

# Analyse des macOS AMP Diagnostic-Pakets für hohe CPU-Auslastung

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Fehlerbehebung](#)

[Überprüfen Sie, ob ein anderer Virenschutz auf dem Computer installiert ist](#)

[Identifizieren der hohen CPU bei Verwendung einer bestimmten Anwendung](#)

[Diagnosepakete für Analyse abrufen](#)

[Debugebene am Endpunkt](#)

[Debug-Ebene in der AMP-Befehlszeilenschnittstelle \(CLI\)](#)

[Debugebene in der Richtlinie](#)

[AMP von anderen Antivirus-Lösungen ausschließen](#)

[Reproduzieren Sie das Problem, und sammeln Sie ein Diagnosepaket.](#)

[Analyse der hohen CPU-Leistung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt die Schritte zur Analyse eines Diagnosepakets von Advanced Malware Protection (AMP) für Endgeräte Public Cloud auf MacOS-Geräten, um eine Fehlerbehebung bei hoher CPU-Auslastung zu ermöglichen.

Mitgeführt von Uriel Torres und herausgegeben von Yeraldin Sanchez, Cisco TAC Engineers.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Navigation in der AMP-Konsole
- Navigation im MAC-Terminal

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- AMP für Endgeräte Konsole 5.4.20200512
- macOS Catalina Version 10.15.4
- AMP-Anschluss 1.12.3.738

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Hintergrundinformationen

Der AMP Connector scannt alle aktiven Dateien (die sich selbst verschieben, kopieren und/oder ändern) auf einem Rechner, es sei denn, dies wird ausdrücklich anders gesagt. Das führt unweigerlich zu Leistungsproblemen, wenn während der Ausführung des Connectors zu viele Prozesse und Abläufe ausgeführt werden. Dies führt zu einer hohen CPU-Auslastung, langsameren Abläufen und in einigen Fällen zu Software, die nicht langsam ausgeführt wird. Darüber hinaus blockiert der AMP Connector Dateien basierend auf ihrer Cloud-Reputation, was manchmal falsch (falsch positiv) sein kann. Die Lösung für beide Probleme besteht darin, diese Pfade und Prozesse auszuschließen.

Der Fluss der Fehlerbehebung bei Leistungsproblemen wird im Bild angezeigt.



## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

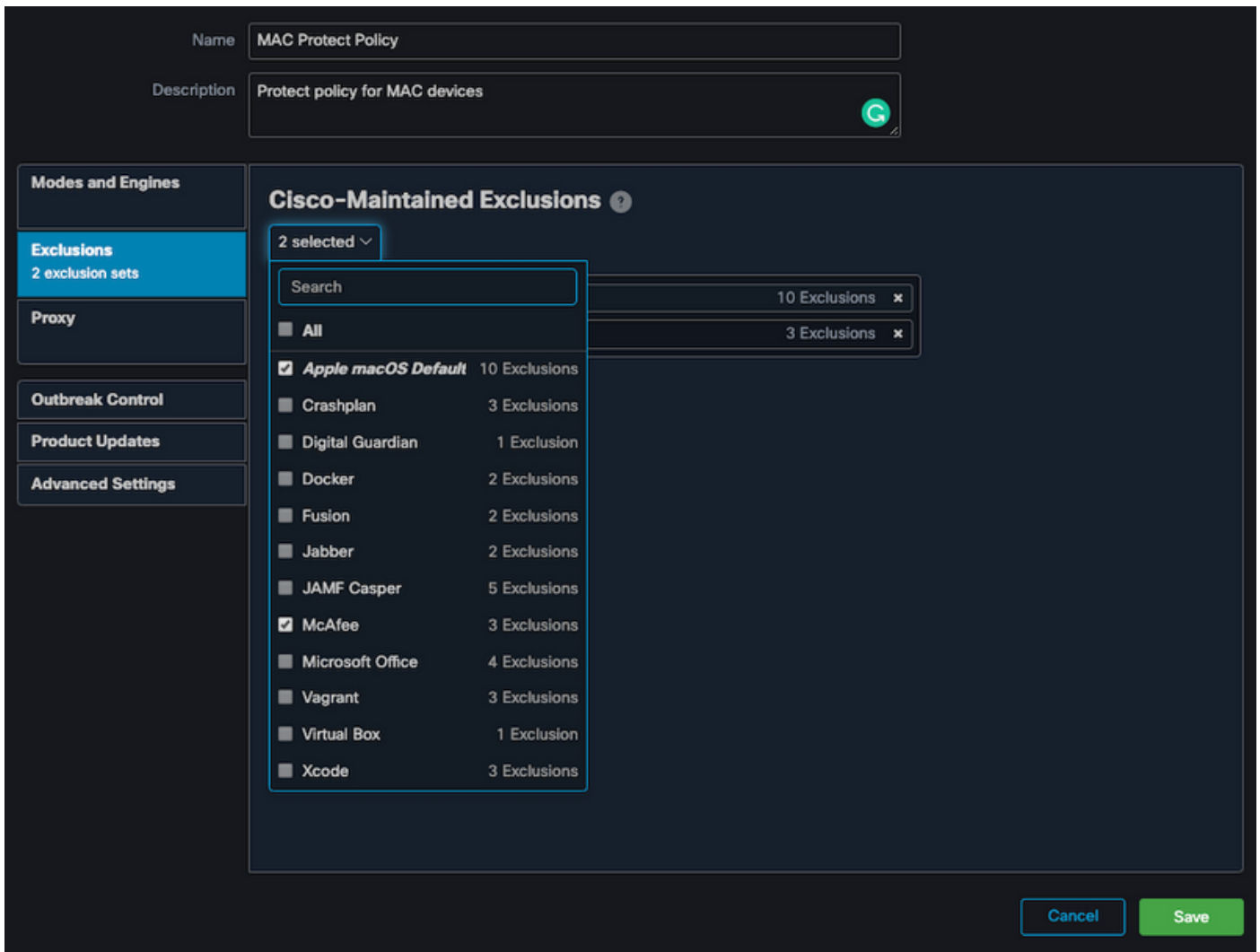
### Überprüfen Sie, ob ein anderer Virenschutz auf dem Computer installiert ist

**Tipp:** Verwenden Sie die von Cisco verwalteten Ausschlüsse, wenn die verwendete Software in der Liste enthalten ist. Beachten Sie, dass diese Ausschlüsse neuen Versionen einer Anwendung hinzugefügt werden können.

So zeigen Sie die Listen an, die in dem von Cisco verwalteten Ausschlussbereich auf der AMP-Konsole verfügbar sind:

- Navigieren Sie zu **Verwaltung > Richtlinien**.
- Suchen Sie die Richtlinie, und klicken Sie auf **Bearbeiten**.
- Klicken Sie in der Richtlinie im Fenster Einstellungen auf **Ausschlüsse**.

Wählen Sie die Geräte aus, die Ihr Endgerät benötigt, entsprechend der aktuell auf dem Computer installierten Software. Speichern Sie dann die Richtlinie, wie im Bild gezeigt.



## Identifizieren der hohen CPU bei Verwendung einer bestimmten Anwendung

Identifizieren Sie, ob das Problem auftritt, während eine oder mehrere Anwendungen ausgeführt werden, wenn Sie das Problem replizieren können, um potenzielle Ausschlüsse zu identifizieren.

