

Analizar el paquete de diagnóstico de MACOS AMP para una CPU elevada

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Troubleshoot](#)

[Compruebe si hay otro antivirus instalado en el equipo](#)

[Identificar la CPU elevada cuando una aplicación específica está en uso](#)

[Obtener un paquete de diagnóstico para el análisis](#)

[Nivel de depuración en el terminal](#)

[Nivel de depuración en la interfaz de línea de comandos \(CLI\) de AMP](#)

[Nivel de depuración en la política](#)

[Excluir AMP de otras soluciones antivirus](#)

[Reproduzca el problema y recopile un paquete de diagnóstico](#)

[Análisis del alto rendimiento de la CPU](#)

[Información Relacionada](#)

Introducción

Este documento describe los pasos para analizar un paquete de diagnóstico de la protección frente a malware avanzado (AMP) para terminales de nube pública en dispositivos macOS para resolver problemas de uso elevado de la CPU.

Colaborado por Uriel Torres y editado por Yeraldin Sanchez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Navegación básica en la consola de AMP
- Navegación del terminal MAC

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Consola de AMP para terminales 5.4.20200512
- versión 10.15.4 de macOS Catalina
- Conector de AMP 1.12.3.738

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El conector de AMP analiza todos los archivos activos (aquellos que se mueven, copian y/o modifican) en una máquina a menos que se les indique explícitamente que no lo hagan, lo que inevitablemente provoca problemas de rendimiento si se ejecutan demasiados procesos y operaciones mientras el conector se está ejecutando, lo que conduce a una alta utilización de la CPU, ralentizaciones y, en algunos casos, software que no se ejecutará o se ejecutará lentamente. Además, AMP Connector puede bloquear los archivos en función de su reputación en la nube, que en ocasiones puede ser errónea (falso positivo). La solución a ambos problemas es excluir estas rutas y procesos.

El flujo de resolución de problemas de rendimiento se muestra en la imagen.



Troubleshoot

Esta sección proporciona la información que puede utilizar para resolver problemas de su configuración.

