# 適用於Mac診斷資料收集的Cisco安全終端聯結器

## 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>背景資訊</u> <u>使用支援工具生成診斷檔案</u> <u>使用macOS Finder啟動支援工具</u> <u>使用macOS終端啟動支援工具</u> <u>疑難排解</u> <u>啟用調試模式</u> <u>啟用單心跳調試模式</u> <u>禁用調試模式</u>

# 簡介

本文檔介紹通過思科安全終端Mac聯結器上提供的支援工具應用程式生成診斷檔案的過程,以及如 何解決效能問題。

# 必要條件

#### 需求

思科建議您瞭解以下主題:

- 安全終端Mac聯結器
- macOS

#### 採用元件

本文檔中的資訊基於安全終端Mac聯結器。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

## 背景資訊

安全終結點Mac聯結器封裝了一個稱為支援工具的應用程式,用於生成有關安裝在Mac上的聯結器 的診斷資訊。診斷資料包含有關Mac的資訊,例如:

- 資源利用率(磁碟、CPU和記憶體)
- 聯結器特定的日誌

• 聯結器配置資訊

# 使用支援工具生成診斷檔案

本節介紹如何從GUI或CLI啟動支援工具應用程式以生成診斷檔案。

#### 使用macOS Finder啟動支援工具

完成以下步驟,以便使用macOS Finder啟動安全終端Mac聯結器支援工具:

1. 導航到Applications資料夾中的Cisco Secure Endpoint目錄,並找到Support Tool啟動程式:



2. 按兩下Support Tool啟動程式,系統提示您輸入管理憑據:

Support Tool wants to make changes. Type your password to allow this.	
Name:	admin
Password:	••••••
	Cancel OK

3. 輸入憑證後, 支座上應會顯示支援工具圖示:



**附註**:「支援工具」應用程式在後台運行,需要一些時間才能完成(大約20-30分鐘)。 4. 當「支援工具」應用程式完成時,會生成一個檔案並將其放到案頭上:



#### 以下是未壓縮輸出的範例:

•••	AMP_Support_2	2019_05_30_14_23_09		
$\langle \rangle$		🖞 🖸 🔍 Search		
Favorites	Name	<ul> <li>Date Modified</li> </ul>	Size	Kind
AirDrop	ampdaemon-sample.txt	Today at 2:23 PM	109 KB	Plain Te:
	ampscansvc-sample.txt	Today at 2:23 PM	13 KB	Plain Te:
Recents	clamav_list.txt	Today at 2:23 PM	2 KB	Plain Te:
Applications	cloud-ec.cert.txt	Today at 2:23 PM	12 KB	Plain Te:
Desktop	cloud-ec.curl-raw.txt	Today at 2:23 PM	711 bytes	Plain Te:
	📄 cpuinfo.txt	Today at 2:23 PM	41 bytes	Plain Te:
Documents	🖹 crashpad.tar	Today at 2:23 PM	10 KB	tar archi
🕒 Downloads	disk.txt	Today at 2:23 PM	796 bytes	Plain Te:
	🖹 dns.txt	Today at 2:23 PM	2 KB	Plain Te:
iCloud	ile_list.txt	Today at 2:23 PM	5 KB	Plain Te:
iCloud Drive	📄 global.xml	Today at 2:23 PM	13 KB	XML
Locations	hostname.txt	Today at 2:23 PM	16 bytes	Plain Te:
	ifconfig.txt	Today at 2:23 PM	3 KB	Plain Te:
Remote Disc	🖿 installer.tar	Today at 2:23 PM	7.8 MB	tar archi
Network	💩 InstallHistory.plist	Today at 2:23 PM	41 KB	Property
	🗋 kext.log	Today at 2:23 PM	382 KB	Log File
Tags	kext.txt	Today at 2:23 PM	25 KB	Plain Te:
🔴 Red	keychain-trust-settings.txt	Today at 2:23 PM	290 bytes	Plain Te:
- Orongo	h locallog.tar	Todav at 2:23 PM	31 KB	tar archi

5. 為了分析資料,請將此檔案提供給思科技術支援團隊。

## 使用macOS終端啟動支援工具

支援工具啟動程式位於以下目錄中:

**附註**:您必須以root使用者身份運行此命令,以確保切換到root使用者或使用sudo作為命令的 字首。

root@mac# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector root@mac# ./SupportTool

附註:此命令以垂直方式運行。完成後,將生成診斷檔案並將其放到案頭上。

## 疑難排解

本節介紹如何在安全終端Mac聯結器上啟用和禁用調試模式,以便解決效能問題。

#### 啟用調試模式

**警告**:只有在思科技術支援工程師請求此資料時,才應啟用調試模式。如果長時間保持啟用調 試模式,則它可能很快地填充磁碟空間,並且由於檔案大小過大,可能會阻止將聯結器日誌和 托盤日誌資料收集到支援診斷檔案中。

調試模式對於嘗試解決安全終端聯結器上的效能問題非常有用。完成以下步驟以啟用調試模式並收 集診斷資料;

