分析高CPU的MacOS AMP诊断套件

目录

简介

本文档介绍从面向MacOS设备上的终端公共云的高级恶意软件防护(AMP)分析诊断捆绑包以排除CPU使用率过高的故障的步骤。

作者：Uriel Torres，编辑者：Cisco TAC工程师Yeraldin Sanchez。

先决条件

要求

Cisco 建议您了解以下主题：

- AMP控制台中的基本导航
- MAC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：

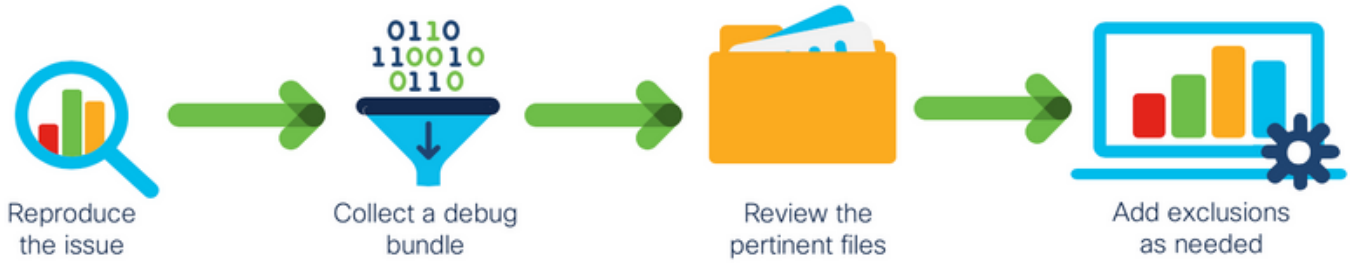
- 面向终端的AMP控制台5.4.20200512
- macOS Catalina版本10.15.4
- AMP连接器1.12.3.738

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

AMP连接器扫描计算机上的所有活动文件（移动、复制和/或修改自己的文件），除非明确告知不要，否则，如果连接器运行时运行的进程和操作过多，将不可避免地带来性能问题，这会导致CPU利用率高、速度慢，在某些情况下，还会导致软件不能运行或运行缓慢。此外，AMP连接器可能会根据文件的云信誉来阻止文件，这有时可能是错误的（误报）。 两个问题的解决方案是排除这些路径和进程。