Compruebe si hay otro antivirus instalado en el equipo

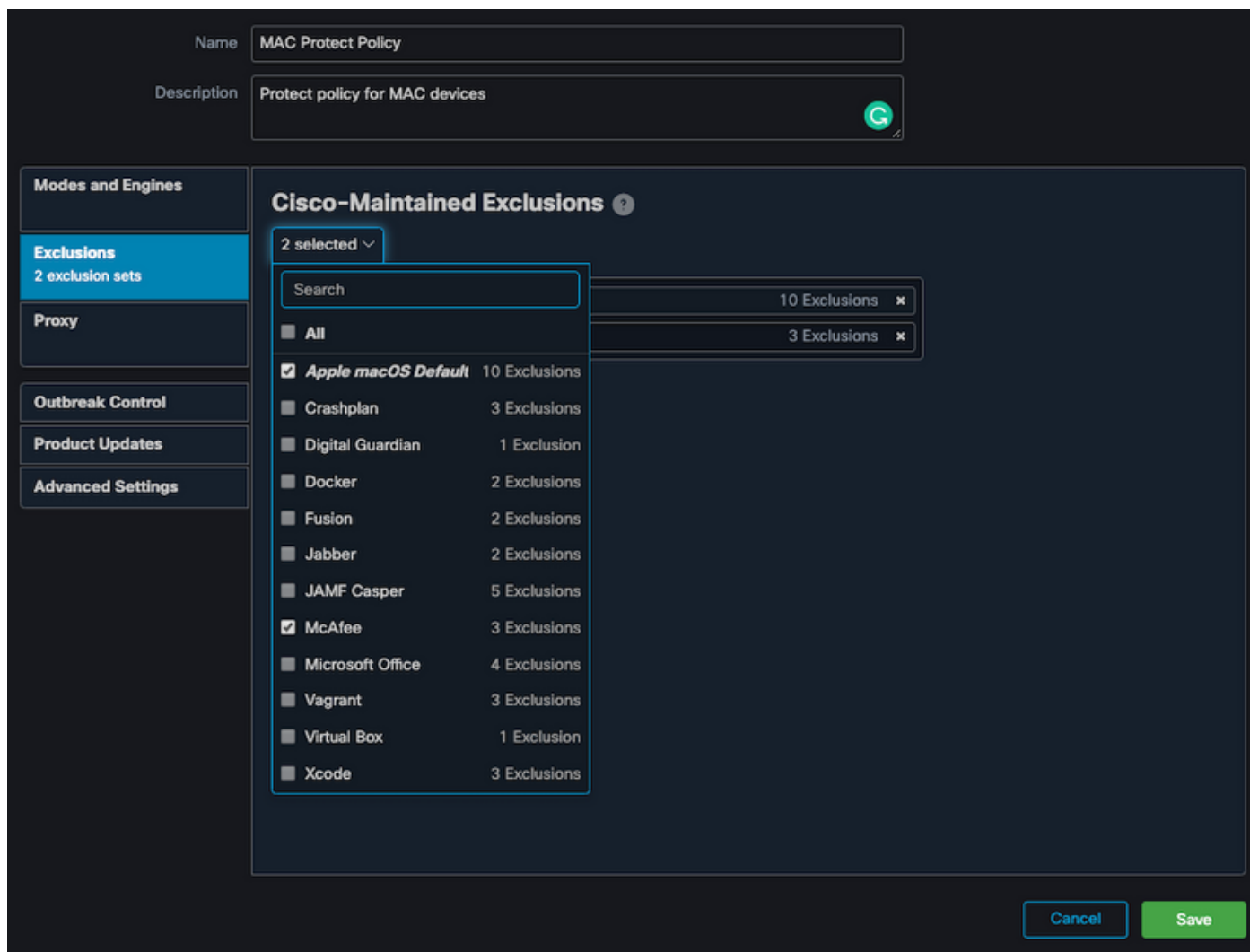
Consejo: Utilice las exclusiones de Cisco mantenidas si el software que se utiliza está incluido en la lista, recuerde que estas exclusiones se pueden agregar a las nuevas versiones de una aplicación.

Para ver las listas disponibles en la sección de exclusiones mantenidas por Cisco en la consola de AMP:

- Vaya a **Administración > Políticas**.
- Busque la política y haga clic en **Editar**.
- En la ventana de políticas, los ajustes hacen clic en **Exclusiones**.

Seleccione los que el terminal necesitaría según el software instalado actualmente en el equipo y,

a continuación, guarde la política, como se muestra en la imagen.



Identificar la CPU elevada cuando una aplicación específica está en uso

Identifique si el problema ocurre mientras se ejecuta una o varias aplicaciones si puede replicar el problema ayuda en el proceso a identificar posibles exclusiones.

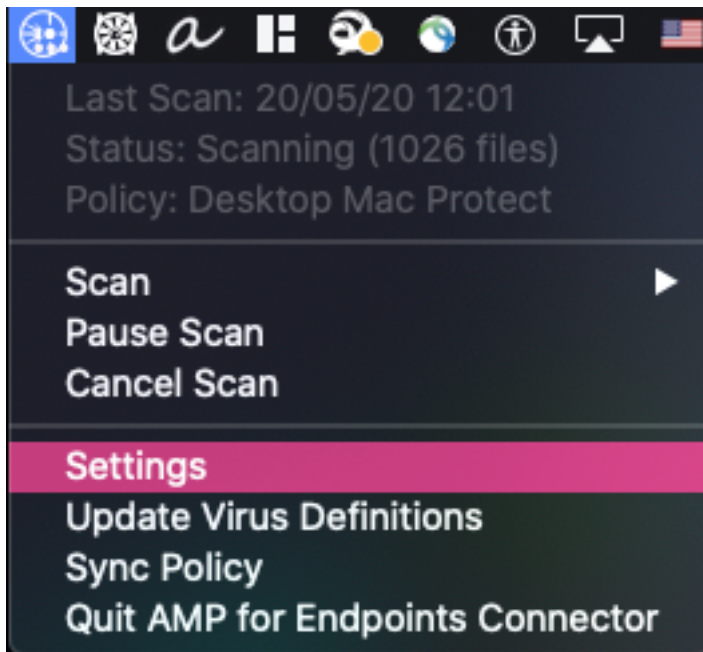
Obtener un paquete de diagnóstico para el análisis

