由于终端安全状态合规性问题，安全客户端AnyConnect VPN访问被拒绝

目录

问题

多个用户无法连接到AnyConnect VPN和零信任访问(ZTA)，并收到错误消息“Login denied.您的环境不符合管理员定义的访问条件。"

此问题与终端安全评估合规性相关，其中终端安全代理要求报告为不匹配。用户尝试通过Cisco安全客户端连接时遇到VPN和ZTA访问拒绝。

状态评估显示Trellix终端安全状态在受影响的终端上失败，阻止对VPN服务的成功身份验证。

环境

- 思科安全客户端（AnyConnect和零信任访问）
- Trellix终端安全代理5.8.4.505版
- VPN终端安全评估配置文件：实施终端安全代理的KFIN_SECURE_VPN
- 状态要求：终端安全代理在最近14天内运行且有更新
- 运行Trellix代理服务的Windows终端
- 在终端上检测到的Umbrella代理进程

分辨率

通过解决Trellix终端安全代理状态合规性问题解决了此问题。实施了以下各节中介绍的故障排除和

解决步骤。

步骤 1：验证状态配置文件配置

检查VPN终端安全评估配置文件以确认终端安全代理要求。KFIN_SECURE_VPN配置文件强制终端安全代理必须在最近14天内运行和更新。

步骤 2：验证Trellix终端安全状态

检查受影响终端上Trellix终端安全代理的当前状态：

```
Trellix Agent Service: masvc.exe
Version: 5.8.4.505
Install Location: C:\Program Files\McAfee\Agent\
Display Name: Trellix Agent
Publisher: Trellix
```

步骤 3：重新安装Trellix终端安全

在受影响的终端上执行Trellix终端安全的完整重新安装：

1.完全卸载现有的Trellix终端安全代理。

2.重新启动系统。

3.按照组织标准安装最新批准的Trellix代理版本。

4.确保代理在安装后成功运行。

5.确认签名/内容更新已成功完成。

步骤 4：为思科安全客户端(ZTA)启用TRACE日志记录

启用详细日志记录以捕获状态评估详细信息。

使用以下内容创建logconfig.json文件：

```
{ "global": "DBG_TRACE" }
```

将文件放在适当的目录中：

- Windows 窗口版本:C:\ProgramData\Cisco\Cisco安全客户端\ZTA
- macOS：/opt/cisco/secureclient/zta

创建文件后重新启动Cisco Secure Client/ZTA服务。

步骤 5：收集更新的DART套件

实施更改后，收集新的DART捆绑包以验证解决方案并确认正确的状态合规性检测。

原因

根本原因被识别为Trellix终端安全代理状态合规性问题。VPN终端安全评估配置文件要求终端安全代理在最近14天内运行更新程序，但Trellix终端安全代理不符合这些合规性标准。终端安全评估模块无法正确检测或验证终端安全代理状态，导致VPN和ZTA连接的访问被拒绝。此问题具体与Trellix代理配置有关，需要Trellix支持团队进行干预以解决基础的代理合规性问题。

相关内容

- 收集详细的ZTNA日志以进行故障排除

- 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）。