

分析高CPU的macOS AMP診斷套件

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[疑難排解](#)

[驗證電腦上是否安裝了另一個防病毒軟體](#)

[確定特定應用程式正在使用時的高CPU](#)

[收集用於分析的診斷包](#)

[終端中的調試級別](#)

[AMP命令列介面\(CLI\)中的調試級別](#)

[策略中的調試級別](#)

[從其他防病毒解決方案中排除AMP](#)

[重現問題並收集診斷捆綁包](#)

[高CPU效能分析](#)

[相關資訊](#)

簡介

本文檔介紹從Advanced Malware Protection(AMP)for Endpoints Public Cloud (在macOS裝置上)分析診斷捆綁包以對高CPU使用率進行故障排除的步驟。

作者：Uriel Torres，編輯者：Yeraldin Sanchez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

- AMP控制檯中的基本導航
- MAC終端的導航

採用元件

本文中的資訊係根據以下軟體和硬體版本：

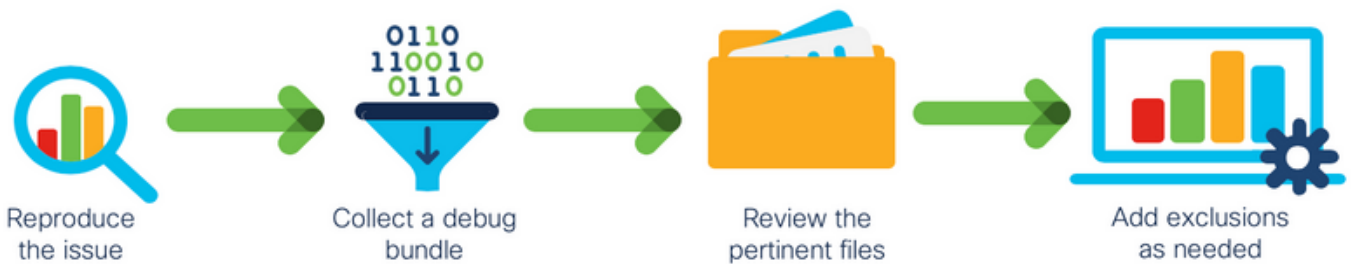
- 適用於終端的AMP主控台5.4.20200512
- macOS Catalina版本10.15.4
- AMP聯結器1.12.3.738

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

AMP聯結器會掃描機器上的所有活動檔案（那些移動、複製和/或修改自己的檔案），除非明確要求不要掃描，否則，如果在聯結器運行時運行過多的進程和操作，將不可避免地帶來效能問題，這會導致CPU使用率高、速度減慢，有時還會導致軟體無法運行或運行緩慢。此外，AMP聯結器可能基於檔案的雲信譽阻止檔案，這有時可能是錯誤的（誤報）。解決這兩個問題的方法是排除這些路徑和進程。

