

Analisar o pacote de diagnóstico AMP do macOS para CPU alta

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Troubleshoot](#)

[Verifique se outro antivírus está instalado na máquina](#)

[Identificar a CPU alta quando um aplicativo específico está em uso](#)

[Obtenha um pacote de diagnóstico para análise](#)

[Nível de depuração no endpoint](#)

[Nível de depuração na CLI \(Command Line Interface, interface de linha de comando\) do AMP](#)

[Nível de depuração na política](#)

[Excluir a AMP de outras soluções antivírus](#)

[Reproduza o problema e reúna um pacote de diagnóstico](#)

[Análise do alto desempenho da CPU](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve as etapas para analisar um pacote de diagnóstico da AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints nuvem pública em dispositivos macOS para solucionar problemas de uso elevado da CPU.

Contribuído por Uriel Torres e editado por Yeraldin Sanchez, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Navegação básica no console AMP
- Navegação do terminal MAC

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- AMP para endpoints Console 5.4.200512
- macOS Catalina versão 10.15.4
- Conector AMP 1.12.3.738

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O conector AMP verifica todos os arquivos ativos (aqueles que se movem, copiam e/ou modificam a si mesmos) em uma máquina, a menos que explicitamente informado para não fazê-lo, isso inevitavelmente trará problemas de desempenho se muitos processos e operações forem executados enquanto o conector estiver em execução, o que leva a uma alta utilização da CPU, retarda e, em alguns casos, um software que não será executado ou executado lentamente. Além disso, o conector AMP pode bloquear arquivos com base na reputação da nuvem, o que pode, às vezes, ser errado (falso positivo). A solução para ambos os problemas é excluir esses caminhos e processos.

O fluxo de problemas de desempenho de solução de problemas é mostrado na imagem.



Troubleshoot

Esta seção fornece as informações que você pode usar para solucionar problemas de sua configuração.

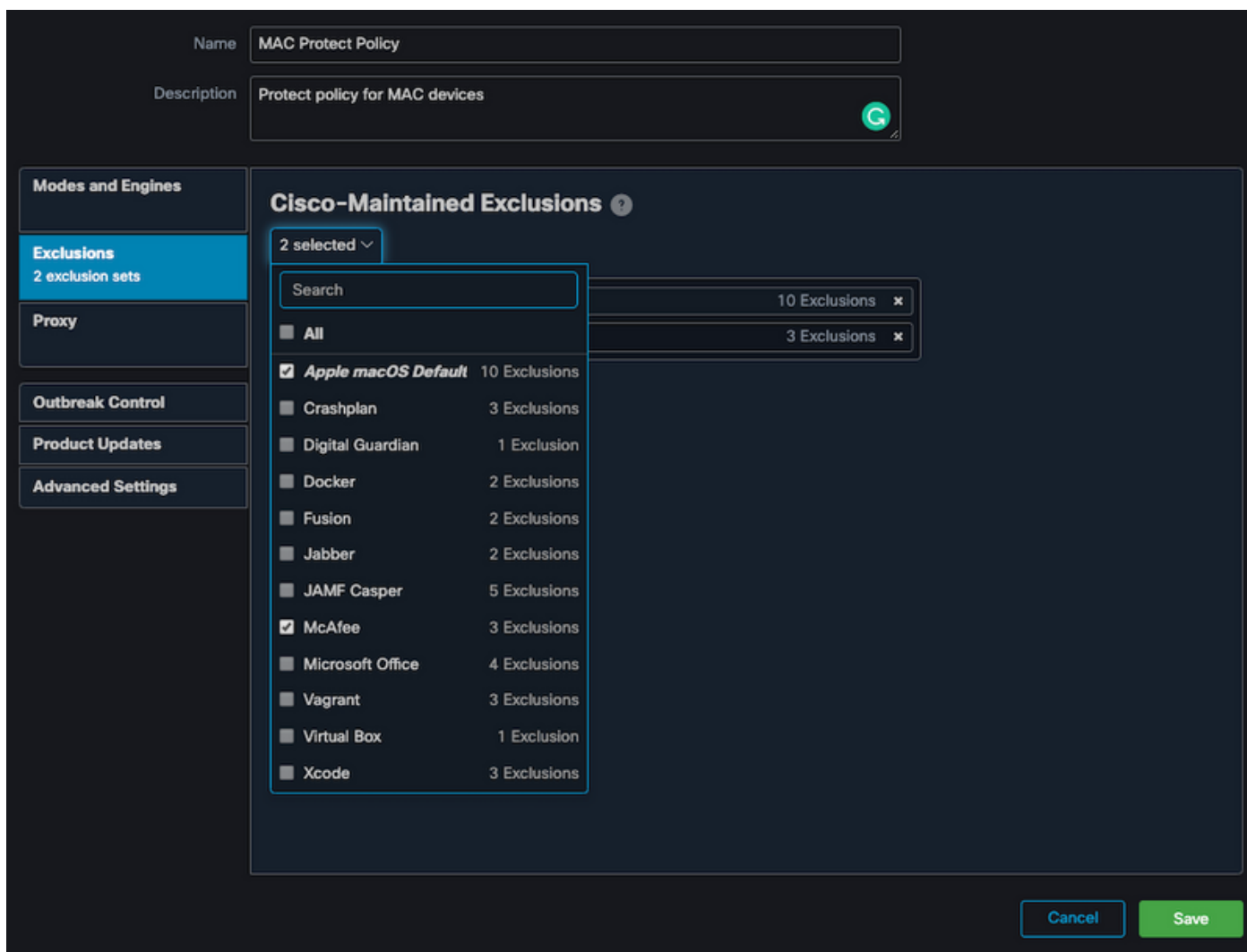
Verifique se outro antivírus está instalado na máquina

