具有SAML身份验证和Bencode字典错误的安全客户端VPN连接故障

目录

问题

使用Cisco Secure Client的VPN连接无法建立，当使用带有Google IdP的SAML身份验证时。虽然SAML身份验证在IdP端成功，但客户端在身份验证后处理过程中失败，并转换为断开状态，从而阻止创建VPN隧道。

环境

- 思科安全客户端5.1.13.177版
- 使用Google IdP配置的SAML身份验证
- 安全访问 — 安全客户端远程访问（VPN、状态、专用资源）
- Google IdP身份验证日志显示成功的SAML身份验证

分辨率

通过重新安装Cisco安全客户端解决了此问题。此故障排除方法记录如下：

初始诊断步骤

步骤 1：从受影响的终端收集DART日志。

解压缩DART套件> Cisco安全客户端> Anyconnect VPN >日志>在VPN文件夹> AnyConnectVPN.txt下显示读取内部设置时出现的这些错误，错误持续出现：

- Bencode词典内部化失败
- 无法创建Bencode字典
- PHONEHOMEVPN_ERROR_UNEXPECTED
- GLOBAL_ERROR_UNEXPTED

步骤 2：检验IdP端的SAML身份验证状态。

确认Google IdP日志显示成功的SAML身份验证，以将问题隔离到客户端身份验证后处理。

解决方案实施

步骤 1：重新安装Cisco Secure Client。

卸载现有的Cisco Secure Client安装并执行客户端软件的全新重新安装。

步骤 2：检验VPN连接恢复。

重新安装后，使用SAML身份验证测试VPN连接，以确认连接成功建立且隧道创建正确。

重新安装Cisco Secure Client恢复了VPN功能，从而允许成功建立SAML身份验证和隧道。

原因

根本原因似乎与Cisco安全客户端安装中的内部配置数据损坏有关，尤其是影响CPhoneHomeVpn/PhoneHomeAgent组件在身份验证后处理期间处理Bencode字典数据的能力。重复出现的“Bencode dictionary internalize failed”和“Failed to create Bencode dictionary”错误表明客户端无法正确解析或处理建立VPN隧道所需的内部配置数据（在成功进行SAML身份验证之后）。

该问题通过客户端重新安装得到解决，表明此问题与损坏的客户端数据有关，而不是服务器端配置或IdP集成问题。

相关内容

- 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）。