Le service de connecteur de FireAMP n'arrête pas en raison de la protection de connecteur

Contenu

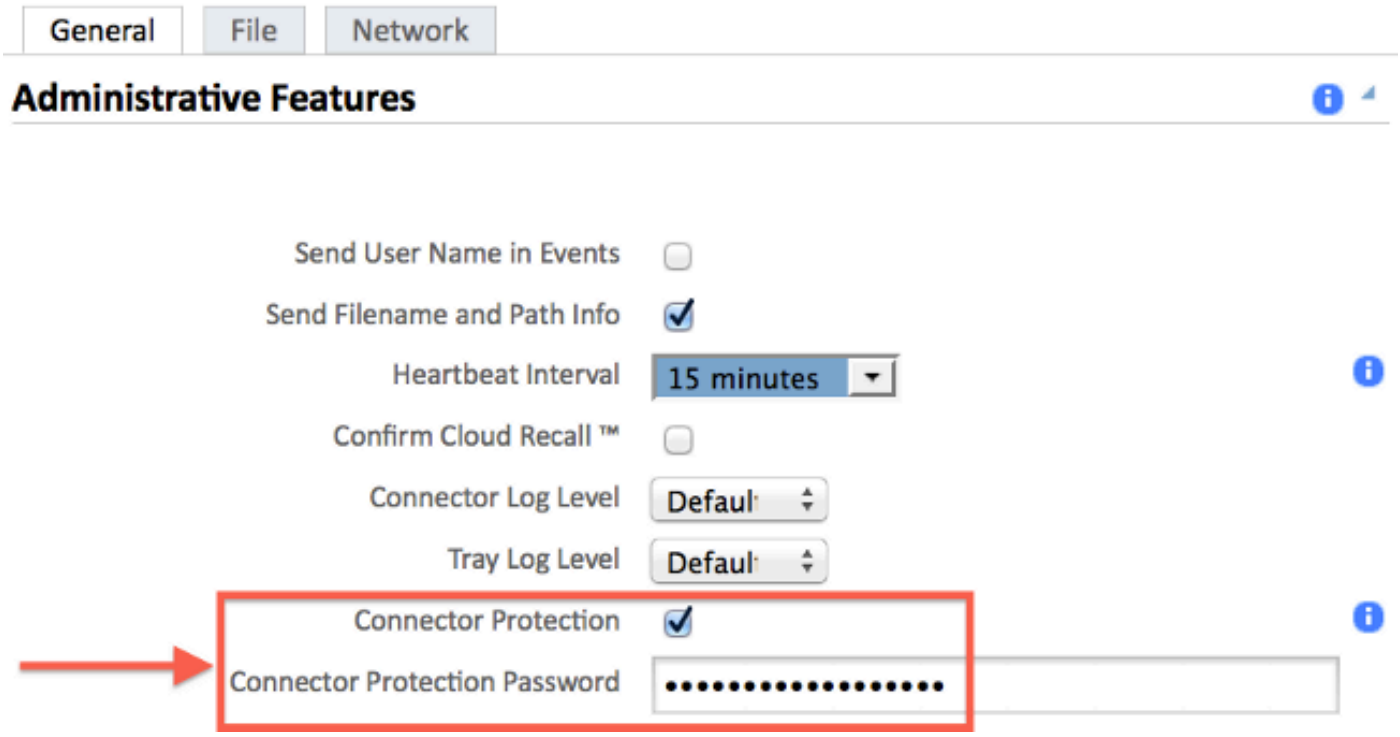
[Introduction](#)
[Configuration de la protection de connecteur](#)
[Gestionnaire d'autoprotection](#)
[Arrêter le service de connecteur de FireAMP](#)
[Raisons pour un arrêt](#)
[Service d'arrêt utilisant le connecteur Properties](#)
[Service d'arrêt utilisant le CLI](#)
[Solution](#)
[Arrêtez le service utilisant la ligne de commande](#)
[Service d'arrêt utilisant l'interface utilisateur](#)

Introduction

Le connecteur de FireAMP a une caractéristique appelée **Connector Protection**. Cette option te permet pour protéger par mot de passe le service de connecteur de FireAMP et pour l'empêcher d'être arrêté ou désinstallé. Cependant, il peut affecter le processus de dépannage étant donné qu'arrêter le service de connecteur de FireAMP ou le désinstaller peut entrer pour lire comme étape de dépannage. Ce document décrit comment désinstaller FireAMP quand il est protégé par mot de passe.

