Conector de FireAMP para la colección de datos diagnósticos del mac

Contenido

Introducción

Este documento describe el proceso que se utiliza para generar un archivo de diagnóstico vía Support tool (Herramienta de soporte) la aplicación que está disponible en el conector de Cisco FireAMP para las máquinas de Macintosh (mac) y cómo resolver problemas los problemas de rendimiento.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conector de Cisco FireAMP para el mac
- Mac OSX

Componentes Utilizados

La información en este documento se basa en el conector de Cisco FireAMP para el mac.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El conector de Cisco FireAMP para el mac instala una aplicación llamada *Support tool (Herramienta de soporte)*, que se utiliza para generar la información de diagnóstico sobre el conector de FireAMP que está instalado en su mac. Los datos diagnósticos incluyen la información sobre su mac por ejemplo:

- Utilización de recursos (disco, CPU, y memoria)
- registros FireAMP-específicos
- Información de la configuración de FireAMP

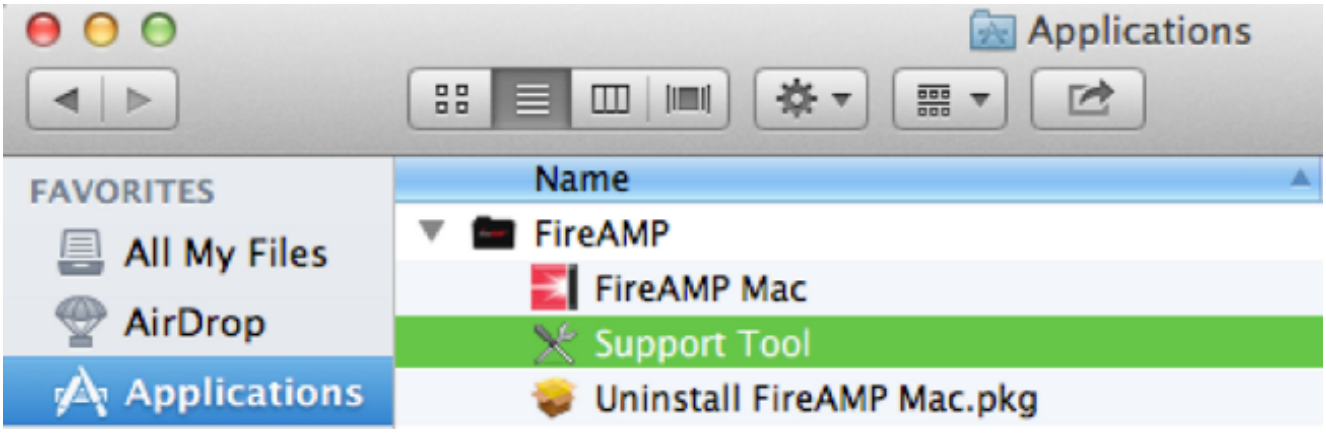
Genere un archivo de diagnóstico con Support tool (Herramienta de soporte)

Esta sección describe cómo poner en marcha Support tool (Herramienta de soporte) la aplicación del GUI o del CLI para generar un archivo de diagnóstico.

