安全终端MAC连接器性能调整指南

目录

[简介](#)
[我们为什么要调音？](#)
[调整类型](#)
[1.安装前调整](#)
[2.支持工具调整](#)
[启用调试日志记录](#)

简介

我们为什么要调音？

每次在Mac终端上创建、移动、复制或执行文件时，该文件的事件都会从操作系统发送到安全终端Mac连接器。事件导致连接器分析该文件。分析过程通常涉及对涉及的文件进行散列处理，并通过计算机和云中的不同分析引擎运行该文件。必须认识到，这种散列操作确实会消耗CPU周期。

在给定终端上执行的文件操作和执行的次数越多，连接器散列所需的CPU周期和I/O资源就越多。为减少开销，连接器中添加了多个功能。例如，如果先前已分析过正在创建、移动或复制的文件，连接器将使用缓存结果。但是，在某些事件（例如执行安全至关重要的事件）中，所有事件始终由连接器进行全面分析。这意味着传播多个重复执行子进程的应用程序或进程（特别是在短时间内）可能导致性能问题。查找并排除重复执行子进程且速率高于每秒一次的应用程序，可显着减少CPU使用率并延长笔记本电脑的电池寿命。

文件操作（如创建和移动）通常比执行的影响小，但过多的文件写入和临时文件创建可能会导致类似的问题。频繁写入日志文件的应用程序或生成多个临时文件的应用程序可能导致安全终端消耗大量具有不必要分析的CPU周期，并且可能为安全终端后端造成大量噪音。区分合法应用的噪音部分是维护高效安全终端的非常重要的步骤。

本文档的目的是帮助区分文件操作（创建、移动和复制）和执行，这些操作会对守护程序的性能产生负面影响并浪费CPU周期。识别这些文件和目录路径将允许您创建和维护适合您组织的排除集。

您可以将预先创建的排除列表添加到由思科维护的策略中，以在安全终端连接器与防病毒、安全或其他软件之间提供更好的兼容性。这些列表在控制台的Exclusions页面上作为Cisco维护的Exclusions提供。

调整类型

有三种排除调整选项可用：

1. **预安装调整 - 在安装安全终端Mac连接器之前可以执行此操作。它将让您最清楚地了解计算机中哪些应用和路径最繁忙。但是，这是一个非常嘈杂的过程，需要用户自己进行一些分析和聚合。**
2. **支持工具调整** - 这可以在安装Mac连接器后完成，并且可以在任何终端上执行，无需其他二进制文件。它的回顾性能有限，非常适合于识别麻烦的应用程序。
3. **Procmon调整** - 此过程还要求安装连接器，但也要求使用Procmon二进制文件，这是我们的自

定义调整工具。它实质上是支持工具调整功能的更复杂版本。此方法需要最大的配置量；但是，它确实提供了最佳结果。

1.安装前调整

预安装调整是最基本的调整形式，主要通过终端会话中的命令行完成。

对于来自OS X El Capitan的较新mac，在引导和禁用dtrace保护时，您需要首先引导到恢复模式（命令 — r）：

```
csrutil enable --without dtrace
```

