O serviço do conector de FireAMP não para devido à proteção do conector

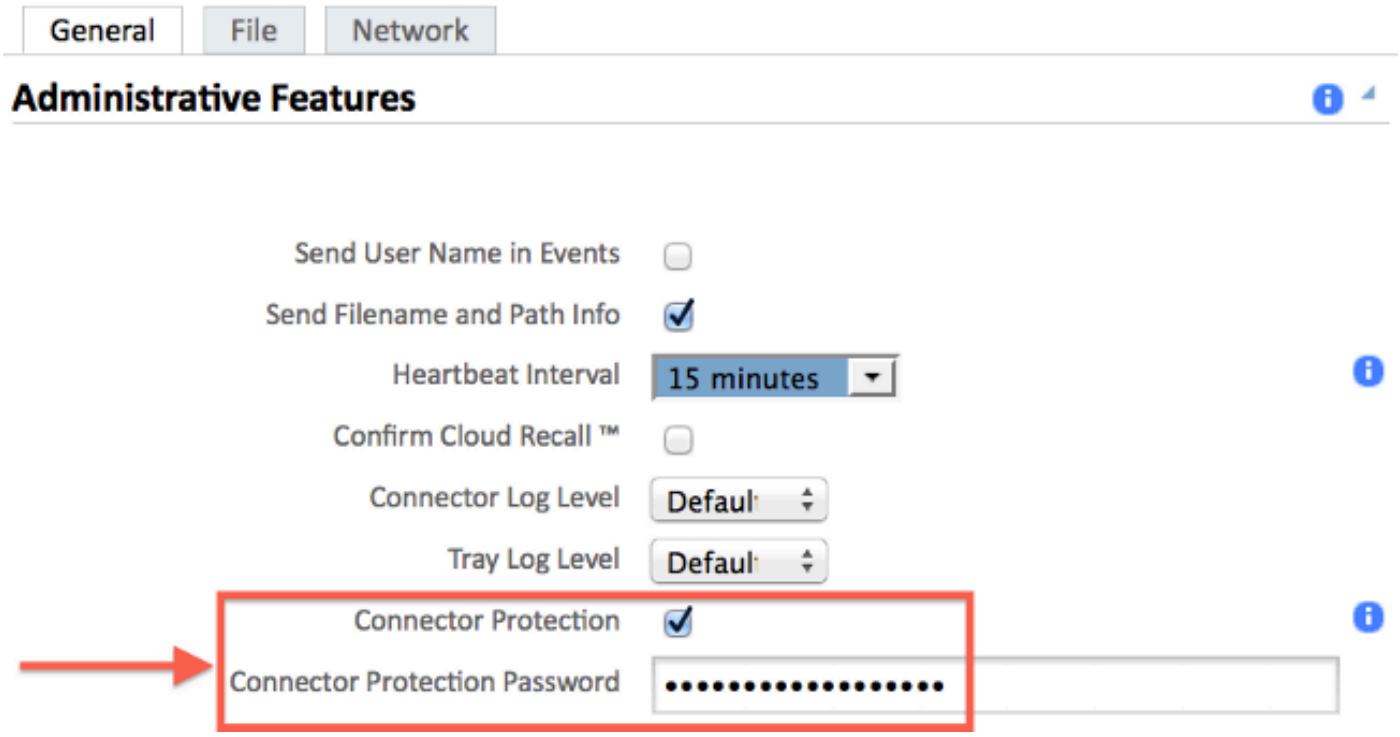
Índice

Introdução

O conector de FireAMP tem uma característica chamada **Conector Proteção**. Esta opção permite-o à senha protege o serviço do conector de FireAMP e impede que esteja parado ou desinstalar. Contudo, pode impactar o processo de Troubleshooting devido ao fato de que parar o serviço do conector de FireAMP ou o desinstalar podem entrar jogar como um passo de Troubleshooting. Este documento descreve como desinstalar FireAMP quando é senha protegida.

Configuração da proteção do conector

A fim permitir a **opção de proteção do conector**, edite sua **política**, vá ao **tab geral**, e expanda **características administrativas**.



