分析高CPU的macOS安全终端诊断套件

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

故障排除

- 验证计算机上是否安装了其他防病毒软件
- 确定正在使用特定应用时的高CPU
- 收集用于分析的诊断包
  - 终端中的调试级别
  - 安全终端命令行界面(CLI)中的调试级别
  - 策略中的调试级别
- 从其他防病毒解决方案中排除安全终端
- 重现问题并收集诊断捆绑包
- 高CPU性能分析

相关信息

简介

本文档介绍从MacOS设备上的安全终端公共云分析诊断捆绑包以排除CPU使用率过高故障的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 安全终端控制台中的基本导航
- MacOS终端的导航

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全终端控制台v5.4.20260915
- macOS：27.0
- 安全终端连接器1.27

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

安全终端连接器会扫描机器上的所有活动文件（移动、复制和/或修改其自身的文件），除非明确要求不要扫描，否则在连接器运行时如果运行太多进程和操作，将不可避免地带来性能问题，这会导致CPU使用率过高、速度降低或崩溃。此外，安全终端连接器可以根据文件的云信誉阻止文件，这种信誉有时可能是错误的（误报）。 解决这两个问题的方法是排除这些路径和进程。

图中显示了对性能问题进行故障排除的流程。



故障排除

本节提供可用于对配置进行故障排除的信息。

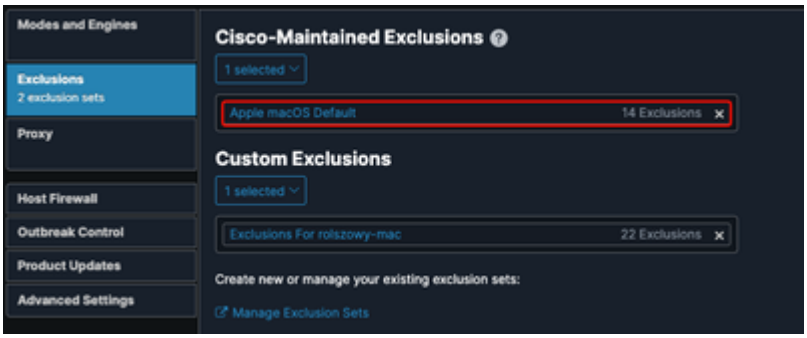
验证计算机上是否安装了其他防病毒软件

提示：如果使用的软件包含在列表中，请使用思科维护的例外项。请记住，这些例外项可以添加到应用的新版本中。

要查看安全终端控制台上思科维护的排除项部分中可用的列表，请执行以下操作：

- 导航到管理 > 策略。
- 找到策略，然后单击Edit。
- 在策略的“设置”窗口中，单击排除。