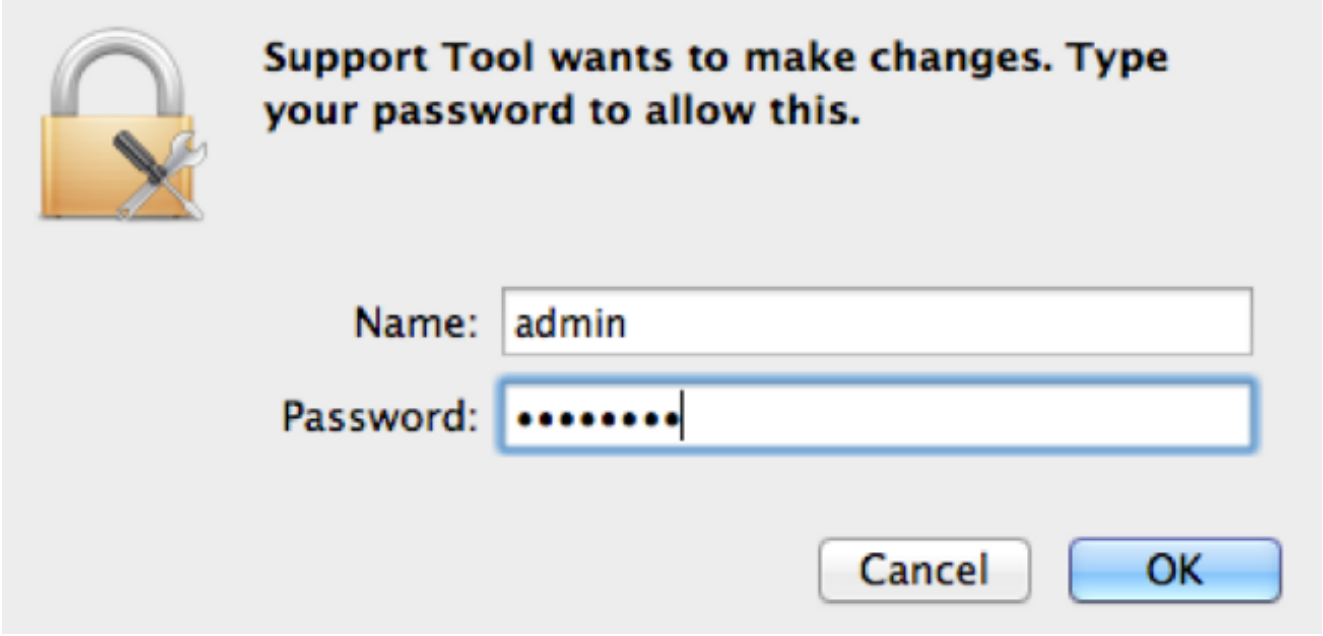
Inicie Support tool (Herramienta de soporte) del GUI

Complete estos pasos para iniciar el conector de FireAMP para el mac Support tool (Herramienta de soporte) del GUI:

1. Navegue al directorio de FireAMP en su carpeta Applications y localice Support tool (Herramienta de soporte) el lanzador:



2. Haga doble clic Support tool (Herramienta de soporte) el lanzador, y le indican para las credenciales administrativas:

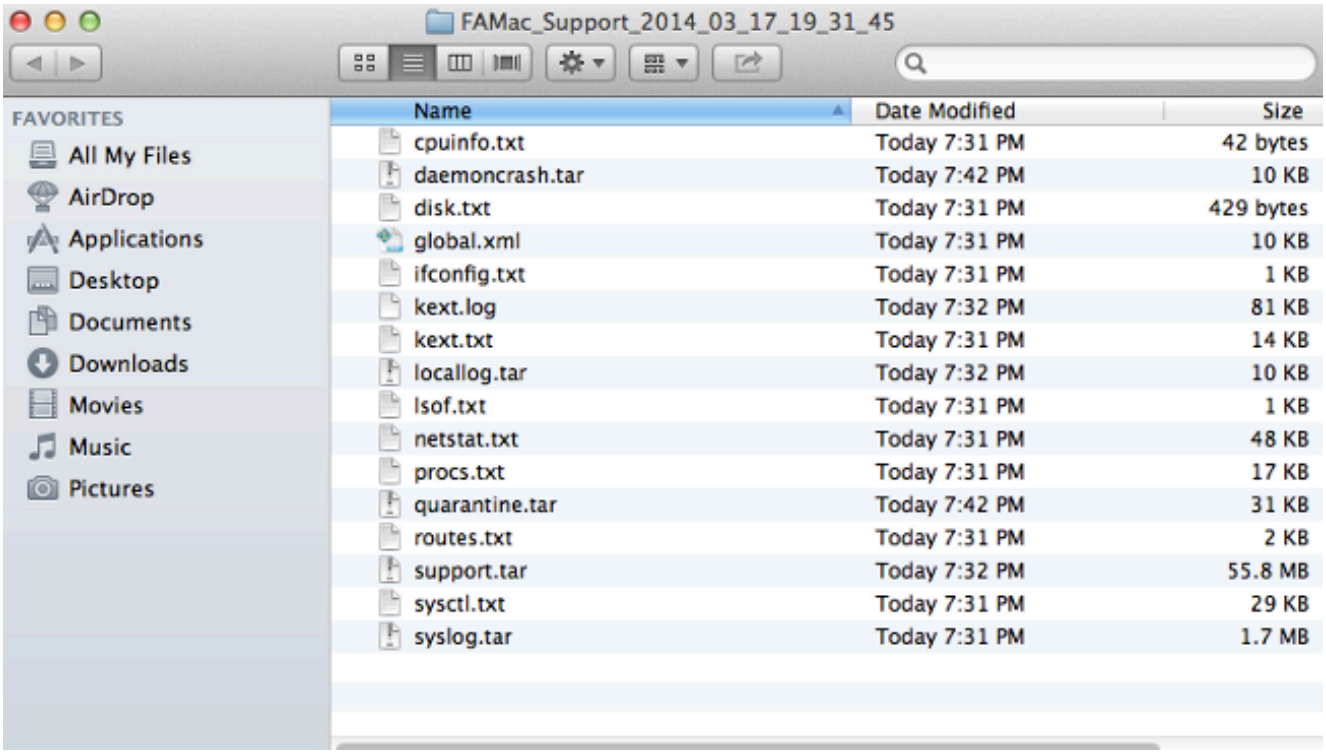


3. Después de que usted ingrese sus credenciales, Support tool (Herramienta de soporte) el icono debe aparecer en su muelle:

Note: Support tool (Herramienta de soporte) la aplicación se ejecuta en el fondo y tarda un cierto tiempo para completar (aproximadamente 20-30 minutos).

4. Cuando Support tool (Herramienta de soporte) la aplicación completa, un archivo se genera y se pone sobre su escritorio:

Aquí está un ejemplo de la salida sin comprimir:



5. Para analizar los datos, proporcione este archivo al equipo de Soporte técnico de Cisco.

Inicie Support tool (Herramienta de soporte) del CLI

Support tool (Herramienta de soporte) el lanzador está situado en este directorio:

```
/Library/Application Support/Sourcefire/FireAMP Mac/
```

Para poner en marcha Support tool (Herramienta de soporte) la aplicación, ingrese este comando en el CLI:

> **Note**: Usted debe funcionar con este comando como raíz, así que asegúrese de que usted conmute para arraigar o para introducir el comando con el **sudo**.

```
root@mac# cd /Library/Application\ Support/Sourcefire/FireAMP\ Mac
root@mac# ./SupportTool
```

> Note: Este comando se ejecuta prolijamente. Una vez que es completo, un archivo de diagnóstico se genera y se pone sobre su escritorio.

Resolución de problemas

Esta sección describe cómo permitir y inhabilitar al modo del debug en el conector de FireAMP para resolver problemas los problemas de rendimiento.