要检查哪些文件执行最普遍，请运行以下命令：

```
$ sudo newproc.d | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

这通常会显示哪些应用程序正在反复运行。许多调配应用程序将在短时间内运行脚本或执行二进制文件，以维护公司软件策略。任何被视为以每秒一次的速率执行或在短突发中多次执行的应用程序，都应被视为排除的好候选项。

要检查哪些文件操作最普遍，请运行以下命令：

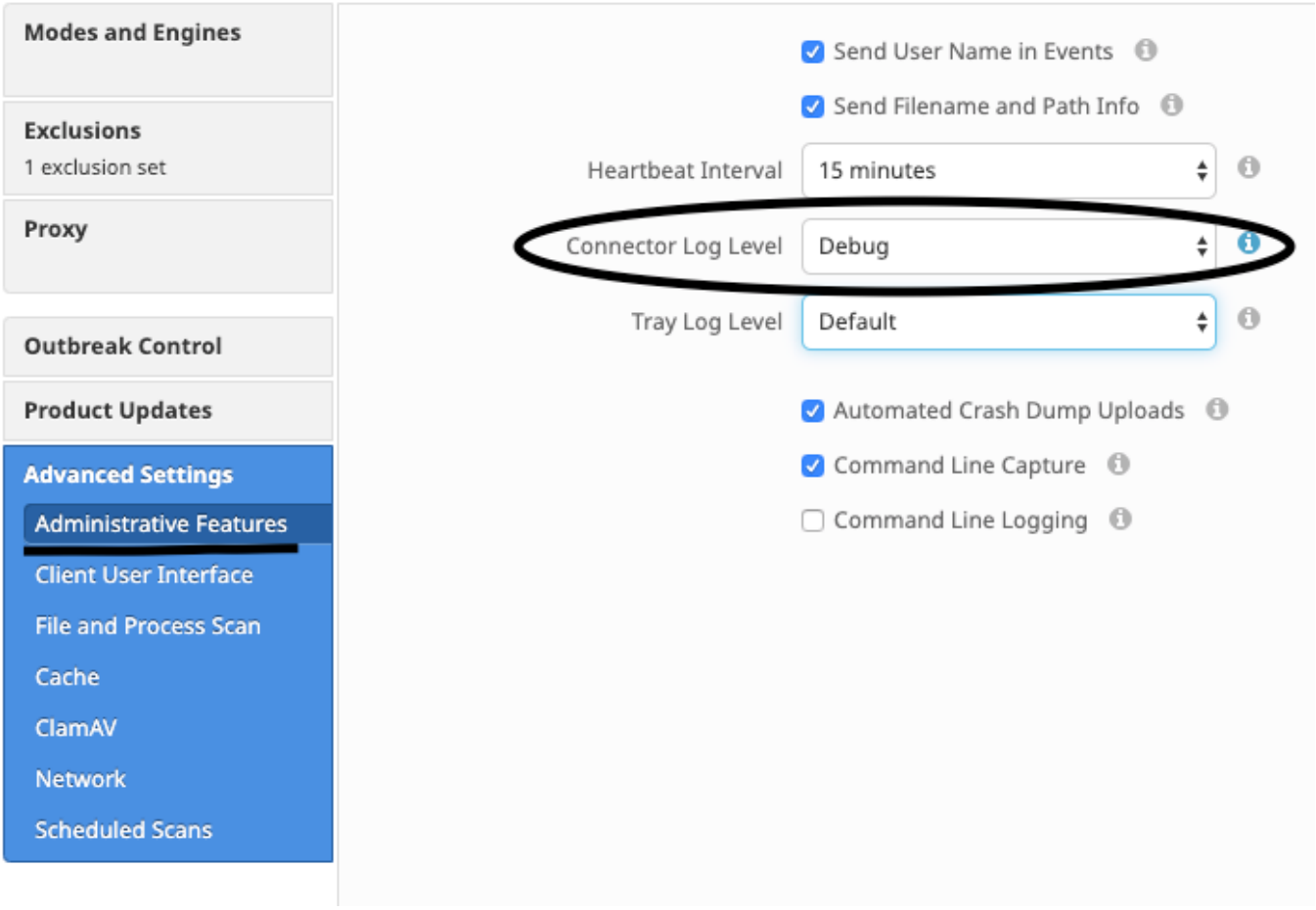
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

您将立即看到哪些文件正在写入到大多数文件。这通常是通过运行应用程序、备份软件复制文件或写入临时文件的电子邮件应用程序写入的日志文件。此外，一个很好的经验法则是，任何具有日志或日志文件扩展名的内容都应被视为适合的排除候选。

2.支持工具 调整

启用调试日志记录

在开始支持文件调整之前，连接器的守护程序需要进入调试日志记录模式。这通过安全终端控制台通过Management -> Policies中连接器的策略设*置来完成*。选择策略，编辑策略，然后转到“高级设置”侧*栏下的*“管理功能”*部分*。将连接*器日志级别*设置更**改为Debug**。



下一步, 保存策略。 保存策略后, 确保同步已优化 到c连接器。 运行c连接器 在此模式下， 至少 在15-20分钟后继续 其余的调谐。

NOTE: 调整完成后，请勿 忘记 更改 *连接器日志级别* 设置返回 **默认** 这样 c连接器 运行 在 它 最高效、 有效模式。

运行支持工具

此方法包括使用支持工具，该工具是安装有安全终端Mac连接器的应用。通过双击/Applications->Cisco Secure Endpoint->Support Tool.app，可以从Applications文件夹访问它。这将生成包含其他诊断文件的完整支持包。

安 替代, 更快, 方法是运行 以下命令行 从 a 终端 会话：