根据计算机上当前安装的软件，选择您的终端所需的策略，然后保存策略，如图所示。



确定正在使用特定应用时的高CPU

如果能够复制问题，请确定在执行一个应用程序或几个应用程序时是否发生问题，以帮助确定潜在的例外情况。

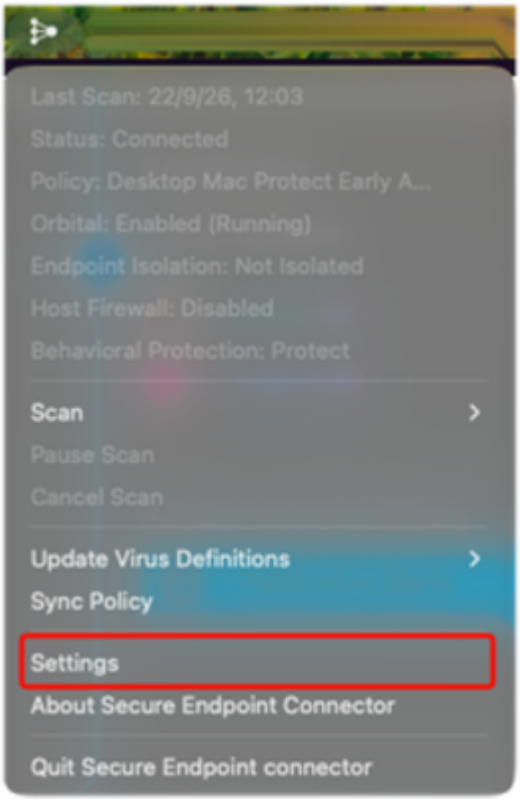
收集用于分析的诊断包

要收集有用的诊断包，必须启用调试日志级别。

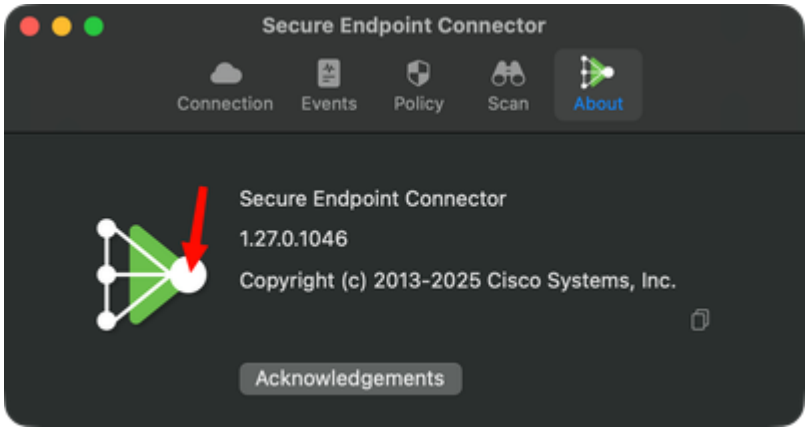
终端中的调试级别

如果您可以复制问题并访问终端，这是捕获诊断捆绑的最佳步骤。

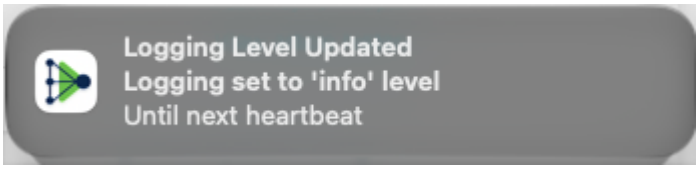
- 在macOS菜单栏上，选择安全终端图标。
- 选择设置:



- 选择About。
- 要启用调试模式，请在安全终端徽标内点击：



通知指示安全终端连接器处于调试模式。



此过程会启用调试日志级别，直到下一个策略检测信号间隔。

安全终端命令行界面(CLI)中的调试级别

- 打开终端
- 运行ampcli

```
/opt/cisco/amp/ampcli
```

- 在安全终端CLI上，启用调试模式

```
ampcli>debuglevel 1
```

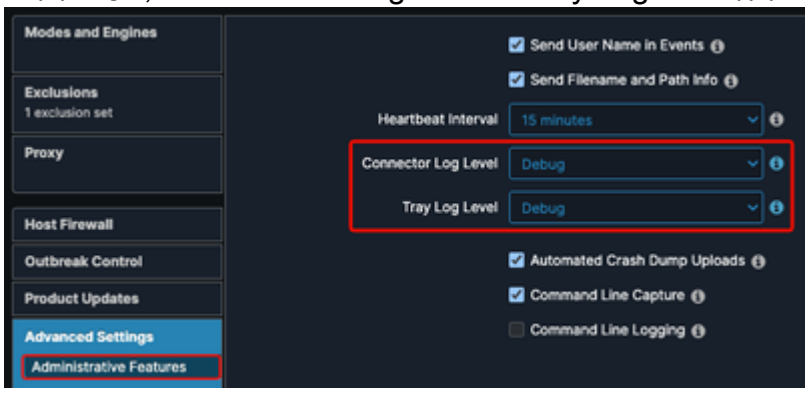
此过程会启用调试日志级别，直到下一个策略检测信号间隔。

策略中的调试级别

如果您没有访问终端的权限或者问题无法一致地再现，则必须在策略中启用调试日志级别。

要通过策略启用调试日志级别，请执行以下操作：

- 选择管理 > 策略。
- 找到策略，然后单击Edit。
- 选择高级设置 > 管理功能。
- 如图所示，将Connector Log Level和Tray Log Level配置为调试并保存策略



⚠ 警告：如果从策略启用调试模式，则所有终端都会收到此配置。

注意：同步终端的策略以确保调试模式。

从其他防病毒解决方案中排除安全终端

根据用户指南，防病毒产品必须排除下一个目录及其中的任何文件、目录和可执行文件，才能与Secure Endpoint Connector for macOS兼容。要排除的目录包括：

