

對Secure Access XDR整合中的模組故障錯誤代碼的運行狀況檢查進行故障排除

目錄

問題

Cisco安全訪問與XDR整合失敗，在運行狀況檢查階段出現HTTP 431「Request Header Fields Too Large」錯誤。整合以前已成功運行，但在嘗試使用從Cisco Secure Access控制面板生成的API金鑰建立連線時，突然開始失敗，並出現此錯誤。

特定錯誤消息顯示為：

```
<#root>
```

```
Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access
```

此錯誤可防止安全訪問資料進入XDR，從而影響安全可視性和監控功能。

環境

- Cisco Secure Access with Advantage許可證
- Cisco XDR訂閱
- 思科安全存取租戶
- 使用Cisco Secure Access控制面板生成的金鑰進行API整合
- 所需的API範圍：「調查」>「只讀」、「報告」>「只讀」、「部署」>「只讀」、「策略」>「讀取/寫入」

解析

通過重新生成Cisco安全訪問中的API金鑰和金鑰解決了此問題。

按照以下步驟解決431錯誤：

步驟 1:生成新的API金鑰

導航到Cisco Secure Access控制面板並使用所需的範圍建立新的API金鑰：

- 調查：唯讀
- 報告：唯讀
- 部署：唯讀
- 策略：讀取/寫入

步驟 2:將新金鑰應用於XDR整合

用新生成的金鑰替換XDR安全訪問整合配置中的現有API金鑰。

步驟 3:驗證整合

測試整合以確認連線成功。API呼叫現在必須返回HTTP 200響應，而不是431錯誤。

主動檢測和預防

要識別並防止將來出現類似的431個錯誤，請執行以下操作：

1. — 通過Postman或瀏覽器控制檯等工具進行調試時，請檢查請求報頭的size列。如果請求報頭接近或超過8 KB（8192位元組），則會在API網關上觸發431錯誤。外部工具（如jwt.io）可用於驗證OAuth令牌大小。

2. — 分析錯誤模式：

- 如果在運行狀況檢查的初始握手期間立即發生431錯誤，則表明靜態憑證有問題
- 如果僅在整合運行幾分鐘後發生431錯誤，則表明在隨後的重試中存在cookie累積

最佳實踐

在整合客戶端/瀏覽器中禁用cookie或會話永續性，以防止報頭大小累積。

原因

HTTP 431錯誤是由特定API金鑰和金鑰對引起的，在為標準HTTP授權標頭編碼Base64時，該金鑰和金鑰對生成異常大的或格式錯誤的授權標頭。

初始API金鑰中的加密字串包含一系列字元，這些字元在編碼時擴展為超過API網關限制的標頭大小，導致「請求標頭欄位過大」被拒絕。

重新生成API金鑰時，新的加密字串會生成大小適當的授權標頭。撤消和生成新金鑰的過程還清除了整合管理器端快取的請求上下文，從而規範了報頭大小。

相關內容

- [Cisco安全存取API驗證](#)
- [Cisco安全訪問整合到XDR](#)
- [從XDR控制檯收集HAR日誌](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。