou-se que a versão do esquema era a versão 10, enquanto a versão 16 estava disponível.

Ambiente

- Organização Cisco Secure Access com configurações Umbrella e Secure Access
- Integração de armazenamento AWS S3 para exportação de log
- Plataforma Microsoft Sentinel SIEM
- Esquema versão 10 em uso (versão 16 disponível)
- A licença do Secure Access mudou de Advantage para Essentials em 23 de junho de 2026
- Registros de eventos de arquivos observados pela última vez em 24 de junho de 2026

Resolução

A investigação revelou que os registros de eventos do arquivo estavam relacionados à funcionalidade DLP/IPS, que requer recursos de licenciamento específicos. A causa raiz foi identificada na próxima análise.

Passo 1: Análise de tráfego

Verifique a pesquisa de atividades no acesso seguro para confirmar os padrões de tráfego:

1.- Navegue até Pesquisa de atividades e filtre o tráfego da Web ou eventos de disposição mal-intencionados. A análise mostrou que o tráfego DNS estava presente, mas nenhum evento de tráfego da Web estava visível nos últimos 30 dias e nenhuma regra com Inspeção de arquivo habilitada foi identificada.
2.- Fluxo de tráfego > Logs no relatório CSA > S3 bucket - SIEM.

Passo 2: Revisão do histórico de licenças

1.- Revise o histórico de licenças no Secure Access para identificar quaisquer alterações que se alinham com o tempo de interrupção do registro de eventos do arquivo.

2.- Navegue até Secure Access > Admin > Subscription para exibir o nível de licença atual e o resumo dos recursos.

A investigação mostrou que a licença do Secure Access mudou de Secure Access Advantage para Secure Access Essentials em 23 de junho de 2026, o que se alinhava com o momento em que os registros de eventos do arquivo paravam de aparecer.

Passo 3: Verificação de recursos

Verifique quais recursos estão incluídos no nível de licença atual. A funcionalidade DLP e IPS, que gera logs de eventos de arquivo, não está incluída na camada de licença Secure Access Essentials.

Passo 4: Confirmação e causa raiz

O tempo da alteração de licença correspondeu perfeitamente quando os logs de eventos de arquivo pararam de aparecer. Como o registro da camada DNS permaneceu funcional e era o requisito principal, o caso foi resolvido com a compreensão de que os registros de eventos de arquivo não estariam disponíveis sob a licença Essentials atual.

Causa

Os registros de eventos de arquivos pararam de ser gerados devido a uma alteração de licença do Secure Access Advantage para o Secure Access Essentials em 23 de junho de 2026. Os logs de eventos de arquivo são associados à funcionalidade DLP e IPS, que não estão incluídos na camada de licença do Essentials. O downgrade de licença removeu o acesso aos recursos de inspeção de arquivos que geram esses tipos de log específicos.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.