Modo del debug del permiso

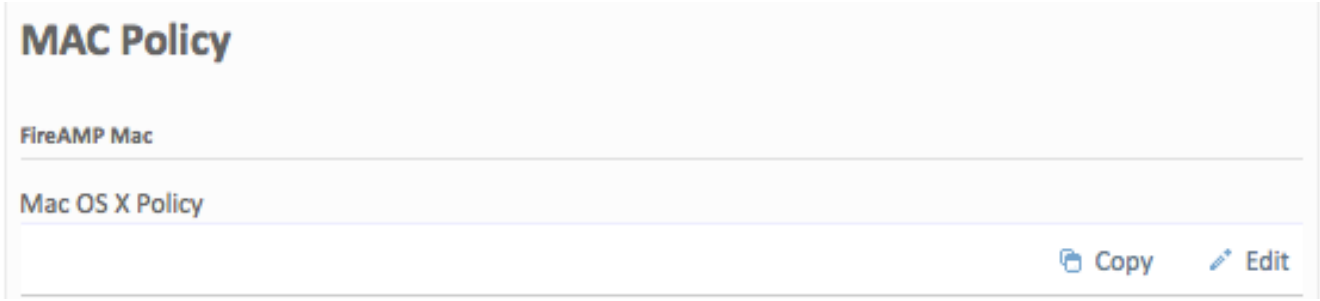
Advertencia: El modo del debug debe ser habilitado solamente si un ingeniero de soporte técnico de Cisco hace una petición estos datos. Si usted mantiene el modo del debug habilitado durante un largo período de tiempo, puede llenar el espacio en disco muy rápidamente y puede ser que evite que los datos de registro del registro y de la bandeja del conector sean recolectados en