Resolver Erro de Acesso Remoto 403 de Eventos de Acesso Remoto da API de Acesso Seguro

Contents

Problema

Ao tentar recuperar logs de acesso remoto de VPN usando o ponto de extremidade da API do Cisco Secure Access /reports/v2/remote-access-events, os usuários recebem consistentemente uma resposta "403 Access Forbidden", apesar de terem habilitado todos os escopos necessários, incluindo reports.granularevents:read. O problema ocorre ao fazer chamadas à API com estes parâmetros:

```
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
```

O erro ocorre apesar de a chave de API ter vários escopos de relatório configurados e outros pontos de extremidade de API funcionando corretamente. Os usuários relatam que podem acessar com êxito outros pontos de extremidade de relatório, mas encontram problemas de autorização específicos com o ponto de extremidade de eventos de acesso remoto.

Ambiente

- API de acesso seguro da Cisco
- Ponto de extremidade da API: /reports/v2/remote-access-events
- Chave de API com escopos 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
- Usuário com permissões de Administrador Total no portal de Acesso Seguro
- Integração de API com sistemas de monitoramento

Resolução

O problema foi resolvido com o uso do escopo de API correto para o ponto de extremidade de eventos de acesso remoto. O escopo documentado e o requisito de implementação real diferem para esse endpoint específico.

Análise da causa raiz

A investigação revelou uma discrepância entre o escopo de API documentado e a implementação real:

- A documentação afirma: O escopo necessário é reports.aggregations:read.
- Implementação real: A ACL de gateway de API externa mapeia relatórios/v2/eventos de acesso remoto para relatórios.utilitários:leitura.

Resultados do teste de escopo

Os testes confirmaram este comportamento de escopo:

```
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
```

Implementação da solução

Para resolver o erro 403 Access Forbidden, configure a chave de API com o escopo correto:

Passo 1: Acesse o Gerenciamento de Chave de API.

Navegue até Admin > API Keys no painel Secure Access.

Passo 2: Criar nova chave de API.

Clique em Adicionar chave de API (+) e configure:

- Nome da chave de API
- Descrição (opcional)
- Data de validade, conforme desejado

Passo 3: Configure O Escopo Correto.

Na seção Escopos, habilite reports.utilities:read para a funcionalidade de eventos de acesso remoto.

Passo 4: Gerar token de portador.

Crie um novo token de portador usando o fluxo de credenciais de cliente OAuth2 com a chave de API atualizada.

Passo 5: Teste a chamada à API.

Repita a chamada à API usando o formato de comando curl :

```
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'
```

Passo 6: Verifique a resolução.

Confirme se a chamada de API retorna o status HTTP 200 e recupera os dados de eventos de acesso remoto esperados.

Causa

A causa raiz é uma incompatibilidade entre os requisitos de escopo de API documentados e a implementação real na ACL de gateway de API externa. A documentação pública da Cisco para GET /reports/v2/remote-access-events afirma incorretamente que o escopo de acesso necessário é reports.aggregations:read, quando a implementação real exige reports.utilities:read. Essa discrepância causa falhas de autenticação mesmo quando os usuários acreditam ter configurado as permissões corretas com base na documentação oficial.

Conteúdo relacionado

- API do Cisco Secure Access - Obter eventos de acesso remoto
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.