Tip: Use as exclusões mantidas pela Cisco se o software usado estiver incluído na lista. Lembre-se de que essas exclusões podem ser adicionadas a novas versões de um aplicativo.

Para ver as listas disponíveis na seção de exclusões mantidas da Cisco no console da AMP:

- Navegue até **Gerenciamento > Políticas**.
- Localize a diretiva e clique em **Editar**.
- Na janela de configurações, clique em **Exclusões**.

Selecione os que seu endpoint precisaria de acordo com o software atualmente instalado na máquina e salve a diretiva, como mostrado na imagem.



Identificar a CPU alta quando um aplicativo específico está em uso

Identifique se o problema acontece enquanto um ou alguns deles são executados se você puder replicar o problema ajuda no processo para identificar possíveis exclusões.

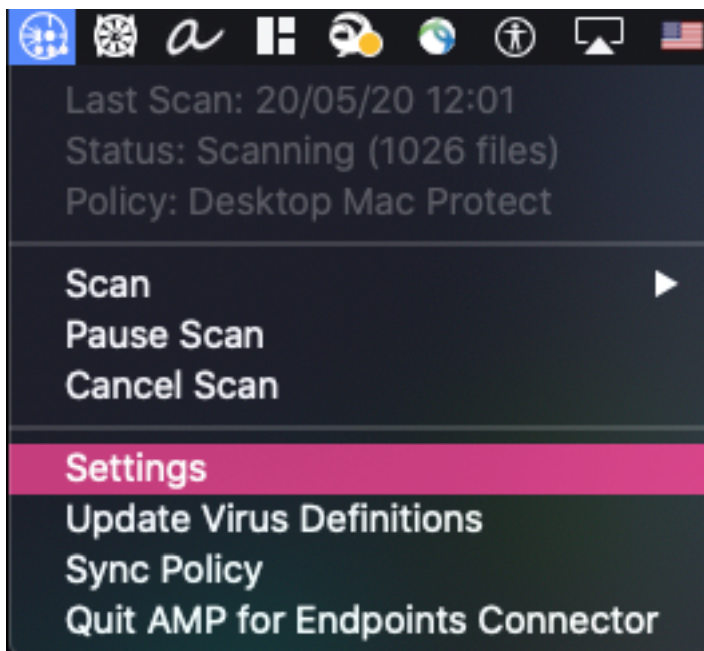
Obtenha um pacote de diagnóstico para análise

Para reunir um pacote de diagnóstico útil, o nível de log de depuração deve ser ativado.

