Secure Access API Remote Access Events 403 Access Forbidden Error oplossen

Inhoud

uitgifte

Wanneer gebruikers proberen om VPN-logboeken voor externe toegang op te halen met behulp van het Cisco Secure Access API-eindpunt/rapporten/v2/gebeurtenissen voor externe toegang, ontvangen ze consequent een "403 Access Forbidden"-antwoord ondanks het feit dat ze alle vereiste scopes hebben ingeschakeld, inclusief rapporten.granularevents:read. Het probleem treedt op bij het maken van API-oproepen met deze parameters:

```
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
```

De fout treedt op ondanks dat de API-sleutel meerdere rapportscopes heeft geconfigureerd en andere API-eindpunten correct functioneren. Gebruikers melden dat ze met succes toegang kunnen krijgen tot andere rapporteindpunten, maar specifiek autorisatieproblemen kunnen tegenkomen met het eindpunt voor gebeurtenissen met externe toegang.

milieu

- Cisco Secure Access API
- API-eindpunt: /reports/v2/gebeurtenissen met externe toegang
- API-sleutel met geconfigureerde scopes: 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

- Gebruiker met volledige beheerdersrechten op Secure Access-portal
- API-integratie met monitoringsystemen

resolutie

Het probleem is opgelost door het juiste API-bereik te gebruiken voor het eindpunt voor gebeurtenissen met externe toegang. De gedocumenteerde reikwijdte en de feitelijke implementatievereisten verschillen voor dit specifieke eindpunt.

analyse van de grondoorzaak

Uit het onderzoek is gebleken dat er een discrepantie bestaat tussen de gedocumenteerde reikwijdte van de API en de daadwerkelijke implementatie:

- Documentatiestatus: Het vereiste bereik is reports.aggregations: read.
- Werkelijke implementatie: de externe API-gateway ACL koppelt rapporten/v2/gebeurtenissen met externe toegang aan reports.utilities:read.

Scope testresultaten

Testen bevestigde dit gedrag van de scope:

```
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
```

Implementatie van oplossing

Om de 403 Access Forbidden-fout op te lossen, configureert u de API-sleutel met het juiste bereik:

Stap 1: Access API Key Management.

Navigeer naar Beheer > API-sleutels in het Dashboard voor beveiligde toegang.

Stap 2: Maak een nieuwe API-sleutel.

Klik op API-sleutel toevoegen (+) en configureer:

- API-sleutelnaam
- Beschrijving (optioneel)
- Vervaldatum zoals gewenst

Stap 3: Configureer het juiste bereik.

Schakel in het gedeelte Scopes de functionaliteit reports.utilities:read for remote access events in.

Stap 4: Genereer token.

Maak een nieuw token aan toonder met behulp van de OAuth2 client-credentials flow met de bijgewerkte API-sleutel.

Stap 5: Test API-oproep.

Probeer de API-aanroep opnieuw met behulp van de werkende curl-opdrachtindeling:

```
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'
```

Stap 6: Controleer de resolutie.

Bevestig dat de API-oproep de HTTP 200-status retourneert en de verwachte gegevens van externe toegangsevenementen ophaalt.

Oorzaak

De hoofdoorzaak is een mismatch tussen de gedocumenteerde API scope requirements en de daadwerkelijke implementatie in de externe API gateway ACL. In de openbare documentatie van Cisco voor GET /reports/v2/remote-access-events wordt ten onrechte vermeld dat het vereiste toegangsbereik reports.aggregations:read is, wanneer de daadwerkelijke implementatie reports.utilities:read vereist. Deze discrepantie veroorzaakt verificatiefouten, zelfs wanneer gebruikers denken dat ze de juiste machtigingen hebben geconfigureerd op basis van de officiële documentatie.

Gerelateerde inhoud

- Cisco Secure Access API - Gebeurtenissen voor externe toegang
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.