Para recopilar un paquete de diagnóstico útil, se debe habilitar el nivel de registro de depuración.

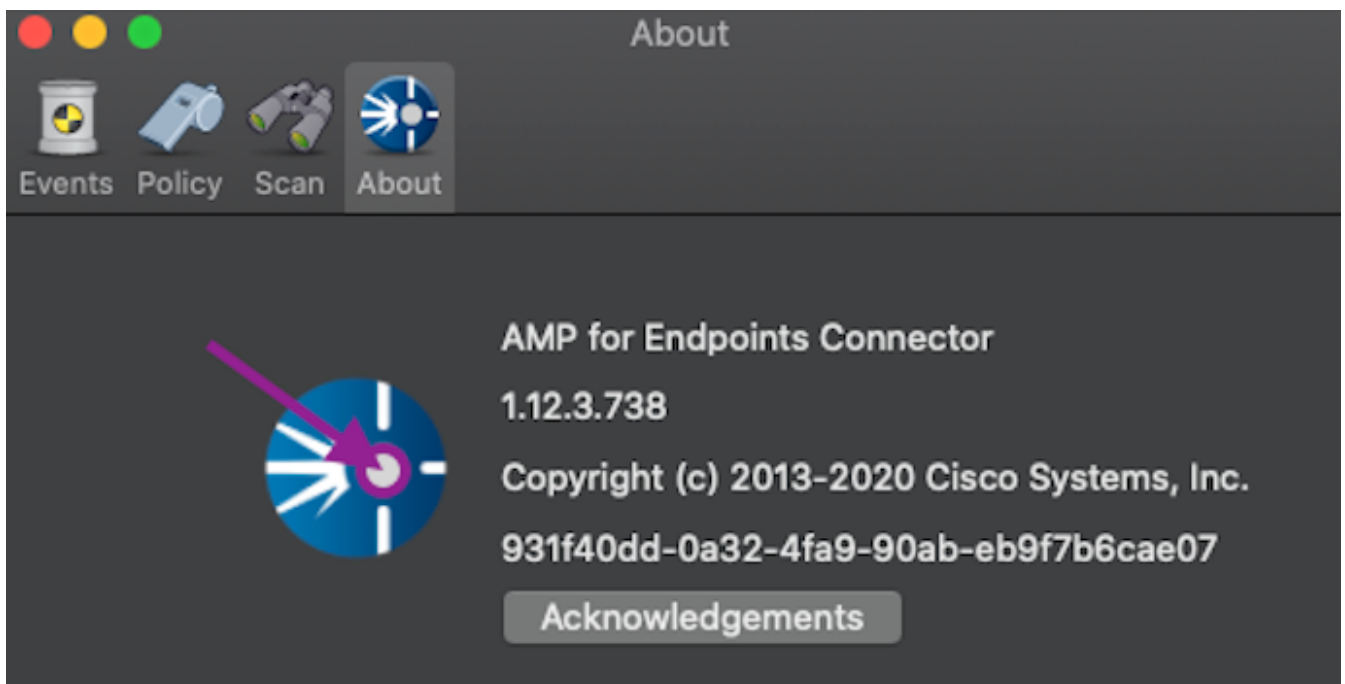
Nivel de depuración en el terminal

Si puede replicar el problema y tener acceso al terminal, a continuación se muestra el mejor procedimiento para capturar el paquete de diagnóstico.

