O FireAMP Connector Service não consegue parar devido à proteção do conector

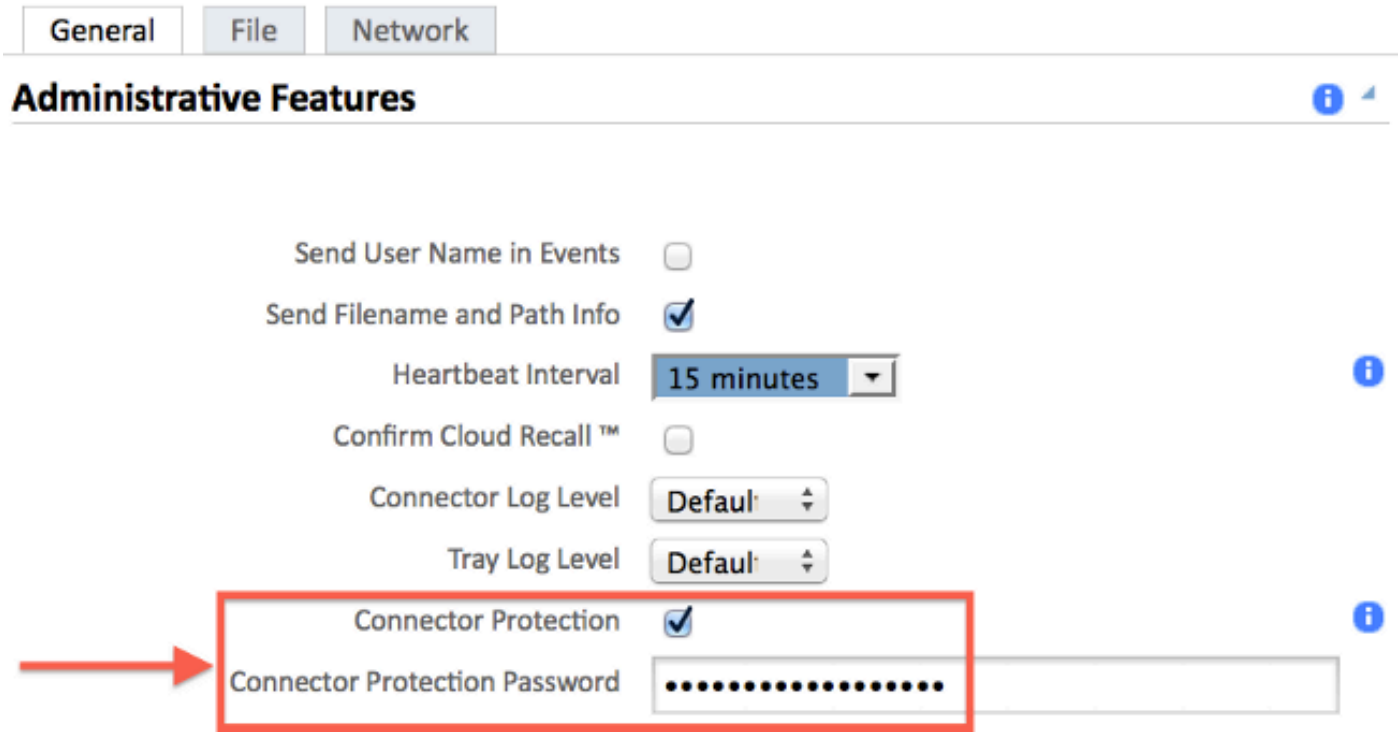
Contents

Introduction

O conector FireAMP tem um recurso chamado **Proteção do conector**. Essa opção permite proteger o serviço FireAMP Connector por senha e impedir que ele seja interrompido ou desinstalado. No entanto, isso pode afetar o processo de solução de problemas devido ao fato de que interromper o serviço do conector FireAMP ou desinstalá-lo pode ser reproduzido como uma etapa de solução de problemas. Este documento descreve como desinstalar o FireAMP quando ele estiver protegido por senha.

Configuração da proteção do conector

Para habilitar a opção **Proteção do Conector**, edite sua **Política**, vá para a guia **Geral** e expanda **Recursos Administrativos**.



