

Analizza il pacchetto diagnostico AMP di macOS per CPU elevata

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Risoluzione dei problemi](#)

[Verificare se nel computer è installato un altro antivirus](#)

[Identificare la CPU elevata quando un'applicazione specifica è in uso](#)

[Ottenere un pacchetto diagnostico per l'analisi](#)

[Livello di debug nell'endpoint](#)

[Debug Level nell'interfaccia della riga di comando di AMP \(CLI\)](#)

[Livello di debug nel criterio](#)

[Escludere AMP da altre soluzioni antivirus](#)

[Riprodurre il problema e raccogliere un pacchetto diagnostico](#)

[Analisi delle prestazioni elevate della CPU](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come analizzare un bundle diagnostico da Advanced Malware Protection (AMP) for Endpoints Public Cloud su dispositivi macOS per risolvere i problemi relativi all'utilizzo elevato della CPU.

Contributo di Uriel Torres e a cura di Yeraldin Sanchez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Navigazione di base in AMP Console
- Navigazione del terminale MAC

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

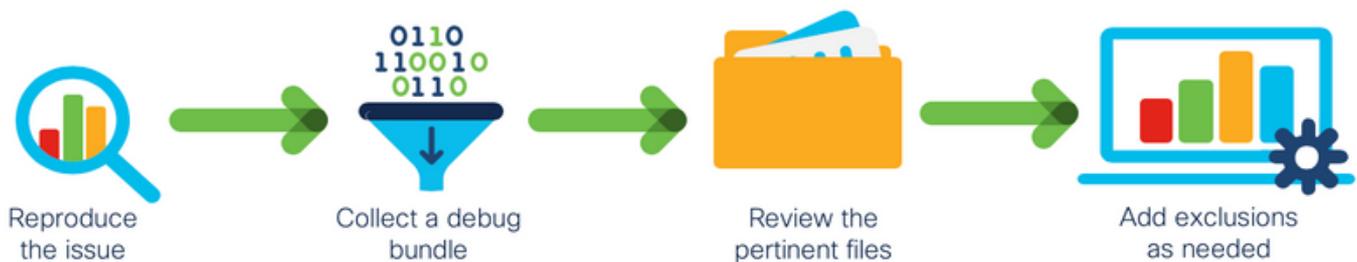
- AMP for Endpoints Console 5.4.20200512
- macOS Catalina versione 10.15.4
- Connettore AMP 1.12.3.738

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

AMP Connector esegue la scansione di tutti i file attivi (quelli che si spostano, copiano e/o modificano da soli) su un computer, a meno che non sia esplicitamente indicato di non farlo. Ciò comporta inevitabilmente problemi di prestazioni se vengono eseguiti troppi processi e troppe operazioni durante l'esecuzione del Connettore, con conseguente elevato utilizzo della CPU, rallentamenti e in alcuni casi software che non viene eseguito o eseguito lentamente. Inoltre, AMP Connector potrebbe bloccare i file in base alla reputazione del cloud, il che può talvolta essere errato (falso positivo). La soluzione a entrambi i problemi consiste nell'escludere questi percorsi e processi.

Il flusso di risoluzione dei problemi relativi alle prestazioni è mostrato nell'immagine.



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Verificare se nel computer è installato un altro antivirus

