FireAMP连接器服务因连接器保护而无法停止

目录

[简介](#)
[连接器保护的配置](#)
[自我保护驱动程序](#)
[停止FireAMP连接器服务](#)
[停止的原因](#)
[使用连接器属性停止服务](#)
[使用CLI停止服务](#)
[解决方案](#)
[使用命令行停止服务](#)
[使用用户界面停止服务](#)

简介

FireAMP连接器具有称为连接器保护的功能。此选项允许您对FireAMP连接器服务进行密码保护，并防止停止或卸载该服务。但是，这可能会影响故障排除过程，因为停止FireAMP连接器服务或卸载该服务可以作为故障排除步骤来执行。本文档介绍如何在FireAMP受到密码保护时将其卸载。

连接器保护的配置

要启用Connector Protection选项，请编辑Policy，转到General选项卡，然后展开Administrative Features。

自我保护驱动程序

连接器保护功能利用自我保护驱动程序来保护FireAMP的目录。自我保护驱动程序执行以下任务：

1. 保护FireAMP使用的注册表项不会被删除和修改。
2. 防止应用程序写入或删除安装目录中的文件。默认安装目录为：

```
"%PROGRAMFILES%\Sourcefire\FireAMP"
```

3. 防止卸载或覆盖FireAMP驱动程序。
4. 通过Windows任务管理器，保护FireAMP应用程序iptray.exe和agent.exe不被“End Processed”。

停止FireAMP连接器服务

停止的原因

您可能希望停止FireAMP连接器服务或卸载FireAMP的一些场景如下：

1. 停止该服务以删除损坏的数据库文件或旧的日志文件。
2. 由于错误、损坏或不完整的安装，请卸载FireAMP。
3. 替换policy.xml文件以诊断连接问题。

使用连接器属性停止服务

如果启用了连接器保护功能，将无法使用“FireAMP连接器属性”窗口停止服务。管理服务的按钮被禁用，如下所示：

使用CLI停止服务

当启用连接器保护功能时尝试停止服务时，您会收到如下故障消息：

```
The requested pause, continue, or stop is not valid for this service.
```

在版本4.3.0+上，可以使用命令“sfc.exe -k password”停止sfc.exe服务，其中“password”是在策略中定义的密码。

解决方案

使用命令行停止服务

注意 — 此命令仅适用于FireAMP连接器版本4.3.0及更高版本。

```
sfc.exe -k password
```

将“password”一词替换为策略中设置的实际密码。

使用用户界面停止服务

您可以从用户界面停止受密码保护的服务。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。