Driver de autoproteção

O recurso Connector Protection utiliza um driver autoprotegido para proteger os diretórios do FireAMP. Um driver de autoproteção executa as seguintes tarefas:

1. Proteja as chaves de registro usadas pelo FireAMP de serem excluídas e modificadas.
2. Proteja os aplicativos de gravar ou excluir arquivos no diretório de instalação. O diretório de instalação padrão é:

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

3. Proteja os drivers do FireAMP de serem descarregados ou sobrescritos.
4. Proteja os aplicativos FireAMP, iptray.exe e agent.exe, de serem "processados pelo fim" através do Gerenciador de tarefas do Windows.

Interrompendo o FireAMP Connector Service

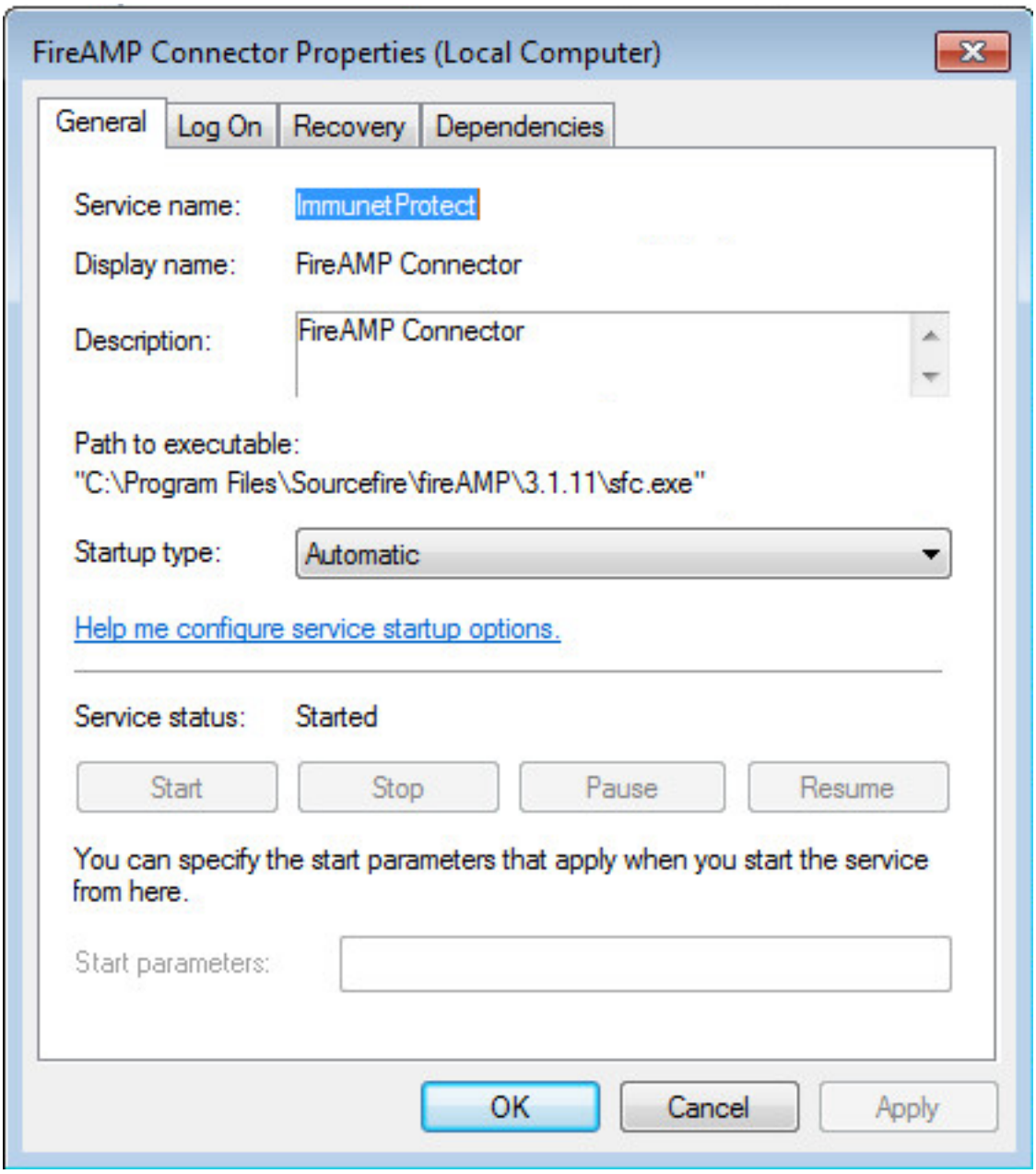
Motivos para uma paragem

Alguns cenários em que você pode querer interromper o serviço do conector FireAMP ou desinstalar o FireAMP seriam:

1. Interrompa o serviço para remover arquivos de banco de dados corrompidos ou arquivos de log antigos.
2. Desinstale o FireAMP devido a um erro, a uma instalação corrompida ou incompleta.
3. Substitua o arquivo policy.xml para diagnosticar problemas de conectividade.

Interromper o serviço usando propriedades do conector

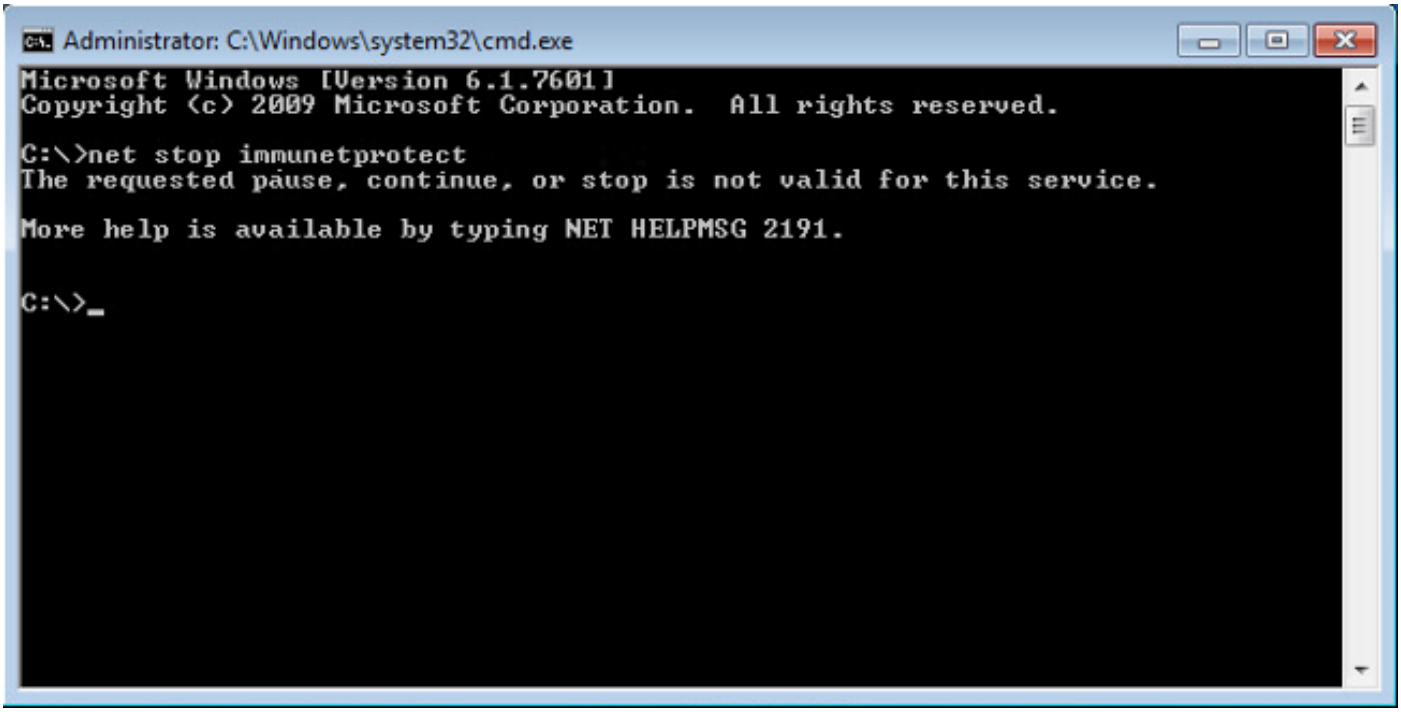
Você não poderá interromper o serviço usando a janela **Propriedades do conector FireAMP** se o recurso **Proteção do conector** estiver ativado. Os botões para gerenciar o serviço estão desabilitados como abaixo:



Parar serviço usando CLI

Quando você tenta parar um serviço enquanto o recurso de proteção do conector está ativado, você recebe uma mensagem de falha como a abaixo:

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



Na versão 4.3.0+, o serviço sfc.exe pode ser interrompido com o comando "sfc.exe -k password", onde 'password' é a senha definida na política.