Direcionador da auto-proteção

Os recursos de proteção do conector utilizam um direcionador da auto-proteção para proteger os diretórios para FireAMP. Um direcionador da auto-proteção executa as seguintes tarefas:

1. Proteja as chaves de registro que FireAMP usa da supressão e a alteração.
2. Proteja aplicativos da escrita ou arquivos da supressão no diretório de instalação. O diretório de instalação padrão é:

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

3. Proteja os direcionadores de FireAMP do descarregamento ou ser overwritten.
4. Proteja aplicativos de FireAMP, `iptray.exe e` agent.exe, `de` ser “extremidade processada” através do gerenciador de tarefa de Windows.

Parando o serviço do conector de FireAMP

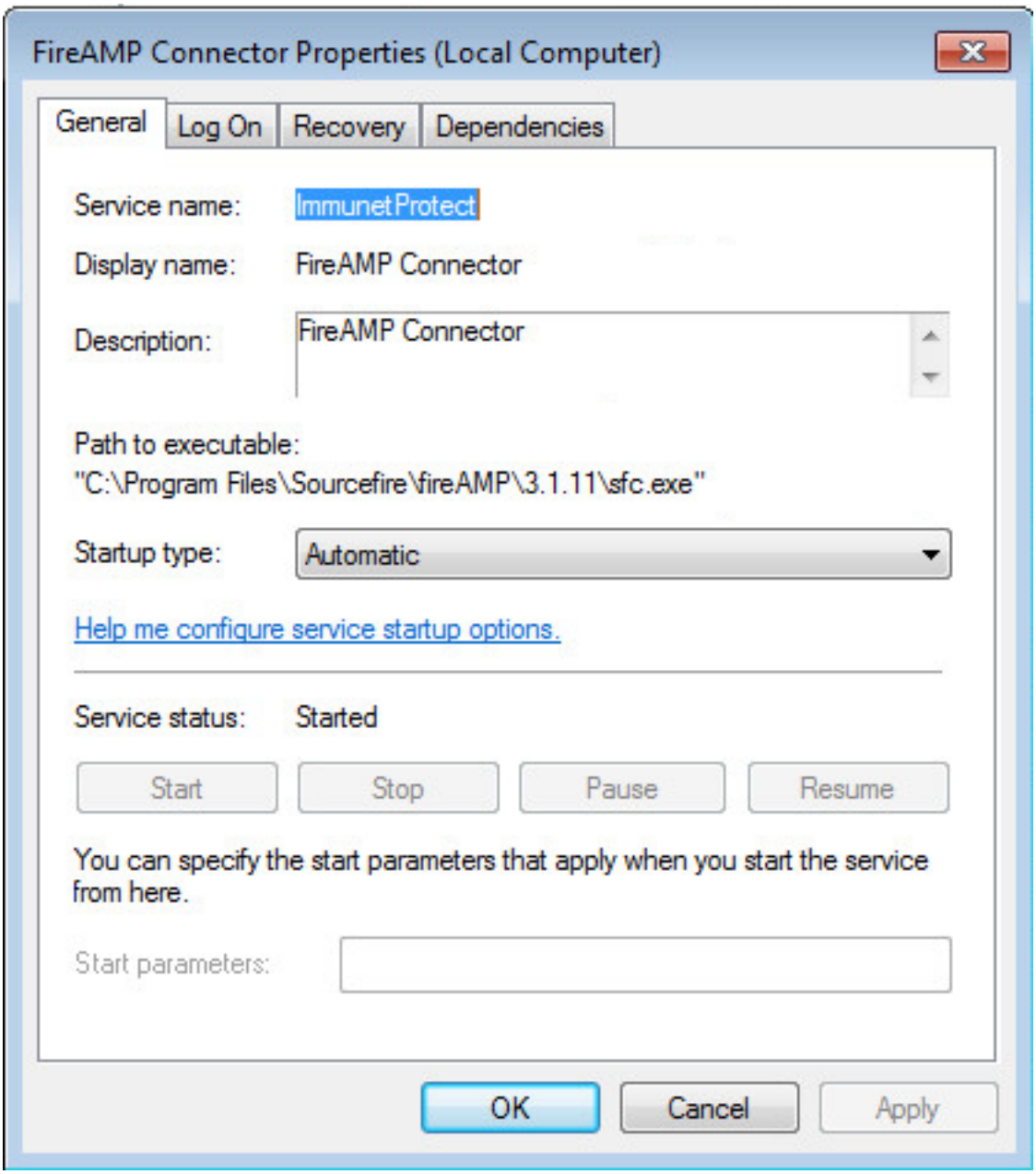
Razões para uma parada

Algumas encenações onde você pode querer parar o serviço do conector de FireAMP ou o desinstalar FireAMP estariam:

1. Pare o serviço a fim remover os arquivos de base de dados corrompido, ou arquivos de registro velhos.
2. Desinstale FireAMP devido a um erro, corrompido, ou à instalação incompleta.
3. Substitua o `arquivo policy.xml` a fim diagnosticar problemas de conectividade.

Pare o serviço usando propriedades do conector

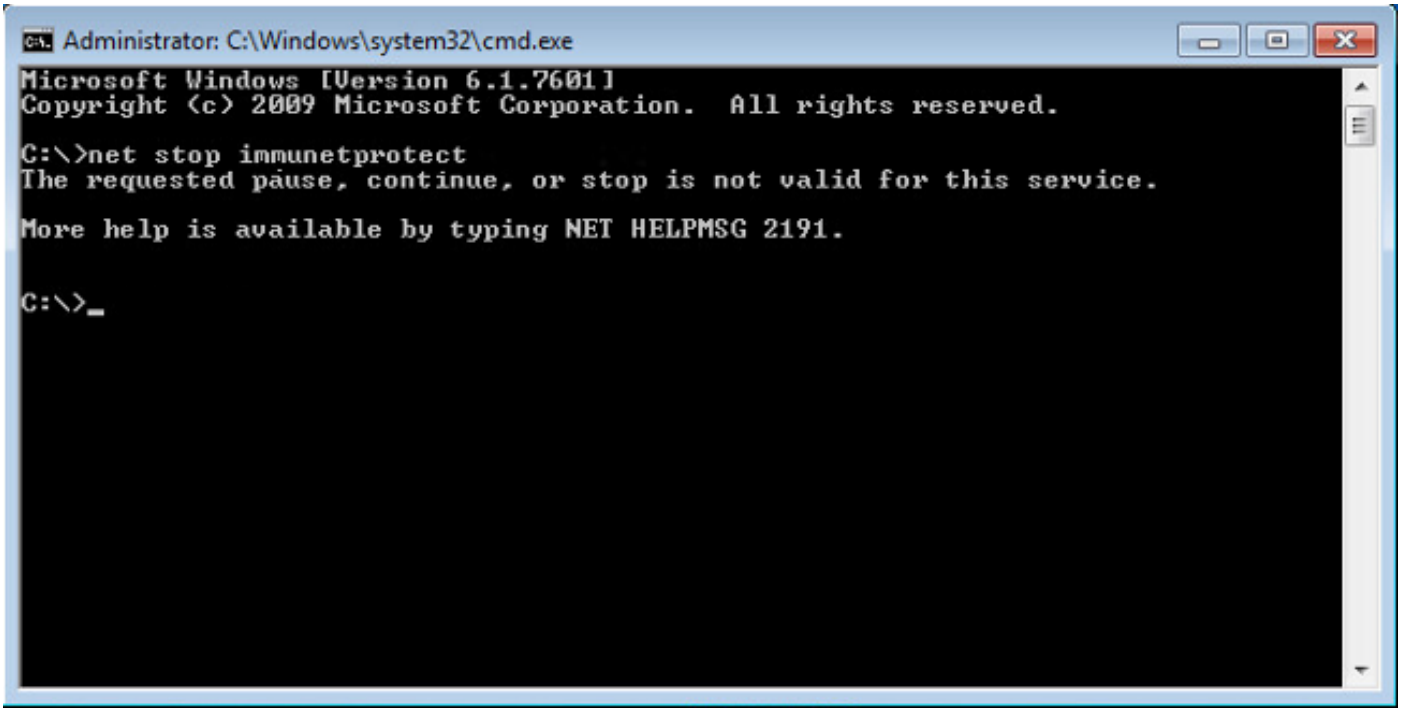
Você não poderá parar o serviço usando a **janela de propriedades do conector de FireAMP** se os **recursos de proteção do conector** são permitidos. Os botões para controlar o serviço são desabilitados como abaixo:



Pare o serviço usando o CLI

Quando você tenta parar um serviço quando os recursos de proteção do conector estiverem permitidos, você recebe um mensagem de falha como abaixo:

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



Na versão 4.3.0+ o serviço sfc.exe pode ser parado com o comando “sfc.exe - senha k” onde a “senha” é a senha definida na política.