- 1. 登入到安全終端控制檯。
- 2. 導航到管理>策略。
- 找到應用於電腦的策略,按一下將展開策略視窗的策略,然後按一下 複製.安全終端控制檯使 用複製的策略進行更新:

**O** View All Changes

Policies

TechZone	٩		
All Products Windows Android	Mac Linux Network iOS		+ New Policy         ⊡         ±
😑 🗯 TechZone MAC Policy			🐮 0 🖵 O
Modes and Engines	Exclusions	Proxy	Groups
FilesQuarantineNetworkAuditClamAVOn	Apple macOS Default	Not Configured	Not Configured
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured
O View Changes Modified 2019-05	-30 14:49:32 UTC Serial Number 100	Download XM	Duplicate F Edit 🗎 Delete

4. 選擇並展開複製策略視窗,按一下 編輯 並更改策略名稱。例如,您可以 調試TechZone MAC策略.

#### 5. 按一下 **高級設定**,選擇 管理功能 從邊欄中選擇 調試 對於聯結器日誌級別和托盤日誌級別下 拉選單:

🗯 Mac			
Name	Debug TechZone MAC Policy		
Description			10
Modes and Engines		Send User Name in Events	
Exclusions		🗹 Send Filename and Path Info 🛛 📵	
1 exclusion set	Heartbeat Interval	15 minutes 🗳	0
Proxy	Connector Log Level	Debug 🔶	0
Outbreak Control	Tray Log Level	Debug 🛟	0
Product Updates		☑ Automated Crash Dump Uploads (	9
Advanced Settings		🗸 Command Line Capture 🛛 🕕	
Administrative Features		Command Line Logging ①	
Client User Interface			
File and Process Scan			
Cache			
ClamAV			
Network			
Scheduled Scans			

#### 6. 按一下儲存存 按鈕儲存更改。

#### 7. 導航至 管理>組 然後按一下 建立組 靠近螢幕右上角。

#### 8. 輸入組的名稱。例如,可以使用Debug TechZone Mac Group。

< New Group

Name	Debug Mac Group	
Description	This group will be used to debug AMP for Endpoints Connector running on Mac	
Parent Group		ŧ
Windows Policy	win_desktop_policy	\$
Android Policy	Default FireAMP Android (Default)	\$
Mac Policy	Debug TechZone MAC Policy	\$
Linux Policy	Audit Policy for FireAMP Linux (Default)	\$
Network Policy	Default Network (Default)	\$
iOS Policy	Audit (Default)	\$
	Cancel Save	

Computers	
Assign computers from th have saved the new group	e Computers page after you

0

- 9. 更改Mac策略 預設Mac策略 複製的新策略,即 調試TechZone Mac策略 在本例中。按一下 儲 存.
- 10. 導航至 管理>電腦 並在清單中識別您的電腦。選擇它並按一下 移動到組......
- 11. 從 選擇組 下拉選單。按一下 移動 將所選電腦移動到新組中。您的Mac現在應該具有功能調 試策略。您可以選擇選單欄上出現的「安全終端」圖示,並確保應用新策略:



#### 啟用單心跳調試模式

此過程僅適用於1.0.4聯結器及更高版本。這允許將單個聯結器置於調試模式,直到下一個心跳為止 。根據具體情況,這可能為我們的開發人員提供足夠的資訊,但取決於心跳的長度,有可能達不到 進行完整的診斷分析所需的所有流程。以下是為單個心跳啟用調試的步驟:

- 1. 訪問聯結器選單欄並轉至 設定。
- 2. 按一下 **關於。**
- 3. 點選安全端點徽標的右半部。



4. 如果操作正確, 螢幕右側將顯示以下通知:

SECURE ENDPOINT CONNECTOR Logging Level Updated Logging set to 'info' level Until next heartbeat

調試將在下次心跳後自動禁用。

#### 禁用調試模式

在調試模式下獲取診斷資料後,必須將安全終端聯結器恢復為正常模式。完成以下步驟即可停用偵 錯模式:

now

- 1. 登入到安全終端控制台。
- 2. 導航到**管理>組**。
- 3. 找到在調試模式下建立的新組Debug TechZone Mac Group。
- 4. 按一下「Edit」。
- 5. 在屏幕右上角的「電腦」視窗中,在清單中找到您的電腦。選擇它,它將帶您進入 Computerspage。再次從清單中選擇您的電腦,然後單**擊「移動到組……」**.
- 6. 從選擇組下拉菜**單中**選擇上一個組。按一下移動將所選電腦移動到上一組。
- 7. 按一下選單欄中的安全終端圖示。從菜單中選擇Sync策略。
- 8. 驗證策略現在是否返回到上一個預設值。在選單欄上選中此項。現在,策略應已恢復為原始策 略,該策略在您將其更改為Debug TechZone Mac Group之前使用:

Last Scan: 2019-05-29, 12:01 PM Status: Connected Policy: Desktop Mac Protect

 Scan

 Pause Scan

 Cancel Scan
 Settings

 Update Virus Definitions
 Sync Policy

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。