安全終端Mac聯結器效能調整指南

目錄

簡介

為什麼我們需要調諧？

每次在Mac端點上建立、移動、複製或執行檔案時，都會從作業系統向安全端點Mac聯結器傳送該檔案的一個事件。該事件導致聯結器正在分析該檔案。分析過程通常涉及對有關檔案進行雜湊並通過電腦和雲中的不同分析引擎運行該檔案。必須認識到，這種雜湊操作確實會消耗CPU週期。

在給定端點上發生的檔案操作和執行越多，聯結器雜湊所需的CPU週期和I/O資源就越多。為減少額外負荷，聯結器增加了幾個功能。例如，如果正在建立、移動或複製的檔案先前已經過分析，則聯結器將使用快取的結果。但是，對於某些事件（例如執行中，安全性是最高的），聯結器總是完全分析所有事件。這意味著傳播多個子進程的重複執行的應用程式或進程（特別是在短時間內）可能會導致效能問題。查詢並排除重複執行子進程的速度大於每秒一次的應用程式，可以顯著降低CPU使用率，延長筆記型電腦的電池壽命。

檔案操作（如建立和移動）的影響通常比執行小，但過多檔案寫入和臨時檔案建立可能導致類似的問題。頻繁寫入日誌檔案的應用程式或生成多個臨時檔案的應用程式可能會使安全端點佔用大量CPU週期進行不必要的分析，並且可能會為安全端點後端建立大量雜訊。區分合法應用程式的雜訊部分是維護高工作效率且安全的終端的重要步驟。

本文檔的目的是幫助區分檔案操作（建立、移動和複製）和執行，這些操作將對守護程式的效能產生負面影響，並浪費CPU週期。識別這些檔案和目錄路徑將允許您為組織建立和維護適當的排除集。

您可以將預先建立的排除清單新增到思科維護的策略中，以便在安全終端聯結器與防病毒、安全或其他軟體之間提供更好的相容性。這些清單在控制檯的Exclusions頁面上作為Cisco維護的Exclusions提供。

調整型別

有三種排除調整選項可供選擇：

1. **安裝前調整 — 可以在安裝安全終端Mac聯結器之前完成此操作。它將讓您最清楚地瞭解哪些應用程式和路徑是您的電腦上最繁忙的。但是，這是一個非常嘈雜的過程，需要使用者自己執行相當多的分析和彙總。**
2. 支援工具調整 - **可以在安裝Mac聯結器後完成此操作，也可以在任何端點上執行而無需其他二進位制檔案。**它執行有限的回溯功能，非常適合於識別有問題的應用程式。
3. Procmon Tuning — 此過程還需要安裝聯結器，但也需要使用我們自定義的最佳化工具

Procmon二進位制。從本質上講，它是「支援工具調整」功能的更高級版本。此方法需要最大量的配置；但是，它確實提供了最佳結果。

1.安裝前調整

安裝前調整是最基本的調整形式，主要通過終端會話中的命令列完成。

對於來自OS X El Capitan的較新mac，在引導和禁用對dtrace的保護時，您需要先引導到恢復模式（命令 — r）：

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

要檢查哪些檔案執行最常見，請運行以下命令：

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

這通常顯示正在反複運行的應用程式。許多預配應用程式將在短期內運行指令碼或執行二進位制檔案，以維護公司的軟體策略。任何被視為以大於每秒一次的速率執行或短時間突發執行多次的應用程式都應被視為排除的良好候選對象。

