终端Mac连接器性能调整指南的AMP

目录

简介

编辑：亚历克斯Yakimenko，软件工程师

为什么需要调整？

在文件在Mac终端时候创建，被移动，复制或者被执行该文件的一个事件从操作系统发送到AMP Mac连接器。事件发生连接器被分析的文件。分析进程通常介入切细有问题的文件和运行它通过不同的分析引擎在计算机和在网云。认为是重要的hashing此操作消耗CPU周期。

越多文件操作和执行在一个给的终端、更多CPU周期和I/O资源发生连接器为切细将要求。有被添加到连接器减少开销的几个功能。例如，如果以前分析了创建，被移动或者复制的文件，连接器将使用一种被缓存的结果。然而，一旦某个事件例如安全是至高无上的执行，总是连接器充分地分析所有事件。这意味着传播子进程多重复性执行-的应用程序或进程特别是短期定期能导致性能问题。查找和排除重复地执行子进程在速率更加极大一次每秒能极大减少您的CPU使用情况和增加在膝上型计算机的电池寿命的应用程序。

文件操作例如创建，并且移动比执行通常有较少影响，但是额外的文件写入，并且临时文件创建能导致相似的问题。频繁地写到日志文件的生成多个临时文件的应用程序或者一个造成AMP消耗与多余的分析的很多CPU周期，并且能创建AMP后端的很多噪声。区分合法应用程序的喧闹的部分是在维护一个有生产力和安全终端的一非常重要一步。

本文目的将帮助区分将有对守护程序的性能和废CPU周期的一个负面影响的文件操作(请创建，移动和复制)和执行。识别这些文件和目录路径将允许您创建，并且维护适当的排除为您的组织设置。

您能添加PRE创建的排除列表到是由Cisco维护为终端连接器提供在AMP之间的更加好的兼容性和防病毒、安全或者其它软件的您的策略。这些列表是可用的在排除页在控制台作为Cisco维护的排除。

调整的类型

有排除调整选项联机的三：

1. **事先装配调整–这可以在安装AMP Mac连接器之前执行。它将给您应用程序和路径是最忙碌在您的计算机的最干净的查看。然而，它是一非常喧闹的进程并且要求用户独自地执行一个一般位分析和聚合。**
2. 支持工具**调整**–这可以执行，在Mac连接器在所有终端安装并且可以执行，不用另外的二进制后。它执行一有限查看上一步并且为识别麻烦应用程序是极大的。

3. **Procmon调整**–此进程也要求将安装的连接器，而且要求使用Procmon二进制，我们的自定义调整工具。它根本是调整功能的支持工具的一个更加复杂的版本。此方法要求配置最大的数额;然而，它提供最好的结果。

1.事先装配调整

事先装配调整是多数基本形式调整和主要通过line命令执行在终端会话上。

对于更新的mac，当启动并且禁用dtrace的时，保护从OS x El Capitan您将需要初次启动恢复模式(r命令）：

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

要检查的文件执行最流行请运行以下：

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

这通常将显示哪些应用程序多次运行。许多提供的应用运行脚本或执行二进制在短的间隔将维护公司软件策略。任何应用程序被看到的被执行在速率极大比，一旦一秒钟或者多次执行在短突发数据，应该认为排除的一好候选。