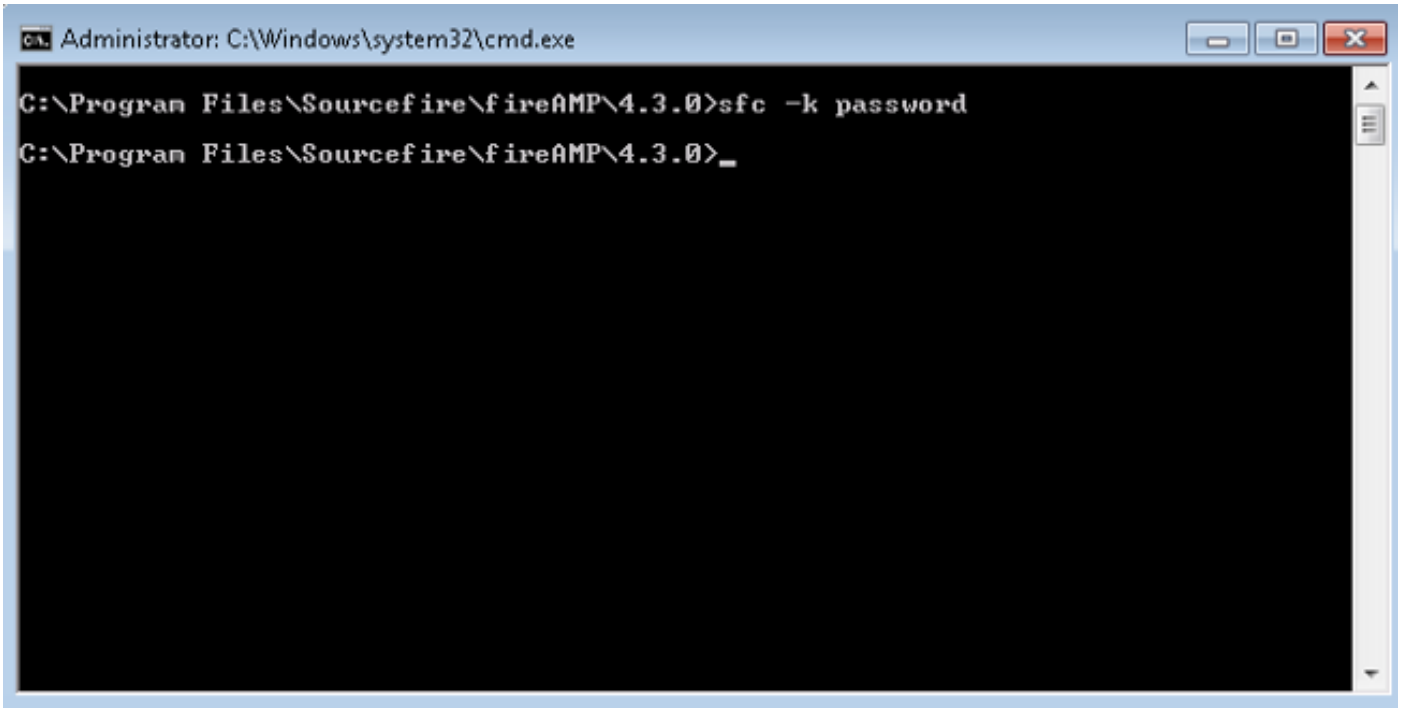
Solução

Pare o serviço usando a linha de comando

Observação: esse comando funciona somente na versão 4.3.0 e posterior do conector FireAMP.

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

Substitua a palavra "senha" pela senha real definida em sua política.



Interromper o serviço usando a interface do usuário

Você pode interromper o serviço protegido por senha na interface do usuário.