Conector de FireAMP para a coleção dos dados de diagnóstico do Mac

Índice

Introdução

Este documento descreve o processo que é usado a fim gerar um arquivo de diagnóstico através do aplicativo da ferramenta de suporte que está disponível no conector de Cisco FireAMP para máquinas de Macintosh (Mac) e de como pesquisar defeitos problemas de desempenho.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conector de Cisco FireAMP para o Mac
- Mac OSX

Componentes Utilizados

A informação neste documento é baseada no conector de Cisco FireAMP para o Mac.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Informações de Apoio

O conector de Cisco FireAMP para o Mac instala um aplicativo chamado a *ferramenta de suporte*, que é usada a fim gerar a informação de diagnóstico sobre o conector de FireAMP que é instalado em seu Mac. Os dados de diagnóstico incluem a informação sobre seu Mac como:

- Utilização de recurso (disco, CPU, e memória)
- logs FireAMP-específicos
- Informação de configuração de FireAMP

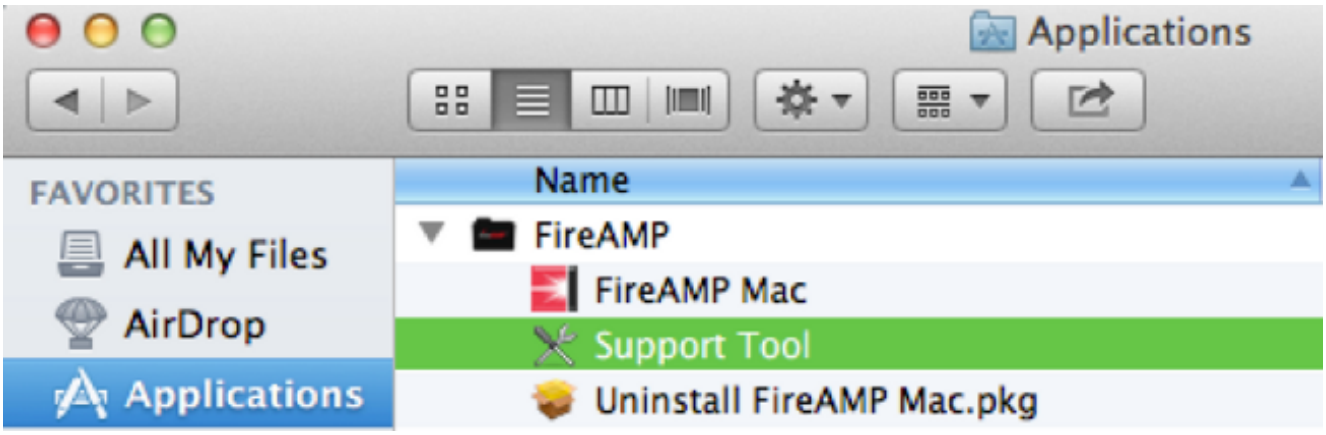
Gerencia um arquivo de diagnóstico com a ferramenta de suporte

Esta seção descreve como lançar o aplicativo da ferramenta de suporte do GUI ou do CLI a fim gerar um arquivo de diagnóstico.

