コンソールでのMACカーネルとフルディスクア クセス – AMP for Endpoints

内容

概要 <u>前提条件</u> <u>要件</u> <u>使用するコンポーネント</u> <u>制限</u> <u>背景説明</u> <u>トラブルシュート</u> <u>コンソールエラー</u> <u>カーネル障害</u> フルディスクアクセス障害

概要

このドキュメントでは、エンドポイントが2つのMac障害を処理するための高度なマルウェア防御 (AMP)におけるトラブルシューティング手順について説明します。フルディスクアクセス(FDA)お よびカーネルモジュールが許可されていません。

著者: Cisco TACエンジニア、Uriel Torres、Javier Jesis Martinez

前提条件

要件

次の項目に関する知識があることが推奨されます。

・Macツールの知識

・管理者権限を持つアカウント

使用するコンポーネント

このドキュメントの情報は、Cisco AMP for Endpoints for MACに基づくものです。

このドキュメントの情報は、特定の環境にあるデバイスから作成されたものです。

• MacOS High Sierra 10.13

制限

これは、OSV-10.4.Xおよびコネクタバージョン1.11.0にインストールされたOSXおよびAMPコネ クタの表面的なバグです。AMPポータルにはFDAの障害メッセージが表示され、ホストには FDAが許可されていることが示されています。 バグID:CSCvq98799

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

背景説明

KEXTのロードが要求されたが、まだ承認されていない場合、ロード要求は拒否されます。 MacOS High Sierra 10.13では新機能が導入されています。これは、新しくインストールされたサ ードパーティ製カーネル拡張(KEXT)をロードする前にユーザが承認を必要とし、承認されたカー ネル拡張だけがシステムにロードされることを意味します。ユーザは、前に説明した手順に従っ て、カーネルエラーを解決する必要があります。

macOS 10.14(Mojave)では、エンドポイント用AMPに影響する新しいセキュリティ機能Macコネ クタが導入されているため、AMPサービスデーモンにFull Disk Accessが許可されていることを確 認する必要があります。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

コンソールエラー

カーネル障害

図に示すように、AMPコンソールは、Kernel Extension(KEXT)をロードする要求が行われ、承認 されていない場合、ロード要求が拒否され、macOSがアラートを表示すると、「Kernel module not authorized」エラーを表示します。 Kernel module not authorized

Requires endpoint user intervention

Critical Fault

The Connector's system extension has been blocked from execution. Open Security and Privacy System Preferences and approve the extension.

Apple macOSのアップグレード後、図に示すように、カーネルの承認に関する公式発表が開始さ れました。

🛕 Mac OS 10.13 - High Sierra Advisory

Apple macOS 10.13 includes additional kernel extension security that requires user interaction for the AMP for Endpoints Mac Connector to run properly. End users must approve the execution of new kernel extensions for Mac devices that are not managed by an MDM. We recommend that you upgrade all your AMP for Endpoints Mac Connectors to v1.4.5 prior to upgrading to macOS 10.13 to have the least amount of user intervention. See this **Apple Tech Note** for details about this feature.

コネクタの拡張を許可するには、図に示すように、[System Preferences] > [Security & Privacy] > [General]に移動します。



Security & Privacy General FileVault Firewall Privacy

図に示すように、[Lock]をクリックしてKEXTを承認します(ユーザによって承認されたカーネル 拡張だけがシステムにロードされます)。



注:ユーザの承認は、アラートの30分後に[Security & Privacy preferences]ペインに表示されます。KEXTが承認された後のロード試行によって承認ユーザインターフェイスが再度表示されますが、別のユーザアラートはトリガーされません。

フルディスクアクセス障害

図に示すように、AMPコンソールに「Disk Access not granted」と表示されます。

Disk access not granted
 Requires endpoint user intervention
 Major Fault
 The Connector cannot access user files for scan. Open Security and Privacy System Preferences and grant Full Disk
 Access to the AMP background service: '/opt/cisco/amp/ampdaemon'.

フルディスクアクセスが許可されていないことを確認します。図に示すように、[シス**テム設定] >** [セキュリティとプライバシー] > [プライバシー]に移動します。

Security & Privacy FileVault Firewall General Privacy

AMPコネクタのフルディスクアクセスを承認するには、[Full Disk Access]に移動し、図に示すようにampdaemonプロセスをチェックします。



端末を開き、AMPサービスを停止し、次のコマンドsudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plistを実行し、図に示すようにチェックボック スをマークします。



キャッシュの問題を回避するには、図に示すように/library/logs/cisco**に移動**し、次のファイルを 消去します。

- ampdaemon.log
- ampscansvc.log



ampdaemon.log ampscansvc.log

sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plistコマンドを使用し てサービスを開始します。

注: ampdeamonファイルが見つからない場合は、[Allow Full Disk Access]リストにドラッ グアンドドロップし、図に示すようにチェックボックスがオンになっていることを確認しま す。

Grant Full Disk Access

(1) (1)	10 and		Security & Privacy	Q Search
	impcli	0	General Fieldault Firewall Priva	Ky .
O Downlo 2	mpdaemon	Location Services	Allow the apps below to acco Messages, Safari, Home, Tim	ess data like Mail, he Machine backups, and
Applicat	mpupdater	Contacts		
Lecations Macinton	Belanmspack	Reminders	-	
@ Remote		Se Photos		
		Camera		
		Microphone	000	
		Cull Plate Access		
	1	Fue brak Aboess		
	Ċ	Click the lock to make ch	unges.	Advanced.

AMP for Endpoints requires Full Disk Access to protect your Mac.

1. In the Security & Privacy System Preferences pane, click the lock and enter your password.

2. Drag the "ampdaemon" program from the "amp" Finder window into the allowed applications list.

OK

Location Services	Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and				
Contacts	certain ad	ministrative	esettings for all us	ers on this Mac	
Calendars	×	ampdaem	ion		
Reminders					
Photos					
Camera					
Microphone	+-				
Accessibility					
Full Disk Access					

フルディスクアクセスを許可するには、カーネルにアクセス許可とMACデバイスの推奨リブート を与え、次回のハートビート間隔で報告されたメッセージがコンソールから消えます。