- En la barra de menú MAC, haga clic en el icono AMP.
- Vaya a la sección **Configuración**, como se muestra en la imagen.



- En las ventanas de configuración, vaya a **About**.
- Para habilitar el modo de depuración, haga clic dentro del logotipo de AMP, como se muestra en la imagen.



Una ventana emergente indica que el conector de AMP está en modo de depuración

Este procedimiento habilita el nivel de registro de depuración hasta el siguiente intervalo de latido de política.

Nivel de depuración en la interfaz de línea de comandos (CLI) de AMP

- Abrir un terminal
- Vaya a `/opt/cisco/amp/bin/`
- Ejecute `ampcli`:
`./ampcli`

- En el modo de depuración de habilitación de AMP CLI:

```
ampcli>debuglevel 1
```

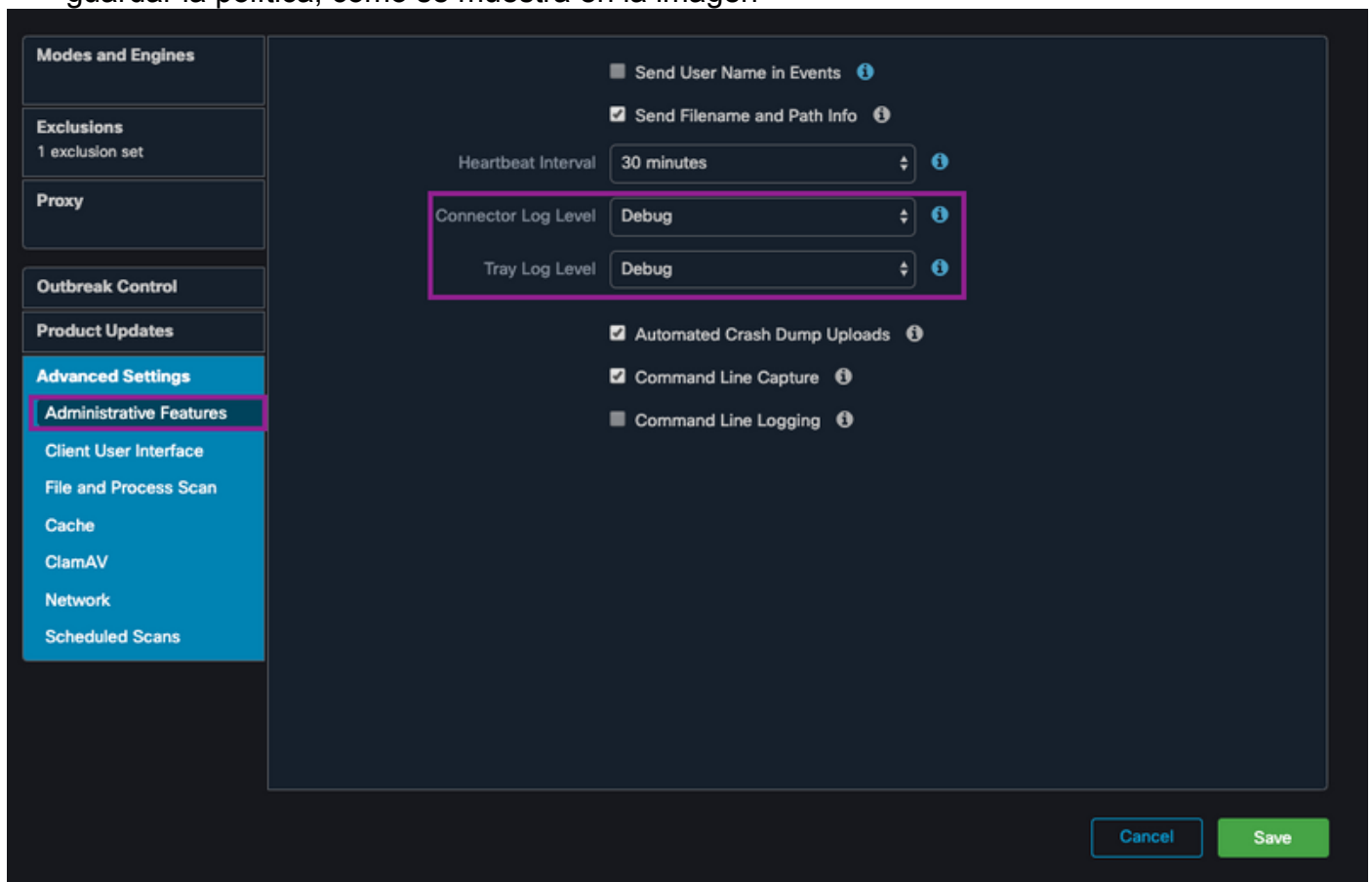
Este proceso habilita el nivel de registro de depuración hasta el siguiente intervalo de latido de política.

