Resolve Secure Access API Remote Access Events 403 Access Forbidden Error(보안 액세스 API 원격 액세스 이벤트 403 액세스 금지 오류 해결)

목차

문제

Cisco Secure Access API 엔드포인트/reports/v2/remote-access-events를 사용하여 VPN 원격 액세스 로그를 검색하려고 시도할 때, 사용자는 reports.granularevents:read를 비롯한 모든 필수 범위를 활성화했는데도 불구하고 "403 Access Forbidden" 응답을 지속적으로 받습니다. 이 문제는 다음 매개 변수를 사용하여 API를 호출할 때 발생합니다.

```
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
```

API 키에 여러 보고서 범위가 구성되어 있고 다른 API 엔드포인트가 올바르게 작동하고 있음에도 불구하고 오류가 발생합니다. 사용자는 다른 보고서 엔드포인트에 성공적으로 액세스할 수 있지만 특히 원격 액세스 이벤트 엔드포인트에 권한 부여 문제가 발생한다고 보고합니다.

환경

- Cisco Secure Access API
- API 엔드포인트: /reports/v2/remote-access-events
- 구성된 범위가 있는 API 키: 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.reports.dlp.events:read
- Secure Access 포털에서 전체 관리자 권한이 있는 사용자
- 모니터링 시스템과 API 통합

해결

원격 액세스 이벤트 끝점에 올바른 API 범위를 사용하여 문제가 해결되었습니다. 문서화된 범위와 실제 구현 요구 사항은 이 특정 엔드포인트에 대해 다릅니다.

근본 원인 분석

조사 결과, 문서화된 API 범위와 실제 구현 간의 불일치가 발견되었습니다.

- 문서 상태: 필수 범위는 reports.aggregations:read입니다.
- 실제 구현: 외부 API 게이트웨이 ACL은 reports/v2/remote-access-events를 reports.utilities:read에 매핑합니다.

범위 테스트 결과

테스트를 통해 이 범위 동작이 확인되었습니다.

```
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
```

솔루션 구현

403 Access Forbidden(403 액세스 금지) 오류를 해결하려면 올바른 범위로 API 키를 구성합니다.

1단계: 액세스 API 키 관리.

Secure Access 대시보드에서 Admin > API Keys로 이동합니다.

2단계: 새 API 키를 만듭니다.

Add API Key (+)(API 키 추가(+))를 클릭하고 다음을 구성합니다.

- API 키 이름
- 설명(선택 사항)
- 만료일(원하는 경우)

3단계: 올바른 범위를 구성합니다.

Scopes 섹션에서 reports.utilities:read for remote access events 기능을 활성화합니다.

4단계: 전달자 토큰 생성.

업데이트된 API 키를 사용하여 OAuth2 클라이언트 자격 증명 흐름을 사용하여 새 베어러 토큰을 만듭니다.

5단계: 테스트 API 호출.

작업 curl 명령 형식을 사용하여 API 호출을 재시도합니다.

```
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'
```

6단계: 해결을 확인합니다.

API 호출이 HTTP 200 상태를 반환하고 예상되는 원격 액세스 이벤트 데이터를 검색하는지 확인합니다.

원인

근본 원인은 문서화된 API 범위 요건과 외부 API 게이트웨이 ACL의 실제 구현이 일치하지 않기 때문입니다. GET /reports/v2/remote-access-events에 대한 Cisco 공용 설명서에 필요한 액세스 범위가 reports.aggregations:read인 것으로 잘못 설명되어 있습니다. 실제 구현시 reports.utilities:read가 필요한 경우. 이러한 불일치는 사용자가 공식 문서를 기반으로 올바른 권한을 구성했다고 생각하는 경우에도 인증 실패를 유발합니다.

관련 콘텐츠

- Cisco Secure Access API - 원격 액세스 이벤트 가져오기
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.