要檢查哪些檔案操作最常見，請運行以下命令：

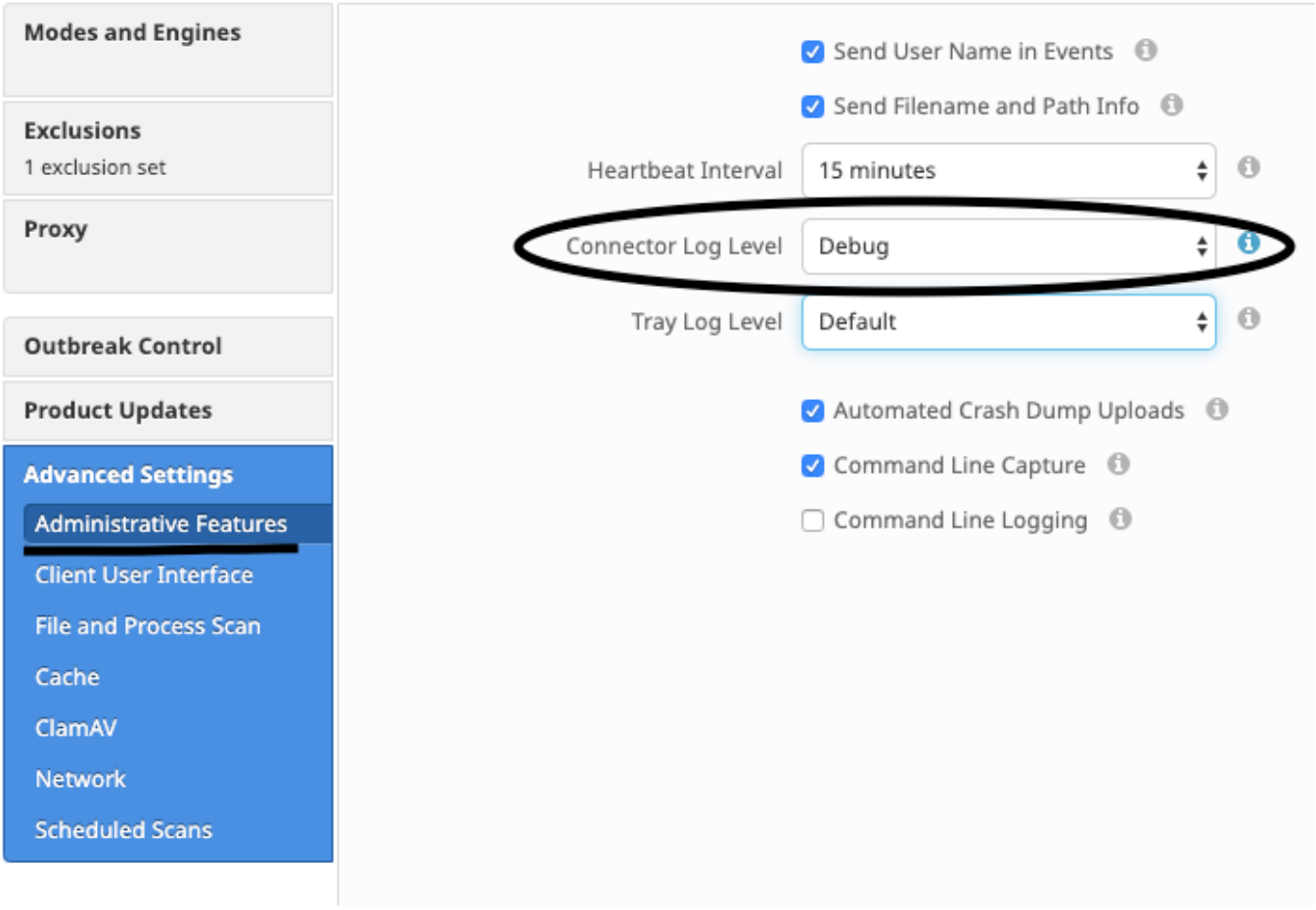
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

您將立即看到寫入的檔案最多。這通常是通過運行應用程式、備份軟體複製檔案或電子郵件應用程式寫入臨時檔案寫入的日誌檔案。除此之外，一個好的經驗法則是，任何帶有日誌或日誌副檔名的東西都應被視為合適的排除候選對象。

2.支援工具 調整

啟用調試日誌記錄

在開始支援檔案調整之前，需要將聯結器的守護程式置於調試日誌記錄模式。這是通過安全終端控制檯通過 *管理* ->策略中的聯結器策略設定完成的。選擇策略，編輯策略，然後轉到*Advanced Settings邊欄下的Administrative Features*部分。將聯結器*日誌級別*設定更改為**調試**。



下一頁中， 儲存策略。 儲存策略後中， 確保已同步已同步 到c聯結器。 運行c聯結器 在此模式下至少 15-20分鐘，然後繼續 其餘調諧.

附註： 完成調整後，不要 忘記了 更改 *聯結器日誌級別* 設定回 **預設** 所以 c聯結器 運行 在 其 最高效且 有效模式。

運行支援工具

此方法涉及使用支援工具，該工具是安裝有Secure Endpoint Mac聯結器的應用程式。通過按兩下/Applications->Cisco Secure Endpoint->Support Tool.app，可以從Applications資料夾訪問它。這將生成包含其他診斷檔案的完整支援包。

