排除安全终端Linux连接器故障

目录

简介

本文档介绍Cisco Secure Endpoint Linux连接器用来通知您影响其正常运行的状况的故障。

背景信息

当思科安全终端Linux连接器检测到影响连接器正常运行的条件时，会通知发生故障的事件。同样，“已清除故障”事件通知条件不再存在。

安全终端Linux连接器故障表

下表介绍了故障及其相关诊断步骤。

故障ID	描述	故障排除/解决方案
5	扫描服务用户不可用	连接器无法创建用户来运行文件扫描进程。连接器使用根用户执行文件扫描作为解决方法。这偏离了预期设计，并非预期结果。 如果 `cisco-amp-scan-svc` 已删除用户或组，或者用户和组的配置已更改，则您可以重新安装连接器以使用必要的配置重新创建用户和组。有关其他详细信息，请参见 /var/log/cisco/ampdaemon.log. 如果通过/etc/login.defs中的设置限制用户组创建，则必须在安装程序运行时临时更改此文件以允许创建用户和组。为此，请将usergroups_enab从no更改为yes。 如果其他程序修改了连接器的一个目录权限（即/opt/cisco或子目录），则在Linux连接器1.15.1及更高版本中可能会引发此故障。要缓解此问题，必须将更改的目录权限重新设置为默认值（即0755），确保将来的程序不会修改/opt/cisco目录（或任何子目录），并重新启动连接器服务。
6	扫描服务频繁重新启动	连接器文件扫描进程遇到反复故障，连接器已重新启动以尝试清除故障。扫描时，系统上的一个或多个文件可能导致扫描算法崩溃。连接器继续尽力扫

		描。 如果在连接器启动后10分钟内没有自动清除此故障，则表示需要进一步用户干预，并且连接器执行扫描的能力已降低。 有关详细信息，请参阅/var/log/cisco/ampdaemon.log和/var/log/cisco/ampscansvc.log。
7	扫描服务启动失败	连接器的文件扫描进程无法启动，连接器已重新启动以尝试清除故障。出现此故障时，文件扫描功能被禁用。 如果在加载新安装的病毒定义文件（.cvd文件）时遇到错误，可能会触发此故障。在激活新的.cvd文件以防止此故障之前，连接器会执行许多完整性和稳定性检查。重新启动时，连接器将删除所有无效的.cvd文件，以便连接器可以恢复。 如果在重新启动连接器时未清除此故障，则表明需要进一步用户干预。如果每次更新.cvd时重复此故障，则表明连接器的.cvd文件完整性检查未正确检测到无效的.cvd文件。 如果计算机的可用内存不足，并且扫描程序服务无法启动，则在Linux连接器中可以触发此故障。有关Linux上的最低系统要求，请参阅《安全终端（以前称为面向终端的AMP）用户指南》。 有关详细信息，请参阅/var/log/cisco/ampdaemon.log和/var/log/cisco/ampscansvc.log。
8	实时文件系统监视无法启动	未加载提供实时文件系统活动监视的内核模块，并且连接器策略启用了“监视文件拷贝和移动”。出现此故障时，连接器中的这些监控功能不可用。当安全终端连接器无法加载文件系统活动监控所需的底层内核模块时，会发生此故障。 必须在系统上禁用UEFI安全引导。 如果禁用安全启动，则此故障可能是由随安全终端连接器提供的ampavflt或ampfsm内核模块与系统上安装的系统内核或其他第三方内核模块之间的不兼容造成的。查看/var/log/messages了解详细信息。 当运行连接器不支持的内核版本时，也可能发生此故障。在这种情况下，可以通过为当前运行的系统内核构建自定义ampfsm内核模块来清除此漏洞。（适用于Linux连接器版本1.16.0及更高版本。）有关构建自定义内核模块的更多信息，请参阅构建Cisco安全终端Linux连接器内核模块
9	无法启动实时网络监控	未加载提供实时网络活动监控的内核模块，并且连接器策略已启用“Enable Device Flow Correlation”。出现此故障时，连接器中的此监控功能不可用。当安全终端连接器无法加载文件系统活动监控所需的底层内核模块时，会