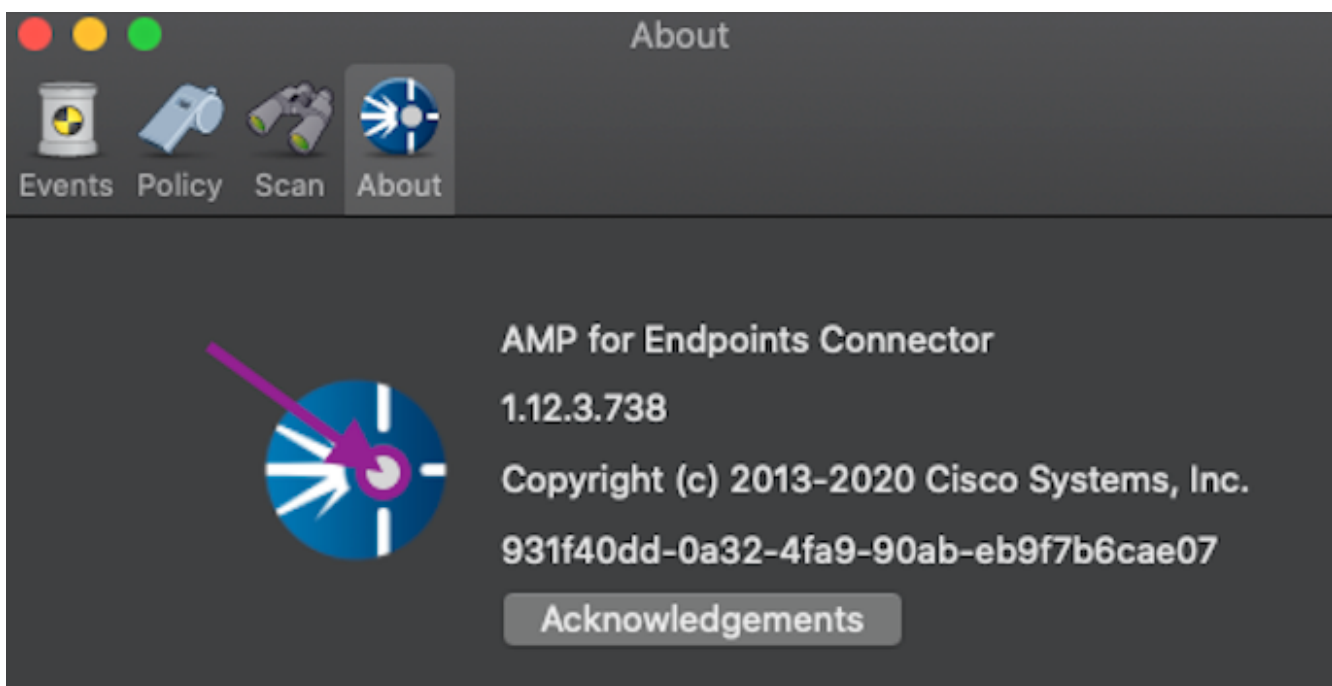
Nível de depuração no endpoint

Se você puder replicar o problema e ter acesso ao endpoint, abaixo está o melhor procedimento para capturar o pacote de diagnóstico.

- Na barra de menus do MAC, clique no ícone AMP.
- Navegue até a seção **Configurações**, conforme mostrado na imagem.



- Nas janelas de configurações, navegue para **Sobre**.
- Para habilitar o modo de depuração, clique dentro do logotipo AMP, como mostrado na imagem.



Um pop-up indica que o conector AMP está no modo de depuração

Este procedimento ativa o nível de log de depuração até o próximo intervalo de pulsação da política.

Nível de depuração na CLI (Command Line Interface, interface de linha de comando) do AMP

- Abrir um terminal
- Navegue até `/opt/cisco/amp/bin/`
- Executar o ampcli:
`./ampcli`