Configuration de la protection de connecteur

Afin d'activer l'option de **protection de connecteur**, éditez votre **stratégie**, allez à l'**onglet Général**, et développez les **caractéristiques administratives**.



Gestionnaire d'autoprotection

La caractéristique de protection de connecteur utilise un gestionnaire d'autoprotection pour protéger les répertoires pour FireAMP. Un gestionnaire d'autoprotection effectue les tâches suivantes :

1. Protégez les clés de registre que FireAMP utilise d'être supprimé et modifié.
2. Protégez les applications contre l'écriture ou des fichiers de supprimer dans le répertoire d'installation. Le répertoire d'installation par défaut est :

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

3. Protégez les gestionnaires de FireAMP contre être déchargé ou remplacé.
4. Protégez les applications de FireAMP, `iptray.exe et` agent.exe, `contre` être « extrémité traitée » par l'intermédiaire du gestionnaire de tâches de Windows.

Arrêter le service de connecteur de FireAMP

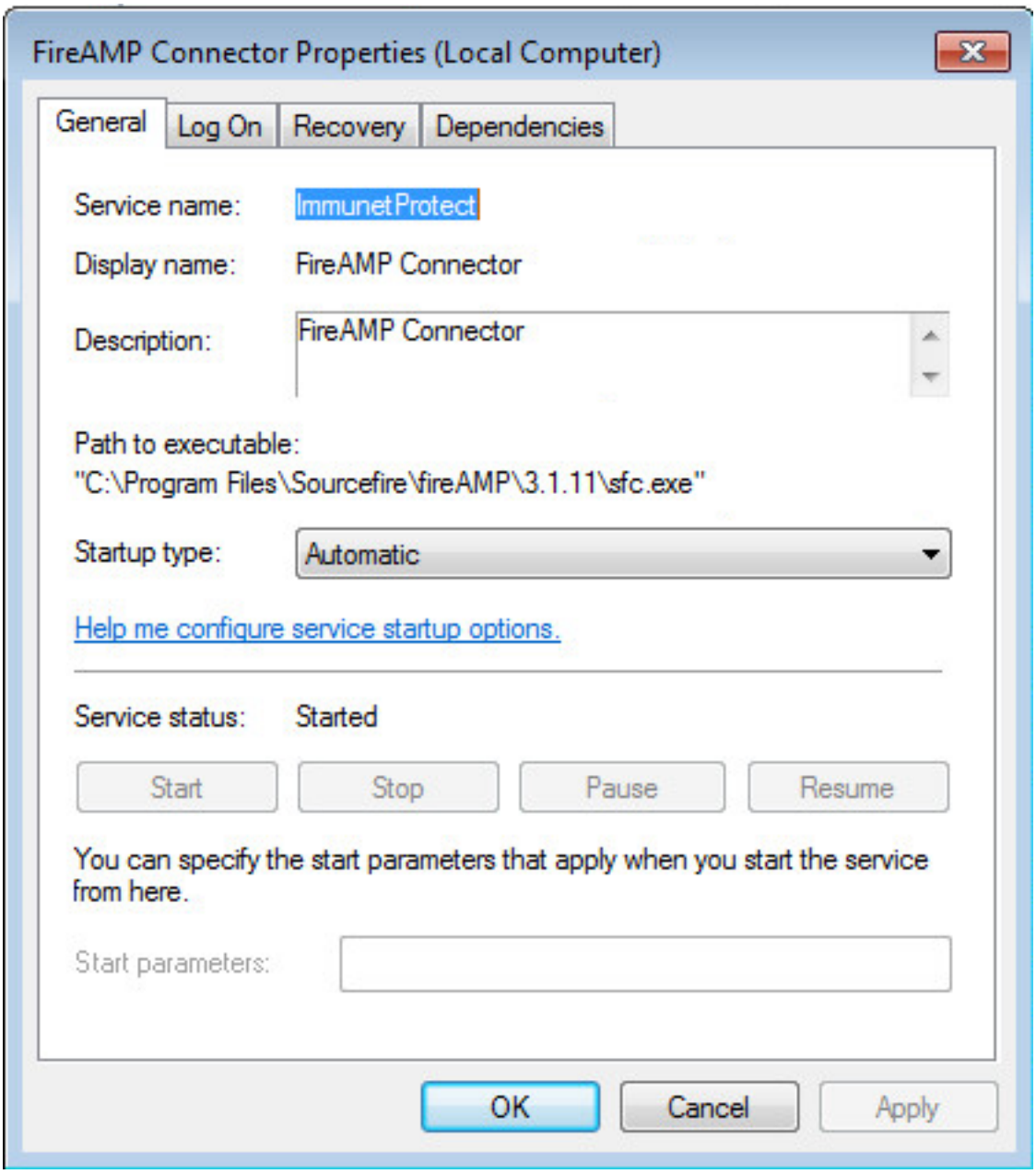
Raisons pour un arrêt

