分析高CPU的MacOS AMP诊断套件

目录

简介 先决条件 要求 使用的组件 背景信息 故障排除 验证计算机上是否安装了其他防病毒软件 确定特定应用使用时的高CPU 用于分析的诊断包的转换器 终端中的调试级别 AMP命令行界面(CLI)中的调试级别 <u>策略中的调试级</u>别 从其他防病毒解决方案中排除AMP 重现问题并收集诊断捆绑包 高CPU性能分析 相关信息

简介

本文档介绍从面向MacOS设备上的终端公共云的高级恶意软件防护(AMP)分析诊断捆绑包以排除 CPU使用率过高的故障的步骤。

作者:Uriel Torres,编辑者:Cisco TAC工程师Yeraldin Sanchez。

先决条件

要求

Cisco 建议您了解以下主题:

- AMP控制台中的基本导航
- MAC终端的导航

使用的组件

本文档中的信息基于以下软件和硬件版本:

- 面向终端的AMP控制台5.4.20200512
- macOS Catalina版本10.15.4
- AMP连接器1.12.3.738

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

背景信息

AMP连接器扫描计算机上的所有活动文件(移动、复制和/或修改自己的文件),除非明确告知不要 ,否则,如果连接器运行时运行的进程和操作过多,将不可避免地带来性能问题,这会导致CPU利 用率高、速度慢,在某些情况下,还会导致软件不能运行或运行缓慢。此外,AMP连接器可能会根 据文件的云信誉来阻止文件,这有时可能是错误的(误报)。 两个问题的解决方案是排除这些路径 和进程。

故障排除性能问题的流程如图所示。



故障排除

本节提供可用于排除配置故障的信息。

验证计算机上是否安装了其他防病毒软件

提示:如果列表中包含思科维护的排除项,请记住这些排除项可以添加到应用的新版本。

要查看AMP控制台上思科维护的排除部分中可用的列表,请执行以下操作:

- 导航至管理>策略。
- 查找策略并单击"编辑"。
- •在策略上,"设置"窗口单击"排除"。

根据计算机上当前安装的软件选择终端需要的软件,然后保存策略,如图所示。

Name	MAC Protect Policy		
Description	Protect policy for MAC devices	G,	
Modes and Engines	Cisco-Maintained Exclusion	s @	
Exclusions	2 selected ~		
2 exclusion sets	Search	10 Exclusions	
Proxy		3 Evolusions	
	Apple macOS Default 10 Exclusions		
Outbreak Control	Crasholan 3 Exclusions		
Product Updates	Digital Guardian 1 Exclusion		
	Docker 2 Evolusions		
Advanced Settings	Fusion 2 Evolusions		
	labber 2 Exclusions		
	JAME Casper 5 Exclusions		
	McAfee 3 Exclusions		
	Microsoft Office 4 Evolusions		
	Vagrant 3 Exclusions		
	Virtual Box 1 Exclusion		
	Xcode 3 Exclusions		
			Cancel

确定特定应用使用时的高CPU

确定问题是否发生在执行一个应用程序或其中几个应用程序时,如果您能够复制该问题,则有助于 确定潜在的排除项。

用于分析的诊断包的转换器

要收集有用的诊断包,必须启用调试日志级别。

终端中的调试级别

如果可以复制问题并有权访问终端,以下是捕获诊断捆绑包的最佳步骤。

- •在MAC菜单栏上,点击AMP图标。
- •导航到**设置**部分,如图所示。

A Status: Scanning (1026 files) Policy: Desktop Mac Protect A Status: Scanning (1026 files) A Status: Scanning (1026 f						
Scan Pause Scan Cancel Scan						
Settings Undate Virus Definitions						
Sync Policy						
Quit AMP for Endpoints Connector						

- •在设置窗口中,导航至**关于**。
- •要启用调试模式,请点击AMP徽标内部,如图所示。



弹出窗口指示AMP连接器处于调试模式

此过程将启用调试日志级别,直到下一个策略心跳间隔。

AMP命令行界面(CLI)中的调试级别

- 打开终端
- 导航至/opt/cisco/amp/bin/
- 运行ampcli: ./ampcli
- 在AMP CLI上启用调试模式: ampcli>debuglevel 1

此过程将启用调试日志级别,直到下一个策略心跳间隔。

策略中的调试级别

如果您无权访问终端或无法一致地重现问题,则必须在策略中启用调试日志级别。

要按策略启用调试日志级别,请执行以下操作:

- 导航至管理>策略
- 查找策略, 然后单击"编辑"
- 导航至高级设置>管理功能
- 如图**所示,将连**接器日志级别和托盘日志级别配置为调试并保存策略

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

警告:如果从策略启用调试模式,则所有终端都会收到此配置。

注意:同步终端的策略以确保调试模式。

从其他防病毒解决方案中排除AMP

根据用户指南,防病毒产品必须排除下一个目录以及其中任何文件、目录和可执行文件,以与AMP Connector for MAC兼容,要排除的目录包括:

- •/库/应用支持/面向终端的思科/AMP连接器
- /opt/cisco/amp

重现问题并收集诊断捆绑包

配置调试级别后,请等待系统上出现"High CPU(高CPU)"状态,或手动重现之前确定的条件,然 后收集诊断捆绑包。

要收集调试捆绑包,请执行以下操作:

- •打开终端。
- •访问超级用户级别,然后导航到/库/应用支持/面向终端的思科/AMP连接器:

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

•要运行支持工具,请使用下一个命令:

./SupportTool



调试捆绑包以.zip文件扩展名保存在Desktop(桌面)文件夹中。

高CPU性能分析

调试诊断捆绑包存储在桌面中,以开始分析:

- 解压诊断捆绑包
- 有2个文件要查看 文件操作: fileops.txt文件执行: execs.txt

	AMP_Support_2020_05_28_16_51_34					
the man the man and the man	TXT	тхт	ТХТ	TXT		
ampdaemon- sample.txt	ampscansvc- sample.txt	clamav_list.txt	cloud-ec.cert.txt	cloud-ec.curl- raw.txt		
тхт	TAR	TXT	Former Fo			
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是排除故障的主要性能工具。它列出连接器运行时终端上当前所有活动操作,如下所示:

<收集捆绑包时在路径上执行的数量扫描> / <扫描路径

>
😑 🕒 📄 fileops.txt
19 /Library/Application Support/Applc/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/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyEventActivityStats.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Uutlook.Settings.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Uutlook.Settings.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Uutlook.Settings.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json 17 /Users/jesutorr/Library/Containers/com.miccrosoft.gut.logk/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json
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/
确定进程后,可以创建排除项 要创建排除项

- •在AMP控制台上,导航至Management > Exclusions
- •选择排除集并单击"编辑"
- •可以添加排除项,如图所示

Edit Excl Mac	usion	Set	
	Name	MAC Protect Exclusion Set	
Wildcard	~	/Users/*/Library/Bin/MyApplication/	
• Execs.txt文件包含 在AMP策略中,因	连接器收集排 为这些是所 [;]	捆绑包时运行的进程使用的所有命令。此处列出的路 有进程都使用的二进制文件(/bin)和系统二进制文件(/	径不能排除 sbin),但是

- ,在Execs.text上,可以提供正在运行的主进程。
- 例如,如果Execs.txt文件显示下一个日志。



由于家庭酿造应用使用bash,您可以确认该应用是

导致CPU使用率较高的原因。

相关信息

- <u>面向终端的AMP:MacOS和Linux中的进程排除</u>
- 面向终端的 AMP 排除项最佳做法
- <u>技术支持和文档 Cisco Systems</u>