故障排除性能问题的流程如图所示。



故障排除

本节提供可用于排除配置故障的信息。

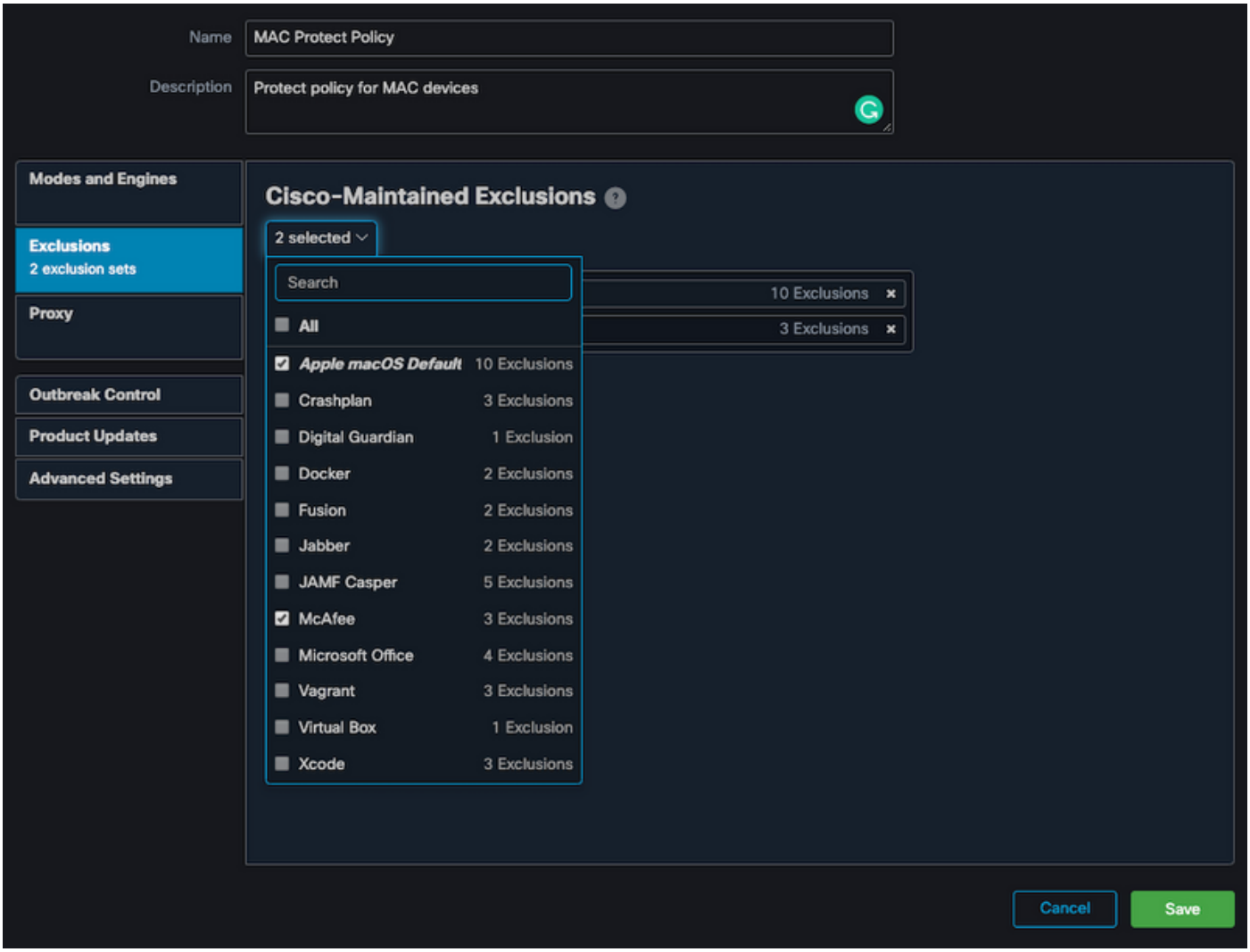
验证计算机上是否安装了其他防病毒软件

> **提示：**如果列表中包含思科维护的排除项，请记住这些排除项可以添加到应用的新版本。

要查看AMP控制台上思科维护的排除部分中可用的列表，请执行以下操作：

- 导航至**管理>策略**。
- 查找策略并单击“编**辑”**。
- 在策略上，“设置”窗口单击“**排除”**。

根据计算机上当前安装的软件选择终端需要的软件，然后保存策略，如图所示。



确定特定应用使用时的高CPU

确定问题是否发生在执行一个应用程序或其中几个应用程序时，如果您能够复制该问题，则有助于确定潜在的排除项。

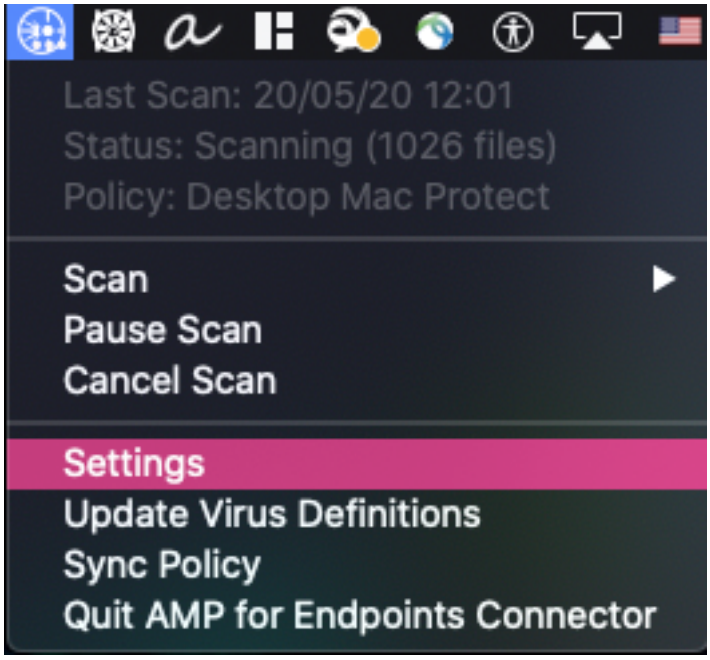