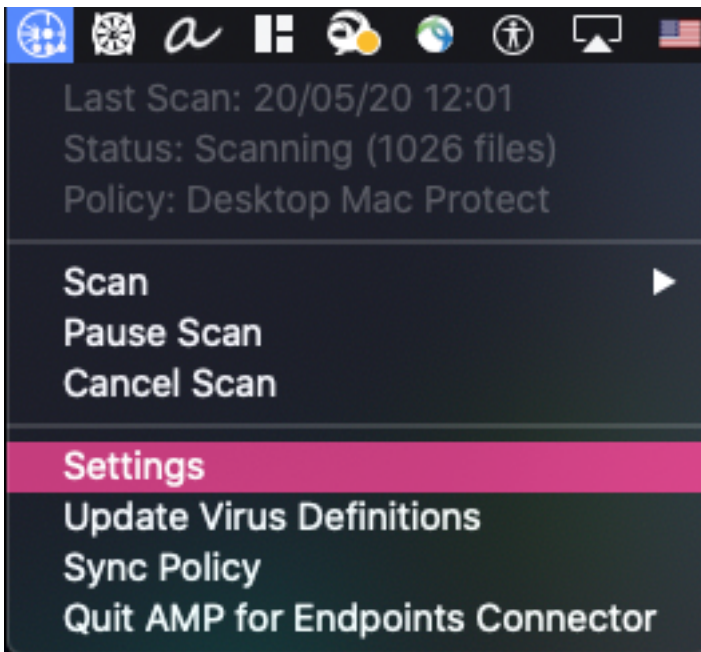
## Diagnosepakete für Analyse abrufen

Um ein nützliches Diagnosepaket zu erfassen, muss die Debug-Protokollstufe aktiviert sein.

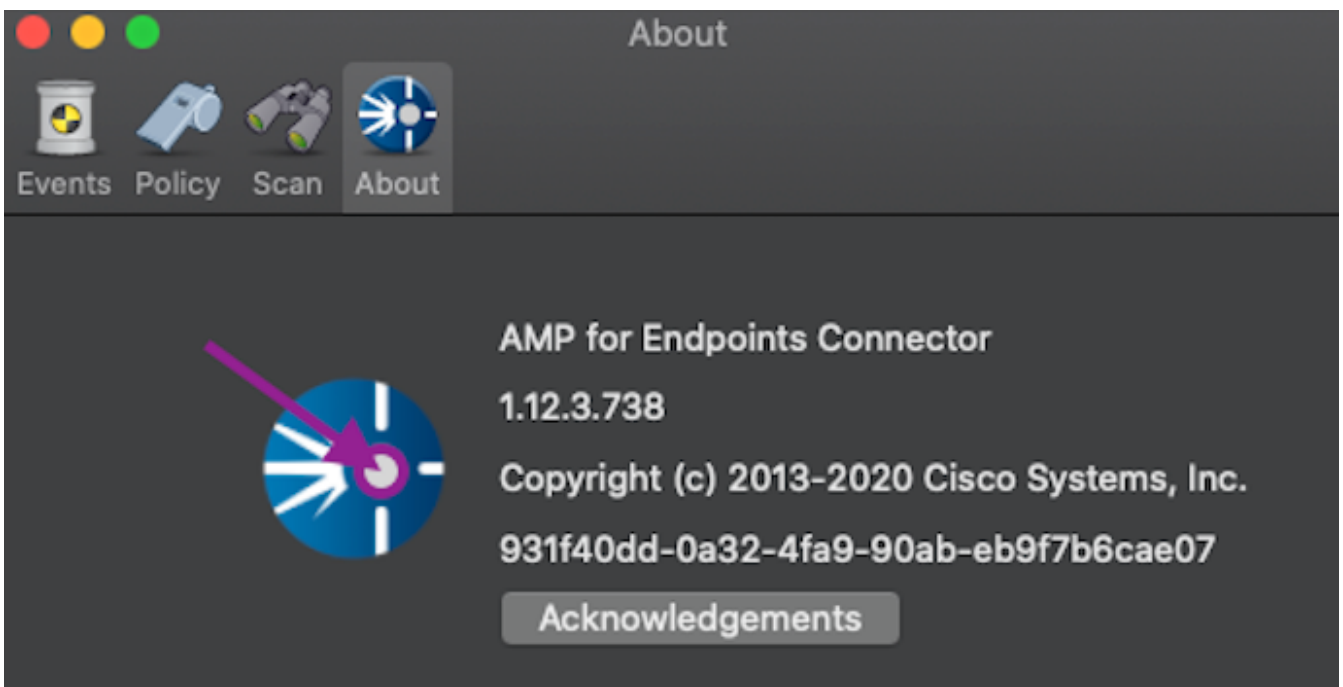
Debugebene am Endpunkt

Wenn Sie das Problem replizieren können und Zugriff auf den Endpunkt haben, ist die unten stehende Vorgehensweise die beste, um das Diagnosepaket zu erfassen.

- Klicken Sie in der MAC-Menüleiste auf das AMP-Symbol.
- Navigieren Sie zum Bereich **Einstellungen**, wie im Bild gezeigt.



