# 分析高CPU的AMP診斷套件

# 目錄

簡介 必要條件 需求 採用元件 疑難排解 驗證電腦上是否安裝了另一個防病毒軟體 確定在使用特定應用程式時是否發生高CPU 收集診斷套件進行分析 啟用調試日誌級別 終結點中的調試級別 策略中的調試級別 重現問題並收集診斷捆綁包 進行分析 Diag\_Analyzer.exe Amphandlecount.ps1 調整排除 將套件組合提交給TAC進行分析

# 簡介

本文檔介紹從Windows裝置上的終端公共雲高級惡意軟體防護(AMP)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:Luis Velazquez,編輯者:Yeraldin Sánchez,思科TAC工程師。

# 必要條件

#### 需求

思科建議您瞭解以下主題:

•訪問AMP控制檯

#### 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5.4.20200204
- Windows作業系統裝置

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。

本節提供的資訊可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

如果安裝了另一個AV(防病毒),請確保在策略配置中排除AV的主進程

**提示:**如果使用的軟體包含在清單中,則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Cisco維護的排除區段中可用的清單,請導覽至**Management > Policies > Edit >** Exclusions > Cisco維護的排除區。

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。

Nama	haivelaz-W7_Policy				
Decodering					
Discipion					
	r			æ	
and Fasher		2			
and Engines	Cisco-Maintal of Exc	clusions			
dusions	5 selected ¥				
schedon sets	Bearch		^	3 Exclusions	
avy .				11 Exclusions	
	Attris by Symantec	3 Exclusions		1 Exclusion	
tbreak Control	Appsense	6 Exclusions		29 Exclusions	
duct Updates	- AVAST	3 Exclusions		3 Exclusions *	
unored Settings	Avira	3 Exclusions			
unced countys	Citrix AppENA	2 Exclusions			
	Citrix Cloud Connector	3 Exclusions			
3	Citrix EdgeSight Server	3 Exclusions		85 Exclusions	
_	Citrix ICA Client	5 Exclusions			
	Citrix Provisioning Server	18 Exclusions			
	Citrix XenApp v6.5 and 7	7 Exclusions			
	Crashplan	3 Exclusions			
	Diebold Warsaw	10 Exclusions			
	Domain Controller	19 Exclusions			<u> </u>
	Hyper-V	17 Exclusions			

確定在使用特定應用程式時是否發生高CPU

確定在執行一個或幾個應用程式時問題是否發生(如果您能夠複製此問題),將有助於確定潛在的 例外情況。

#### 收集診斷套件進行分析

為了收集有用的診斷捆綁包,必須啟用調試日誌級別。

#### 終結點中的調試級別

如果您可以複製問題並訪問終端,則下面是捕獲診斷捆綁包的最佳步驟:

- 1. 開啟AMP GUI
- 2. 導航到**設定**
- 3. 滾動到AMP GUI底部,然後開啟Cisco AMP聯結器設定
- 4. 按一下Enable Debug Logging
- 5. 調試日誌記錄狀態必須更改為已啟動。此過程將啟用調試級別,直到下一個策略檢測訊號(預 設值為15分鐘)

^[A-Za-z]:\\/Wildcard/A ^[A-Za-z]:\\Wildcard\a ^[A-Za-z]:\\pagefile\.sy	II/Drive I∖ drives s
Scan Settings	•
Notification Settings	<b>V</b>
Proxy Settings	<b>V</b>
Cisco AMP Connector Settings	
Service Status:	Started
Password:	
Stop Service	
Debug Logging Status:	Stopped
Enable Debug Logging	

#### 策略中的調試級別

如果您無權訪問終結點或無法一致重現問題,則必須在策略中啟用調試日誌級別。

若要按原則啟用偵錯日誌級別,請導覽至Management > Policies > Edit > Advanced Settings > Connector Log Level and Management > Policies > Edit > Advanced Settings > Tray Log Level,然後選擇Debug並儲存策略,如下圖所示。

