解决安全访问API远程访问事件403访问禁止错误

目录

问题

当尝试使用思科安全访问API终端/reports/v2/remote-access-events检索VPN远程访问日志时，用户始终会收到“403 Access Forbidden”响应，尽管已启用所有必需的范围，包括reports.granularevents:read。使用以下参数进行API调用时出现问题：

```
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
```

尽管API密钥配置了多个报告作用域，并且其他API终端运行正常，但仍会发生错误。用户报告他们可以成功访问其他报告端点，但会遇到远程访问事件端点的授权问题。

环境

- 思科安全访问API
- API终结点：/reports/v2/remote-access-events
- 具有已配置作用域的API密钥：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
- 在安全访问门户上具有完全管理员权限的用户
- API与监控系统集成

分辨率

通过使用适用于远程访问事件终结点的正确API作用域解决了此问题。对于此特定终端，记录的范围和实际实施要求会有所不同。

根本原因分析

调查发现，所记录的API范围与实际实施之间存在差异：

- 文档说明:所需的作用域是reports.aggregations:read。
- 实际实施:外部API网关ACL将reports/v2/remote-access-events映射到reports.utilities:read。

范围测试结果

测试确认了此范围行为：

```
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
```

解决方案实施

要解决403 Access Forbidden错误，请使用正确的范围配置API密钥：

步骤 1：访问API密钥管理。

在安全访问控制面板中导航到Admin > API Keys。

步骤 2：创建新API密钥。

单击Add API Key(+)并配置：

- API密钥名称
- 说明 (可选)
- 到期日期（根据需要）

步骤 3：配置正确范围。

在Scope部分，启用reports.utilities:read以获取远程访问事件功能。

步骤 4：生成承载令牌。

使用具有更新的API密钥的OAuth2客户端凭证流创建新的承载令牌。

步骤 5：测试API调用。

使用工作curl命令格式重试API调用：

```
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'
```

步骤 6：检验分辨率。

确认API调用返回HTTP 200状态并检索预期的远程访问事件数据。

原因

根本原因是所记录的API范围要求与外部API网关ACL中的实际实施不匹配。Cisco GET /reports/v2/remote-access-events的公共文档错误地指出所需的访问作用域是reports.aggregations:read，而实际实施需要reports.utilities:read。即使用户认为他们根据官方文档配置了正确的权限，这种差异也会导致身份验证失败。

相关内容

- 思科安全访问API — 获取远程访问事件
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。