- No modo de depuração do AMP CLI:

```
ampcli>debuglevel 1
```

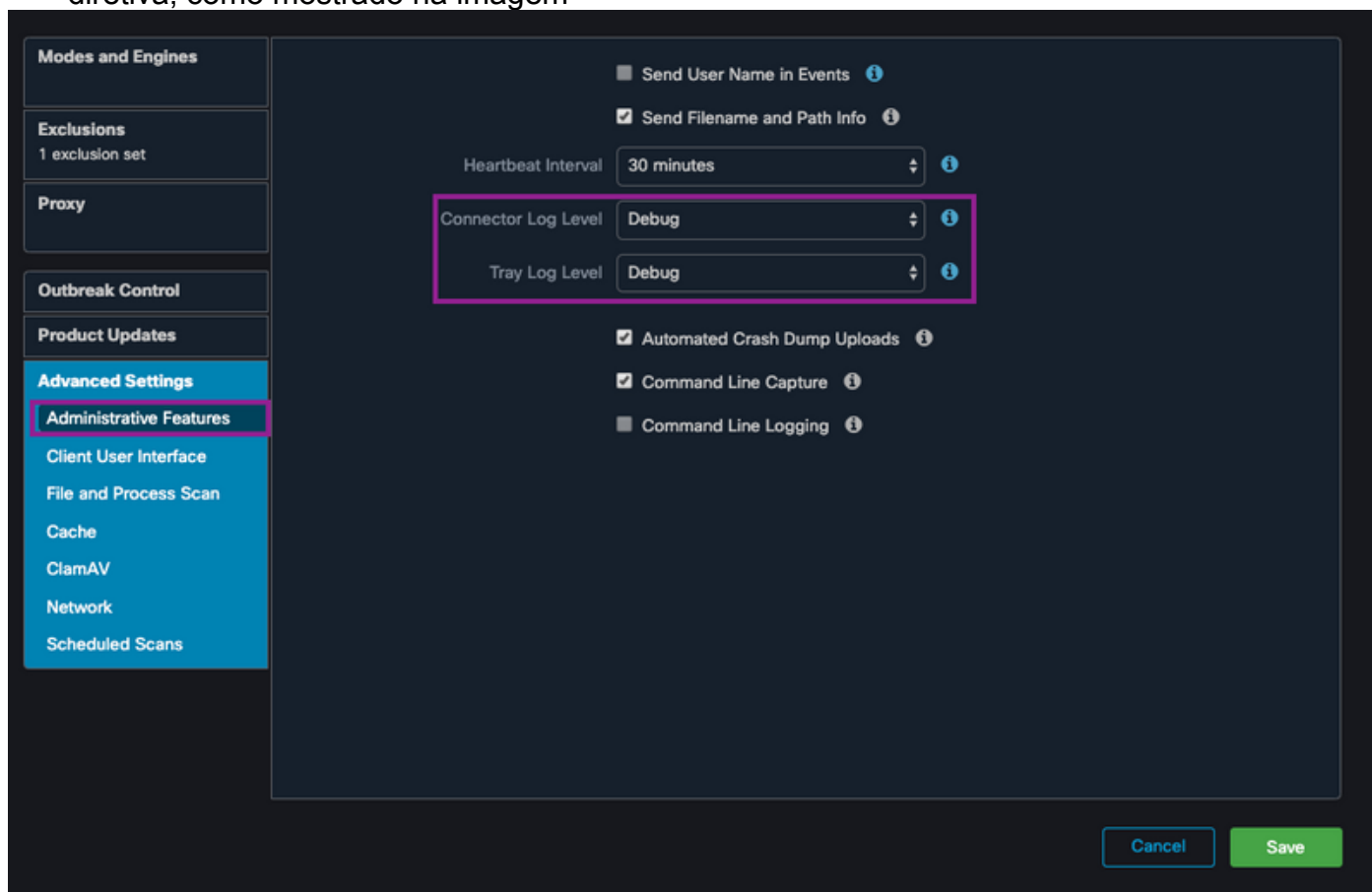
Esse processo ativa o nível de log de depuração até o próximo intervalo de pulsação da política.

Nível de depuração na política

Se você não tiver acesso ao endpoint ou se o problema não puder ser reproduzido de forma consistente, o nível de log de depuração deverá estar ativado na política.

Para habilitar o nível de log de depuração pela política:

- Navegue até **Gerenciamento > Políticas**
- Localize a diretiva e clique em **Editar**
- Navegue até **Configurações avançadas > Recursos administrativos**
- Configure o **Nível de log do conector** e o **Nível de log da bandeja** para **Depurar** e salvar a diretiva, como mostrado na imagem



Caution: Se o modo de depuração estiver ativado na política, todos os endpoints receberão essa configuração.

Note: Sincronize a política do endpoint para garantir o modo de depuração.

Excluir a AMP de outras soluções antivírus

De acordo com o guia do usuário, os produtos antivírus devem excluir os próximos diretórios e arquivos, diretórios e arquivos executáveis dentro deles para serem compatíveis com o conector

AMP para MAC, os diretórios a serem excluídos são os seguintes:

- `/Library/Supporte a aplicativos/Cisco/AMP para conector de endpoints`
- `/opt/cisco/amp`

Reproduza o problema e reúna um pacote de diagnóstico

Quando o nível de depuração estiver configurado, aguarde até que o estado de CPU alta ocorra no sistema ou reproduza manualmente as condições identificadas anteriormente e reúna o pacote de diagnóstico.