用于分析的诊断包的转换器

要收集有用的诊断包，必须启用调试日志级别。

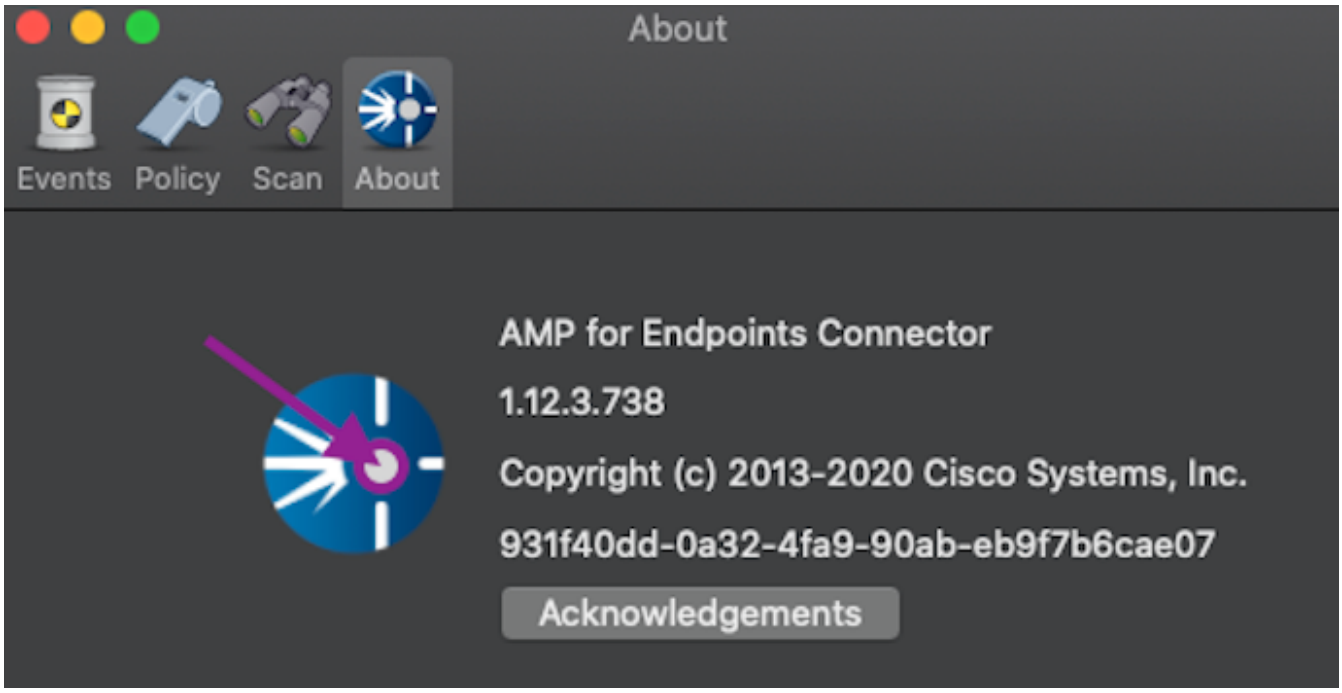
终端中的调试级别

如果可以复制问题并有权访问终端，以下是捕获诊断捆绑包的最佳步骤。

- 在MAC菜单栏上，点击AMP图标。
- 导航到**设置**部分，如图所示。



- 在设置窗口中，导航至**关于**。
- 要启用调试模式，请点击AMP徽标内部，如图所示。



弹出窗口指示AMP连接器处于调试模式

此过程将启用调试日志级别，直到下一个策略心跳间隔。

AMP命令行界面(CLI)中的调试级别

- 打开终端
- 导航至**/opt/cisco/amp/bin/**
- 运行ampcli:
  ```
  ./ampcli
  ```
- 在AMP CLI上启用调试模式：
  ```
  ampcli>debuglevel 1
  ```