Quelques scénarios où vous pouvez vouloir arrêter le service de connecteur de FireAMP ou désinstaller FireAMP seraient :

1. Cessez le service afin de retirer les fichiers de base de données corrompus, ou les vieux fichiers journal.
2. Désinstallez FireAMP dû à une erreur, corrompue, ou à l'installation inachevée.
3. Remplacez le `fichier policy.xml` afin de diagnostiquer des problèmes de connectivité.

Service d'arrêt utilisant le connecteur Properties

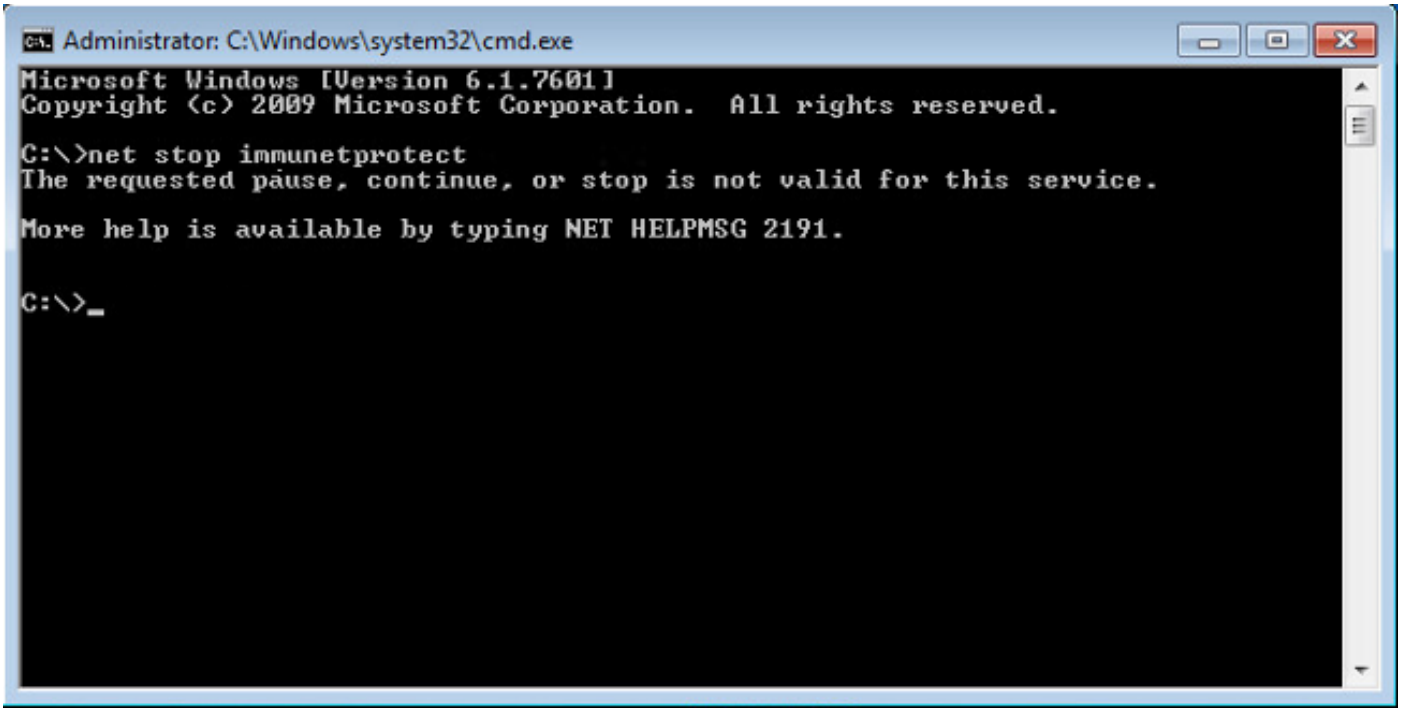
Vous ne pourrez pas arrêter le service utilisant la fenêtre de **Properties de connecteur de FireAMP** si la caractéristique de **protection de connecteur** est activée. Les boutons pour gérer le service sont désactivés en tant que ci-dessous :



Service d'arrêt utilisant le CLI

Quand vous tentez d'arrêter un service tandis que la caractéristique de protection de connecteur est activée, vous recevez un message d'échec comme ci-dessous :

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



Sur la version 4.3.0+ le service sfc.exe peut être arrêté avec la commande « sfc.exe - mot de passe k » où le « mot de passe » est le mot de passe défini dans la stratégie.

