# 许可证更改后SIEM中缺少安全访问文件事件日志

## 目录

## 问题

当DNS日志继续成功传送时，SIEM停止从AWS S3存储接收文件事件日志。文件事件数据连接器在SIEM界面中显示“断开连接”图标。停止显示的日志被标识为DLP/IPS相关的文件事件记录。DNS层日志在整个发布期间保持正常运行。

迁移期间，环境同时使用了Umbrella和安全访问，日志发送到同一个AWS存储桶。钥匙已轮换、确认工作正常。模式版本被注意到为版本10，而版本16可用。

## 环境

- 具有Umbrella和安全访问配置的思科安全访问组织
- 用于日志导出的AWS S3存储集成
- Microsoft Sentinel SIEM平台
- 正在使用的架构版本10（提供版本16）
- 2026年6月23日，安全访问许可证从Advantage更改为Essentials
- 上次观察到的文件事件日志为2026年6月24日

## 分辨率

调查发现，文件事件日志与DLP/IPS功能相关，而后者需要特定的许可功能。通过下一步分析确定了根本原因。

### 步骤 1：流量分析

检查安全访问中的活动搜索以确认流量模式：

1. — 导航到活动搜索并过滤网络流量或恶意处置事件。分析显示DNS流量存在，但过去30天内未显示任何Web流量事件，并且未识别启用了文件检查的规则。
2.- Traffic Flow > Logs on the CSA report > S3 bucket - SIEM。

### 步骤 2：许可证历史记录审核

1. — 在Secure Access中查看许可证历史记录，以确定与文件事件日志停止时间一致的任何更改。

2. — 导航到安全访问>管理>订用，查看当前许可证级别和功能摘要。

调查显示，安全访问许可证在2026年6月23日从Secure Access Advantage变为Secure Access Essentials，与文件事件日志停止出现的时间一致。

### 步骤 3：功能验证

验证当前许可证级别中包括的功能。生成文件事件日志的DLP和IPS功能不包括在安全访问基础许可证层中。

### 步骤 4：确认和根本原因

当文件事件日志停止显示时，许可证更改的时间完全匹配。由于DNS层日志记录仍可正常运行并且是主要要求，因此解决该问题的前提是，在当前的Essentials许可证下，文件事件日志将不可用。

## 原因

由于许可证从Secure Access Advantage更改为Secure Access Essentials，文件事件日志已于2026年6月23日停止生成。文件事件日志与DLP和IPS功能相关联，而Essentials许可证层不包含这些功能。许可证降级删除了对生成这些特定日志类型的文件检查功能的访问。

## 相关内容

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。