<	Edit Policy					
	Name	luivelaz-W7_Policy				
	Description			4		
	Modes and Engines		Send User Name in Events			
	Exclusions 6 exclusion sets		Send Filename and Path Info 0			
	Proxy	2 Connector Log Level	Debug v	0		
	Outbreak Control	Tray Log Level	Debug v	0		
	Product Updates		Enable Connector Protection			
	Administrative Features	Connector Protection Password		0		
	Client User Interface File and Process Scan		Automated Crash Dump Uploads			
	Cache Endpoint Isolation		Command Line Logging 0			
	Orbital Engines					
	Network Scheduled Scars					
	Identity Persistence					
					Cancel	Save

注意:如果從策略啟用調試模式,則所有終端都會收到此更改。

附註:同步終結點的策略以確保應用調試級別或等待心跳間隔(預設情況下為15分鐘)。

#### 重現問題並收集診斷捆綁包

當配置調試級別時,請等待系統發生「高CPU」狀態或手動重現之前確定的條件,然後收集診斷捆 綁包。

若要收集套件組合,請導覽至C:\Program Files\Cisco\AMP\X.X.X(其中X.X.X是系統上安裝的最新 AMP版本),然後執行應用程式ipsupporttool.exe,此程式會在名為 CiscoAMP\_Support\_Tool\_%date%。7z的案頭上建立.7z檔案

**附註**:聯結器版本6.2.3及更高版本可以遠端請求捆綁包,導航到**管理>電腦**,展開終端記錄並 使用Diagnose選項。

附註:診斷套件組合也可以透過以下命令在CMD提示中執行:"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe"或"C:\Program Files\Cisco\AMP\X.X.X\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To",其中X.X.X是安裝的 最新AMP版本,可以使用第二個命令來選擇。7z檔案的輸出資料夾。

## 進行分析

分析診斷檔案的方法有兩種:

- Diag\_Analyzer.exe
- Amphandlecount.ps1

#### Diag\_Analyzer.exe

步驟1.在此處下載應用程式。

步驟2.在GitHub頁面中,有一個自述檔案,其中包含使用方法的進一步說明。

步驟4.執行應用程式 Diag\_Analyzer.exe。



步驟5.在新提示符中,確認是否要使用Y或N獲取策略中的排除項。

步驟6.指令碼結果包含:

- 前10個流程
- 前10個檔案
- 前10個擴展
- 前100個路徑
- 所有檔案

**附註**:Diag\_Analyzer.exe會檢查所提供的AMP診斷檔案中的sfc.exe.log檔案。然後,使用診 斷檔名建立一個新目錄,並將日誌檔案儲存在。7z之外,儲存在診斷的父目錄中,在此之後 ,它將分析日誌並確定前10個進程、檔案、副檔名和路徑,最後,它會將資訊列印到螢幕上 ,並將資訊列印到{Diagnostic}-summary.txt檔案中。

#### Amphandlecount.ps1

步驟1.從Review Scanned Files from AMP的社群底部下載指令碼amphandlecounts.txt。

步驟2.要在Windows中運行指令碼,請將其重新命名為amphandlecount.ps1。

步驟3.為方便起見,將amphandlecount.ps1檔案複製到他自己的資料夾中。



步驟4.解壓縮CiscoAMP\_Support\_Tool\_%date%。7z檔案,並識別路徑上的sfc.log檔案 CiscoAMP\_Support\_Tool\_2019\_06\_13\_18\_26\_37\Program Files\Cisco\AMP\X.X.X。

	Name	Date modified	Туре	Size		
	ConnectivityTool.exe.log	18/06/2019 01:46	LOG File	32 KB		
*	🧧 globalaml	08/06/2019 11:23	XML File	24 KB	_	
. *	📕 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB		
1	5 sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB		
ent ⊭	5 sfc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB		
	5 sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB		
	sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB		
	5 sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB		
	sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB		
	sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB		
	sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB		
	sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB		