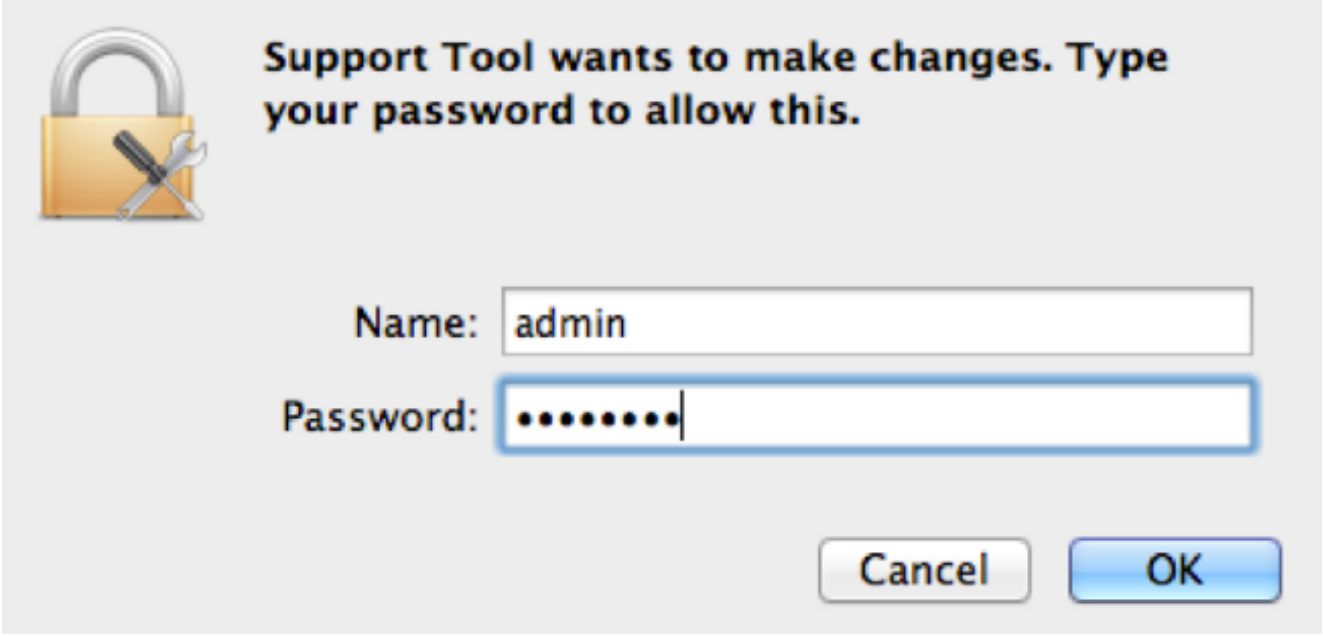
Lance a ferramenta de suporte do GUI

Termine estas etapas a fim lançar o conector de FireAMP para a ferramenta de suporte do Mac do GUI:

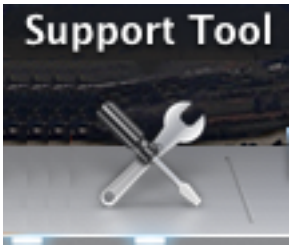
1. Navegue ao diretório de FireAMP em sua pasta de aplicativos e encontre o lançador da ferramenta de suporte:



2. Fazer duplo clique o lançador da ferramenta de suporte, e você é alertado para credenciais administrativas:



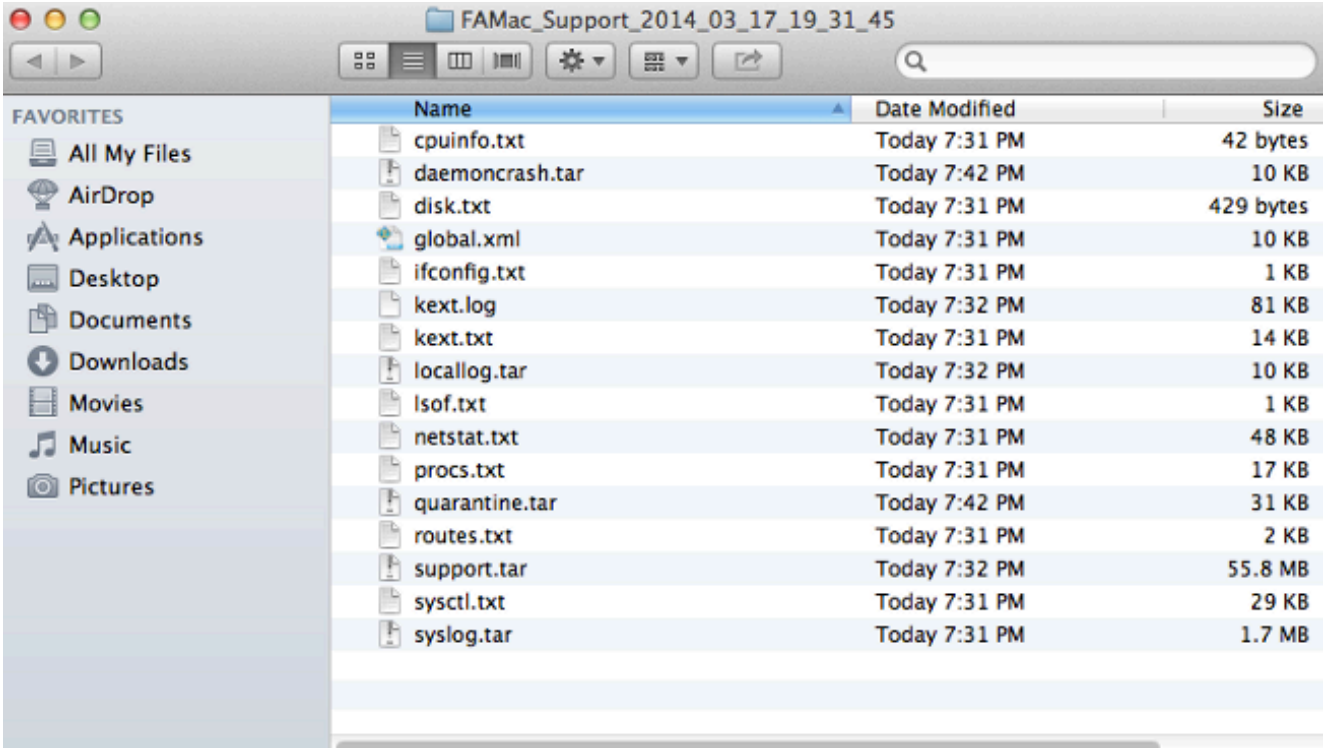
3. Depois que você incorpora suas credenciais, o ícone da ferramenta de suporte deve aparecer em sua doca:



Note: O aplicativo da ferramenta de suporte é executado no fundo e toma algum tempo para terminar (aproximadamente 20-30 minutos).

4. Quando o aplicativo da ferramenta de suporte termina, um arquivo está gerado e colocado em seu desktop:

Está aqui um exemplo da saída descompactado:



5. A fim analisar os dados, forneça este arquivo à equipe de Suporte técnico de Cisco.

Lance a ferramenta de suporte do CLI

O lançador da ferramenta de suporte é ficado situado neste diretório:

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

A fim lançar o aplicativo da ferramenta de suporte, incorpore este comando no CLI:

> **Note**: Você deve executar este comando como a raiz, assim que assegure-se de que você comute para enraizar ou prefaciar o comando com o **sudo**.

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

> Note: Este comando é executado verbosely. Uma vez que está completo, um arquivo de diagnóstico está gerado e colocado em seu desktop.

Troubleshooting

Esta seção descreve como permitir e o desabilitação debuga o modo no conector de FireAMP a fim pesquisar defeitos problemas de desempenho.

Permita debugam o modo

> **aviso:** Debugar o modo deve ser permitido somente se um engenheiro de suporte técnico de