效能問題疑難排解的流程如下圖所示。



疑難排解

本節提供的資訊用於對組態進行疑難排解。

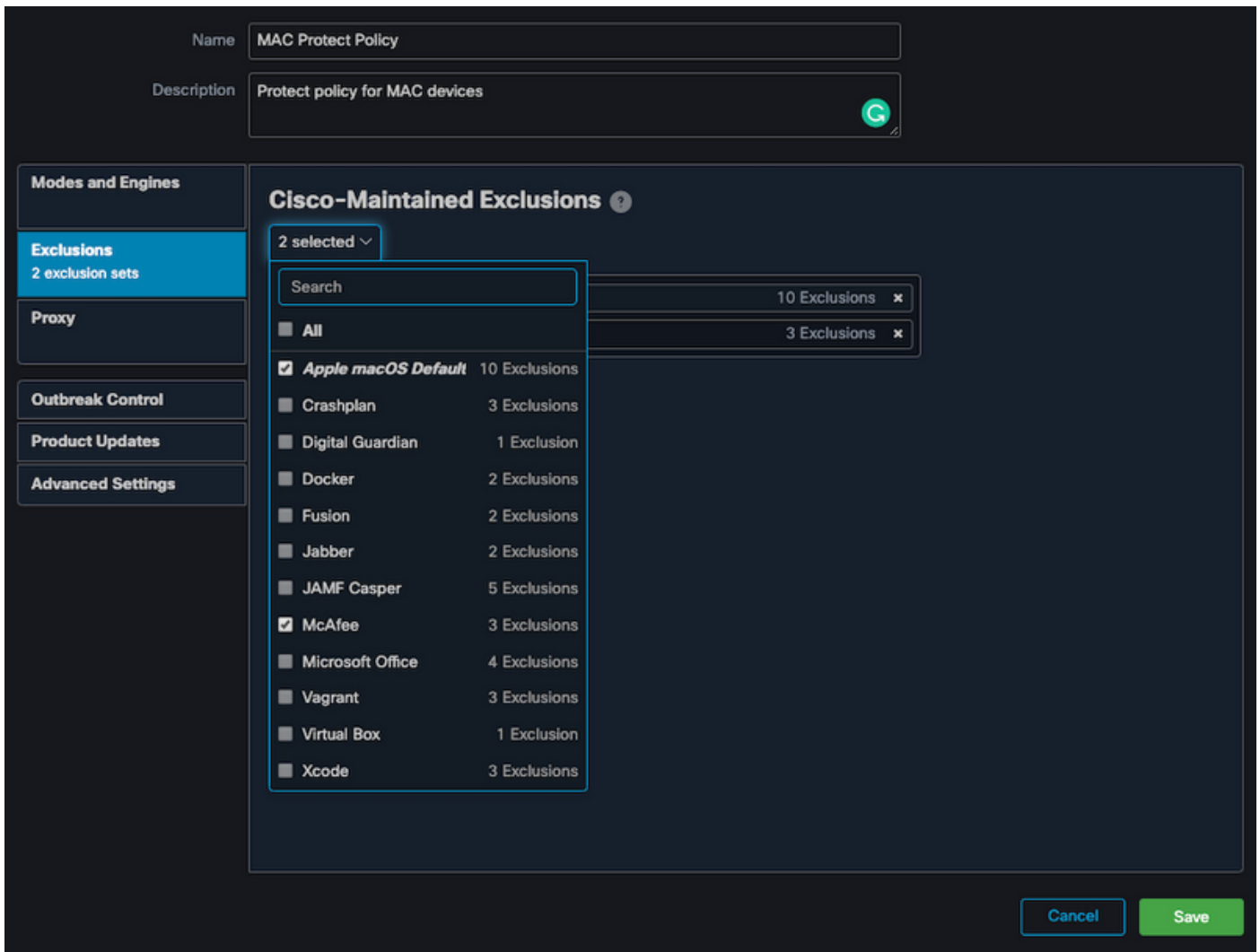
驗證電腦上是否安裝了另一個防病毒軟體

提示：如果使用的軟體包含在清單中，請使用思科維護的排除項。請記住，這些排除項可以新增到應用程式的新版本中。

若要檢視AMP控制檯上思科維護的排除項部分中可用的清單：

- 導航到**管理>策略**。
- 找到策略並按一下**Edit**。
- 在策略的「設定」視窗中，按一下**排除**。

根據電腦上當前安裝的軟體，選擇終端需要使用的策略，然後儲存策略，如下圖所示。



確定特定應用程式正在使用時的高CPU

確定在執行一個或幾個應用程式時問題是否發生（如果您能夠複製問題），將有助於確定流程中潛在的排除項。

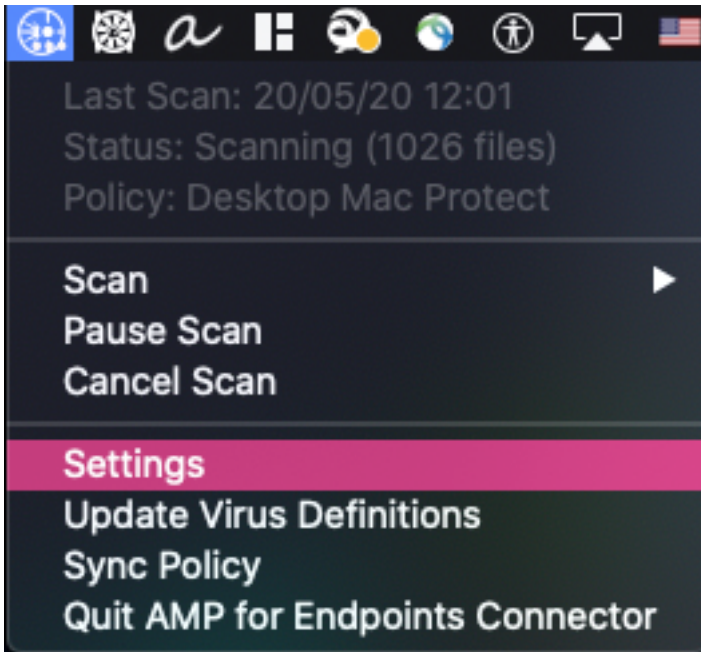