Nivel de depuración en la política

Si no tiene acceso al terminal o el problema no puede reproducirse de forma consistente, el nivel de registro de depuración debe estar habilitado en la política.

Para habilitar el nivel de registro de depuración por la política:

- Vaya a **Gestión > Políticas**
- Busque la política y haga clic en **Editar**
- Vaya a **Configuración avanzada > Funciones administrativas**
- Configure **Nivel de Registro de Conector** y **Nivel de Registro de Bandeja para Depurar** y guardar la política, como se muestra en la imagen



Precaución: Si el modo de depuración se habilita desde la política, todos los terminales reciben esta configuración.

Nota: Sincronice la política del punto final para asegurar el modo de depuración.

Excluir AMP de otras soluciones antivirus

Según la guía del usuario, los productos antivirus deben excluir los directorios siguientes y los

archivos, directorios y archivos ejecutables que contengan para ser compatibles con el conector de AMP para MAC, los directorios que se excluyen son los siguientes:

- **/Biblioteca/Soporte de aplicaciones/Conector de Cisco/AMP para terminales**
- **/opt/cisco/amp**

Reproduzca el problema y recopile un paquete de diagnóstico

Cuando se configure el nivel de depuración, espere hasta que se produzca el estado de High CPU en el sistema o reproduzca manualmente las condiciones previamente identificadas y luego reúna el paquete de diagnóstico.

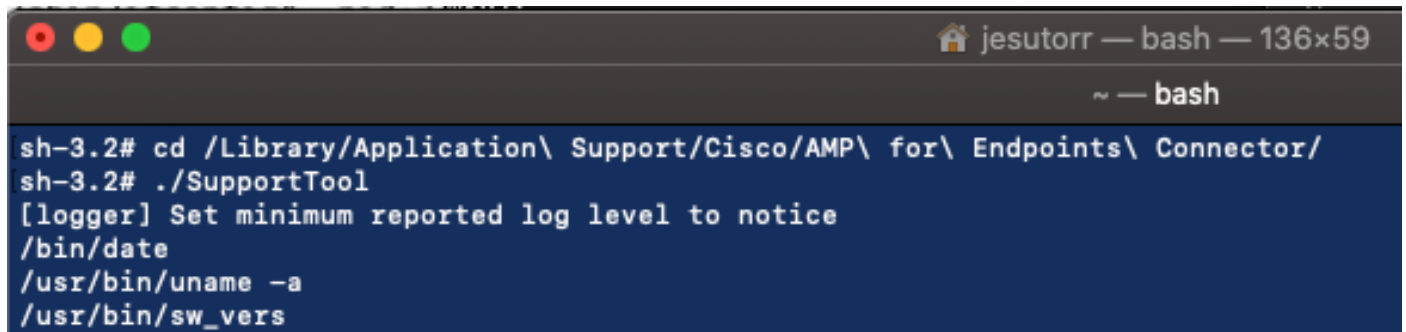
Para recopilar el paquete de depuración:

- Abra un Terminal.
- Acceso al nivel de superusuario y, a continuación, navegue hasta **/Biblioteca/Soporte de aplicaciones/Cisco/AMP para el conector de terminales**:

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

- Para ejecutar la Herramienta de soporte utilice el siguiente comando:

```
./SupportTool
```



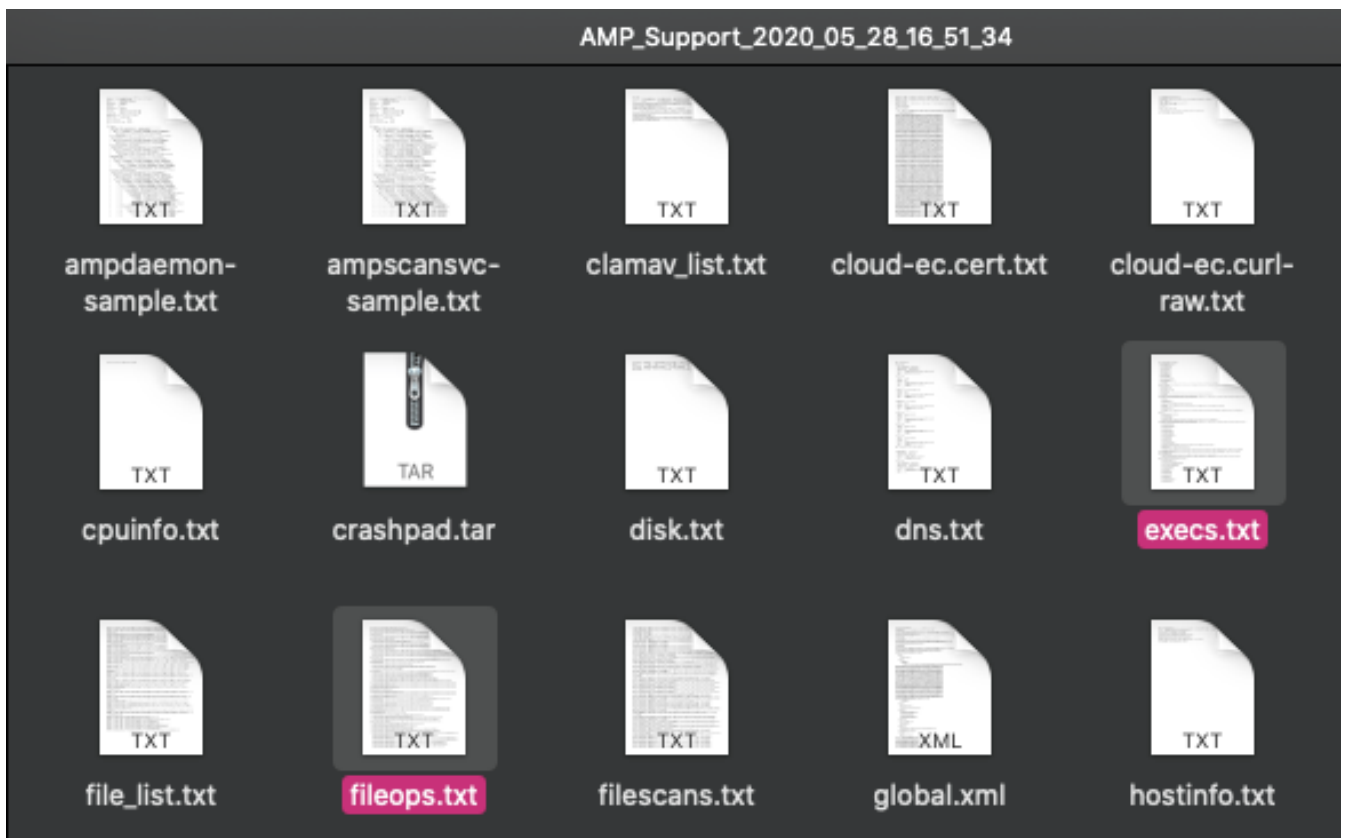
```
jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers
```

El paquete de depuración se guarda en la carpeta Escritorio como extensión de archivo .zip.