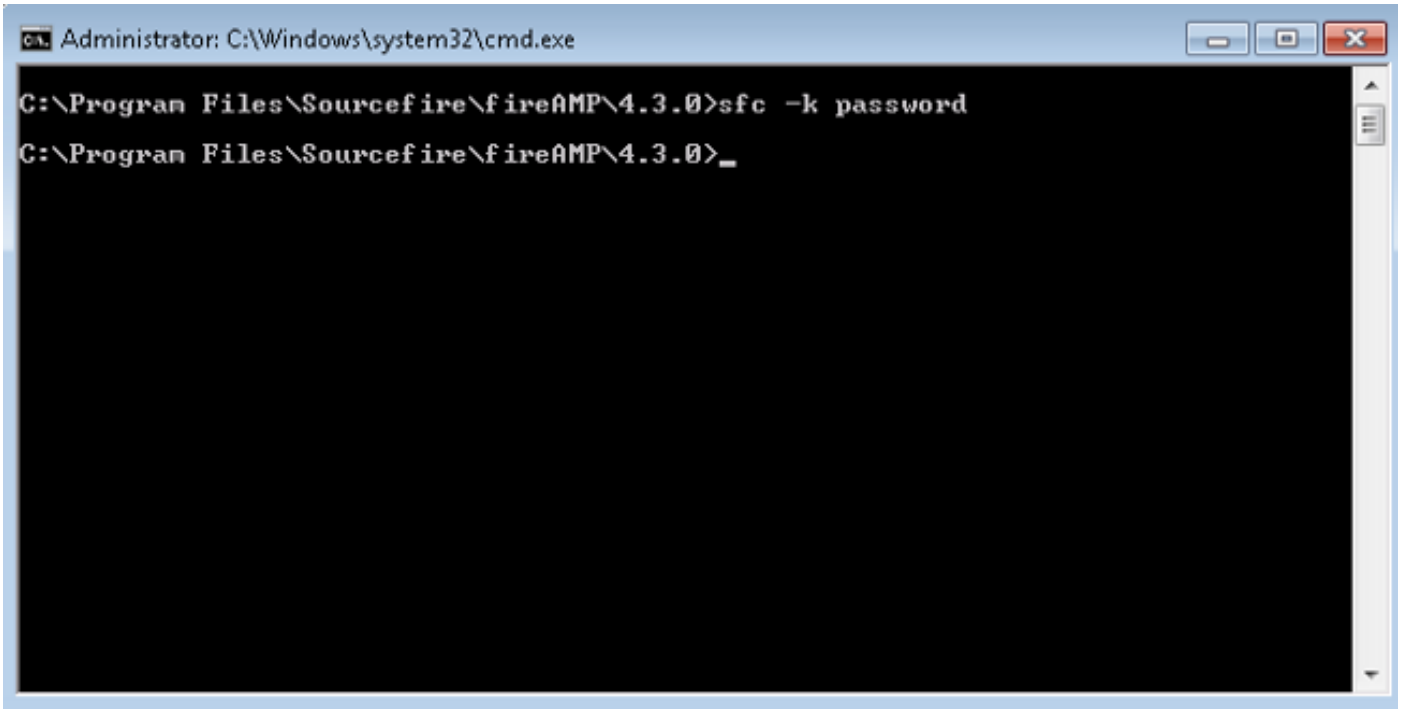
Solução

Pare o serviço usando a linha de comando

Nota - Este comando trabalha somente na versão 4.3.0 e mais recente do conector de FireAMP.

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

Substitua a palavra “senha” com o conjunto de senha real em sua política.



Pare o serviço usando a interface do utilizador

Você pode parar o serviço protegido senha da interface do utilizador.