收集用於分析的診斷包

為了收集有用的診斷捆綁包，必須啟用調試日誌級別。

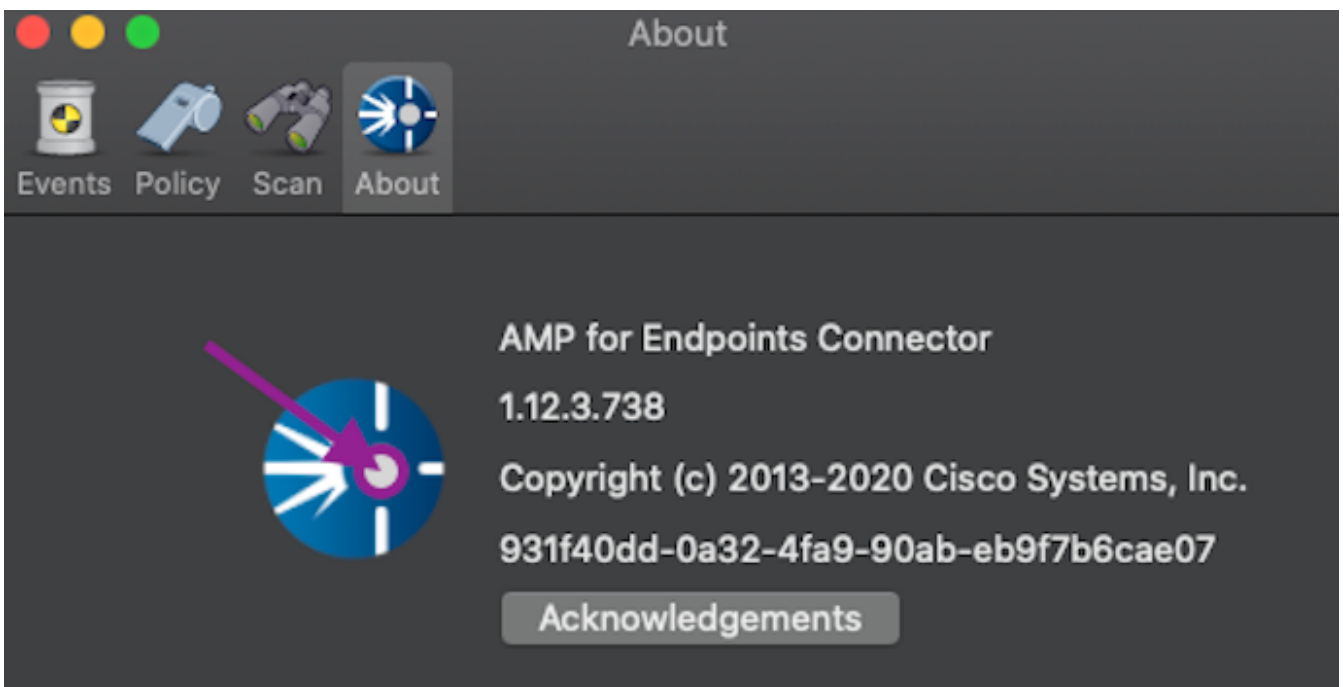
終端中的調試級別

如果您可以複製問題並具有終端訪問許可權，則下面是捕獲診斷捆綁包的最佳步驟。

- 在MAC選單欄中，按一下AMP圖示。
- 導覽至Settings部分，如下圖所示。



- 在「設定」視窗中，導航至關於。
- 若要啟用偵錯模式，請在AMP徽標內按一下，如下圖所示。



彈出視窗表示AMP連結器處於調試模式

此過程會在下一個策略檢測訊號間隔之前啟用調試日誌級別。

AMP命令列介面(CLI)中的調試級別

- 開啟終端
- 導覽至 `/opt/cisco/amp/bin/`
- 運行ampcli:
`./ampcli`
- 在AMP CLI上啟用調試模式：
`ampcli>debuglevel 1`