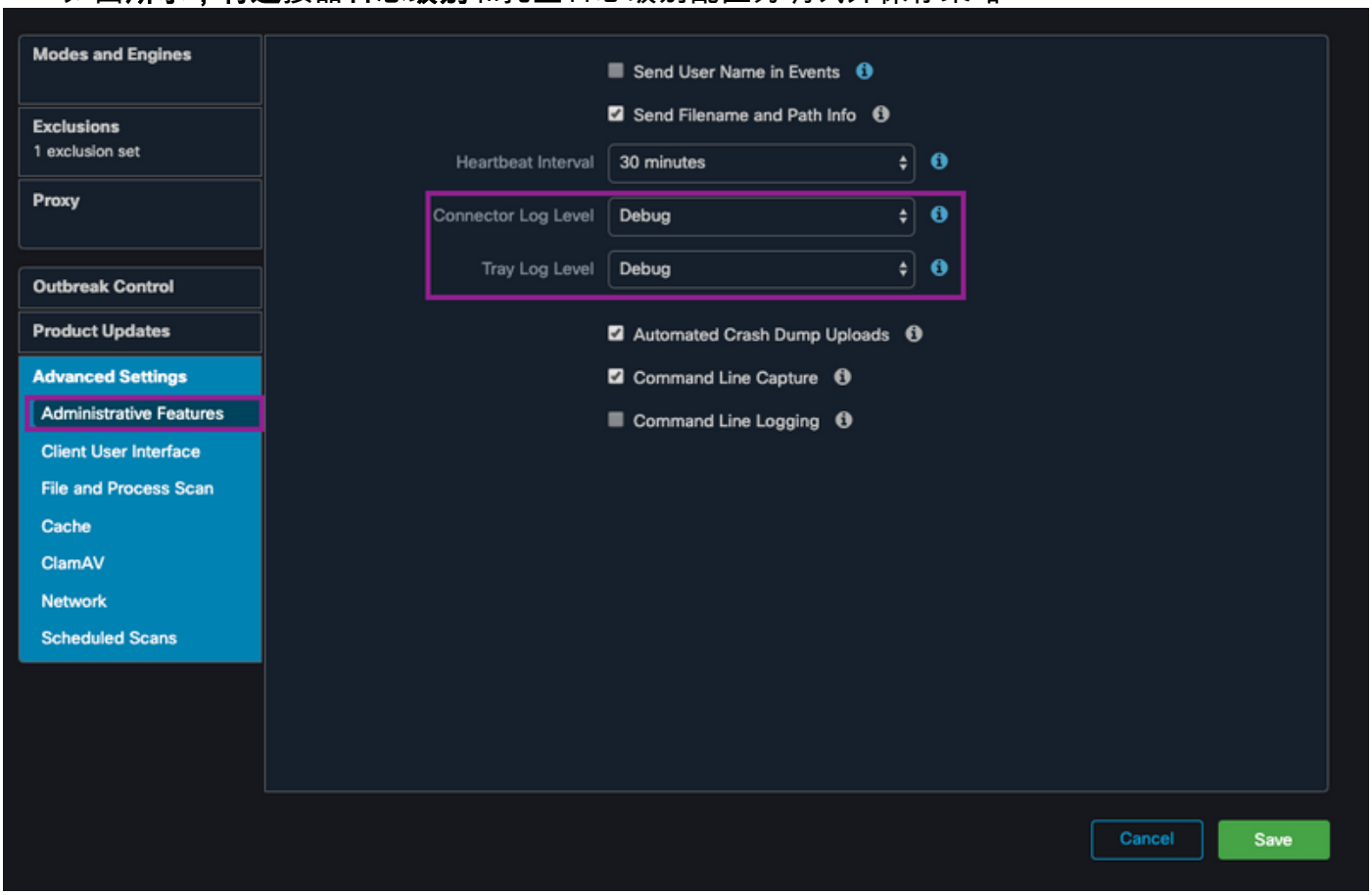
此过程将启用调试日志级别，直到下一个策略心跳间隔。

策略中的调试级别

如果您无权访问终端或无法一致地重现问题，则必须在策略中启用调试日志级别。

要按策略启用调试日志级别，请执行以下操作：

- 导航至**管理>策略**
- 查找策略，然后单击"编辑"
- 导航至高**级设置>管理功能**
- 如图**所示，将连**接器**日志级别**和托盘日志级别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AMP

