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 <u>策略中的調試級</u>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。

Name	MAC Protect Policy			
Description	Protect policy for MAC devices		C	
Modes and Engines	Cisco-Maintained Exc	clusion	s 😧	
Exclusions	2 selected ~			
2 exclusion sets	Search		10 Exclusions x	
Proxy	I All		3 Exclusions ×	
	Apple macOS Default 10 E	xclusions		
Outbreak Control	Crashplan 3 E	xclusions		
Product Updates	Digital Guardian 1	Exclusion		
Advanced Settings	Docker 2 E	xclusions		
	Fusion 2 E	xclusions		
	Jabber 2 E	xclusions		
	JAMF Casper 5 E	xclusions		
	McAfee 3 E	xclusions		
	Microsoft Office 4 E	xclusions		
	Vagrant 3 E	xclusions		
	Virtual Box 1	Exclusion		
	Xcode 3 E	xclusions		
				Cancel Save

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。

 Weight Design of the second status in the second status ini
Scan Pause Scan Cancel Scan
Settings
Update Virus Definitions
Sync Policy
Quit AMP for Endpoints Connector

- •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聯結器處於調試模式

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

Modes and Engines		Send User Name in Events ()				
Exclusions		Send Filename and Path Info 0				
1 exclusion set	Heartbeat Interval	30 minutes	\$	0		
Proxy	Connector Log Level	Debug	¢	0		
Outbreak Control	Tray Log Level	Debug	¢	0		
Product Updates		Automated Crash Dump Uploads	0			
Advanced Settings		Command Line Capture 0				
Administrative Features		Command Line Logging 🚯				
Client User Interface						
File and Process Scan						
Cache						
ClamAV						
Scheduled Scans						
					Cancel	Save

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端點聯結器:

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



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

	AMP_Support_2020_05_28_16_51_34				
ne me se me """"""""""""""""""""""""""""""""""""	TXT	TXT	TXT	TXT	
ampdaemon- sample.txt	ampscansvc- sample.txt	clamav_list.txt	cloud-ec.cert.txt	cloud-ec.curl- raw.txt	
тхт	TAR	TXT	Para- Para-		
cpuinfo.txt	crashpad.tar	disk.txt	dns.txt	execs.txt	
TxT file_list.txt	TXT fileops.txt	TxT filescans.txt	global.xml	TXT hostinfo.txt	

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

<收集捆绑包時對路徑執行的次數掃描> /<路徑掃描

>
😑 🕒 📄 fileops.txt
<pre>19 /Library/Application Support/Apple/ParentalControls/Users/jesutorr/2020/05/21-usage.data 18 /Users/jesutorr/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/Config/dummy.phoneInfo 17 /Users/jesutorr/Library/Containers/<u>com.microsoft,Outlook</u>/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft,Outlook</u>/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft,Outlook</u>/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyEventActivityStats.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft.00</u>tato/Library/Application Support/Microsoft/Office/16.0/Floodgate/Utlook.Settings.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft.00</u>tato/Library/Application Support/Microsoft/Office/16.0/Floodgate/Utlook.Settings.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft.00</u>tato/Library/Application Support/Microsoft/Office/16.0/Floodgate/Utlook.Settings.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft.00</u>tato/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json 17 /Users/jesutorr/Library/Containers/<u>com.microsoft.00</u>tato/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json</pre>
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/
🛑 😑 🧶 📄 fileops.txt — Edited
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

Edit Excl Mac	usion	Set	
	Name	MAC Protect Exclusion Set	
Wildcard	~	/Users/*/Library/Bin/MyApplication/	
• Execs.txt檔案包含職 在AMP策略中,因為 是,在Execs.text上	₩結器收集 協它們是所 ,它們可以	軟體包時運行的進程使用的所有命令。此處列出的路 有進程使用的二進位制檔案(/bin)和系統二進位制檔緊 \提供正在運行的主進程。	·徑不能排除 髹(/sbin),但

例如,如果Execs.txt檔案顯示下一個日誌。



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