Mac诊断数据数据收集的FireAMP连接器

目录

简介

本文描述使用为了通过支持工具应用程序是可用的在思科FireAMP连接器为麦金塔的进程(Mac)机器和如何排除故障性能问题生成诊断文件。

先决条件

要求

Cisco 建议您了解以下主题：

- Mac的思科FireAMP连接器
- Mac OSX

使用的组件

本文档中的信息根据Mac的思科FireAMP连接器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

Mac的思科FireAMP连接器安装呼叫*支持工具的*应用程序，用于为了生成关于FireAMP连接器的诊断信息在您的Mac安装。诊断数据包括关于您的Mac的信息例如：

- 资源利用率(磁盘、CPU和内存)
- FireAMP特定日志
- FireAMP配置信息

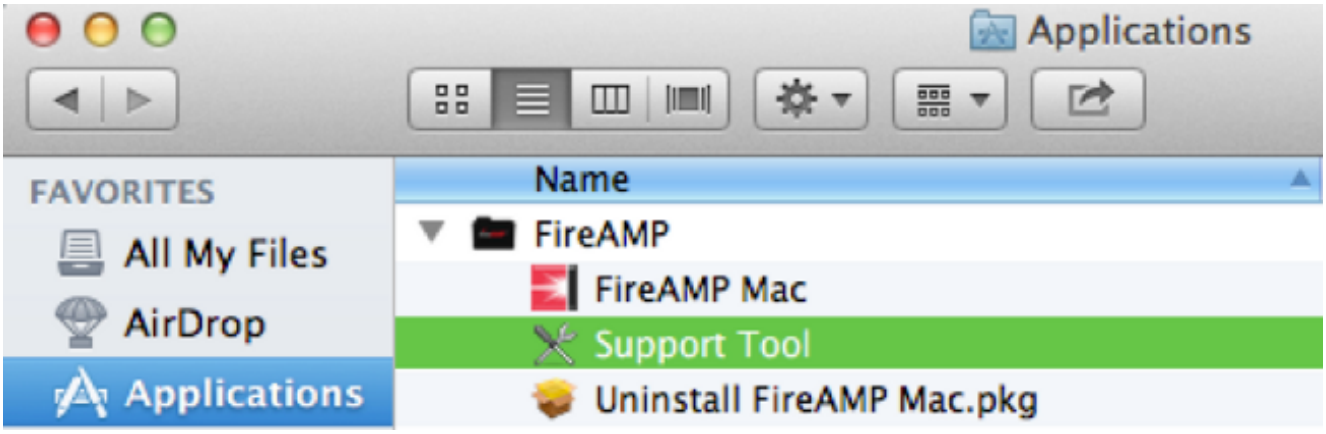
生成诊断文件用支持工具

此部分描述如何启动从GUI或CLI的支持工具应用程序为了生成诊断文件。

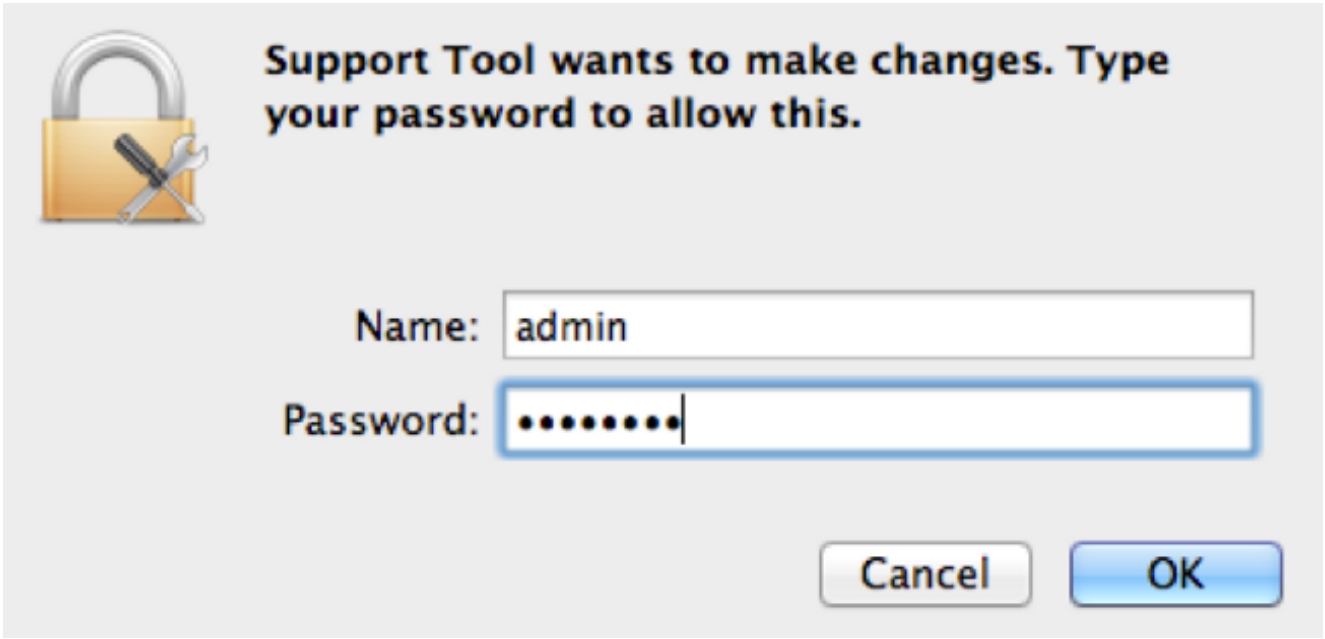
启动从GUI的支持工具

完成这些步骤为了启动Mac支持工具的FireAMP连接器从GUI ：

1. 导航对在您的应用程序文件夹的FireAMP目录并且找出支持工具发射器：



2. 双击支持工具发射器，并且提示对于管理凭证：

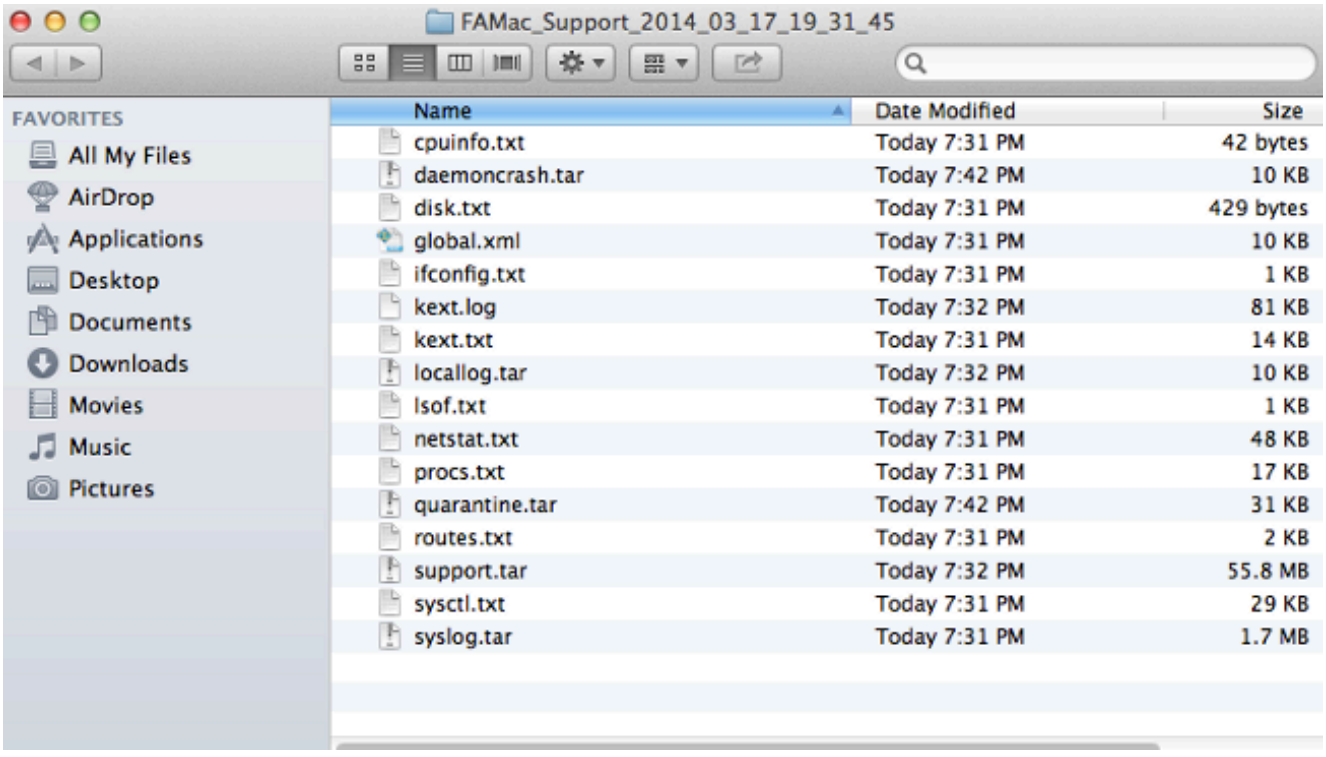


3. 在您输入您的凭证后，支持工具图标应该在您的码头出现：

Note:支持工具应用程序在背景运行并且采取一些时间完成(大约20-30分钟)。