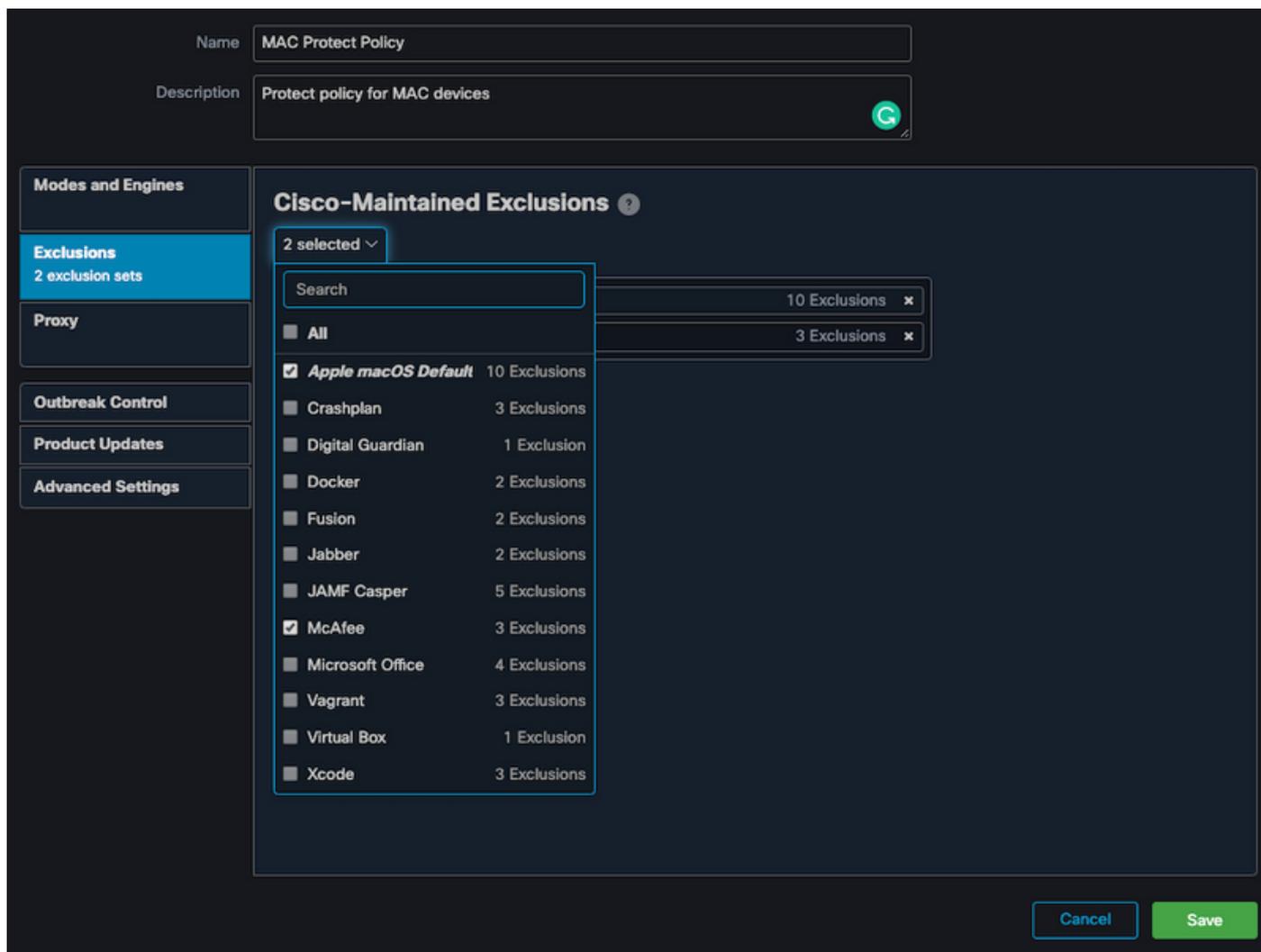
Suggerimento: Utilizzare le esclusioni gestite da Cisco se il software in uso è incluso nell'elenco, tenere presente che tali esclusioni possono essere aggiunte alle nuove versioni di un'applicazione.

Per visualizzare gli elenchi disponibili nella sezione delle esclusioni gestite da Cisco sulla console AMP:

- Passare a **Gestione > Criteri**.
- Trovare il criterio e fare clic su **Modifica**.
- Sul criterio, finestra impostazioni fare clic su **Esclusioni**.

Selezionare quelli necessari all'endpoint in base al software attualmente installato nel computer,

quindi salvare il criterio, come mostrato nell'immagine.



Identificare la CPU elevata quando un'applicazione specifica è in uso

Identificare se il problema si verifica durante l'esecuzione di un'applicazione o di alcune di esse, se si è in grado di replicare il problema, in modo da identificare potenziali esclusioni.