```
sudo/Library/Application Support/Cisco/AMP for Endpoints/SupportTool-x
```

这将导致支持文件的大小大大减少，只包含相关调整文件。

无论您选择哪种运行方式，支持工具都会在桌面上生成一个包含两个优化支持文件的zip文件：fileops.txt和execs.txt。fileops.txt包含计算机上最频繁创建和修改的文件的列表。execs.txt将包含执行频率最高的文件列表。两个列表都按扫描计数排序，这意味着最频繁扫描的路径出现在列表顶部。

使连接器在调试模式下运行15-20分钟，然后运行支持工具。一个好的经验法则是，在此期间平均点击次数达到或超过1000次的任何文件或路径都是应该排除的优秀候选者。

创建路径、通配符、文件名和文件扩展名排除

开始使用路径排除规则的一种方法是从fileops.txt中查找最频繁扫描的文件和文件夹路径，然后考虑为这些路径创建排除规则。下载策略后，监控新的CPU使用率。策略更新后可能需要5到10分钟，您才会注意到CPU使用率下降，因为守护程序可能需要一些时间才能赶上。如果您仍在看到问题，请再次运行该工具以查看您观察到的新路径。

- 一个好的经验法则是，任何具有日志或日志文件扩展名的内容都应被视为合适的排除候选项。

创建进程排除

NOTE: Process Exclusions on Mac can only be implemented for Mach-O files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts) or .app (Application Bundles).
有关流程排除的最佳实践，请参阅：安全终端：MacOS和Linux中的进程排除

一个好的调整模式是首先从execs.txt中识别执行量较大的进程，找到可执行文件的路径，并为此路径创建排除项。但是，有些进程不应包括，这包括：

- 一般公用程序 — 不建议排除一般公用程序(例如：usr/bin/grep)，但不考虑以下因素。 用户可以确定调用该流程的应用程序(例如：查找正在执行grep的父进程)并排除父进程。如果且仅当父进程可以安全地设置为进程排除时，才应执行此操作。如果父排除适用于子代，则父进程中对任何子代的调用也将被排除。可以确定正在执行该进程的用户。（例如：如果用户“root”在大量调用进程，则可以排除该进程，但仅针对指定用户“root”，这将允许安全终端监控非“root”的任何用户对给定进程的执行。)**注意：Process Exclusions是连接器版本1.11.0及更高版本中的新增功能。因此，一般实用程序可用作连接器版本1.10.2及更旧版本中的路径排除。但是，只有在绝对需要取舍性能时，才建议采用此做法。**

查找父进程对于进程排除非常重要。一旦找到进程的父进程和/或用户，用户就可以为特定用户创建排除项并将进程排除项应用到子进程，子进程又将排除本身不能被设置为进程排除项的噪声进程。

确定父进程

1. 从execs.txt中确定高容量流程(例如：/bin/rm）。
2. 从支持包打开ampdaemon.log，解压缩syslog.tar，然后按照路径/Library/Logs/Cisco/ampdaemon.log(仅在afullsupport包中可用，而不是从使用默认选项生成的支持包中可用)。
3. 搜索ampdaemon.log以排除进程。查找显示进程执行的日志行(例如：8月19日09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]:守护程序Rx:VNODE:EXECUTE X:6210 P:3296 PP:3200 U:502 [/bin/rm])。
4. 使用以下方法之一确定父进程： 确定可能遵循要排除的进程路径的父进程路径(例如：[/bin/rm] [*父进程路*径])。如果日志不包括父进程路径，请从日志行的PP：部父进程ID(例如：PP:3200)。
5. 使用父进程路径或父进程ID，重复步骤3和4以确定当前父进程的父进程。继续此流程，直到无法确定父进程或父进程ID = 1(例如：PP:1)。
6. 一旦知道进程树，请查找包含应排除的大多数或所有操作并唯一标识应用程序的程序路径。这可最大限度地减少意外排除其他应用执行的操作的可能性。

确定流程用户

1. 按照上述“识别父进程”的步骤1-3操作。
2. 使用以下方法之一确定进程的用户： 从U：在日志行中查找给定进用户ID(例如：U:502)。在“终端”窗口中，运行以下命令：`dscllist /Users UniqueID | grep #`，其中#是用户ID。您应看到类似于的输出`:Username 502`，其中`Username` 是给定进程的用户。
3. 此用户名可以添加到“用户”类别下的“进程排除”(Process Exclusion)，以缩小排除范围，这对于某些“进程排除”(Process Exclusions)非常重要。 **注意：如果进程的用户是计算机的本地用户，并且此排除必须应用于具有不同本地用户的多台计算机，则必须将“用户”类别留空，以允许进程排除应用于所有用户。**