要检查的文件操作最流行，请运行以下命令：

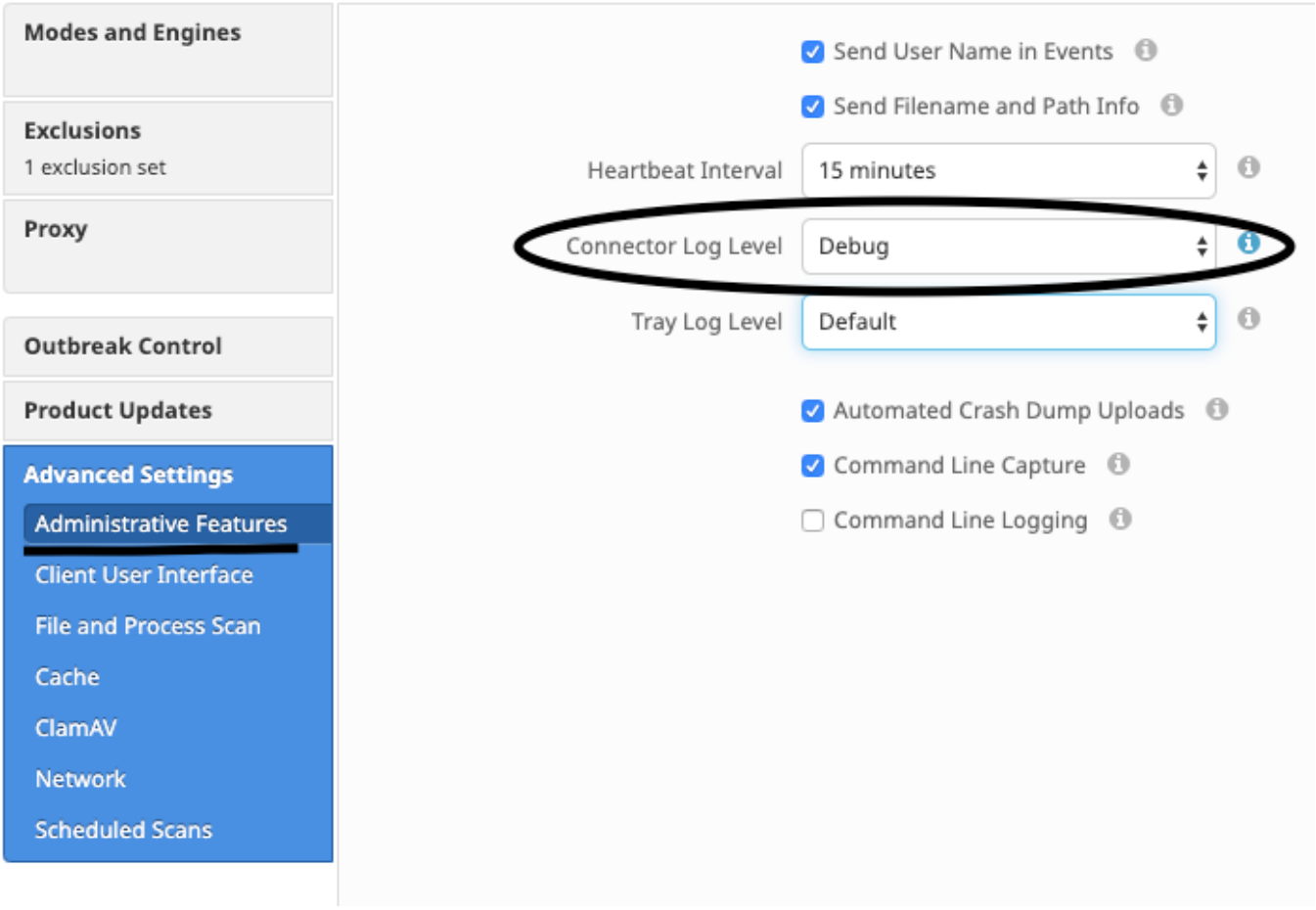
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

您将立即看到哪些文件写入对多数。通常这将是写入对通过运行的日志文件应用程序、写入临时文件的备份软件复制文件的或者电子邮件应用程序。除此之外，一好经验做法是应该认为任何与日志或日志文件扩展一适当的排除候选。

2. 支持工具调整

启用Debug日志

连接器的守护程序需要被放到Debug日志模式在开始支持文件调整前。这通过终端的AMP执行通过连接器的策略设置控制，在*管理- >策略*。选择策略，编辑策略，并且去*管理功能*部分在*先进的设置*侧边栏下。更改*连接器日志级别*设置**调试**。



其次，请保存您的策略。一旦您的策略保存，请保证它同步到连接器。在继续之前运行在此模式的连接器至少15-20分钟以调整的其余。

NOTE:当您调整完成时，请勿忘记更改*连接器日志级别*设置回到默认，以便连接器在其最高效和有效方式运行。

运行支持工具

此方法介入使用支持工具，安装的应用程序以AMP Mac连接器。它可以从应用程序文件夹访问通过双击在/Applications- >Cisco AMP->Support Tool.app。这将生成包含另外的诊断文件的完全支持包。