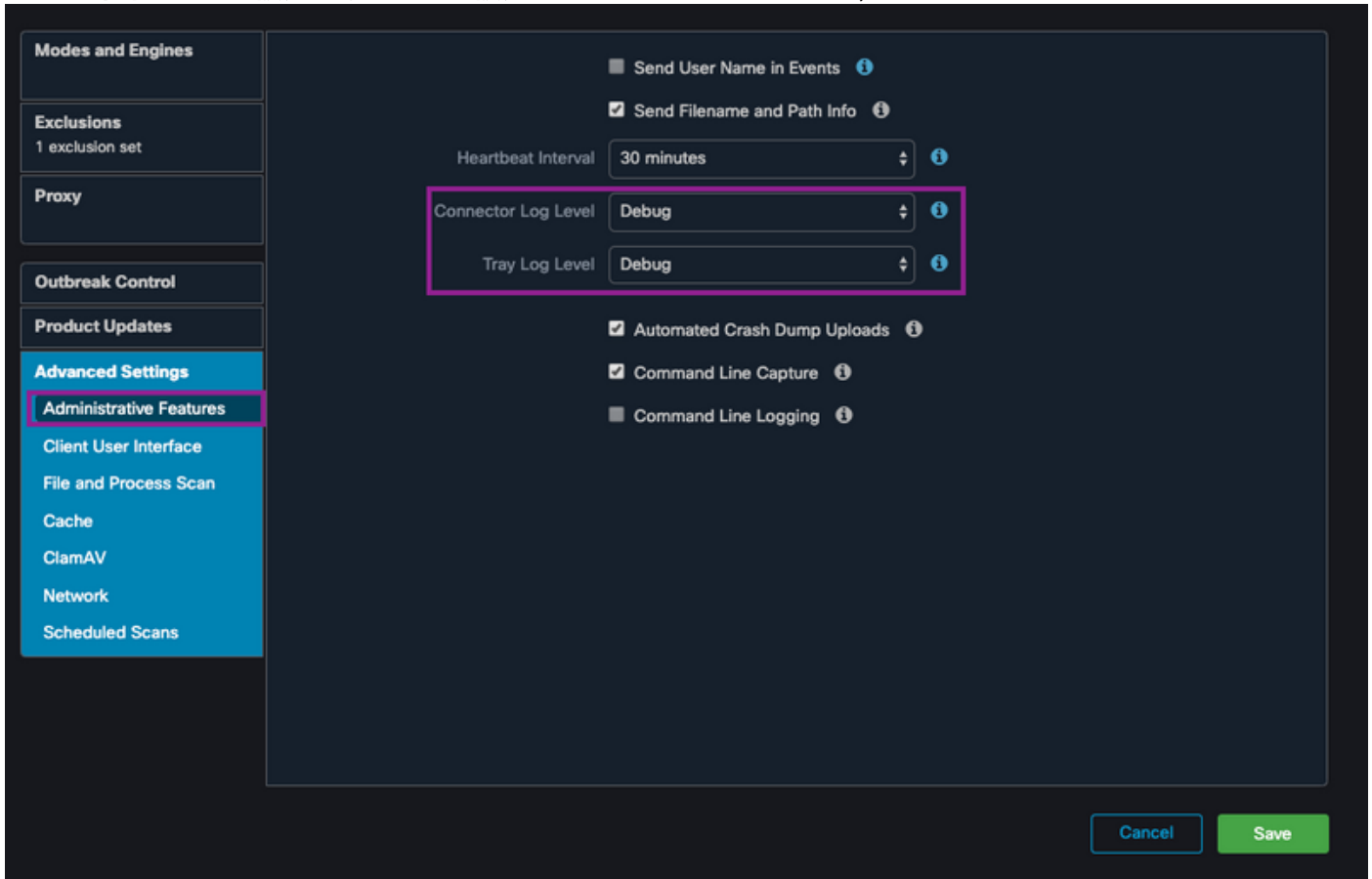
此進程將啟用調試日誌級別，直到下一個策略檢測訊號間隔。

策略中的調試級別

如果您沒有終端訪問許可權或問題無法持續再現，則必須在策略中啟用調試日誌級別。

若要按策略啟用調試日誌級別，請執行以下操作：

- 導航到**管理>策略**
- 查詢策略並按一下**Edit**
- 導覽至**Advanced Settings > Administrative Features**
- 將**聯結器日誌級別**和**托盤日誌級別**配置為調試並儲存策略，如下圖所示



注意：如果從策略啟用調試模式，則所有終端都將收到此配置。

附註：同步終結點的策略以確保調試模式。