		发生此故障。 必须在系统上禁用UEFI安全引导。 如果禁用安全启动，则此故障可能是由随安全终端连接器提供的ampavflt或ampfsm内核模块与系统上安装的系统内核或其他第三方内核模块之间的不兼容造成的。查看/var/log/messages了解详细信息。 当运行连接器不支持的内核版本时，也可能发生此故障。在这种情况下，可以通过为当前运行的系统内核构建自定义ampfsm内核模块来清除此漏洞。（适用于Linux连接器版本1.16.0及更高版本。）有关构建自定义内核模块的更多信息，请参阅构建Cisco安全终端Linux连接器内核模块
11	缺少必需的内核级包	安全终端连接器使用eBPF模块监控文件系统、进程和网络活动。连接器需要系统上提供某些软件包，以加载和运行这些eBPF模块。要解决此故障，请按如下所述安装Linux发行版所需的软件包，并重新启动连接器。 对于基于Red Hat的分配，当内核级软件包缺失时会发生此故障。安装内核级软件包，然后重新启动连接器。（仅适用于Linux连接器版本1.13.0及更高版本。） 对于Oracle Linux UEK 6及更高版本，内核级时会发生此故障缺少包。安装内核级软件包并重新启动连接器。（仅适用于Linux连接器版本1.18.0及更高版本。） 对于基于Debian的分配，当缺少linux-headers包时，会引发此故障。安装linux-headers程序包，然后重新启动连接器。（适用于Linux连接器版本1.15.0及更高版本。） 有关更多信息，请参阅： Linux内核级故障
16	不兼容的内核	当前运行的内核与当前运行的连接器不兼容，并且连接器策略已启用“监控文件复制和移动”或“启用设备流关联”。 将内核降级到支持的版本，或将连接器升级到支持此内核的较新版本。 有关支持的内核版本的详细信息，请参阅： Cisco Secure Endpoint Linux Connector OS兼容性
18	连接器事件监控超载	当连接器由于大量系统事件而承受重负载时，会发生此故障。系统保护会受到限制，并且连接器会监控较少的几个系统关键事件，直到整体系统活动减少为止。 此故障可能表示恶意系统活动或系统中非常活跃的应用程序。 如果活动应用程序是良性的且受用户信任，则可将其添加到进程排除集中，以减少连接器上的监控负载。此操作足以清除故障。

		如果没有良性进程导致负载过重，则需要执行一些调查以确定活动增加是否源于恶意进程。 如果连接器在短时间内负载过重，则此故障可能会自行消除。 如果经常发生此故障，则不会出现会导致负载过重的良性进程，且不会发现恶意进程，则需要重新调配系统来处理负载过重的进程。
19	SELinux策略缺失或禁用	当系统上的Secure Enterprise Linux(SELinux)策略阻止连接器监视系统活动时，会引发此故障。如果SELinux已启用且处于实施模式，则Connector在SELinux Policy中需要此规则： `allow uncontained_service_t self:bpf { map_create map_read map_write prog_load prog_run };` 在基于Red Hat的系统（包括RHEL 7和Oracle Linux 7）上，此规则在默认SELinux策略中不存在。在安装或升级期间，连接器会尝试通过安装名为SELinux策略模块来添加此规则 `cisco-secure-bpf`.如果 `cisco-secure-bpf` 无法安装和加载，或者已禁用，则会引发故障。 要解决故障，请确保已安装系统软件包policycoreutils-python。重新安装或升级连接器以触发`cisco-secure-bpf`的安装，或者将规则手动添加到现有SELinux策略并重新启动连接器。 有关修改SELinux策略以解决此故障的更多详细说明，请参阅SELinux策略故障。

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）。