Errore di risoluzione eventi di accesso remoto dell'API Secure Access 403 Accesso negato

Sommario

Problema

Quando si tenta di recuperare i registri di accesso remoto VPN utilizzando l'endpoint /reports/v2/remote-access-events dell'API Cisco Secure Access, gli utenti ricevono costantemente una risposta "Accesso 403 vietato" nonostante abbiano abilitato tutti gli ambiti richiesti, inclusi reports.granularevents:read. Il problema si verifica quando si effettuano chiamate API con questi parametri:

```
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
```

L'errore si verifica nonostante la chiave API abbia più ambiti di report configurati e altri endpoint API funzionino correttamente. Gli utenti segnalano di essere in grado di accedere ad altri endpoint di report, ma rilevano problemi di autorizzazione specifici con l'endpoint degli eventi di accesso remoto.

Ambiente

- Cisco Secure Access API
- Endpoint API: /reports/v2/remote-access-events
- Chiave API con ambiti configurati: admin.vpn:read, admin.users:read, admin.alertrules:read, admin.alert:read, admin.sentinel:read, reports.aggregations:read, reports.granularevents:read, reports.malware:read, reports.incident:read, reports.dlp.events:read

- Utente con autorizzazioni di amministratore completo sul portale Secure Access
- Integrazione delle API con i sistemi di monitoraggio

Risoluzione

Il problema è stato risolto utilizzando l'ambito API corretto per l'endpoint degli eventi di accesso remoto. L'ambito documentato e i requisiti di implementazione effettivi differiscono per questo endpoint specifico.

Analisi della causa principale

Dalle indagini è emersa una discrepanza tra l'ambito API documentato e l'implementazione effettiva:

- Nella documentazione si afferma: L'ambito richiesto è reports.aggregations:read.
- Attuazione effettiva: L'ACL del gateway API esterno mappa reports/v2/remote-access-events a reports.utilities:read.

Risultati test ambito

Il test ha confermato questo comportamento dell'ambito:

```
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
```

Implementazione della soluzione

Per risolvere l'errore 403 Accesso negato, configurare la chiave API con l'ambito corretto:

Passaggio 1: Accedere a Gestione chiavi API.

Passare a Amministrazione > Chiavi API nel dashboard Accesso sicuro.

Passaggio 2: Crea nuova chiave API.

Fare clic su Add API Key (+) e configurare:

- Nome chiave API
- Descrizione (facoltativa)
- Data di scadenza desiderata

Passaggio 3: Configurare l'ambito corretto.

Nella sezione Ambiti abilitare la funzionalità reports.utilities:read for remote access events.

Passaggio 4: Generare un token di connessione.

Creare un nuovo token di connessione utilizzando il flusso di credenziali client OAuth2 con la chiave API aggiornata.

Passaggio 5: Chiamata API di test.

Riprovare la chiamata API utilizzando il formato di comando curl di lavoro:

```
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'
```

Passaggio 6: Verificare la risoluzione.

Confermare che la chiamata API restituisca lo stato HTTP 200 e recuperi i dati degli eventi di accesso remoto previsti.

Causa

La causa principale è una mancata corrispondenza tra i requisiti dell'ambito API documentati e l'implementazione effettiva nell'ACL del gateway API esterno. Nella documentazione pubblica Cisco per GET /reports/v2/remote-access-events viene erroneamente indicato che l'ambito di accesso richiesto è reports.aggregations:read, quando l'implementazione effettiva richiede reports.utilities:read. Questa discrepanza causa errori di autenticazione anche quando gli utenti ritengono di aver configurato le autorizzazioni corrette in base alla documentazione ufficiale.

Contenuto correlato

- Cisco Secure Access API - Recupera eventi di accesso remoto
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).