- /Applications/Cisco Secure Endpoint/Secure Endpoint Service.app

重现问题并收集诊断捆绑包

配置调试级别后，请等待系统出现高CPU状态或手动重现之前确定的条件，然后收集诊断捆绑包。

要收集调试捆绑包，请执行以下操作：

- 打开终端
- 使用命令

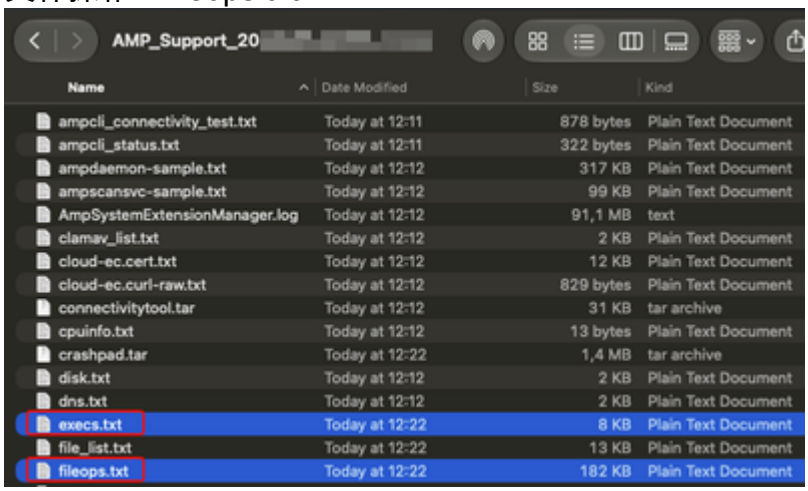
```
sudo /Applications/Cisco\ Secure\ Endpoint/Secure\ Endpoint\ Service.app/Contents/MacOS/SupportTool
```

调试包以.zip文件扩展名保存在~/Desktop文件夹中。

高CPU性能分析

debug diagnostic bundle is storage in the Desktop（调试诊断捆绑包存储在桌面中），以开始分析：

- 解压诊断套件
- 有2个文件要查看
  - 文件执行：execs.txt
  - 文件操作：fileops.txt



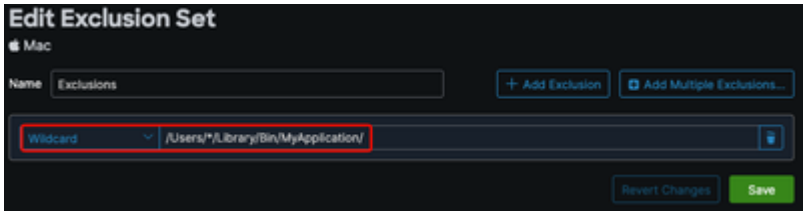
- fileops.txt用作进行故障排除的主要性能工具。它列出连接器运行时终端上当前所有活动操作，读取为：
  <收集捆绑包时在路径上执行的次数扫描>/<路径扫描>



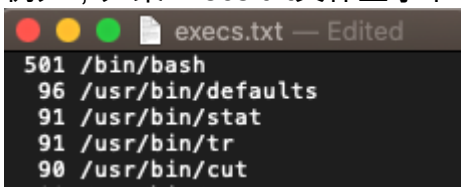
例如，如果您有一个家庭应用程序，fileops.txt将显示下一个活动操作：

```
639 /Users/user/Library/Bin/MyApplication/support/
460 /Users/user/Library/Bin/MyApplication/logs/
219 /Users/user/Library/Bin/MyApplication/Collection/Node/Server/
```

- 确定流程后，创建例外项：选择Management > Exclusions。
- 选择例外项集，然后选择编辑。
- 添加排除：



- Execs.txt文件包含在连接器收集捆绑包时运行的进程使用的所有命令。此处列出的路径不能排除在安全终端策略之外，因为它们是二进制文件(/bin)和系统二进制文件(/sbin)，所有进程都使用这些文件，但是，在Execs.text上，它们可以提供正在运行的主要进程。
  例如，如果Execs.txt文件显示下一个日志。



由于homebrew应用程序使用bash，因此您可以确认该应用程序是CPU使用率较高的原因。

相关信息

- 配置和识别安全终端排除
- 技术支持和文档

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）。