步驟5.將sfc.log的檔案複製到amphandlecount.ps1檔案夾。

	Name	Date modified	Туре	Size
	ConnectivityTool.exe.log	18/06/2019 01:46	LOG File	32 KB
<i>*</i>	Imx.ladolp	08/06/2019 11:23	XML File	24 KB
*	🧧 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB
*	sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB
A.	5fc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB
	sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB
	sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB
	sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB
	sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB
	sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB
	sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB
	5 sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB

步驟6.使用PowerShell運行**amphandlecount.ps1**,然後開啟一個視窗,根據終端上的執行策略可以 請求運行許可權。

,p

**提示**:要更改執行策略,請開啟Windows PowerShell並使用以下命令: 將策略設定為允許不受限制的執行訪問 — Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Unrestricted 設定策略以限制執行訪問 — Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted

步驟7.完成PowerShell後(可能需要一些時間,具體取決於資料夾中的sfc.log數量),將在資料夾 上建立四個檔案:

- data.csv
- results.txt
- sorted\_results.txt
- terms.txt

	> Thi	is PC > Documents > Review Bundle			~ Ö	Search Review Bundle	P
		Name	Date modified	Туре	Size		
tss		amphandlecount.ps1	26/04/2019 09:44 a	Windows PowerS	3 KB		
nts	×	🕒 data.csv	22/06/2019 03:28	Microsoft Excel C	754 KB		
ds	R	🗾 results.txt	22/06/2019 03:28	TXT File	3 KB		
	R	🗾 sfc.exe.log	18/06/2019 01:46	LOG File	46,634 KB		
		sfc.exe_20190614_171821.log	14/06/2019 05:18	LOG File	6,912 KB		
		5fc.exe_20190616_123123.log	16/06/2019 12:31	LOG File	51,201 KB		
indle		sfc.exe_20190616_131825.log	16/06/2019 01:18	LOG File	51,201 KB		
		sfc.exe_20190616_134500.log	16/06/2019 01:45	LOG File	51,201 KB		
		sfc.exe_20190616_140234.log	16/06/2019 02:02	LOG File	51,201 KB		
		sfc.exe_20190616_150139.log	16/06/2019 03:01	LOG File	51,201 KB		
		sfc.exe_20190618_133822.log	18/06/2019 01:38	LOG File	51,201 KB		
		sfc.exe_20190618_134032.log	18/06/2019 01:40	LOG File	51,201 KB		
s		sfc.exe_20190618_134240.log	18/06/2019 01:42	LOG File	51,201 KB		
	_	sorted_results.bt	22/06/2019 03:28	TXT File	3 KB		
ts		📕 terms.txt	22/06/2019 03:28	TXT File	3 KB		
de.							

步驟8.這4個新檔案包含分析結果:

- data.csv:包含已掃描檔案的完整路徑以及建立/修改/移動檔案的父進程
- results.txt:包含AMP掃描的進程清單
- sorted\_results.txt:包含AMP掃描的進程清單以及掃描最多的進程
- terms.txt:包含AMP掃描的進程的名稱

步驟9.從data.csv中的sorted\_results.txt中篩選具有高計數的進程名稱,您可以用其完整路徑標識父 進程,然後繼續向自定義清單中的策略新增排除項(如果受信任)。

要查詢的進程:

- 1. 控制+F在「data.csv」和搜尋
- 2. AMP掃描的檔案的路徑
- 3. 複製/移動/修改檔案的父進程的路徑

**附註**:附註:通常排除為「Process:正在獲取掃描的父進程的「檔案掃描」和「子進程包括」

4>	1	sorted_results.txt •	A			A PanelInstallerTemp\nvmobESN.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-
1		1075 setup.exe		3	_	
2		442 firefox.exe				H J K L M N O P O R S T
3		243 container.exe				
4		243 Container.exe	1	Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPanelInstallerTemp\nvmob	DESM.	.cnm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCpISetupInt.exe
5		243 container.exe	2	Jun 18 13:42:40,C:\Temp\NVIDIA\ControlPaneIInstallerTemp\nvmob	DESN.	.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
6		243 Container.exe	3	lun 18 12:42:40 C-\Tomn\N\VIDIA\ControlDanolinctallorTomn\numoh	EIN.C	chm.C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AF9-B7D4-551FE0F3AFF7}\NvCplSetupInt.exe
7		243 container.exe		Find and Replace 2 X	< 1	
8		243 Container.exe	4		- a.	.cnm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NVCpISetupInt.exe
9		243 container.exe	5		В.	.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
10		120 NvCplSetupInt.exe	6	Find Reglace	N	.chm.c:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
11		54 chille.exe		Findersheet II. Colfestinated and	n 16	
12		p /ershell.exe	/	rigd what: wvcpisetupint.exe		cnm, c:\Program Files (NVIDIA Corporation (Installer2/Display.Driver. (C9752557-A557-4AE9-B7D4-551FE0F3AFE7) (NVCpiSetupint.exe
13		a sass.exe	8		4.	.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
14		svchost.exe	9		R	.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
15		/ OUTLOOK.EXE	10	Options >>		shm C) Brogram Eiler/Mi/DIA Concentration/Installer/) Direlay Driver (C0752557, A557, A659, P704, 55155052A5573) Aur/ol/Saturolationa
16		7 nvstinst.exe	10	2		compc. (Program Files (IVAIDIA Corporation (Instance Z) Orspital Display. Driver. (C5752557-A557-44C5-B704-551E0F5AFE7/(IVACDISELD) Interes
17		5 explorer.exe	11		R	t.chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
18		4 rundl132.exe	12	Find All Eind Next Close	. C.	chm,C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557-4AE9-B7D4-551FE0F3AFE7}\NvCplSetupInt.exe
19		3 Indexe	12	Iun 18 13:42:41 C:\Temn\NVIDIA\ControlPanelinstallerTemn\nymoh	DTR	chm C1/Brogram Files/NV/DIA Corporation/Installer2/Display Driver (C9752557.4557.4659.8704.551EE0E3AEE7)/NvColSetupInt exe
20		3 outlook-exe	10	von zo zorezrezie (remp (remp (remove (control Panelinistalier remp (remov	er (0.)	sented in the provide the providence of the prov
		1 1	1.1.4	lun 18 12/12/11 C·\Tomn\NIVIDIA\ControlPanelInstallerTemn\nymob	DTG	chm C*\Program Eilec\N\/IDIA Cornoration\Installer?\Display Driver (C9752557, 8577, 8557

附註:<u>在此</u>處,您可以找到與建立排除的最佳實踐相關的詳細資訊。

#### 調整排除

識別出進程或路徑後,可以將它們新增到連結到終端上應用的策略的排除清單中,導航到 Management > Exclusions > Exclusions > Edit,如下圖所示。

Threat	CSIDL_V	VINDOWS\Temp\_avast_\	Ì						
Path	[Any Driv	re]:\ pagefile.sys							
File Extension		Apply to all drive letters Path exclusion							
Wildcard	Path exc								
Process:	Threat or	valuaion							
File Scan	Threater	Inreat exclusion							
Malicious Activity	Wildcard	Wildcard							
System Process	Apply	/ to all drive letters							
Process	Path	C:\Program Files\NVIDIA Corporation\Installer2\Display.Driver.{C9752557-A557.4AE9-B7D4-55		1					
File Scan	SHA			ł					
	You can	provide path and/or SHA-256. If you specify both a path and SHA-256 then both conditions must		I					
	he met f	or the process to be excluded.							
	be met it		-						
	Apply	to child processes							
	Apply	/ to child processes		ļ					

## 將套件組合提交給TAC進行分析

ATS TAC可幫助排除這些情況的故障,如果出現這種情況,請準備在建立案例時提供下一個資訊:

- 此問題何時開始?
- •最近有變化嗎?
- •特定應用程式是否出現問題?如果是,哪一個應用程式?
- •系統中是否有其他防病毒軟體?如果是,哪種防病毒軟體?
- 重現問題的同時收集調試捆綁包: 收集調試捆綁包的步驟