根据用户指南，防病毒产品必须排除下一个目录以及其中任何文件、目录和可执行文件，以与AMP Connector for MAC兼容，要排除的目录包括：

- **/库/应用支持/面向终端的思科/AMP连接器**
- /opt/cisco/amp

重现问题并收集诊断捆绑包

配置调试级别后，请等待系统上出现“High CPU（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。

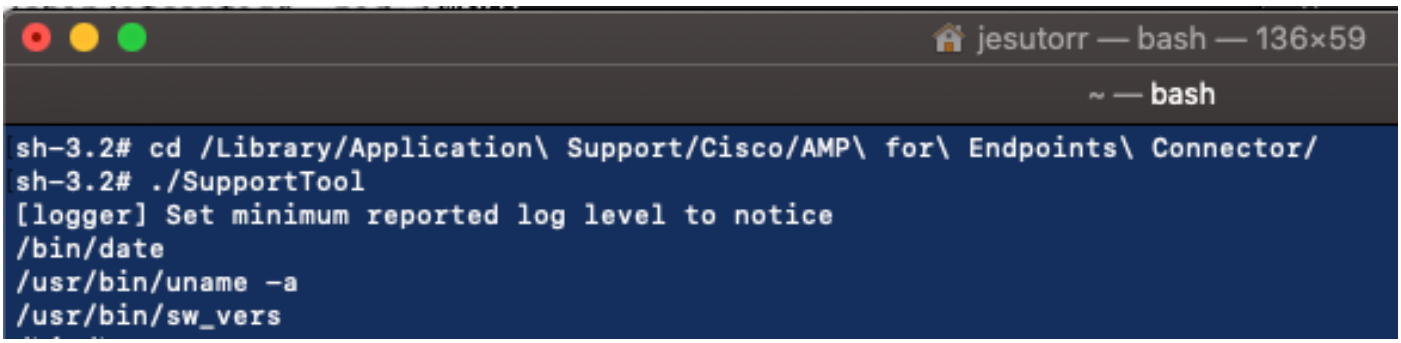
要收集调试捆绑包，请执行以下操作：

- 打开终端。
- 访问超级用户级别，然后导航到**/库/应用支持/面向终端的思科/AMP连接器**:

```
cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
```

