セキュアアクセスAPIリモートアクセスイベントの解決403アクセス禁止エラー

内容

問題

Cisco Secure Access API(SAPI)エンドポイント/reports/v2/remote-access-eventsを使用してVPNリモートアクセスログを取得しようとすると、reports.granularevents:readを含むすべての必要なスコープを有効にしているにもかかわらず、ユーザには常に「403 Access Forbidden」という応答が返されます。この問題は、次のパラメータを使用してAPIコールを行う場合に発生します。

```
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
```

このエラーは、APIキーに複数のレポートスコープが設定されていて、他のAPIエンドポイントが正常に機能しているにもかかわらず発生します。ユーザは、他のレポートエンドポイントには正常にアクセスできるものの、リモートアクセスイベントエンドポイントでは特に認証の問題が発生していると報告しています。

環境

- シスコセキュアアクセスAPI
- APIエンドポイント：/reports/v2/remote-access-events
- スコープが構成されたAPIキー： 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

- セキュアアクセスポータルの完全な管理者権限を持つユーザ
- モニタリングシステムとのAPI統合

解決方法

リモートアクセスイベントのエンドポイントに正しいAPIスコープを使用することで、問題が解決されました。この特定のエンドポイントでは、文書化された範囲と実際の実装要件が異なります。

根本原因の分析

調査の結果、文書化されているAPIの範囲と実際の実装との間に不一致があることが判明しました。

- ドキュメントの状態：必要なスコープはreports.aggregations:readです。
- 実際の実装：外部APIゲートウェイACLは、reports/v2/remote-access-eventsをreports.utilities:readにマッピングします。

範囲テストの結果

テストにより、このスコープの動作が確認されました：

```
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
```

ソリューションの実装

403 Access Forbiddenエラーを解決するには、正しいスコープでAPIキーを設定します。

手順1:APIキー管理にアクセスします。

セキュアアクセスダッシュボードで、Admin > API Keysの順に移動します。

手順2:新しいAPIキーを作成します。

Add API Key (+)をクリックして、次のように設定します。

- APIキー名
- 説明（オプション）
- 必要に応じて有効期限

手順3:正しいスコープを設定します。

範囲セクションで、reports.utilities:readを有効にして、リモートアクセスイベント機能を使用できるようにします。

手順4:ベアラトークンを生成します。

更新されたAPIキーを使用して、OAuth2 client-credentialsフローを使用して新しいベアラトークンを作成します。

手順5:APIコールをテストします。

curl コマンドの作業形式を使用してAPI呼び出しを再試行します。

```
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'
```

手順6:解決を確認します。

API呼び出しがHTTP 200ステータスを返し、予期されるリモートアクセスイベントデータを取得することを確認します。

原因

根本的な原因は、文書化されているAPIスコープの要件と、外部APIゲートウェイACLでの実際の実装との不一致です。GET /reports/v2/remote-access-eventsに関するシスコの公開ドキュメントには、実際の実装にreports.utilities:readが必要な場合に、必要なアクセススコープがreports.aggregations:readであると誤って記載されています。この不一致により、公式のドキュメントに基づいて正しい権限を設定したとユーザが判断した場合でも、認証が失敗します。

関連コンテンツ

- Cisco Secure Access API：リモートアクセスイベントの取得
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。