Logbestanden voor beveiligde toegang ontbreken in SIEM na wijziging van licentie

Inhoud

uitgifte

Logboeken voor bestandsevenementen worden niet meer door de SIEM ontvangen van AWS S3-opslag terwijl DNS-logboeken met succes werden geleverd. De bestandsgebeurtenisgegevensaansluitingen toonden een pictogram "losgekoppeld" in de SIEM-interface. De logs die niet meer werden weergegeven, werden geïdentificeerd als DLP/IPS-gerelateerde bestandsgebeurtenisrecords. DNS-layer logs bleven functioneel gedurende de hele uitgifteperiode.

De omgeving gebruikte tijdens de migratie zowel Umbrella als Secure Access, waarbij logs naar dezelfde AWS-emmer werden verzonden. De toetsen waren gedraaid en er werd bevestigd dat ze goed werkten. De schema-versie werd genoteerd op versie 10, terwijl versie 16 beschikbaar was.

milieu

- Cisco Secure Access-organisatie met zowel Umbrella- als Secure Access-configuraties
- AWS S3-opslagintegratie voor het exporteren van logbestanden
- Microsoft Sentinel SIEM-platform
- Schema versie 10 in gebruik (versie 16 beschikbaar)
- Secure Access-licentie gewijzigd van Advantage naar Essentials op 23 juni 2026
- File Event logs voor het laatst waargenomen op 24 juni 2026

resolutie

Uit het onderzoek bleek dat de logbestanden van de bestandsevenementen verband hielden met de DLP/IPS-functionaliteit, waarvoor specifieke licentiefuncties vereist zijn. De oorzaak is vastgesteld in de volgende analyse.

Stap 1: Verkeersanalyse

Controleer de zoekfunctie voor activiteiten in Veilige toegang om verkeerspatronen te bevestigen:

1.- Navigeer naar Activiteit zoeken en filter voor webverkeer of kwaadaardige dispositie gebeurtenissen. Uit de analyse bleek dat er DNS-verkeer aanwezig was, maar dat er de afgelopen 30 dagen geen webverkeersgebeurtenissen zichtbaar waren en dat er geen regels met bestandsinspectie zijn geïdentificeerd.
2.- Verkeersstroom > Logs op het CSA-rapport > S3-emmer - SIEM.

Stap 2: Overzicht licentiegeschiedenis

1.- Controleer de licentiegeschiedenis in Secure Access om eventuele wijzigingen te identificeren die overeenkomen met de timing van de bestandslogboekonderbreking.

2.- Navigeer naar Veilige toegang > Beheer > Abonnement om het huidige licentieniveau en het overzicht van functies te bekijken.

Uit het onderzoek bleek dat de Secure Access-licentie op 23 juni 2026 is veranderd van Secure Access Advantage naar Secure Access Essentials, wat overeenkomt met de timing wanneer File Event-logboeken niet meer worden weergegeven.

Stap 3: Verificatie van kenmerken

Controleer welke functies zijn opgenomen in het huidige licentieniveau. DLP- en IPS-functionaliteit, die logboeken voor bestandsevenementen genereert, is niet opgenomen in de licentielaag Secure Access Essentials.

Stap 4: Bevestiging en oorzaak

De timing van de licentiewijziging kwam perfect overeen wanneer bestandsgebeurtenislogboeken niet meer werden weergegeven. Aangezien logboekregistratie op de DNS-laag functioneel bleef en de primaire vereiste was, werd de kwestie opgelost met dien verstande dat logboeken voor bestandsevenementen niet beschikbaar zouden zijn onder de huidige Essentials-licentie.

Oorzaak

De logbestanden voor bestandsevenementen zijn op 23 juni 2026 niet meer gegenereerd vanwege een wijziging van de licentie van Secure Access Advantage naar Secure Access Essentials. Logboeken voor bestandsevenementen zijn gekoppeld aan DLP- en IPS-functionaliteit, die niet zijn opgenomen in de licentielaag Essentials. De licentieverlaging heeft de toegang tot de mogelijkheden voor bestandsinspectie die deze specifieke logtypen genereren, verwijderd.

Gerelateerde inhoud

- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.