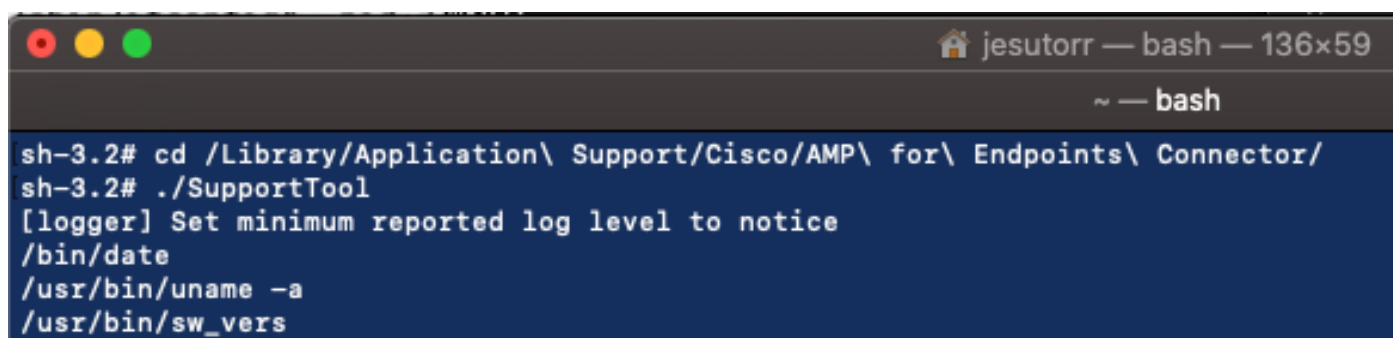
Para coletar o pacote de depuração:

- Abra um terminal.
- Acesso ao nível de superusuário e, em seguida, navegue até `/Library/Application Support/Cisco/AMP for Endpoints Connector/`

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

- Para executar a ferramenta de suporte, use o próximo comando:

```
./SupportTool
```



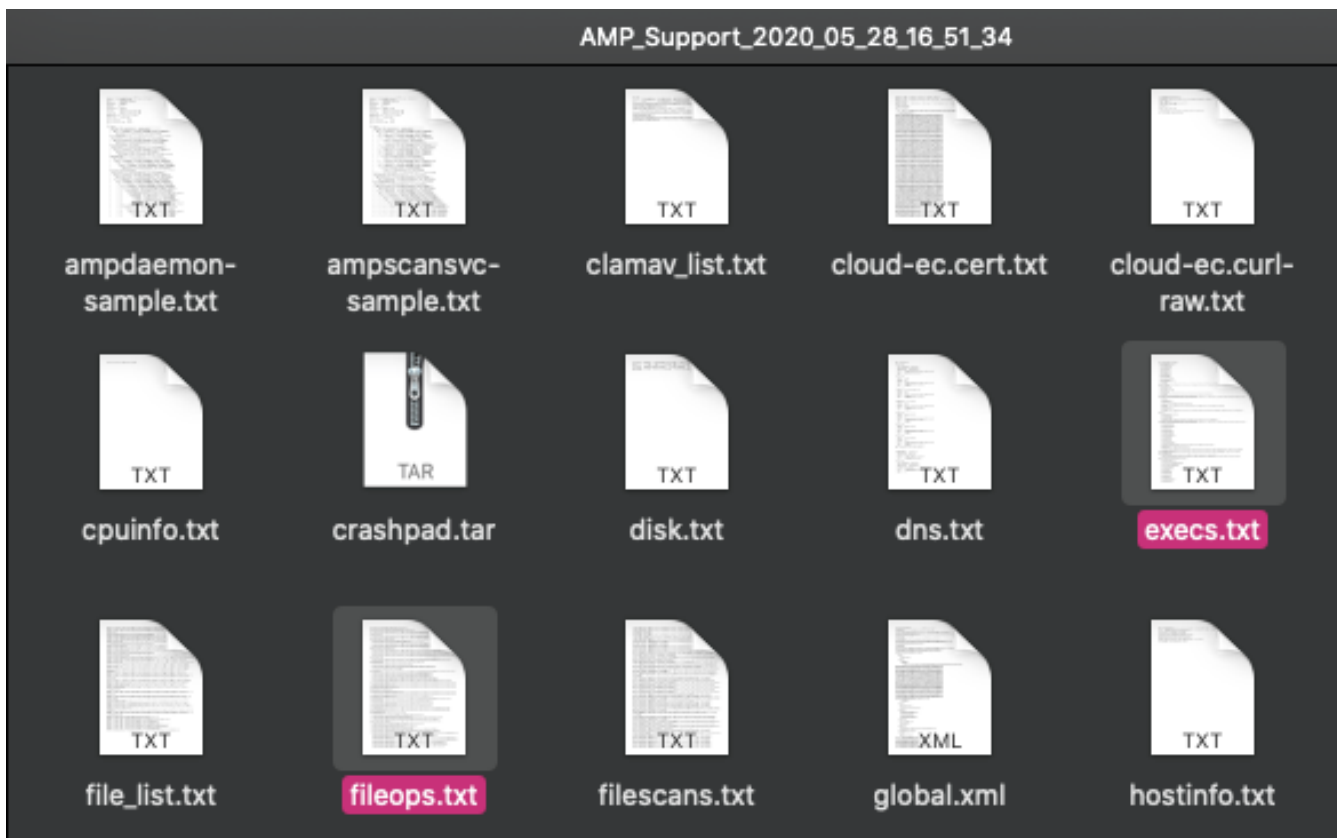
```
jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers
```

