解決安全訪問API遠端訪問事件403訪問禁止錯誤

目錄

問題

嘗試使用思科安全訪問API終端/reports/v2/remote-access-events檢索VPN遠端訪問日誌時，使用者始終會收到「403 Access Forbidden」響應，儘管已經啟用所有必需的範圍，包括reports.granularevents:read。使用以下引數進行API呼叫時出現問題：

```
Authorization: Bearer <token>
Accept: application/json
Endpoint: https://api.sse.cisco.com/reports/v2/remote-access-events
Params: {"limit": 500, "from": "-6000minutes", "to": "now"}
HTTP status: 403
Events retrieved: 0
Access Forbidden
```

儘管API金鑰配置了多個報告作用域，並且其他API終結點工作正常，但仍會發生錯誤。使用者報告他們可以成功訪問其他報告終結點，但會特別遇到遠端訪問事件終結點的授權問題。

環境

- 思科安全存取API
- API終結點：/reports/v2/remote-access-events
- 具有已配置作用域的API金鑰：admin.vpn:read， admin.users:read， admin.alertrules:read， admin.alerts:read， admin.sentinel:read， reports.aggregations:read， reports.granularevents:read， reports.malware:read， reports.incidents:read， reports.dlp.events:read
- 對Secure Access門戶具有完全管理員許可權的使用者
- API與監控系統的整合

解析

通過使用適用於遠端訪問事件終結點的正確API作用域解決了此問題。對於此特定端點，所記錄的範圍和實際實施要求會有所不同。

根本原因分析

調查發現，所記錄的API範圍與實際實施之間存在差異：

- 文檔說明:所需的作用域是reports.aggregations:read。
- 實際實施:外部API網關ACL將reports/v2/remote-access-events對映到reports.utilities:read。

範圍測試結果

測試確認此範圍行為：

```
Token Scope: reports.aggregations:read
GET /reports/v2/remote-access-events
Response: 403

Token Scope: reports.utilities:read
GET /reports/v2/remote-access-events
Response: 200

Token Scope: reports.* (All Reports)
GET /reports/v2/remote-access-events
Response: 200
```

解決方案實施

要解決403 Access Forbidden錯誤，請使用正確的範圍配置API金鑰：

步驟 1:存取API金鑰管理。

在Secure Access控制面板中導航到Admin > API Keys。

步驟 2:建立新API金鑰。

按一下Add API Key(+)並配置：

- API金鑰名稱
- 說明（可選）
- 到期日期（如果需要）

步驟 3:配置正確範圍。

在「範圍」部分中，啟用reports.utilities:read以獲取遠端訪問事件功能。

步驟 4:生成承載令牌。

使用具有更新的API金鑰的OAuth2客戶端憑證流建立新的承載令牌。

步驟 5:測試API呼叫。

使用工作curl命令格式重試API呼叫：

```
curl -L --request GET \
--url 'https://api.sse.cisco.com/reports/v2/remote-access-events?limit=10&from=-60minutes&to=now' \
--header 'Authorization: Bearer <Bearer token>' \
--header 'Accept: application/json'
```

步驟 6:驗證解析度。

確認API呼叫返回HTTP 200狀態並檢索預期的遠端訪問事件資料。

原因

根本原因是所記錄的API範圍要求與外部API網關ACL中的實際實現不匹配。Cisco GET /reports/v2/remote-access-events的公共文檔錯誤地宣告，當實際實施需要reports.utilities:read時，所需的訪問作用域為reports.aggregations:read。這種差異會導致身份驗證失敗，即使使用者認為他們根據官方文檔配置了正確的許可權。

相關內容

- Cisco安全訪問API — 獲取遠端訪問事件
- 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）。