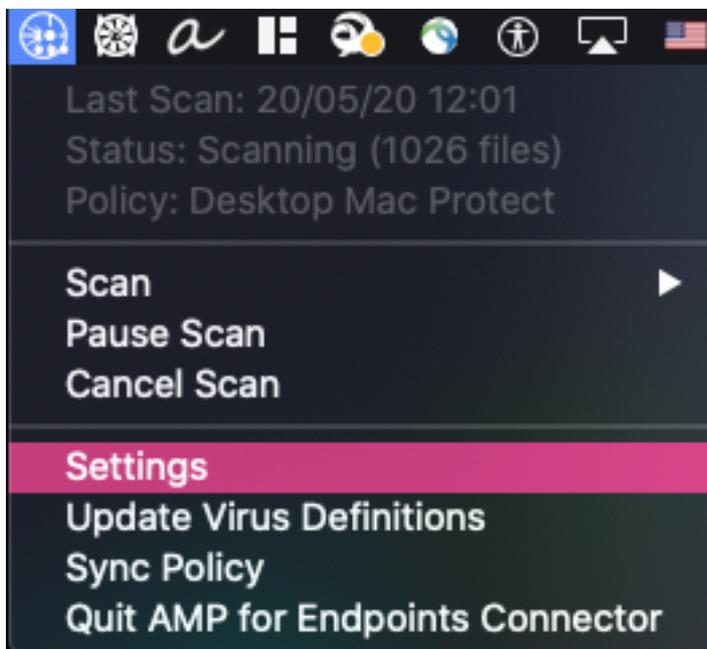
Ottenere un pacchetto diagnostico per l'analisi

Per raccogliere un pacchetto diagnostico utile, è necessario abilitare il livello del log di debug.

