

在安全访问XDR集成中对模块运行状况检查失败 错误代码进行故障排除

目录

问题

思科安全访问与XDR集成在运行状况检查阶段失败，出现HTTP 431“Request Header Fields Too Large”错误。集成以前成功运行，但在尝试使用从思科安全访问控制面板生成的API密钥建立连接时，突然开始因此错误而失败。

特定错误消息显示为：

<#root>

Health check of Module failed: - [v2 Reporting API] There was a client error in the Cisco Secure Access

此错误可防止安全访问数据进入XDR，从而影响安全可视性和监控功能。

环境

- Cisco Secure Access with Advantage许可证
- Cisco XDR订用
- 思科安全访问租户
- 使用思科安全访问控制面板生成的密钥进行API集成
- 所需的API范围：Investigate > Read-Only，Reports > Read-only，Deployments > Read-only，Policies > Read/Write

分辨率

通过在思科安全访问中重新生成API密钥和密钥解决了此问题。

按照以下步骤解决431错误：

步骤 1：生成新的API密钥

导航到Cisco Secure Access控制面板并使用所需的范围创建新的API密钥：

- 调查：只读
- Reports:只读
- 部署：只读
- 策略：读/写

步骤 2：将新密钥应用于XDR集成

用新生成的密钥替换XDR安全访问集成配置中的现有API密钥。

步骤 3：验证集成

测试集成以确认连接成功。API调用现在必须返回HTTP 200响应，而不是431错误。

主动检测和防御

要识别并防止将来出现类似的431个错误，请执行以下操作：

1. — 通过Postman或浏览器控制台等工具进行调试时，请检查请求报头的大小列。如果请求报头接近或超过8 KB（8192字节），则会在API网关上触发431错误。外部工具（如jwt.io）可用于验证OAuth令牌大小。

2. — 分析错误模式：

- 如果在运行状况检查的初始握手期间立即发生431错误，则表明存在静态凭证问题
- 如果仅在集成运行几分钟后发生431错误，则表明在后续重试中存在cookie累积

最佳实践

在集成客户端/浏览器中禁用cookie或会话持久性，以防止报头大小累积。

原因

HTTP 431错误是由特定API密钥和密钥对引起的，在为标准HTTP授权报头编码Base64时，该密钥和密钥对生成异常大的或格式错误的授权报头。

初始API密钥中的加密字符串包含一系列字符，这些字符在编码时扩展为超出了API网关限制的报头大小，导致“请求报头字段过大”被拒绝。

重新生成API密钥时，新的加密字符串生成了大小适当的授权报头。撤销和生成新密钥的过程还清除了集成管理器端缓存的请求上下文，从而规范化报头大小。

相关内容

- [思科安全访问API身份验证](#)
- [思科安全访问集成到XDR](#)
- [从XDR控制台收集HAR日志](#)
- [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）。