Résoudre les événements d'accès à distance de l'API d'accès sécurisé 403 Accès interdit Erreur

Table des matières

Problème

Lors de la tentative de récupération des journaux d'accès à distance VPN à l'aide du point de terminaison /rapports/v2/remote-access-events de l'API d'accès sécurisé Cisco, les utilisateurs reçoivent systématiquement une réponse « Accès interdit 403 » malgré l'activation de toutes les étendues requises, y compris reports.granularevents:read. Le problème se produit lors d'appels d'API avec ces paramètres :

```
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'erreur se produit bien que la clé API ait plusieurs étendues de rapport configurées et que les autres points de terminaison API fonctionnent correctement. Les utilisateurs signalent qu'ils peuvent accéder avec succès à d'autres points de terminaison de rapport, mais qu'ils rencontrent des problèmes d'autorisation avec le point de terminaison des événements d'accès distant.

Environnement

- API d'accès sécurisé Cisco
- Point de terminaison API : /reports/v2/remote-access-events
- Clé API avec étendues configurées : 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

- Utilisateur disposant d'autorisations d'administrateur complet sur le portail Secure Access
- Intégration API aux systèmes de surveillance

Résolution

Le problème a été résolu à l'aide de l'étendue API correcte pour le point de terminaison des événements d'accès à distance. La portée documentée et les exigences de mise en oeuvre réelles diffèrent pour ce terminal spécifique.

Analyse de la cause première

L'enquête a révélé une divergence entre la portée de l'API documentée et la mise en oeuvre réelle :

- La documentation indique : L'étendue requise est reports.aggregations:read.
- Mise en oeuvre réelle : La liste de contrôle d'accès de la passerelle d'API externe mappe les événements d'accès à distance/v2/reports.utility:read.

Résultats des tests de portée

Les tests ont confirmé ce comportement de portée :

```
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
```

Implémentation de la solution

Pour résoudre l'erreur Accès interdit 403, configurez la clé API avec la portée correcte :

Étape 1: Accédez à Gestion des clés API.

Accédez à Admin > API Keys dans le tableau de bord Secure Access.

Étape 2: Créer une nouvelle clé API.

Cliquez sur Add API Key (+) et configurez :

- Nom de clé API
- Description (facultatif)
- Date d'expiration souhaitée

Étape 3: Configurez l'étendue correcte.

Dans la section Étendues, activez la fonctionnalité reports.utility:read for remote access events.

Étape 4: Générer un jeton porteur.

Créez un nouveau jeton de support à l'aide du flux d'informations d'identification du client OAuth2 avec la clé API mise à jour.

Étape 5: Tester l'appel API.

Réessayez l'appel API en utilisant le format de commande curl de travail :

```
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'
```

Étape 6: Vérifiez la résolution.

Confirmez que l'appel API renvoie l'état HTTP 200 et récupère les données d'événements d'accès à distance attendues.

Motif

La cause principale est une non-correspondance entre les exigences documentées de l'étendue de l'API et l'implémentation réelle dans la liste de contrôle d'accès de la passerelle API externe. La documentation publique Cisco pour GET /reports/v2/remote-access-events indique à tort que l'étendue d'accès requise est reports.aggregations:read, lorsque l'implémentation réelle nécessite reports.utility:read. Cette différence entraîne des échecs d'authentification même lorsque les utilisateurs pensent avoir configuré les autorisations correctes en fonction de la documentation officielle.

Autres informations utiles

- API d'accès sécurisé Cisco - Obtenir des événements d'accès à distance
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.