حل الخطأ الممنوع للوصول الآمن لأحداث API 403 للوصول عن بعد

المحتويات

مسألة

عند محاولة إسترداد سجلات الوصول عن بعد إلى VPN باستخدام نقطة نهاية /تقارير/API، يستقبل المستخدمون بشكل ثابت Cisco/v2/أحداث الوصول عن بعد، للوصول الآمن من "منع الوصول وفقا لمعيار 403" على الرغم من تمكين جميع النطاقات المطلوبة لإستجابة API باستخدام reports.granularevents:read. تحدث المشكلة عند إجراء إستدعاءات API بما في ذلك المعلمات التالية:

```
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
```

يحدث الخطأ بالرغم من أن مفتاح API له نطاقات تقارير متعددة تم تكوينها، ونقاط نهاية نقاط الوصول إلى API الأخرى تعمل بشكل صحيح. يبلغ المستخدمون عن قدرتهم على الوصول إلى نقطة نهاية التقرير الأخرى بنجاح ولكن يصادفون على وجه التحديد مشاكل التفويض مع نقطة نهاية أحداث الوصول عن بعد.

البيئة

- واجهة برمجة تطبيقات الوصول الآمن من Cisco
- نقطة نهاية واجهة برمجة التطبيقات: /reports/v2/remote-access-events
- مفتاح API مع النطاقات التي تم تكوينها: admin.vpn:read، admin.users:read، admin.alert:read، admin.alerts:read، admin.sentinel:read، reports.aggregations:read، reports.granularevents:read، reports.malware:read، reports.incidents:read، reports.incidents:read، reports.dlp.events:read

- مستخدم لديه أذونات المسؤول الكامل على مدخل الوصول الآمن
- دمج واجهة برمجة التطبيقات مع أنظمة المراقبة

قرار

تم حل المشكلة باستخدام نطاق واجهة برمجة التطبيقات الصحيح لنقطة نهاية أحداث الوصول عن بعد. يختلف النطاق الموثق ومتطلب التنفيذ الفعلي لهذه النقطة النهائية المحددة.

تحليل السبب الجذري

كشف التحقيق عن وجود تباين بين نطاق واجهة برمجة التطبيقات الموثقة والتنفيذ الفعلي:

- تذكر الوثائق: النطاق المطلوب هو reports.aggregations:read.
- التنفيذ الفعلي: تقارير خرائط قائمة التحكم في الوصول (ACL) لبوابة واجهة برمجة التطبيقات الخارجية/الإصدار 2/أحداث الوصول عن بعد إلى التقارير.أدوات المساعدة:للقراءة.

نتائج إختبار النطاق

أكد الاختبار سلوك النطاق هذا:

```
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
```

لحل التطبيق

لحل الخطأ "منع الوصول إلى 403"، قم بتكوين مفتاح API باستخدام النطاق الصحيح:

الخطوة 1: إدارة مفتاح واجهة برمجة التطبيقات للوصول.

انتقل إلى Admin > مفاتيح API في لوحة معلومات الوصول الآمن.

الخطوة 2: إنشاء مفتاح واجهة برمجة تطبيقات جديد.

لإنشاء مفتاح API جديد، انقر فوق (+) وأدخل:

- اسم مفتاح API
- الوصف (إختياري)
- تاريخ انتهاء الصلاحية حسب الرغبة

الخطوة 3: قم بتكوين النطاق الصحيح.

في قسم النطاقات، قم بتمكين التقارير.utilities:القراءة لوظيفة أحداث الوصول عن بعد.

الخطوة 4: إنشاء رمز الحامل المميز.

قم بإنشاء رمز مميز جديد لحامله باستخدام تدفق بيانات اعتماد عميل OAuth2 باستخدام مفتاح API المحدث.

الخطوة 5: إختبار إستدعاء واجهة برمجة التطبيقات.

أعد محاولة إستدعاء API باستخدام تنسيق الأمر curl العامل:

```
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'
```

الخطوة 6: تحقق من الدقة.

تأكيد إستدعاء واجهة برمجة التطبيقات ترجع حالة HTTP 200 وتسترجع بيانات أحداث الوصول عن بعد المتوقعة.

السبب

السبب الرئيسي هو عدم تطابق بين متطلبات نطاق واجهة برمجة التطبيقات (API) الخاصة بواجهة الوصول (ACL) في قائمة التحكم في الوصول الفعلي والتنفيذ الموثقة. تذكر وثائق Cisco العامة لـ GET /reports/v2/remote-access-events برمجة التطبيقات الخارجية. عندما، reports.aggregation:read هو نطاق الوصول المطلوب بشكل غير صحيح أن reports.utilities:read. يتسبب هذا التباين في حدوث حالات فشل يتطلب التنفيذ الفعلي في المصادقة حتى عندما يعتقد المستخدمون أنهم قاموا بتكوين الأذونات الصحيحة استنادا إلى الوثائق الرسمية.

المحتوى ذي الصلة

- Cisco Secure Access - Get Remote Access Events واجهة برمجة تطبيقات
- Cisco من الدعم الفني والتنزيلات

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).