思科安全终端MAC连接器故障

目录

简介

当连接器检测到影响连接器正常工作的情况时，它可能会通知您发生故障。同样，“故障清除”事件也表明该条件不再存在。

连接器故障表

下表介绍故障和相应的诊断步骤。

故障ID	门户文本	终端描述	故障排除/解决
1	内核模块未授权	系统扩展未授权	连接器的系统扩展已被阻止执行。 打开“安全和隐私系统首选项”并批准延期。 或者，可以使用移动设备管理(MDM)配置文件远程批准系统扩展。
2	版本不匹配	系统扩展版本不匹配	安装的连接器软件损坏。重新安装连接器。 注意：当运行Mac Connector版本1.14.0及更高版本时，重新启动计算机可能会此故障的某些发生。
3	未授予磁盘访问权限	未授予完全磁盘访问权限	连接器无法访问用户文件进行扫描。打开安全和隐私系统首选项并授予对AMP完全磁盘访问权限。 对于1.14.0之前的Mac连接器版本，此进程名为*/opt/cisco/amp/ampdaemon*。 对于Mac Connector版本1.14.0及更高版本，以下两个应用需要完全磁盘访问，取决于macOS版本： • *面向终端的 AMP 服务*（所有macOS版本均需要） • *AMP安全扩展*（在macOS 10.15.5及更高版本上需要） 对于Mac Connector版本1.14.1及更高版本，以下两个应用需要完全磁盘访问，取决于macOS版本： • *面向终端的 AMP 服务*（所有macOS版本均需要） • *AMP安全扩展*（在MacOS 11及更高版本上需要） 本技术说明中提供了其他详细信息。
4	内核模块未加载	无法加载系统扩展；重新安装连接器	对于1.14.0之前的Mac连接器版本，或在macOS 10.14或10.15上运行时，此故障示连接器的系统扩展版本正确，并已获得执行批准，但仍未加载。有关详*细信息*查看/Library/Logs/Cisco/ampdaemon.log。卸载和重新安装连接器也可能清除此。
5	扫描服务用户不可用	扫描服务用户不可用	连接器无法创建用户以运行文件扫描进程。连接器通过使用根用户执行文件扫描决此问题。这偏离了预期设计，不是预期的。 如果 `cisco-amp-scan-svc` 用户或组已被删除，或用户和组的配置已更改，重新安接器将使用必要的配置重新创建用户和组。更多详情请参阅*/Library/Logs/Cisco/ampdaemon.log*。

			连接器的文件扫描过程遇到重复的故障，连接器已重新启动以尝试清除故障。扫 ，系统上的一个或多个文件可能导致扫描算法崩溃。连接器继续以尽力扫描。
6	扫描服务频繁重新启动	扫描服务频繁重新启动	如果在连接器启动后10分钟内未自动清除此故障，则表明需要进一步的用户干预 且连接器执行扫描的能力将降低。
7	扫描服务无法启动	扫描服务无法启动	审核 */Library/Logs/Cisco/ampdaemon.log* 和 */Library/Logs/Cisco/ampscansvc.* 解详细信息。 连接器的文件扫描进程无法启动，并且连接器已重新启动以尝试清除故障。在引 故障时，文件扫描功能被禁用。 如果加载新安装的病毒定义文件（.cvd文件）时遇到错误，可触发此故障。 连接 激活新的.cvd文件之前执行多次完整性和稳定性检查，以防止此故障。重新启动 ，连接器将删除所有无效的.cvd文件，以便连接器可以恢复。 如果在连接器重新启动时未清除此故障，则表明需要进一步的用户干预。如果每 .cvd更新都重复出现此故障，则表明连接器的.cvd文件完整性检查未正确检测到 的.cvd文件。
10	加载内核模块或系统扩展需要重新启动	加载系统扩展时需要重新启动	审核 */Library/Logs/Cisco/ampdaemon.log* 和 */Library/Logs/Cisco/ampscansvc.* 解详细信息。 重新启动系统。 对于Mac Connector版本1.11.1和1.14.0，如果系统扩展无法加载，可能会引发此 障。在这种情况下，可以通过重新安装连接器来清除此故障。 请注意，如果系统上安装了太多网络内容过滤器系统扩展，Mac Connector 1.1 更高版本可能会引发此故障。如果重新启动计算机未清除此故障，请参阅以下故 13指南了解更多详细信息。 策略中的“启用设备流关联”功能需要网络过滤器。要清除此故障，请允许“面向终 AMP服务”过滤终端上的网络内容。
12	不允许网络过滤器	不允许网络过滤器	通过点击“代理”菜单中列出的活动故障并遵循所提供的指南，可以访问允许网络 器的macOS对话框。 有关其他详细信息，包括网络过滤器远程授权的MDM配置文件设置，请参阅 这 术说明。
13 个	网络内容过滤器系统扩展太多	网络内容过滤器系统扩展太多	对于Mac Connector 1.14.0，启动网络内容过滤器系统扩展时，由于macOS漏洞 故障经常引起。重新启动计算机将清除此故障。 策略中的“启用设备流关联”功能需要使用防火墙级macOS网络内容过滤器。 MacOS 限制可运行的网络内容过滤器的数量。 如果此故障已引发且未通过重新启动计算机清除，卸载不再需要的防火墙级网络 过滤器并重新启动连接器。
14	终端安全系统扩展太多	终端安全系统扩展太多	MacOS限制可运行的终端安全系统扩展的数量。Mac连接器要求在策略中为“监 件副本和移动”和“监控进程执行”功能提供以下终端安全系统扩展之一。 要清除此故障，请卸载不再需要的终端安全系统扩展并重新启动连接器。
15	系统扩展需要完全磁	系统扩展需要完全磁盘访问	Mac连接器的macOS系统扩展无法访问用户文件进行扫描。打开安全和隐私系统 选项并授予对AMP安全扩展的完*整磁盘访问权*。

			本技术说明中提供了其他详细信息，包括MDM配置文件设置，用于远程授权具 统扩展的完整磁盘访问。
		盘访问	请注意，在授予MacOS 11.0.0的Bug权限后，MacOS 11.0.0上的Bug可能会导 重新启动时自动清除完整磁盘访问设置。此Bug已在MacOS 11.0.1中修复。
17	未授予Orbital全磁盘访问权限	未授予Orbital全磁盘访问权限	**Orbital需要完全磁盘访问才能访问受保护的文件和目录以进行查询。**打开安全和 系统首选项，授予对Cisco Orbital的完整磁*盘访问权限*。