- Navigieren Sie in den Einstellungsfenstern zu **Info**.
- Um den Debugmodus zu aktivieren, klicken Sie in das AMP-Logo, wie im Bild gezeigt.



Ein Popup-Fenster zeigt an, dass sich der AMP-Anschluss im Debugmodus befindet

Mit diesem Verfahren wird die Debug-Protokollstufe bis zum nächsten Richtlinienkartenintervall aktiviert.

### Debug-Ebene in der AMP-Befehlszeilenschnittstelle (CLI)

- Terminal öffnen
- Navigieren Sie zu `/opt/cisco/amp/bin/`.
- Ampcli ausführen:  
`./ampcli`
- Aktivieren Sie in der AMP-CLI den Debugmodus:

```
ampcli>debuglevel 1
```

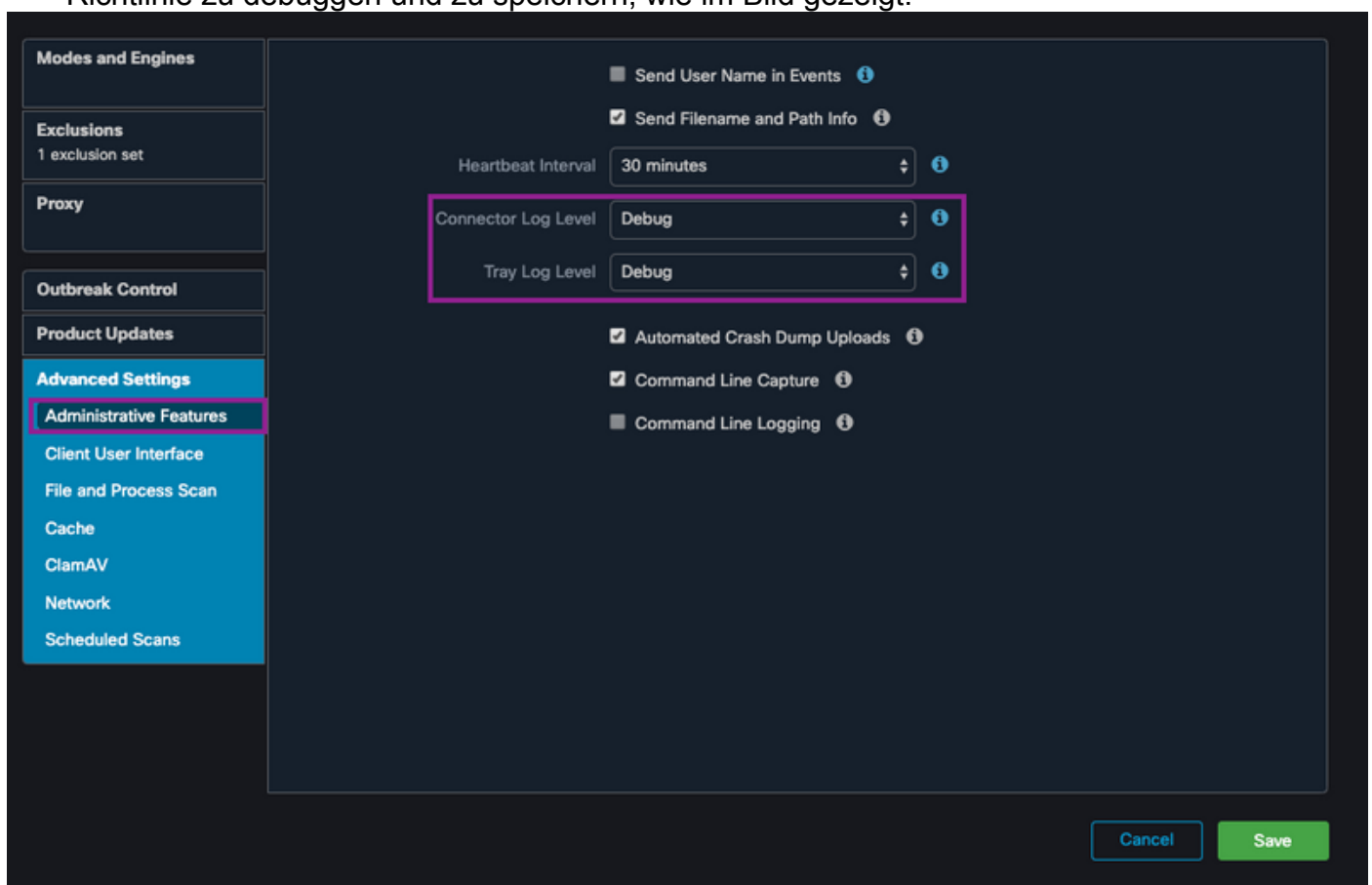
Dieser Prozess aktiviert die Debug-Protokollebene bis zum nächsten Richtlinienkatalog-Intervall.