從其他防病毒解決方案中排除AMP

根據使用手冊，防病毒產品必須排除下一個目錄及其中的任何檔案、目錄和執行檔，才能與AMP Connector for MAC相容，排除的目錄如下：

- /Library/Application Support/Cisco/AMP for Endpoints**聯結器**
- /opt/cisco/amp

重現問題並收集診斷捆綁包

設定偵錯層級後，請等待系統中發生高CPU狀態或手動重現先前識別的條件，然後收集診斷套件組合。

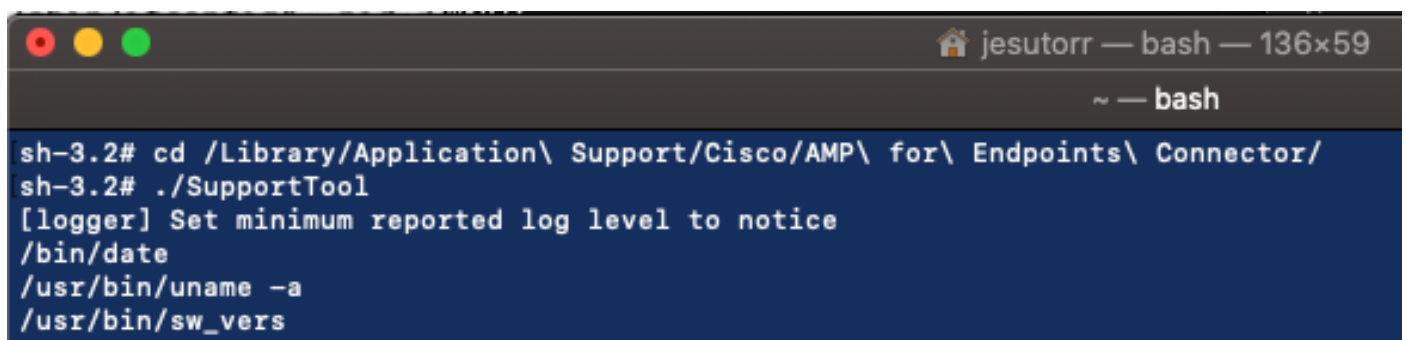
若要收集偵錯套件組合：

- 開啟終端。
- 訪問超級使用者級別，然後導航到/庫/應用支援/思科/AMP端點連結器:

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

- 若要運行支援工具，請使用以下命令：

```
./SupportTool
```



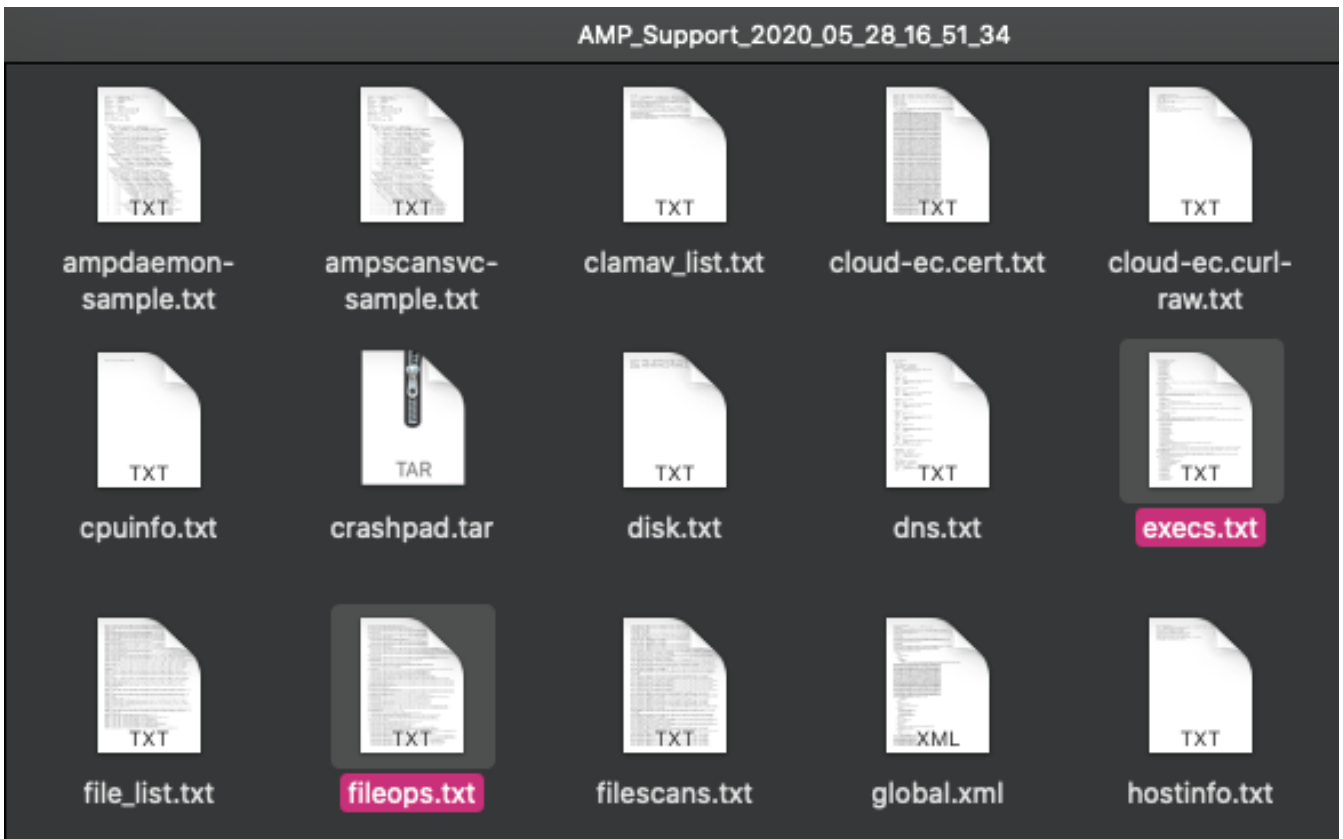
```
jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers
```