4. 当支持工具应用程序完成时，文件生成并且被放置在您的桌面上：

这是未压缩的输出的示例：



5. 为了分析数据，请提供此文件给思科技术支持流动代课教师组。

启动从CLI的支持工具

支持工具发射器在此目录查找：

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

为了启动支持工具应用程序，请输入此命令到CLI ：

Note:您必须运行此命令作为根，因此请保证您交换根源或加序言命令与sudo。

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

Note:此命令冗长地运行。一旦它完成，诊断文件生成并且被放置在您的桌面上。

排除故障

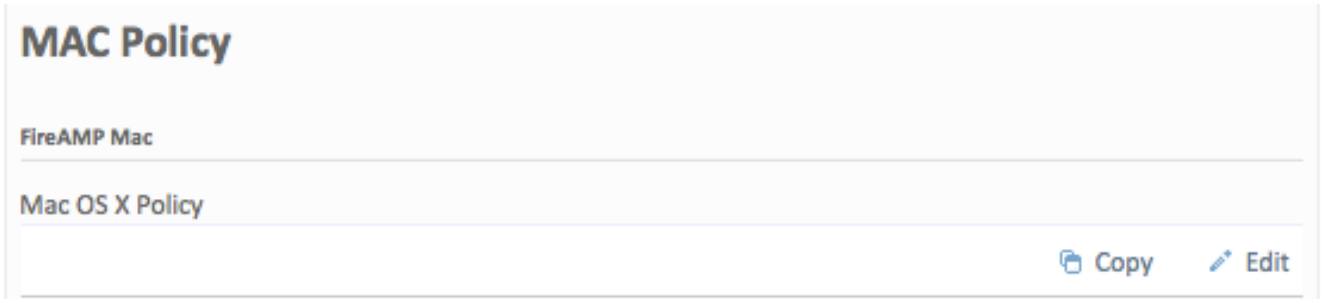
