Resolución de Eventos de Acceso Remoto API de Acceso Seguro 403 Error de Acceso Prohibido

Contenido

Problema

Al intentar recuperar los registros de acceso remoto VPN mediante el terminal /informes/v2/eventos de acceso remoto de la API de Cisco Secure Access, los usuarios reciben de forma sistemática una respuesta de "403 Access Forbidden" a pesar de haber habilitado todos los ámbitos requeridos, incluidos los informes.eventos granulares:lectura. El problema ocurre cuando se realizan llamadas API con estos parámetros:

```
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
```

El error se produce a pesar de que la clave de la API tiene varios ámbitos de informe configurados y de que otros extremos de la API funcionan correctamente. Los usuarios informan de que pueden obtener acceso correctamente a otros extremos del informe, pero, en concreto, encuentran problemas de autorización con el extremo de eventos de acceso remoto.

Entorno

- API de Cisco Secure Access
- Extremo de API: /reports/v2/remote-access-events
- Clave de API con ámbitos configurados: 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.incidentes:read, reports.dlp.events:read
- Usuario con permisos de administrador completos en el portal de acceso seguro
- Integración de API con sistemas de supervisión

Resolución

El problema se resolvió mediante el ámbito de API correcto para el extremo de eventos de acceso remoto. El alcance documentado y el requisito de implementación real difieren para este terminal específico.

Análisis de causa raíz

La investigación reveló una discrepancia entre el alcance de la API documentada y la implementación real:

- La documentación indica: El ámbito requerido es reports.aggregations:read.
- Implementación real: La ACL de gateway de API externa asigna los eventos de informes/v2/acceso remoto a reports.utilities:read.

Resultados de pruebas de alcance

Las pruebas confirmaron este comportamiento de ámbito:

```
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
```

Implementación de soluciones

Para resolver el error 403 Access Forbidden, configure la clave API con el alcance correcto:

Paso 1: Acceso a la administración de claves API.

Vaya a Admin > API Keys en el panel Secure Access.

Paso 2: Crear nueva clave de API.

Haga clic en Add API Key (+) y configure:

- Nombre de clave de API
- Descripción (opcional)
- Fecha de vencimiento deseada

Paso 3: Configure el alcance correcto.

En la sección Ámbitos, habilite reports.utilities:read para la funcionalidad de eventos de acceso remoto.

Paso 4: Generar token portador.

Cree un nuevo token portador mediante el flujo de credenciales del cliente OAuth2 con la clave de API actualizada.

Paso 5: Prueba de llamada API.

Vuelva a intentar la llamada a la API utilizando el formato de comando curl en funcionamiento:

```
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'
```

Paso 6: Verifique la resolución.

Confirmar que la llamada API devuelve el estado HTTP 200 y recupera los datos de eventos de acceso remoto esperados.

Causa

La causa raíz es una discordancia entre los requisitos de alcance de la API documentada y la implementación real en la ACL de gateway de la API externa. La documentación pública de Cisco para GET /reports/v2/remote-access-events indica incorrectamente que el ámbito de acceso requerido es reports.aggregations:read, cuando la implementación real requiere reports.utilities:read. Esta discrepancia provoca errores de autenticación incluso cuando los usuarios creen que han configurado los permisos correctos en función de la documentación oficial.

Contenido relacionado

- API de Cisco Secure Access: Obtenga eventos de acceso remoto
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).