替代方案和更加快速，方法是从终端会话运行以下line命令：

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

这将导致包含仅相关调整的文件的一个更加小的支持文件。

不管怎样您选择运行它，支持工具将生成在包含两个调整的支持文件的您的桌面的压缩文件：fileops.txt和execs.txt。fileops.txt包含频繁地创建的和被修改的文件的列表在您的计算机的。execs.txt将包含频繁地被执行的文件的列表。两列表由扫描计数排序，含义频繁地被扫描的路径出现在列表顶部。

留下在调试模式的连接器运行15-20分钟内的，然后运行支持工具。一好经验做法是平均为1000命中数的所有文件或路径或更多在那时是好候选将被排除。

创建路径、通配符、文件名和文件扩展排除

一种方式开始与路径排除规则查找从fileops.txt的频繁地被扫描的文件和文件夹路径然后考虑创建那些路径的排除规则。一旦策略下载，请监控新的CPU使用情况。它也许花费5到10分钟，在策略更新后，在您注意CPU使用情况丢弃前，这也许需要守护程序的时间追上。如果仍然看到问题，再请运行工具发现哪些新建的路径您观察。

- 一好经验做法是应该认为任何与日志或日志文件扩展一适当的排除候选。

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).
对于关于进程的最佳实践排除看到：终端的AMP ：在macOS和Linux的进程排除

一个好调整的模式是第一识别与大容积的进程从execs.txt的执行，查找路径对可执行，并且创建此路径的排除。然而，有不应该包括的一些进程，这包括：

- 一般实用工具程序-没有推荐排除一般实用工具程序(前：usr/bin/grep)没有占以下。 用户能确定什么应用程序呼叫进程， (前：查找执行grep)的父进程并且排除父进程。应该执行这，如果，并且，只有当，父进程可以安全做成进程排除。如果parent排除适用于孩子，则对所有孩子的呼叫从父进程也将被排除。执行进程的用户可以确定。(前：如果进程呼叫在大容积由用户“根”，一个能排除进程，但是仅为指定的用户‘根”，这将准许AMP由不是“根”)的所有用户监控一给的进程的执行。**NOTE:**进程排除在连接器版本1.11.0和以上新建。因此，一般实用工具程序可能是使用作为路径排除在连接器版本1.10.2和更加旧有。然而，此实践，当性能折衷方案是绝对必要的时，只推荐。

查找父进程对进程排除是重要。一旦寻找进程的父进程和用户，用户能创建一个特定用户的排除和应用进程排除到子进程，反之将排除喧闹的进程不可能他们自己做成进程排除。

识别父进程

1. 从execs.txt，请识别大容积进程(前：/bin/rm)。
2. 打开从支援程序包的ampdaemon.log，解syslog.tar压缩，然后跟随路径/Library/Logs/Cisco/ampdaemon.log (仅可得到在afullsupport包，不从支援程序包生成与默认选项)。
3. 搜索ampdaemon.log将被排除的进程。查找显示进程执行的记录行(前：八月19 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962] ：守护程序Rx ：VNODE ：执行X:6210 P:3296 PP:3200 U:502 [/bin/rm])。
4. 使用其中一以下方法，识别父进程： 识别可能跟随将被排除的进程路径的父进程路径(前：[/bin/rm] [Parent Process path])。如果日志不包括父进程路径，请识别从父进程ID 记录行的部分(前：PP:3200)。
5. 使用parent路径或父进程ID，请重复步骤3 & 4确定当前父进程的parent。请继续此进程，直到可以确定二者之一没有parent，或者父进程ID= 1 (前：PP:1)。
6. 一旦进程树知道，请寻找报道多数或所有操作应该排除和独特识别应用程序的程序路径。这最小化机会的无心地除了另一应用程序执行的操作。

识别进程的用户

1. 遵从步骤1-3从上面识别父进程。
2. 识别进程的用户使用一个以下方法： 查找给的进程的用户ID从U 在记录行(前：U:502)。从运行以下命令的终端窗口： `dscl/Users UniqueID|grep #`，其中#用户ID。您应该看到输出类似于： `502`，其中是给的进程的用户。
3. 此用户名可以被添加到在用户类别下的进程排除减少排除的范围，对某些进程排除，是重要。 **NOTE:** 如果进程的用户是计算机的本地用户，并且此排除必须适用于用不同的本地用户的多台机器，用户类别必须是允许进程排除的左空白适用于所有用户。