Análisis del alto rendimiento de la CPU

El paquete de diagnóstico de depuración se almacena en el escritorio para iniciar el análisis:

- Descomprima el paquete de diagnóstico
- Hay 2 archivos que revisar Operaciones de archivo: fileops.txtEjecuciones de archivos: execs.txt



- El archivo fileops.txt funciona como la principal herramienta de rendimiento para resolver problemas. Enumera todas las operaciones actuales activas en su terminal mientras se ejecuta el conector. Se lee de la siguiente manera:

<Los números escanean realizados en la trayectoria cuando se recopila el paquete> / <Ruta escaneada>

```

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/

```

Por ejemplo, si tiene una aplicación homebrew, fileops.txt muestra las siguientes operaciones activas:

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

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

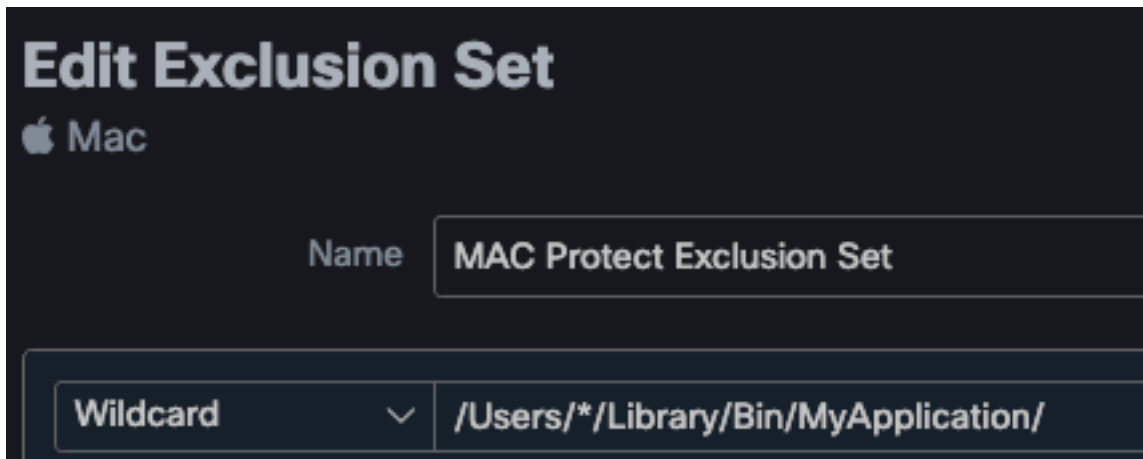
```
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```

```

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/

```

- Una vez identificado el proceso, se puede crear una exclusión
- Para crear la exclusión
- En la consola de AMP, navegue hasta **Administración > Exclusiones**
- Seleccione el conjunto de exclusión y haga clic en **Editar**
- La exclusión se puede agregar como se muestra en la imagen



- El archivo Execs.txt contiene todos los comandos que utilizan los procesos que se ejecutan mientras el conector recopila paquetes. Las rutas enumeradas aquí no se deben excluir en la política de AMP, ya que son binarios (/bin) y binarios del sistema (/sbin) que todos los procesos utilizan, sin embargo, en Execs.txt puede proporcionar el proceso principal que se está ejecutando.

Por ejemplo, si el archivo Execs.txt muestra los registros siguientes.

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

Dado que la aplicación de inicio utiliza bash, puede confirmar que la aplicación es la causa del uso excesivo de la CPU.

Información Relacionada

- [AMP para terminales: Exclusiones de procesos en MacOS y Linux](#)
- [Procedimientos recomendados para las exclusiones de AMP for Endpoints](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)