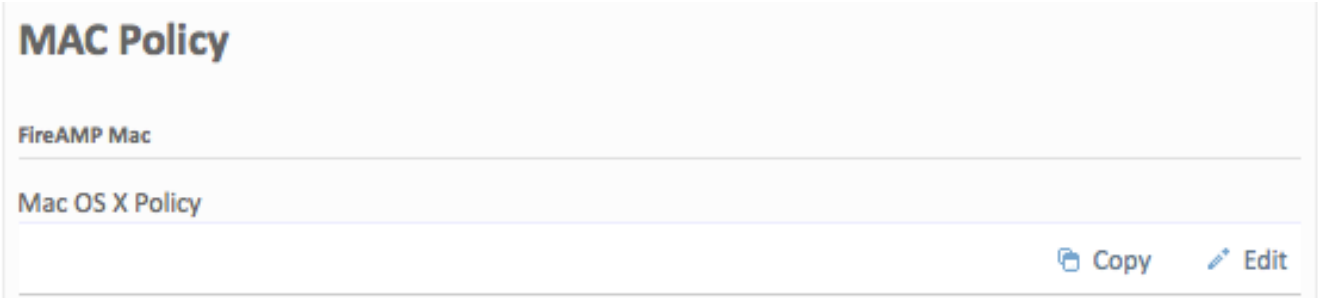
Cisco faz um pedido para estes dados. Se você se mantém para debugar o modo permitido por um período de tempo prolongado, pode encher acima o espaço de disco muito rapidamente e pôde impedir que os dados de registro do log e da bandeja do conector estejam recolhidos no arquivo de diagnóstico do apoio devido ao tamanho do arquivo excessivo.