el archivo de diagnóstico del soporte debido al tamaño del archivo excesivo.

El modo del debug es útil con las tentativas de resolver problemas los problemas de rendimiento en un conector de FireAMP. Complete estos pasos para habilitar el modo del debug y recoger el data&colon de diagnóstico;

1. Inicie sesión a la consola de la nube de FireAMP.

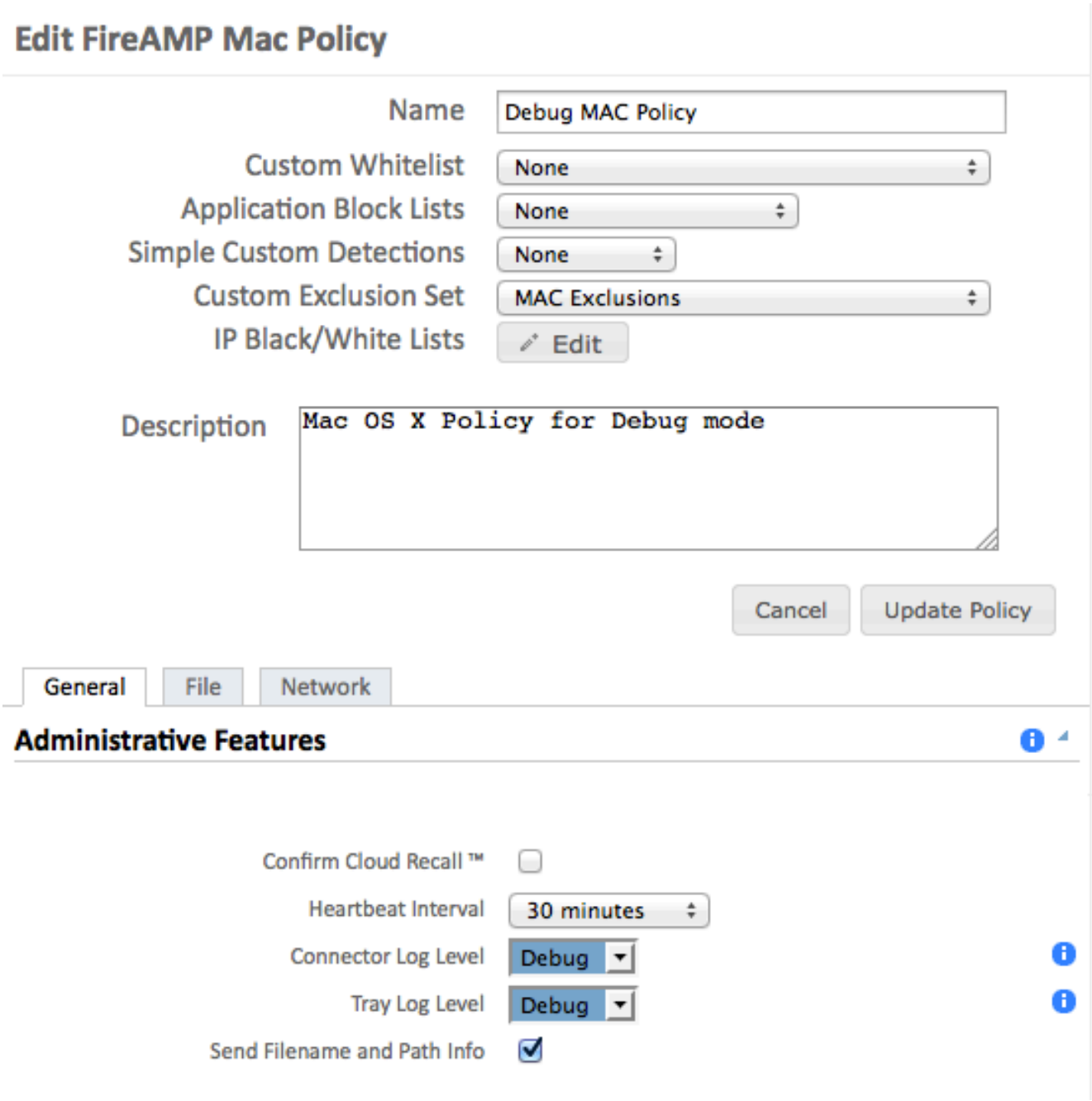
2. Navegue a la **Administración > a las directivas**.