## Debugebene in der Richtlinie

Wenn Sie keinen Zugriff auf den Endpunkt haben oder das Problem nicht konsistent reproduziert werden kann, muss die Debug-Protokollstufe in der Richtlinie aktiviert sein.

So aktivieren Sie die Debug-Protokollebene mithilfe der Richtlinie:

- Navigieren Sie zu **Verwaltung > Richtlinien**.
- Suchen Sie die Richtlinie, und klicken Sie auf **Bearbeiten**.
- Navigieren Sie zu **Erweiterte Einstellungen > Verwaltungsfunktionen**.
- Konfigurieren Sie die **Verbindungsprotokollebene** und die **Tray-Protokollstufe**, um die Richtlinie zu debuggen und zu speichern, wie im Bild gezeigt.



**Vorsicht:** Wenn der Debugmodus von der Richtlinie aktiviert ist, erhalten alle Endpunkte diese Konfiguration.

**Hinweis:** Synchronisieren Sie die Richtlinie des Endpunkts, um den Debugmodus sicherzustellen.

## AMP von anderen Antivirus-Lösungen ausschließen

Gemäß dem Benutzerhandbuch müssen Virenschutzprodukte die nächsten Verzeichnisse und alle darin enthaltenen Dateien, Verzeichnisse und ausführbaren Dateien ausschließen, um mit

dem AMP Connector für MAC kompatibel zu sein. Folgende Verzeichnisse werden ausgeschlossen:

- `/Library/Application Support/Cisco/AMP` für Endpoints-Anschluss
- `/opt/cisco/amp`

## Reproduzieren Sie das Problem, und sammeln Sie ein Diagnosepaket.

Wenn die Debugging-Stufe konfiguriert ist, warten Sie, bis der Status der High CPU auf dem System auftritt, oder reproduzieren Sie manuell die zuvor identifizierten Bedingungen, und sammeln Sie dann das Diagnosepaket.

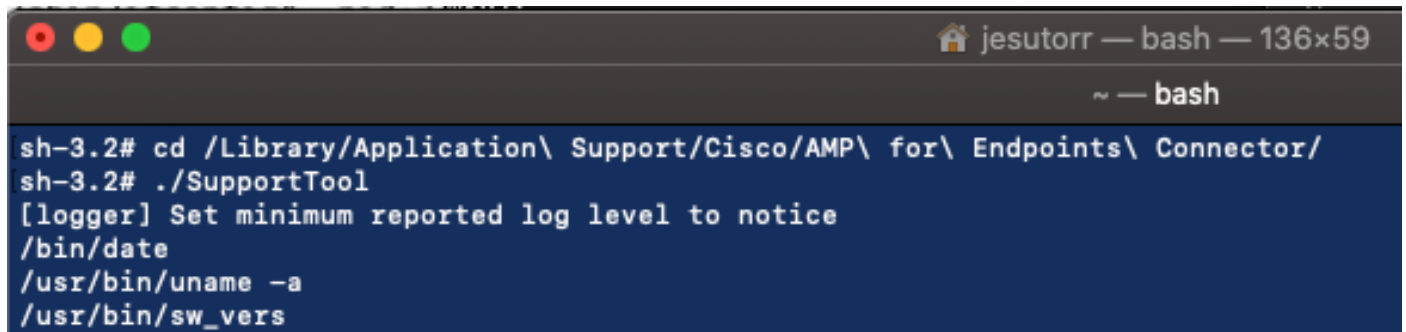
So sammeln Sie das Debugpaket:

- Öffnen Sie ein Terminal.
- Zugriff auf die Superuser-Ebene und Navigieren Sie dann zu `/Library/Application Support/Cisco/AMP` für Endpoints Connector:

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

- Verwenden Sie zum Ausführen des Support-Tools den folgenden Befehl:

```
./SupportTool
```



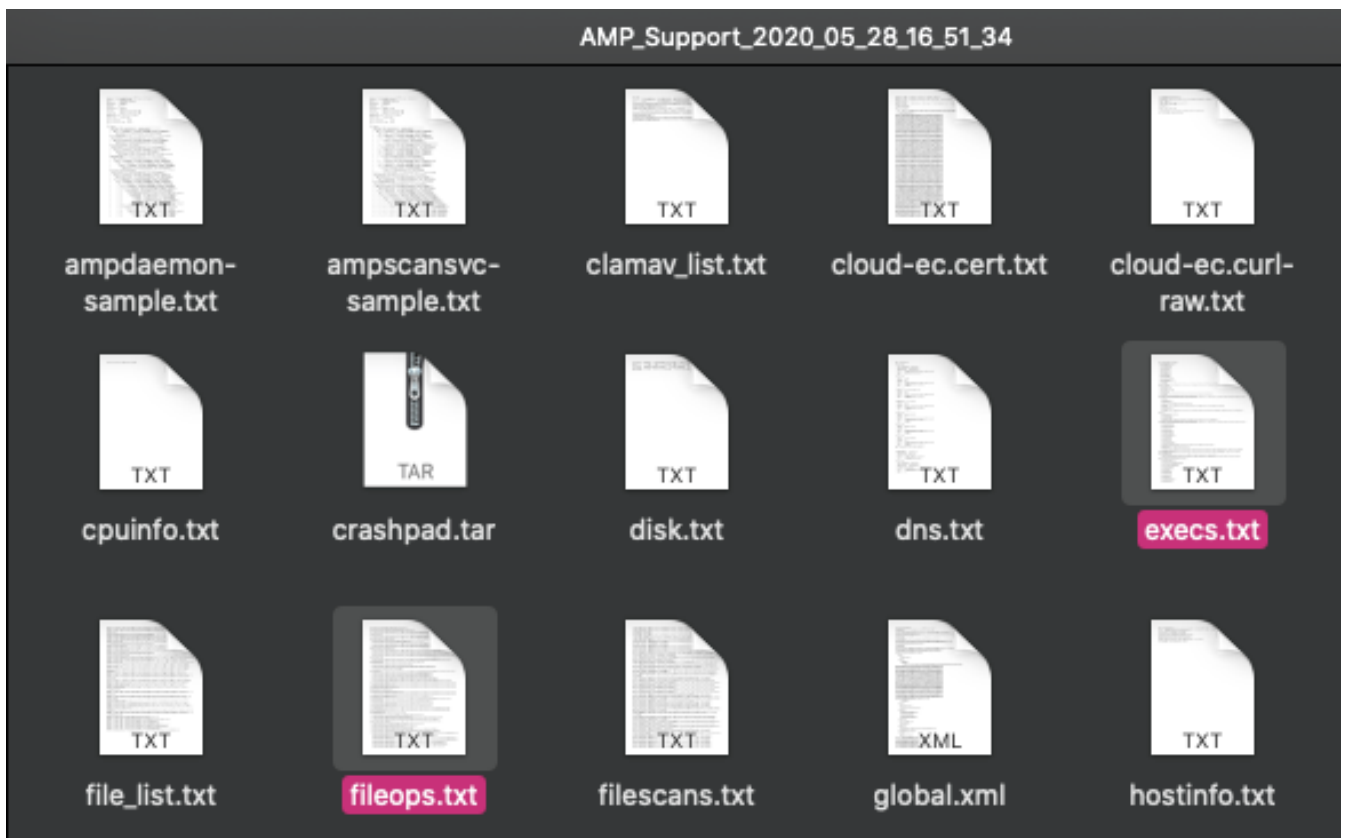
```
jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers
```

Das Debugpaket wird als ZIP-Dateierweiterung im Desktop-Ordner gespeichert.