Debugar o modo é útil com tentativas de pesquisar defeitos problemas de desempenho em um conector de FireAMP. Termine estas etapas a fim permitir debugam o modo e recolhem o data&colon diagnóstico;

1. Entre ao console da nuvem de FireAMP.

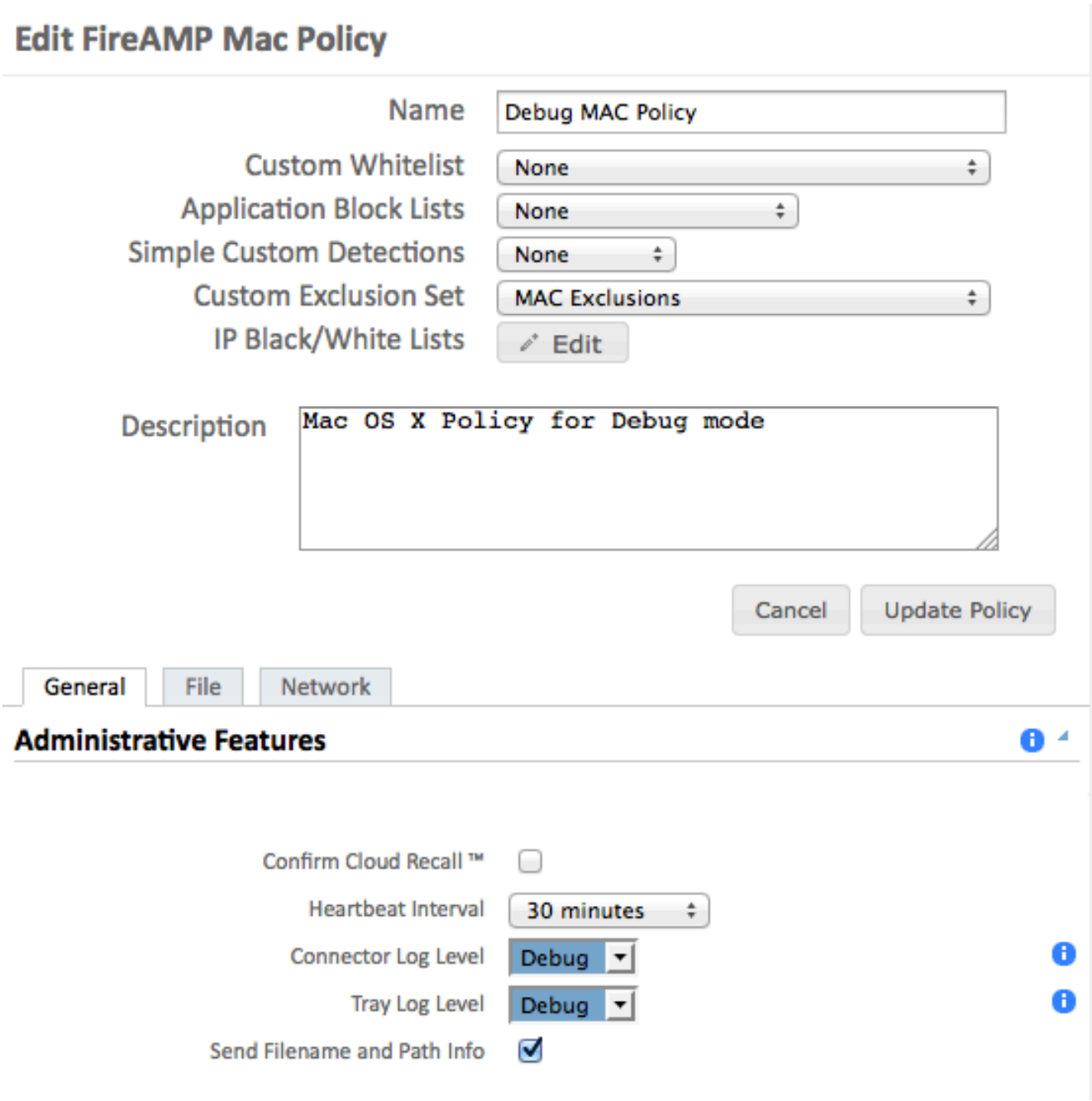
2. Navegue ao **Gerenciamento > às políticas**.