此部分描述如何启动和禁用在FireAMP连接器的调试模式为了排除故障性能问题。

Enable (event)调试模式

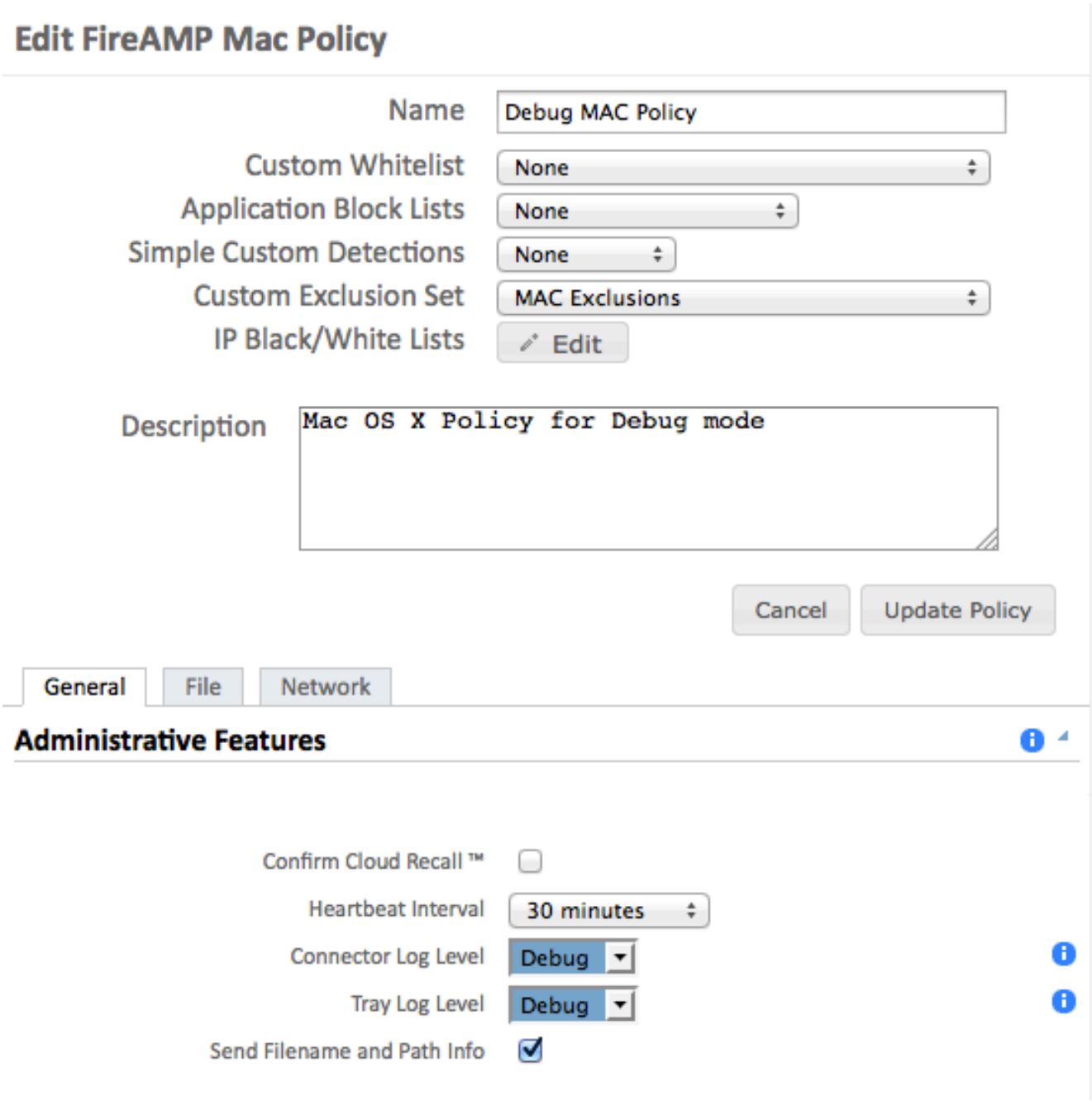
> 警告：调试模式，只有当思科技术支持工程师做一个要求此数据，应该启用。如果保持调试模式长时间启用，在支持诊断文件非常迅速填满磁盘空间并且也许防止连接器日志和盘日志数据被采集由于额外的文件大小。

调试模式是有用的与尝试排除故障在FireAMP连接器的性能问题。完成这些步骤为了启动调试模式和收集诊断data:

1. 登陆到FireAMP Cloud控制台。
2. 导航对**Management>策略**。
3. 找出应用到计算机的策略并且点击**“Copy”**。与复制的策略的FireAMP控制台更新：