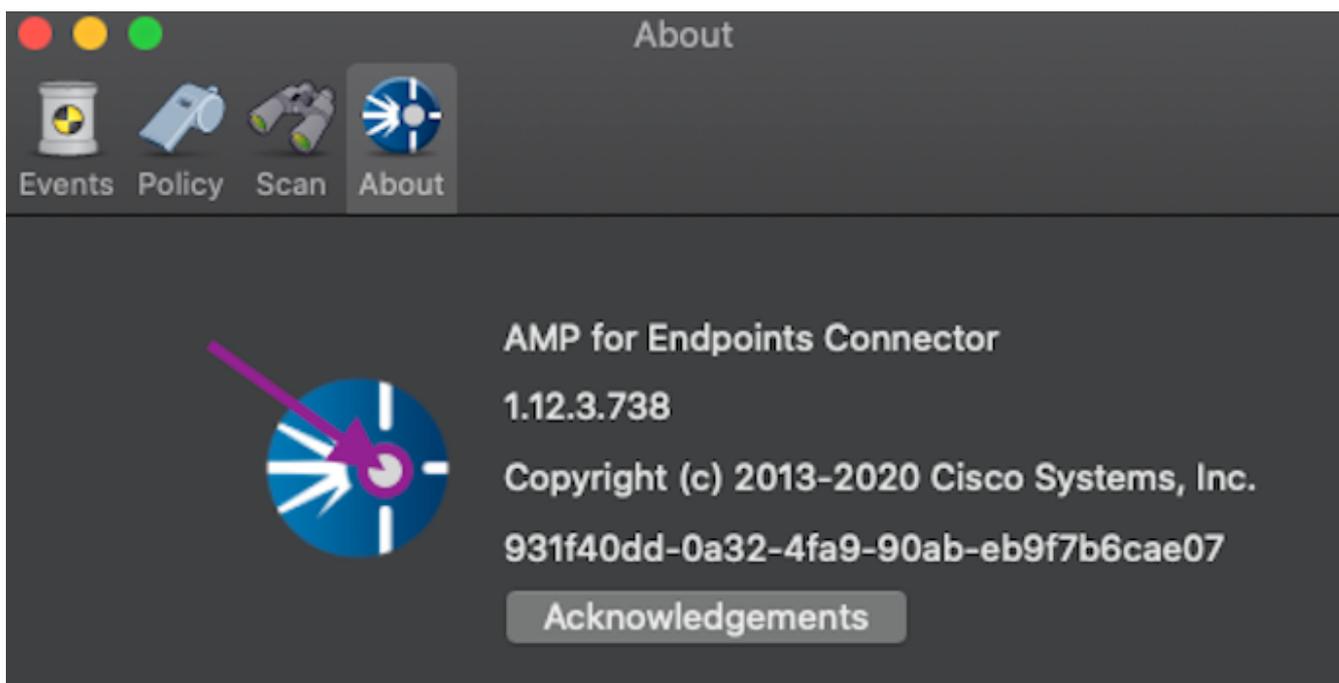
Livello di debug nell'endpoint

Se è possibile replicare il problema e accedere all'endpoint, di seguito è riportata la procedura ottimale per acquisire il bundle di diagnostica.

- Sulla barra del menu MAC fare clic sull'icona AMP.
- Passare alla sezione **Settings** (Impostazioni), come mostrato nell'immagine.



- Nelle finestre delle impostazioni, passare a **Informazioni su**.
- Per abilitare la modalità di debug, fare clic all'interno del logo AMP, come mostrato nell'immagine.



Un menu di scelta rapida indica che il connettore AMP è in modalità di debug

Questa procedura abilita il livello del registro di debug fino al successivo intervallo di heartbeat dei criteri.

Debug Level nell'interfaccia della riga di comando di AMP (CLI)

- Apri terminale
- Andare sul sito `/opt/cisco/amp/bin/`
- Esegui `ampcli`:
`./ampcli`

- Dalla CLI di AMP abilitare la modalità di debug:

```
ampcli>debuglevel 1
```

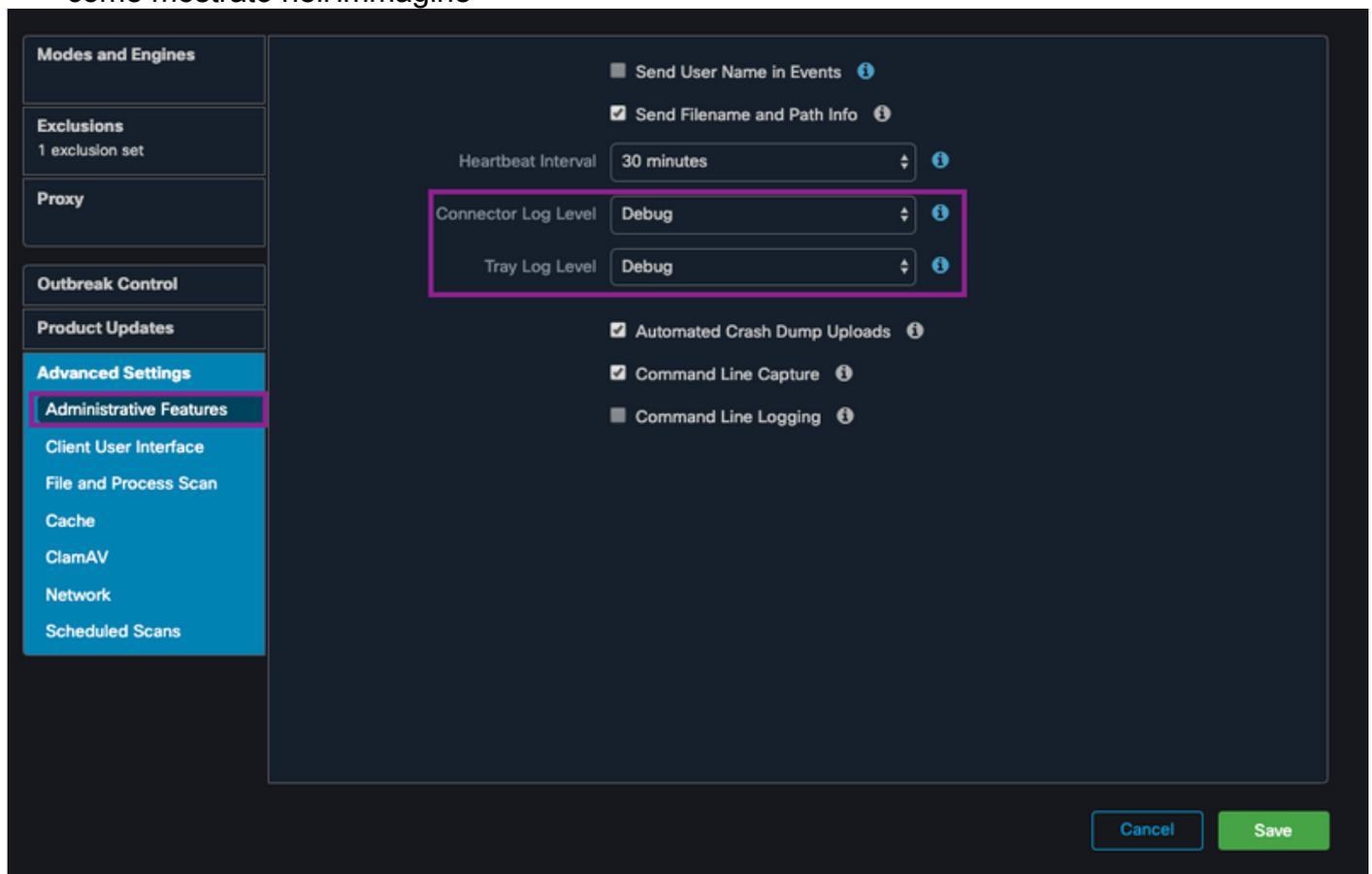
Questo processo abilita il livello del registro di debug fino al successivo intervallo di heartbeat dei criteri.