3. Encontre uma política que seja aplicada a um computador e clique a **cópia**. As atualizações do console de FireAMP com a política copiada:



4. Clique **editam** e mudam o nome da política. Por exemplo, você poderia usar-se *debuga a política MAC.*

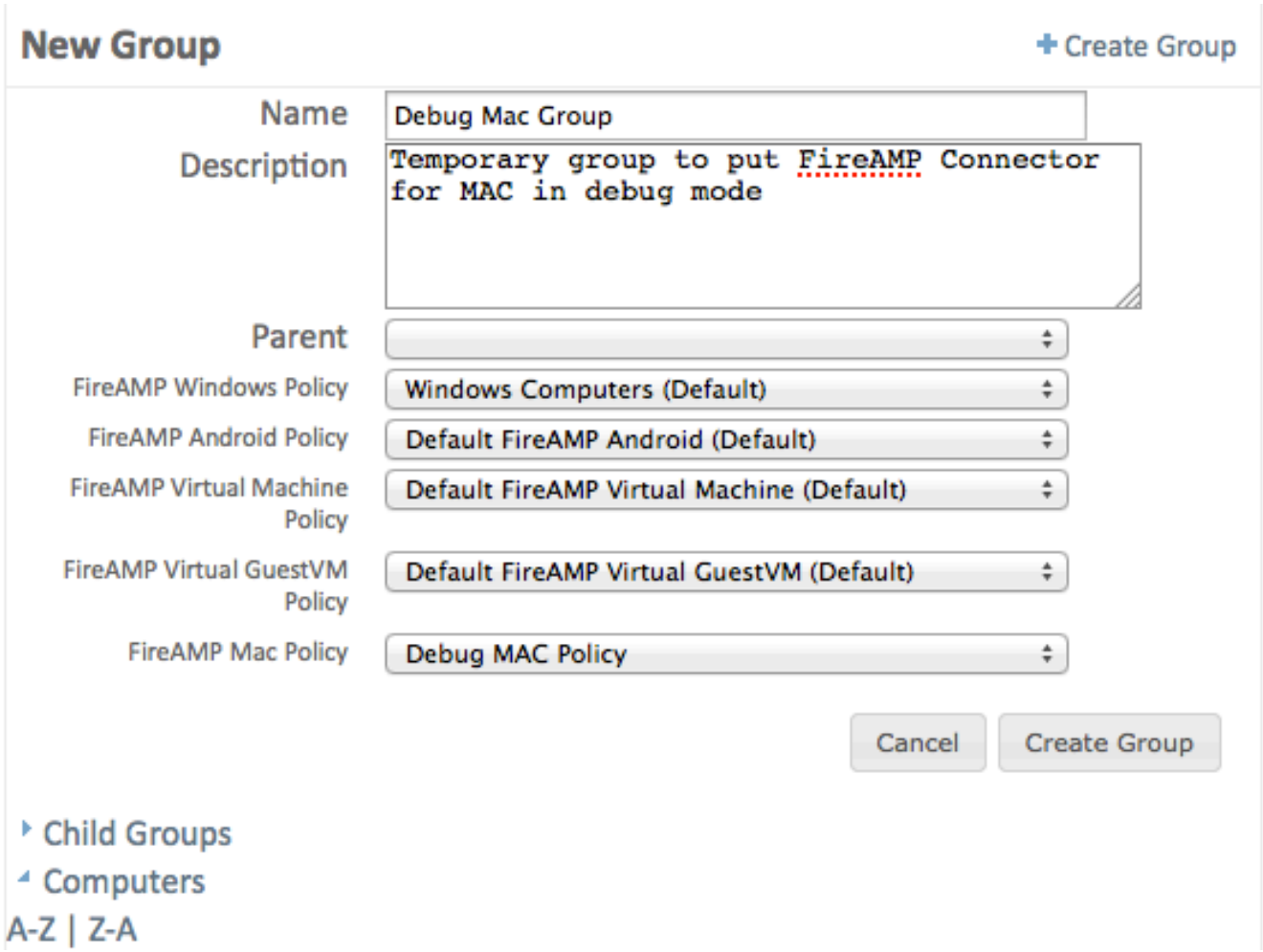
5. **As características do** clique e seletos **administrativos debugam de** ambos o nível do log da bandeja e o nível do log do conector deixa cair para baixo menus:



6. Clique o botão da **política da atualização** a fim salvar as mudanças.

7. Navegue ao **Gerenciamento > aos grupos** e clique o **grupo +Create** perto do lado de direita superior de sua tela.

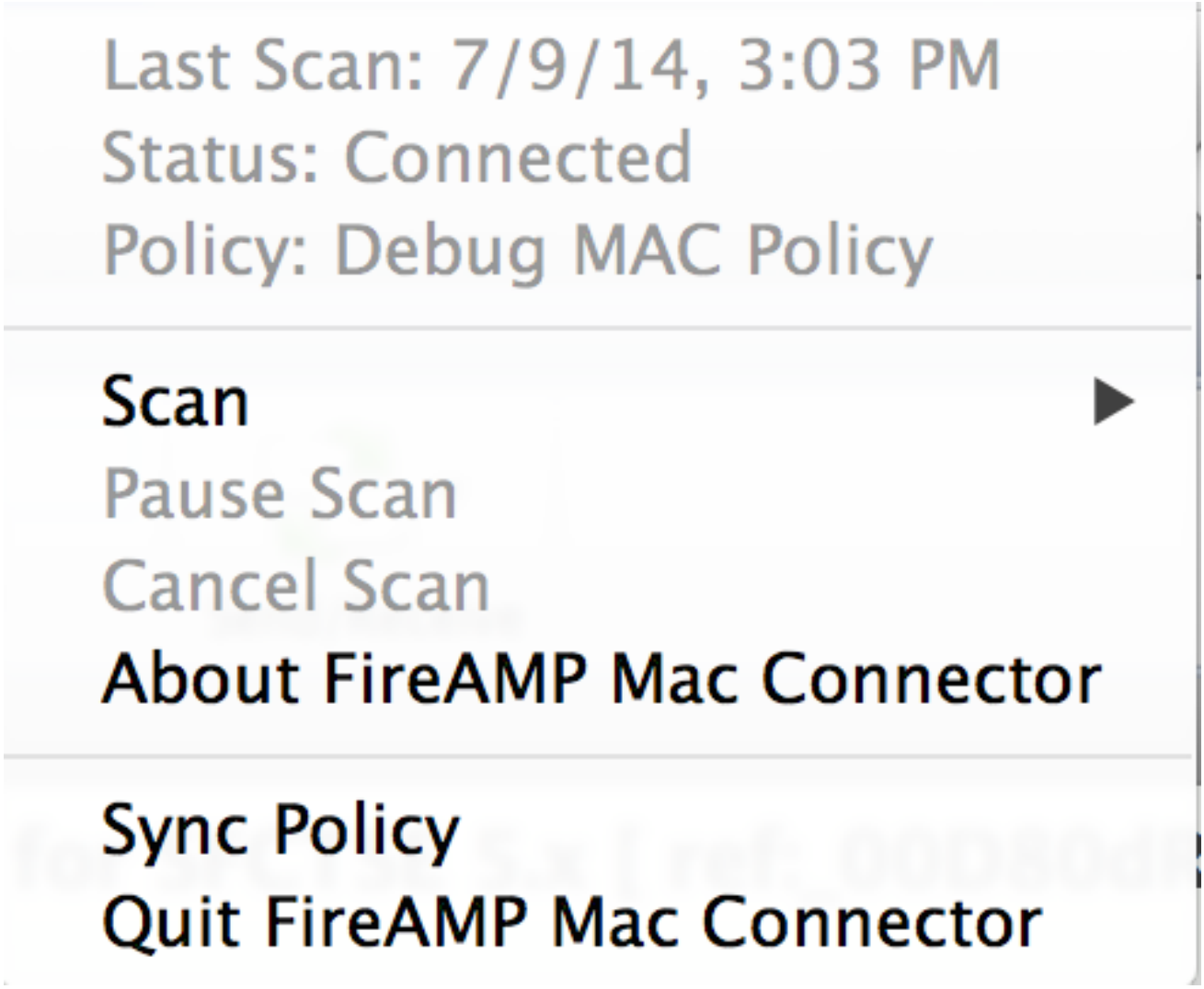
8. Dê entrada com um nome para o grupo. Por exemplo, você poderia usar-se *debuga o grupo do Mac*.



9. Mude a política de FireAMP MAC da *política do MAC padrão à* política copiada, nova que você apenas criou, que é **debuga a política MAC n**este exemplo.

10. Clique **computadores** e identifique seu computador na lista. Selecione-a e o clique **adiciona selecionado**.

11. O clique **cria o grupo**. Seu Mac deve agora mandar um funcional debugar a política. Você pode selecionar o ícone de FireAMP que aparece em sua barra de menus e assegura-se de que a política nova seja aplicada:

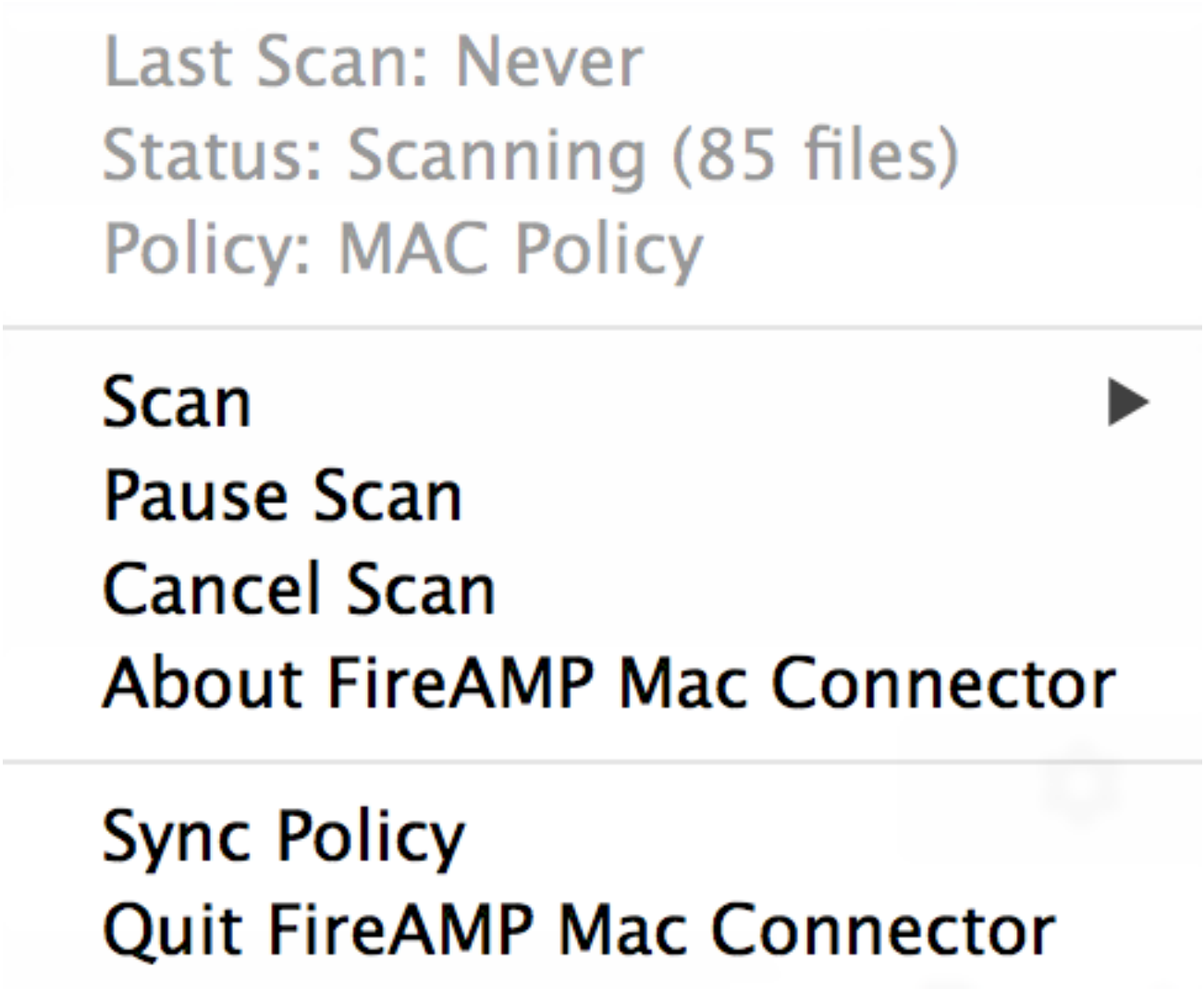


O desabilitação debuga o modo

Depois que os dados de diagnóstico debugam dentro o modo está obtido, você deve reverter o conector de FireAMP de volta ao modo normal. Termine estas etapas a fim desabilitar debugam o modo:

1. Entre ao console da nuvem de FireAMP.
2. Navegue ao **Gerenciamento > aos grupos**.
3. Encontre o grupo novo, *debugar o grupo MAC*, que você criou debuga dentro o modo.
4. O clique **edita**.
5. Clique **computadores** e encontre seu computador na lista. Selecione-a e o clique **remove selecionado**.
6. **Grupo da atualização do** clique.
7. Clique a **política da sincronização na** barra de menus onde o ícone de FireAMP é encontrado.

8. Verifique que a política está retornada agora ao valor padrão precedente. Verifique isto na barra de menus. A política deveu agora ter revertido de volta à política original que foi usada antes que você a mudou à *política debugar MAC*:



Debugar o modo é desabilitado agora, e o conector de FireAMP deve funcionar normalmente.