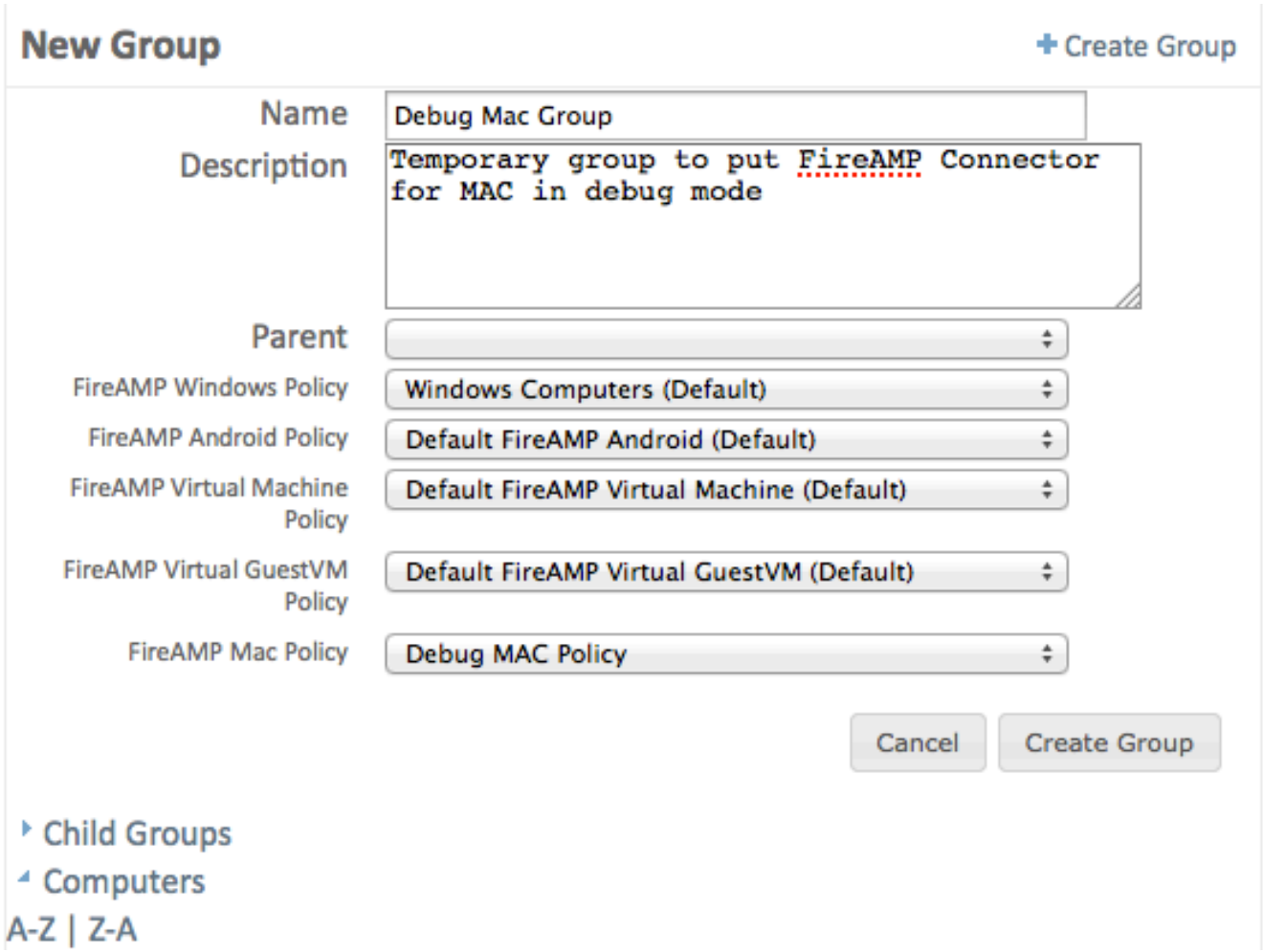
4. 单击**编辑**并且更改策略的名称。例如，您可能使用*调试MAC策略*。
5. 点击**管理功能**并且选择从两个的**调试**盘日志级别和连接器日志级别下拉菜单：