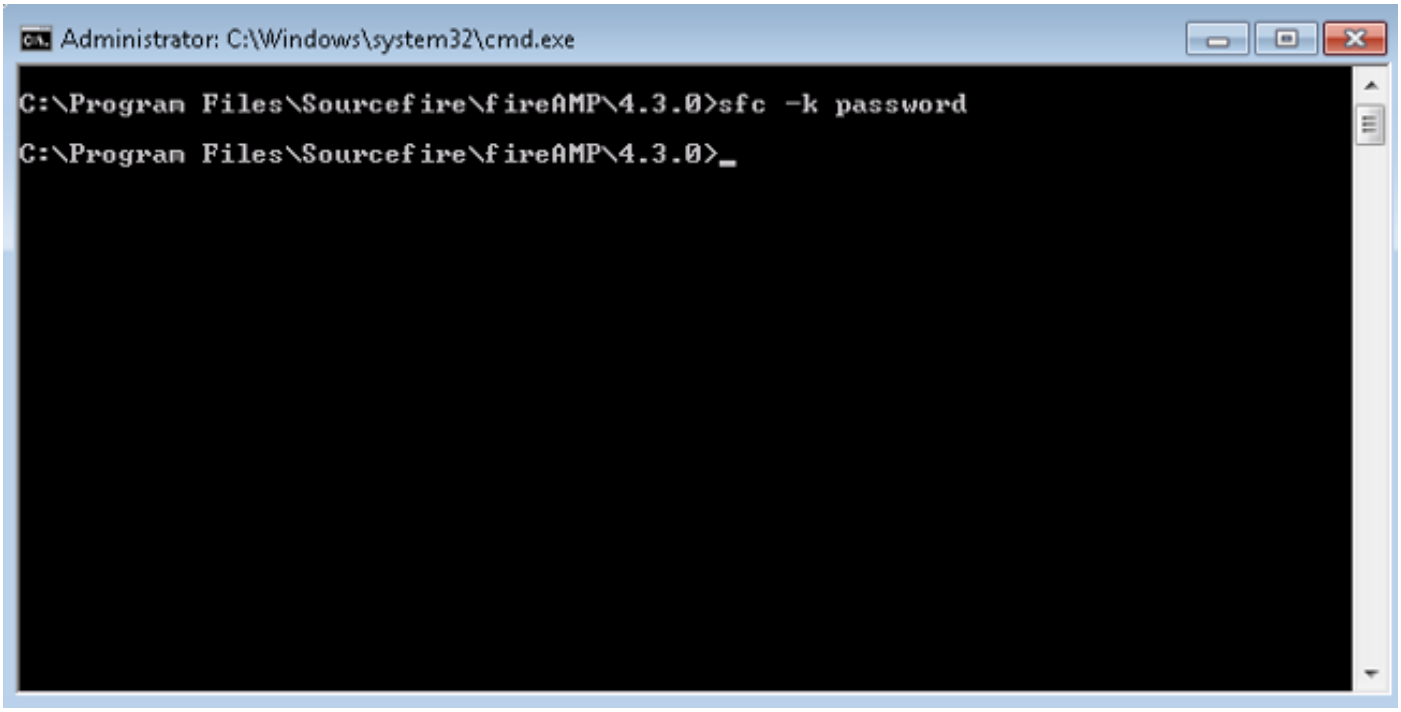
Solution

Arrêtez le service utilisant la ligne de commande

Note - Cette commande travaille seulement sur la version 4.3.0 et ultérieures du connecteur de FireAMP.

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

Remplacez le mot « mot de passe » par le mot de passe réel réglé dans votre stratégie.



Service d'arrêt utilisant l'interface utilisateur

Vous pouvez arrêter le service protégé par mot de passe de l'interface utilisateur.