安 備選中， 更快中， 方法是運行 以下命令列 自 答 終端 會話：

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

這將產生一個較小的支援檔案，該檔案僅包含相關的最佳化檔案。

無論選擇哪種運行方式，支援工具都會在案頭上生成包含兩個最佳化支援檔案的zip檔案：fileops.txt和execs.txt。fileops.txt包含您電腦上最頻繁建立和修改的檔案清單。execs.txt將包含最頻繁執行的檔案的清單。這兩個清單均按掃描計數排序，表示最頻繁掃描的路徑出現在清單頂部。

使聯結器在調試模式下運行15-20分鐘，然後運行支援工具。經驗法則表明，在該時間內，平均命中次數為1000次或以上的任何檔案或路徑都是要排除的良好候選路徑。

建立路徑、萬用字元、檔名和副檔名排除項

開始使用路徑排除規則的一種方法是，從fileops.txt中查詢最頻繁掃描的檔案和資料夾路徑，然後考慮為這些路徑建立排除規則。下載策略後，監控新的CPU使用情況。在更新策略後可能需要5到10分鐘才能注意到CPU使用率下降，因為守護程式可能需要一段時間才能趕上。如果仍然遇到問題，請再次運行該工具以檢視您觀察到的新路徑。

- 一個好的經驗法則是，任何具有日誌或日誌副檔名的事物都應被視為合適的排除候選對象。

建立進程排除

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).
有關流程排除的最佳實踐，請參閱：安全終端：MacOS和Linux中的進程排除

一個好的最佳化模式是，首先從execs.txt中識別執行量大的進程，找到執行檔的路徑，然後建立此路徑的排除。但是，有些流程不應包括在內，其中包括：

- 常規實用程式 — 建議不要排除常規實用程式(例如：usr/bin/grep)，而不考慮以下情況。 使用者可以確定哪個應用程式正在呼叫該過程(例如：查詢執行grep)的父進程，並排除父進程。若且唯若父進程可以安全轉換為進程排除時，才應執行此操作。如果父項排除應用於子項，則來自父進程的任何子項的呼叫也將被排除。可以確定正在執行此過程的使用者。(例如：如果使用者「root」正在高容量呼叫進程，則可以排除該進程，但只能針對指定的使用者「root」，這將允許安全終端監控非「root」使用者執行給定進程。**注意：進程排除項是聯結器1.11.0版及更新版本中的新增項。因此，通用實用程式可用作聯結器1.10.2及更舊版本中的路徑排除。但是，只有在絕對有必要進行效能折衷時，才建議使用此方法。**

查詢父進程對於進程排除非常重要。一旦找到該進程的父進程和/或使用者，該使用者就可以為特定使用者建立排除，並將該進程排除應用於子進程，而子進程又將排除本身不能成為進程排除的雜訊進程。

標識父進程

1. 從execs.txt中，識別高流量流程(例如：/bin/rm)。
2. 從支援包中開啟ampdaemon.log ，解壓縮syslog.tar ，然後按照路徑/Library/Logs/Cisco/ampdaemon.log(僅在aflsupport包中可用，而不是從使用預設選項生成的支援包中可用)。
3. 搜尋ampdaemon.log以排除進程。查詢顯示流程執行的日誌行(例如：8月19日09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]:守護程式Rx:VNODE：執行X:6210 P:3296 PP:3200 U:502 [/bin/rm])。
4. 使用以下方法之一確定父流程： 標識可能遵循要排除的進程的路徑的父進程路徑(例如：[/bin/rm] [父進*程路徑*])。如果日誌不包括父進程路徑，請從日誌行的PP：部分識別父進程ID(例如：PP:3200)。
5. 使用父路徑或父進程ID，重複步驟3和4以確定當前父進程的父進程。繼續此流程，直到無法確定父進程ID或父進程ID = 1(例如：PP:1)。
6. 知道進程樹後，請查詢包含應排除的大多數或全部操作的程式路徑，並唯一標識應用程式。這將無意中排除由另一個應用程式執行的操作的可能性降至最低。

確定流程使用者

1. 按照上述步驟1-3確定父進程。
2. 使用以下方法之一確定進程的使用者： 從U：在日誌行中查詢給定進程的使用者ID(例如：U:502)。在Terminal（終端）視窗中運行以下命令：`dscl /UniqueID | grep #`，其中#是使用者ID。您應該會看到類似以下的輸出：`Username 502`，其中Username是給定進程的使用者。
3. 此使用者名稱可以新增到User類別下的Process Exclusion中，以縮小排除的範圍，對於某些進程排除而言，此作用非常重要。 **注意：如果進程的使用者是電腦的本地用戶，並且此排除必須應用於具有不同本地使用者的多個電腦，則「使用者」類別必須保留空白以允許「進程排除」應用於所有使用者。**