6. 点击**更新策略**按钮为了保存更改。

7. 导航给**Management>组**并且在您的屏幕附近右侧单击**+Create组**。

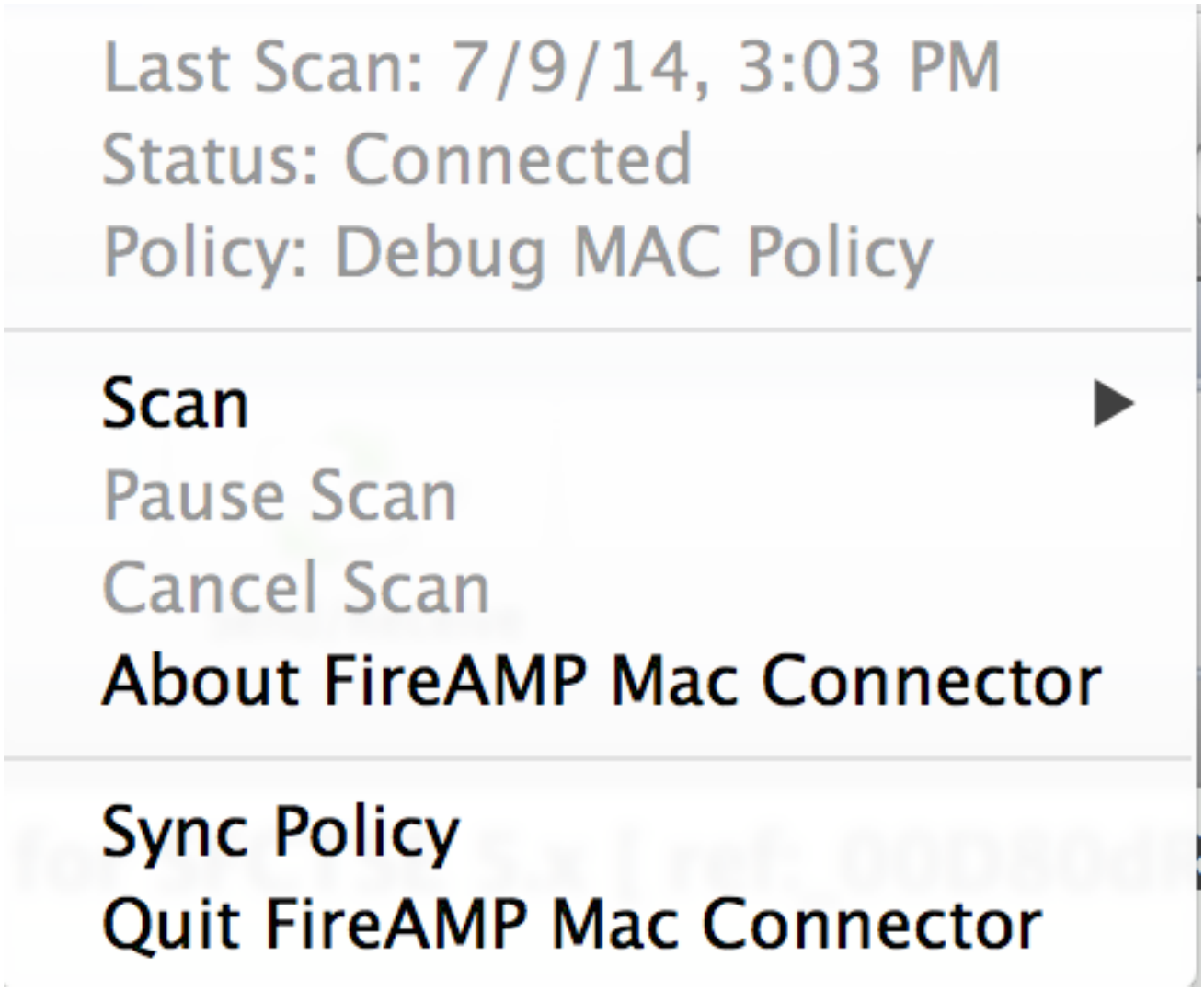
8. 输入组的名称。例如，您可能使用*调试Mac组*。



9. 更改从*默认MAC策略的*FireAMP MAC策略到您创建，是**调试**在本例中的**MAC策略的**复制的，新建的策略。

10. 点击**计算机**并且识别您的在列表的计算机。选择它并且单击**添加选定**。

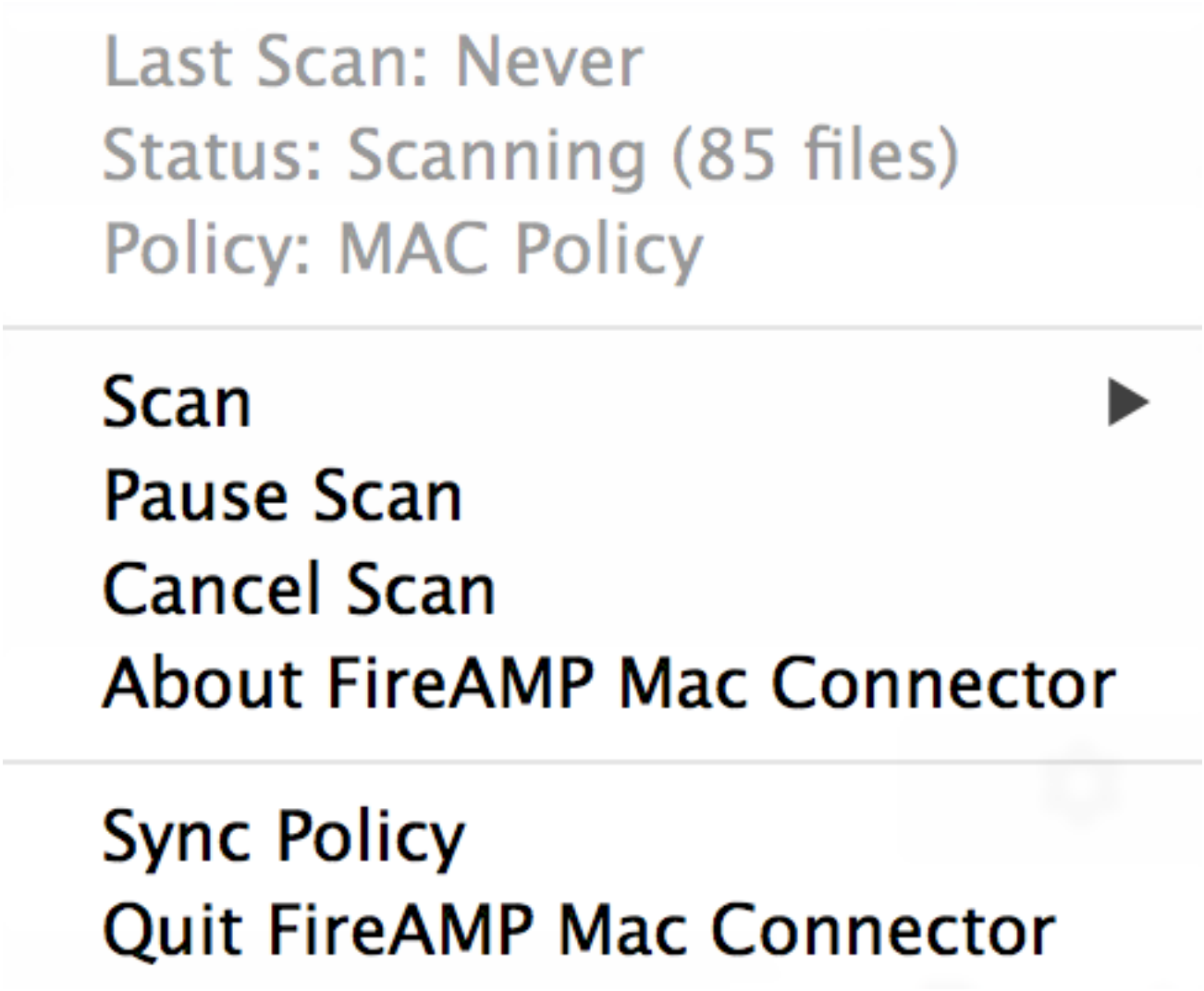
11. 单击**创建组**。您的Mac应该当前有一项功能调试策略。您能选择出现在您的菜单栏的FireAMP图标并且保证新的策略应用：



禁用调试模式

在调试模式的诊断数据得到后，您必须恢复FireAMP连接器回到正常模式。完成这些步骤为了禁用调试模式：

1. 登陆到FireAMP Cloud控制台。
2. 导航给**Management>组**。
3. 找出新的组，*调试MAC组*，该您创建在调试模式。
4. 单击 **Edit**。
5. 点击**计算机**并且找出您的在列表的计算机。选择它并且点击**选择的删除**。
6. 点击**更新组**。
7. 点击在FireAMP图标查找的菜单栏的**同步策略**。
8. 验证策略当前返回对上一个默认值。检查此在菜单栏。策略应该当前恢复了回到使用的原始策略，在您更改它对*调试MAC策略前*：



调试模式当前禁用，并且FireAMP连接器应该通常作用。