debug bundle將以.zip副檔名儲存在Desktop資料夾中。

高CPU效能分析

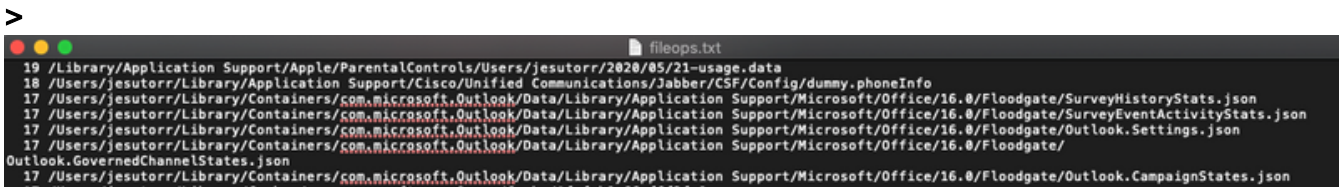
debug diagnostic bundle儲存在案頭中，以開始分析：

- 解壓診斷捆綁包
- 有2個檔案要檢視 檔案操作：fileops.txt檔案執行：execs.txt



- fileops.txt用作故障排除的主要效能工具。它列出了連結器運行時終端上當前所有活動的操作，如下所示：

<收集捆綁包時對路徑執行的次數掃描> /<路徑掃描

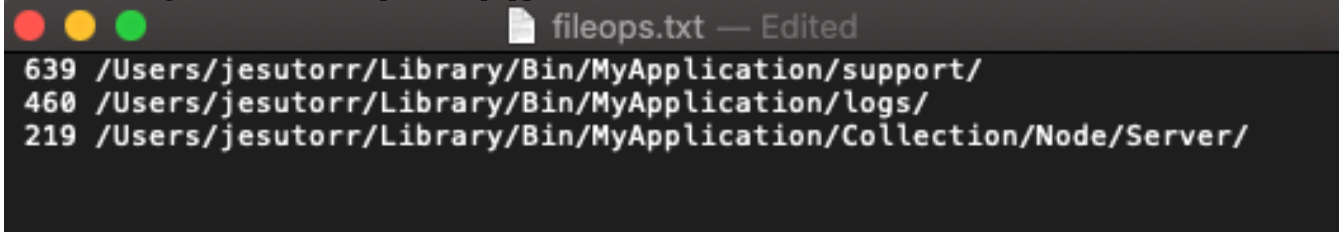


例如，如果您有一個家庭應用程式，fileops.txt將顯示下一個活動操作：

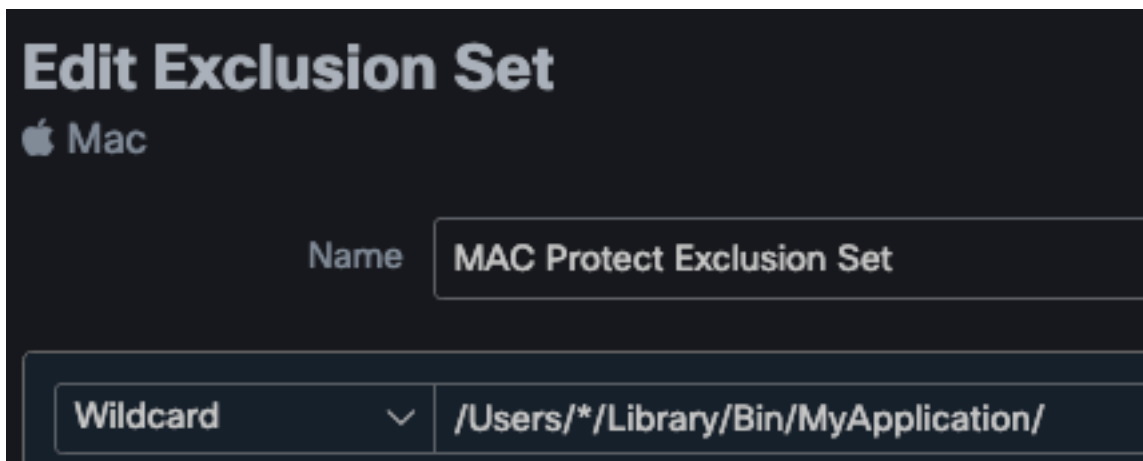
```
639 /Users/jesutorr/Library/Bin/MyApplication/support/
```

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

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



- 識別進程後，即可建立排除
- 要建立排除
- 在AMP控制檯上，導航到**管理>排除**
- 選擇排除集並按一下**Edit**
- 您可以新增排除，如下圖所示



- Execs.txt檔案包含連結器收集軟體包時運行的進程使用的所有命令。此處列出的路徑不能排除在AMP策略中，因為它們是所有進程使用的二進位制檔案(/bin)和系統二進位制檔案(/sbin)，但是，在Execs.txt上，它們可以提供正在運行的主進程。

例如，如果Execs.txt檔案顯示下一個日誌。

```
execs.txt — Edited
501 /bin/bash
96 /usr/bin/defaults
91 /usr/bin/stat
91 /usr/bin/tr
90 /usr/bin/cut
```

由於homebrew應用程式使用bash，因此您可以確

認該應用程式是CPU使用率較高的原因。

相關資訊

- [AMP端點版：MacOS和Linux中的進程排除](#)
- [AMP 終端版排除項目的最佳作法](#)
- [技術支援與文件 - Cisco Systems](#)