O pacote de depuração é salvo na pasta Desktop como uma extensão de arquivo .zip.

Análise do alto desempenho da CPU

O pacote de diagnóstico de depuração é o armazenamento na área de trabalho, para iniciar a análise:

- Descompacte o pacote de diagnóstico
- Há dois arquivos para revisar Operações de arquivo: `fileops.txt` Execuções de arquivo: `execs.txt`



- O fileops.txt funciona como a principal ferramenta de desempenho para solucionar problemas. Ele lista todas as operações atualmente ativas em seu endpoint enquanto o conector é executado. Ele é lido da seguinte maneira:

<Varredura de números realizada no caminho quando o pacote é coletado> / <Caminho digitalizado>

```

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

```

Por exemplo, se você tem um aplicativo homebrew, fileops.txt mostra as próximas operações ativas:

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

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

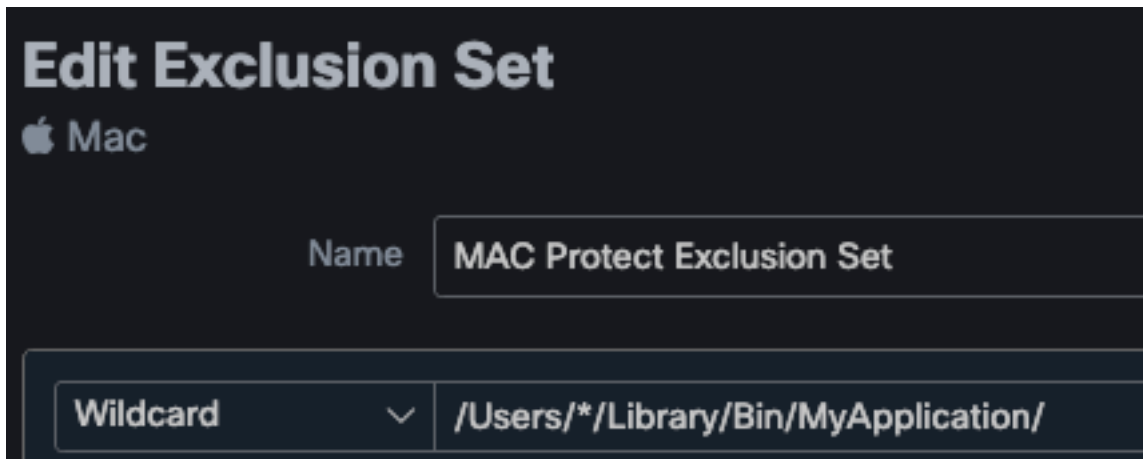
```
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```

```

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/

```

- Uma vez identificado o processo, uma exclusão pode ser criada
- Para criar a exclusão
- No Console do AMP, navegue para **Gerenciamento > Exclusões**
- Selecione o conjunto de exclusões e clique em **Editar**
- A exclusão pode ser adicionada conforme mostrado na imagem



- O arquivo Execs.txt contém todos os comandos usados por processos executados enquanto o conector coleta pacotes. Os caminhos listados aqui não devem ser excluídos na política AMP, pois são binários (/bin) e binários de sistema (/sbin) que todos os processos utilizam, no entanto, no Execs.txt pode fornecer o processo principal que está sendo executado. Por exemplo, se o arquivo Execs.txt mostrar os próximos logs.

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

Como o aplicativo homebrew usa bash, você pode confirmar se o aplicativo é a causa da alta CPU.

Informações Relacionadas

- [AMP para endpoints: Exclusões de processos em MacOS e Linux](#)
- [Práticas recomendadas para exclusões da AMP para endpoints](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)