- 要运行支持工具，请使用下一个命令：

```
./SupportTool
```

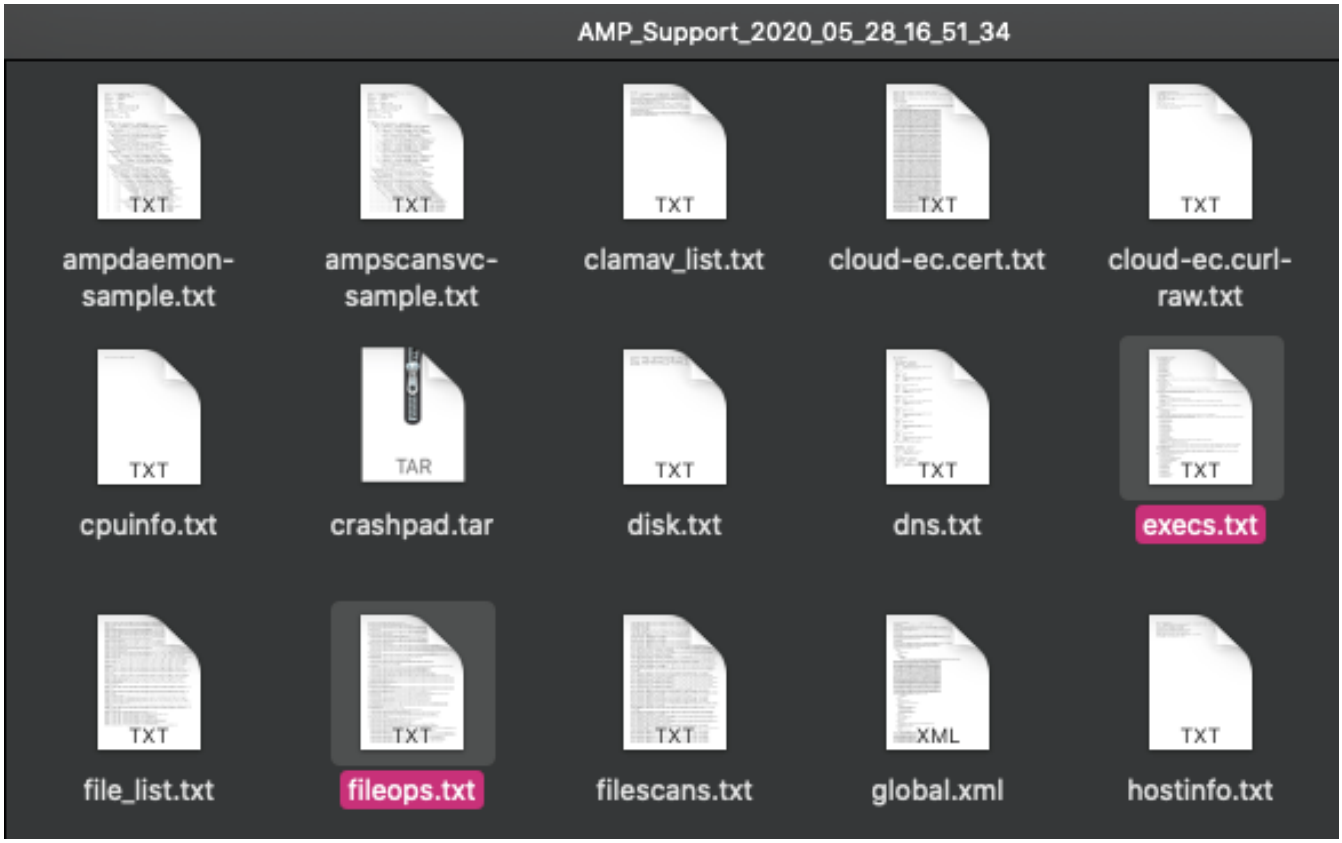


调试捆绑包以.zip文件扩展名保存在Desktop（桌面）文件夹中。

高CPU性能分析

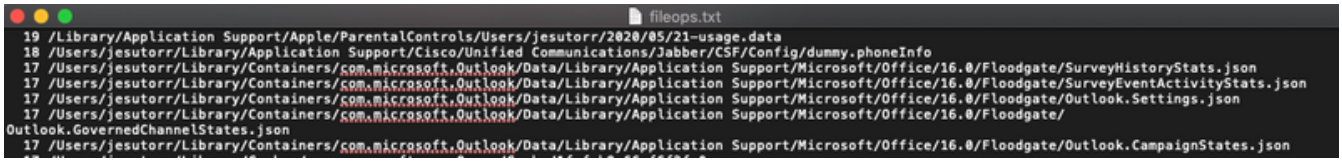
调试诊断捆绑包存储在桌面中，以开始分析：

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



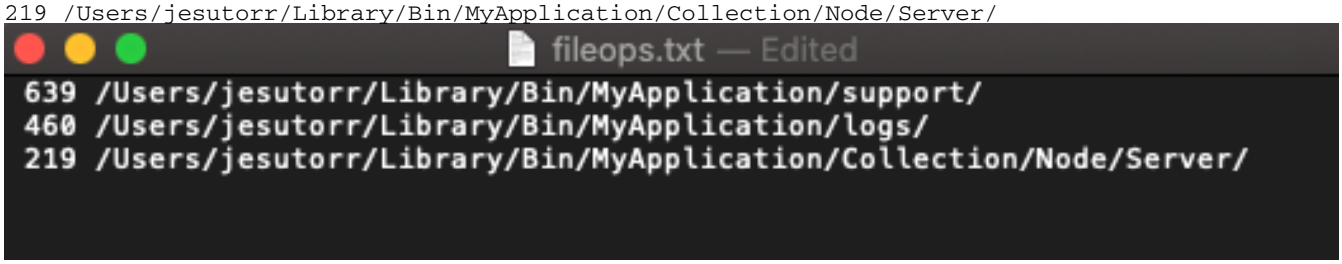
- fileops.txt是排除故障的主要性能工具。它列出连接器运行时终端上当前所有活动操作，如下所示：

<收集捆绑包时在路径上执行的数量扫描> / <扫描路径>

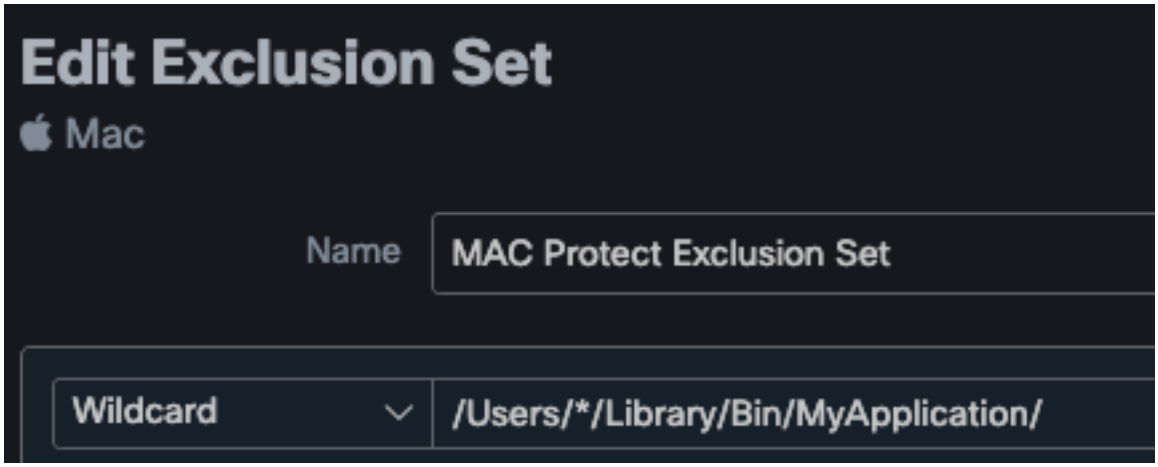


例如，如果您有家庭酿制应用，fileops.txt将显示下一个活动操作：

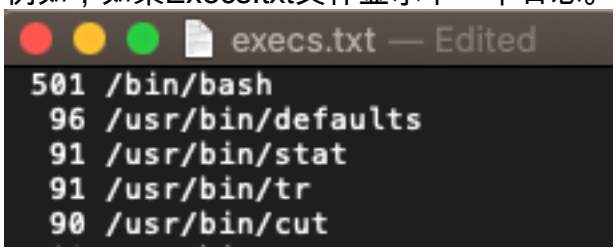
```
639 /Users/jesutorr/Library/Bin/MyApplication/support/

460 /Users/jesutorr/Library/Bin/MyApplication/logs/

219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```



- 确定进程后，可以创建排除项
- 要创建排除项
- 在AMP控制台上，导航至**Management > Exclusions**
- 选择排除集并单击“编辑”
- 可以添加排除项，如图所示



- Execs.txt文件包含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AMP策略中，因为这些是所有进程都使用的二进制文件(/bin)和系统二进制文件(/sbin)，但是，在Execs.text上，可以提供正在运行的主进程。
  例如，如果Execs.txt文件显示下一个日志。



由于家庭酿造应用使用bash，您可以确认该应用是导致CPU使用率较高的原因。

相关信息

- 面向终端的AMP:MacOS和Linux中的进程排除
- 面向终端的 AMP 排除项最佳做法
- 技术支持和文档 - Cisco Systems