3. Localice una directiva que se aplique a un ordenador y haga clic la **copia**. Las actualizaciones de la consola de FireAMP con la directiva copiada:



4. Haga clic **editan** y cambian el nombre de la directiva. Por ejemplo, usted podría utilizar la *directiva del debug MAC.*

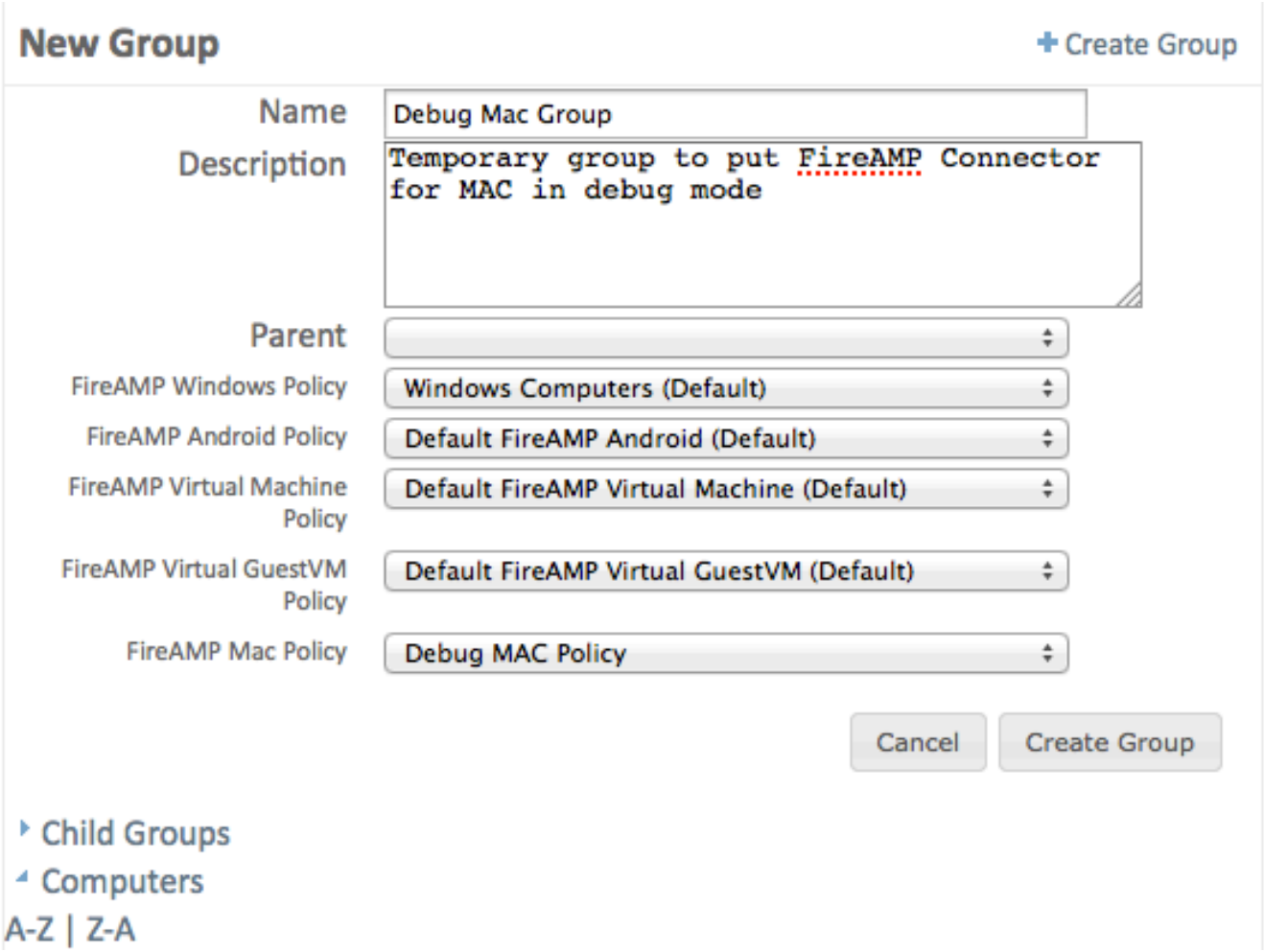
5. Haga clic las **características administrativas** y seleccione el **debug de** ambos el nivel del registro de la bandeja y el nivel del registro del conector los menúes de persiana:



6. Haga clic el botón de la **directiva de la actualización** para salvar los cambios.

7. Navegue a la **Administración > Groups** y haga clic al **grupo +Create** cerca del derecho de su pantalla.

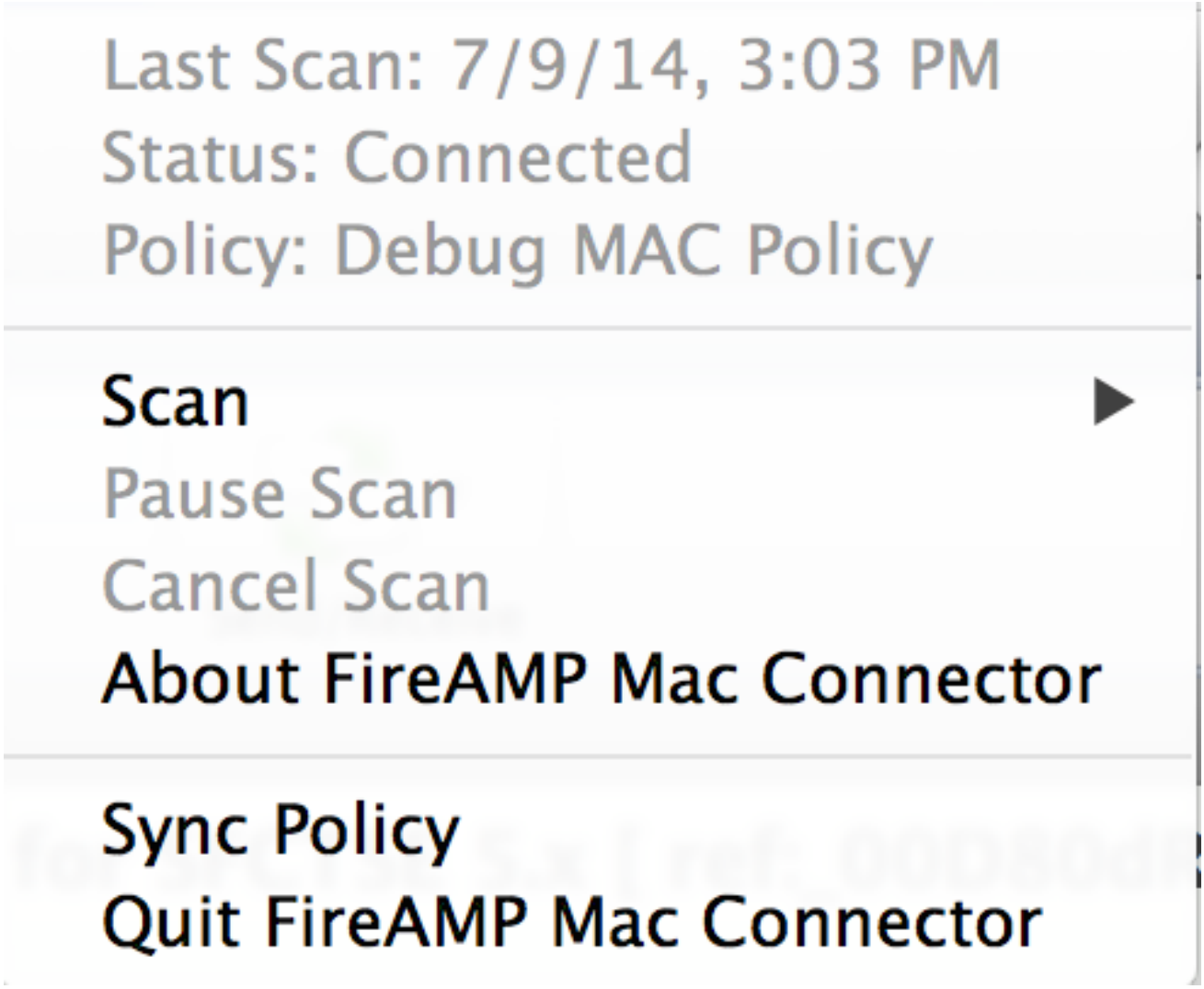
8. Ingrese un nombre para el grupo. Por ejemplo, usted podría utilizar el *grupo del mac del debug.*



9. Cambie la directiva de FireAMP MAC de la *directiva de la MAC predeterminada a la* directiva copiada, nueva que usted acaba de crear, que es **directiva del debug MAC** en este ejemplo.

10. Haga clic las **Computadoras** e identifique su ordenador en la lista. Selecciónela y el tecleo **agrega seleccionado**.

11. El tecleo **crea al grupo**. Su mac debe ahora tener una directiva funcional del debug. Usted puede seleccionar el icono de FireAMP que aparece en su barra de menú y se asegura de que la nueva directiva es aplicada:

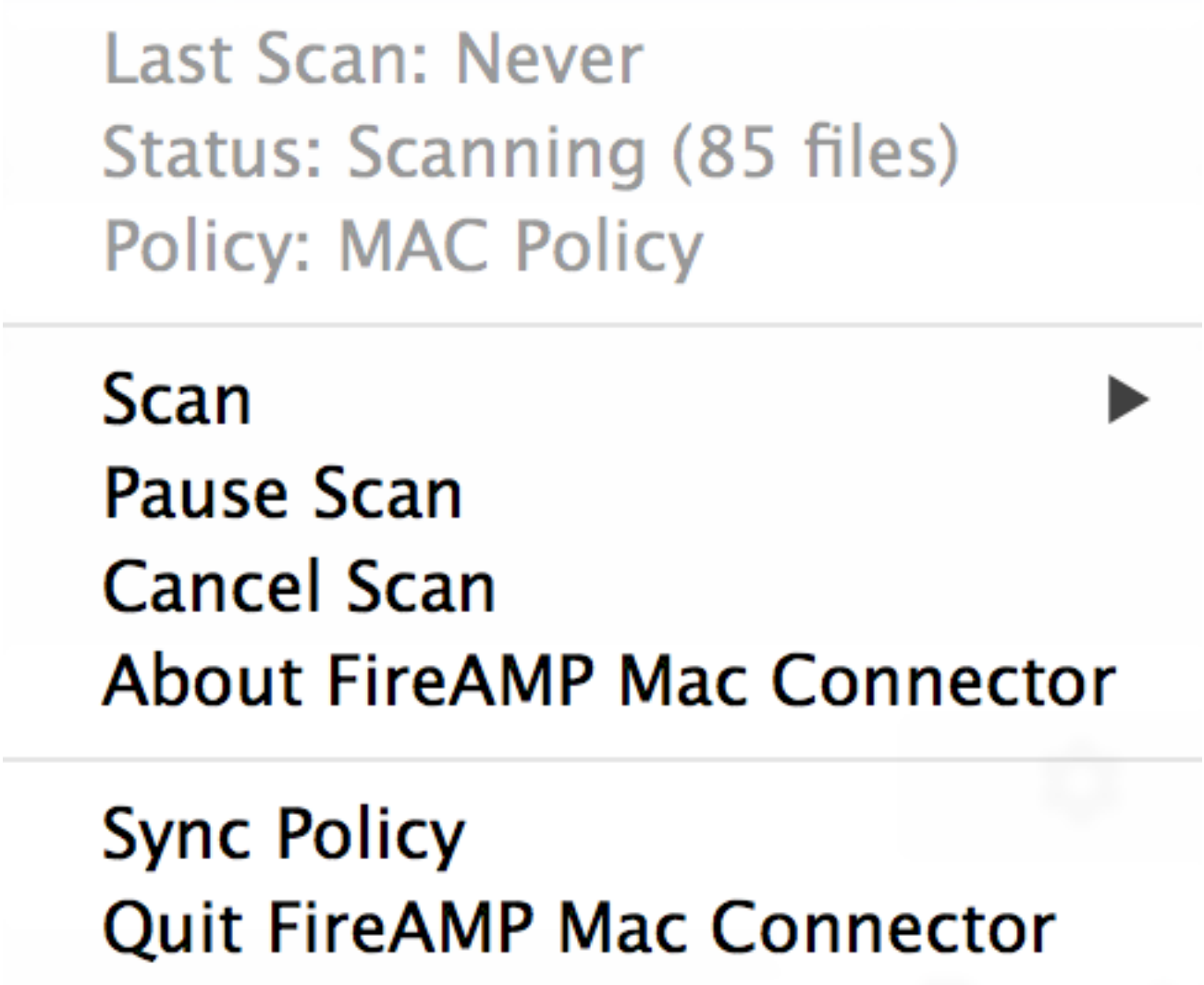


Modo del debug de la neutralización

Después de que los datos diagnósticos en el modo del debug se obtengan, usted debe invertir el conector de FireAMP de nuevo al modo normal. Complete estos pasos para inhabilitar el modo del debug:

1. Inicie sesión a la consola de la nube de FireAMP.
2. Navegue a la **Administración > Groups**.
3. Localice al nuevo grupo, el *grupo del debug MAC*, que usted creó en el modo del debug.
4. Haga clic en **Editar**.
5. Haga clic las **Computadoras** y localice su ordenador en la lista. Selecciónela y el tecleo **quita seleccionado**.
6. **Grupo de la actualización del** tecleo.
7. El tecleo **sincroniza la directiva** en la barra de menú donde se localiza el icono de FireAMP.
8. Verifique que la directiva ahora esté vuelta al valor predeterminado anterior. Compruebe

esto la barra de menú. La directiva debe ahora haber invertido de nuevo a la directiva original que fue utilizada antes de que usted la cambiara a la *directiva del debug MAC*:



El modo del debug ahora se inhabilita, y el conector de FireAMP debe funcionar normalmente.