## Analyse der hohen CPU-Leistung

Das Debug-Diagnosepaket ist im Desktop gespeichert, um die Analyse zu starten:

- Dekomprimieren des Diagnosepakets
- Es müssen zwei Dateien überprüft werden. Dateioperationen: `fileops.txt` Dateiausführungen: `Execs.txt`



- Die Datei fileops.txt dient als Hauptleistungstool zur Fehlerbehebung. Es listet alle aktuell aktiven Vorgänge auf dem Endpunkt auf, während der Connector ausgeführt wird. Es wird wie folgt angezeigt:

### <Bei Paketerfassung durchgeführte Nummernprüfungen auf dem Pfad> / <Scan auf Pfad>

```

fileops.txt
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/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyEventActivityStats.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.Settings.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.GovernedChannelStates.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json

```

Wenn Sie z. B. eine homebrew-Anwendung haben, zeigt fileops.txt die nächsten aktiven Operationen an:

```
639 /Users/jesutorr/Library/Bin/MyApplication/support/
```

```
460 /Users/jesutorr/Library/Bin/MyApplication/logs/
```

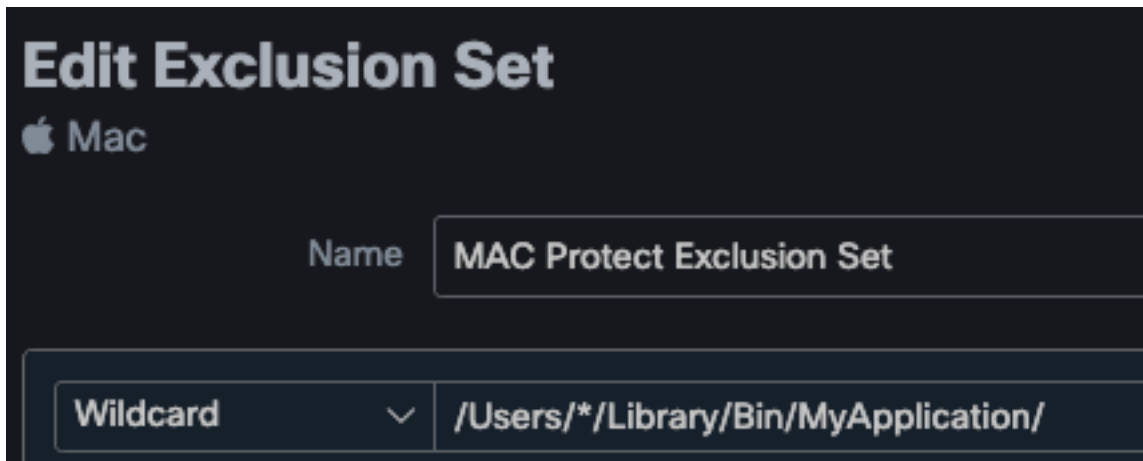
```
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```

```

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/

```

- Nachdem der Prozess identifiziert wurde, kann ein Ausschluss erstellt werden.
- Um den Ausschluss zu schaffen
- Navigieren Sie in der AMP-Konsole zu **Verwaltung > Ausschlüsse**.
- Wählen Sie den Ausschlusssatz aus, und klicken Sie auf **Bearbeiten**.
- Der Ausschluss kann wie im Bild gezeigt hinzugefügt werden.



- Die Datei Execs.txt enthält alle Befehle, die von Prozessen verwendet werden, die ausgeführt werden, während Connector Pakete sammelt. Die hier aufgelisteten Pfade dürfen in der AMP-Richtlinie nicht ausgeschlossen werden, da es sich um Binärdateien (/bin) und Systembinärdateien (/sbin) handelt, die von allen Prozessen verwendet werden. Auf der Execs.txt kann jedoch der Hauptprozess, der ausgeführt wird, bereitgestellt werden. Wenn z. B. die Datei Execs.txt die nächsten Protokolle anzeigt.

```
execs.txt — Edited
501 /bin/bash
96 /usr/bin/defaults
91 /usr/bin/stat
91 /usr/bin/tr
90 /usr/bin/cut
```

Da die Homebrew-Anwendung Bash verwendet, können Sie bestätigen, dass die Anwendung die Ursache für die hohe CPU ist.

## Zugehörige Informationen

- [AMP für Endgeräte: Prozessausschlüsse in MacOS und Linux](#)
- [Best Practices für Ausschlüsse von AMP für Endgeräte](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)