Livello di debug nel criterio

Se non si dispone dell'accesso all'endpoint o se il problema non può essere riprodotto in modo coerente, è necessario abilitare il livello del registro di debug nel criterio.

Per abilitare il livello di log di debug in base al criterio:

- Passare a **Gestione > Criteri**
- Trovare il criterio e fare clic su **Modifica**
- Selezionare **Impostazioni avanzate > Funzioni amministrative**
- Configurare **Connector Log Level** e **Tray Log Level** per eseguire il debug e salvare il criterio, come mostrato nell'immagine



Attenzione: Se la modalità di debug è abilitata dal criterio, tutti gli endpoint ricevono questa configurazione.

Nota: Sincronizzare i criteri dell'endpoint per verificare la modalità di debug.

Escludere AMP da altre soluzioni antivirus

Secondo la guida per l'utente, i prodotti antivirus devono escludere le directory successive e tutti i

file, le directory e i file eseguibili al loro interno per essere compatibili con AMP Connector for MAC, le directory da escludere sono le seguenti:

- /Library/Supporto applicazioni/Cisco/AMP for Endpoints Connector
- /opt/cisco/amp

Riprodurre il problema e raccogliere un pacchetto diagnostico

Quando il livello di debug è configurato, attendere che sul sistema si verifichi lo stato High CPU (CPU elevata) o riprodurre manualmente le condizioni precedentemente identificate, quindi raccogliere il pacchetto di diagnostica.

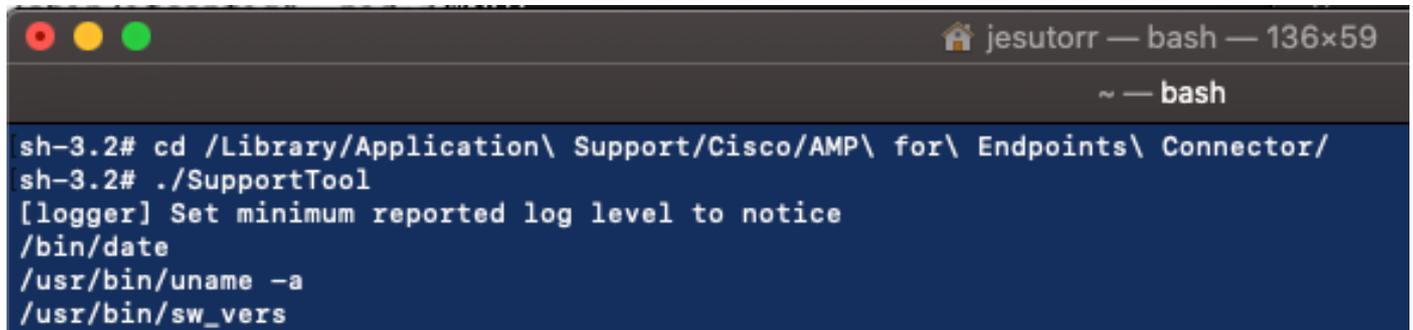
Per raccogliere il bundle di debug:

- Aprire un terminale.
- Accedere al livello superuser, quindi selezionare **/Library/Application Support/Cisco/AMP for Endpoints Connector**:

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

- Per eseguire lo strumento di supporto, usare il comando seguente:

```
./SupportTool
```



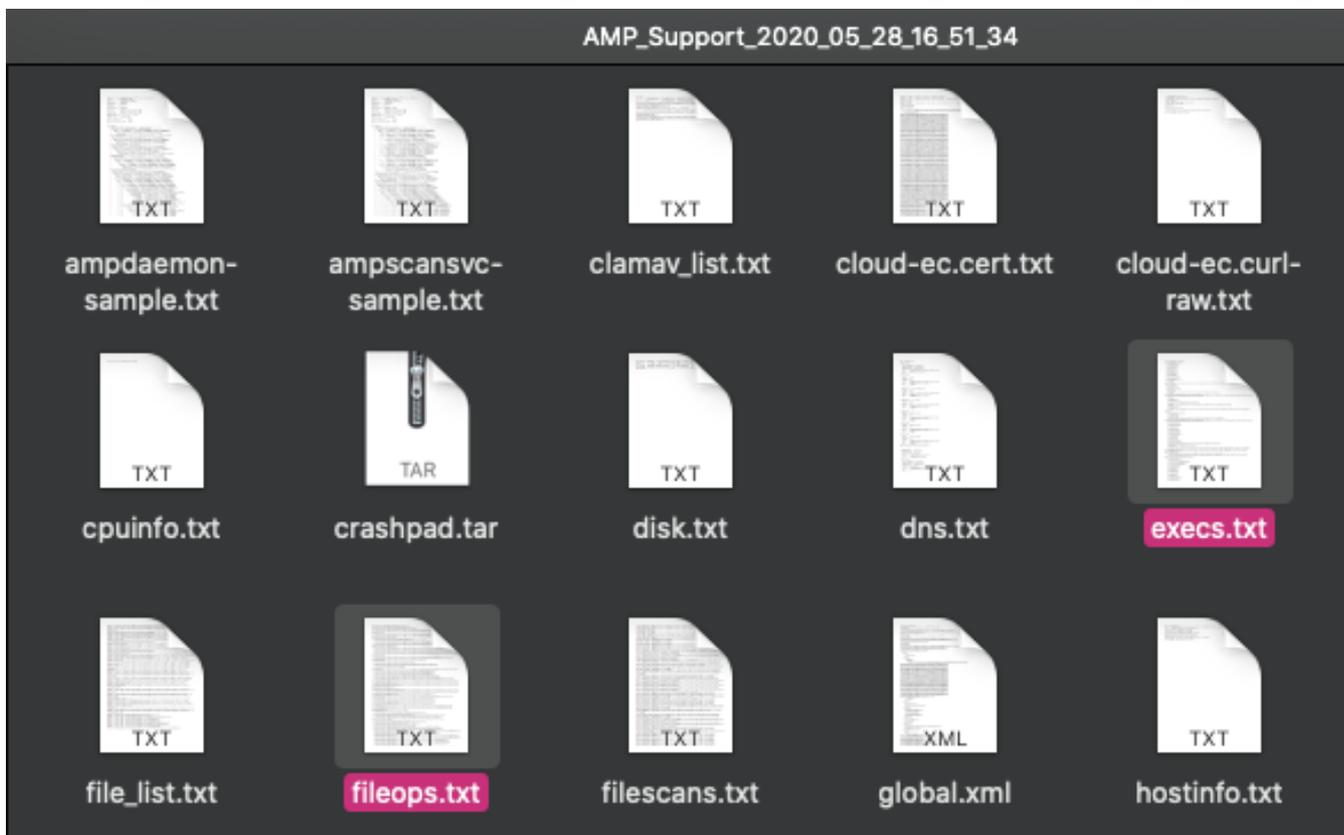
```
jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers
```

Il bundle di debug viene salvato nella cartella Desktop con estensione .zip.

Analisi delle prestazioni elevate della CPU

Il bundle di diagnostica per il debug è lo storage nel desktop, per avviare l'analisi:

- Decomprimi pacchetto diagnostico
- Ci sono 2 file da rivedere Operazioni sui file: fileops.txt Esecuzioni file: execs.txt



- Il file fileops.txt funge da strumento di prestazioni principale per la risoluzione dei problemi. Durante l'esecuzione del connettore, vengono elencate tutte le operazioni attualmente attive sull'endpoint. Di seguito è riportato l'elenco:

<Numero di scansioni eseguite sul percorso al momento della raccolta del bundle> /
 <Percorso scansionato>

```

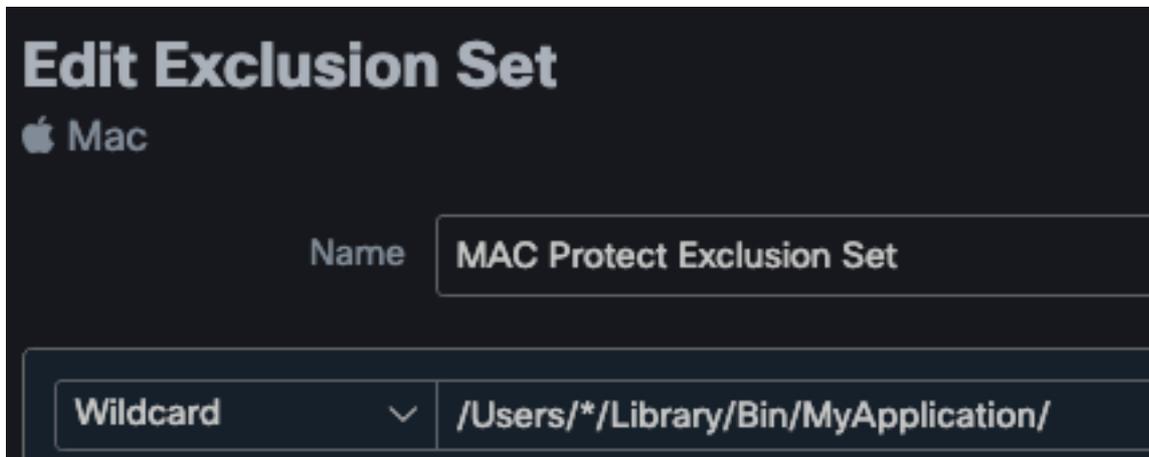
fileops.txt
19 /Library/Application Support/Apple/ParentalControls/Users/jesutorr/2020/05/21-usage.data
18 /Users/jesutorr/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/Config/dummy_phoneInfo
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json
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
  
```

Ad esempio, se si dispone di un'applicazione homebrew, il file fileops.txt mostra le successive operazioni attive:

```

639 /Users/jesutorr/Library/Bin/MyApplication/support/
460 /Users/jesutorr/Library/Bin/MyApplication/logs/
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
  
```

- Una volta identificato il processo, è possibile creare un'esclusione
- Per creare l'esclusione
- In AMP Console passare a **Gestione > Esclusioni**
- Selezionare il set di esclusione e fare clic su **Modifica**
- L'esclusione può essere aggiunta come mostrato nell'immagine



- Il file Execs.txt contiene tutti i comandi utilizzati dai processi che vengono eseguiti durante la raccolta dei bundle da parte del connettore. I percorsi elencati non devono essere esclusi dai criteri AMP, poiché si tratta di binari (/bin) e binari di sistema (/sbin) utilizzati da tutti i processi, tuttavia, in Execs.txt è in grado di fornire il processo principale in esecuzione. Ad esempio, se il file Execs.txt visualizza i log successivi.

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

Poiché l'applicazione homebrew utilizza bash, è possibile confermare che l'applicazione è la causa dell'elevata CPU.

Informazioni correlate

- [AMP for Endpoints: Esclusioni dei processi in macOS e Linux](#)
- [Best practice per le esclusioni di AMP for Endpoints](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)