Impossibile arrestare il servizio connettore FireAMP a causa della protezione del connettore

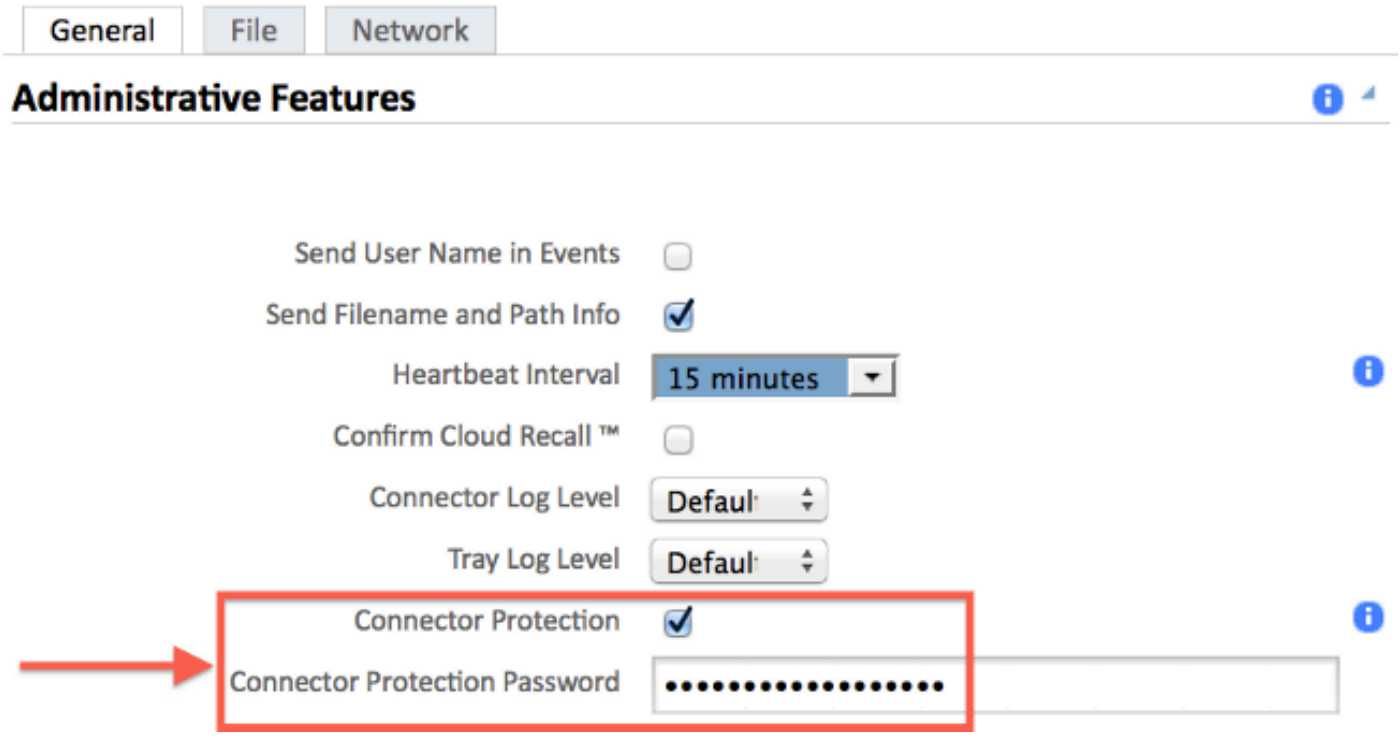
Sommario

Introduzione

Il connettore FireAMP dispone di una funzione chiamata **Protezione connettore**. Questa opzione consente di proteggere con password il servizio FireAMP Connector e di impedirne l'arresto o la disinstallazione. Tuttavia, potrebbe influire sul processo di risoluzione dei problemi poiché l'arresto o la disinstallazione del servizio del connettore FireAMP può essere utile come fase di risoluzione dei problemi. Questo documento descrive come disinstallare FireAMP quando è protetto da password.

Configurazione della protezione del connettore

Per abilitare l'opzione **Protezione connettore**, modificare il **criterio**, passare alla scheda **Generale** ed espandere **Funzionalità amministrative**.



Driver autoprotezione

La funzione Connector Protection utilizza un driver con protezione automatica per proteggere le directory di FireAMP. Un driver con protezione automatica esegue le seguenti attività:

1. Impedisce l'eliminazione e la modifica delle chiavi del Registro di sistema utilizzate da FireAMP.
2. Proteggere le applicazioni dalla scrittura o dall'eliminazione di file nella directory di installazione. La directory di installazione predefinita è:

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

3. Proteggere i driver FireAMP dallo scaricamento o dalla sovrascrittura.
4. Proteggere le applicazioni FireAMP, iptray.exe e agent.exe, dalla condizione di "Fine elaborazione" tramite Gestione attività Windows.

Arresto del servizio FireAMP Connector

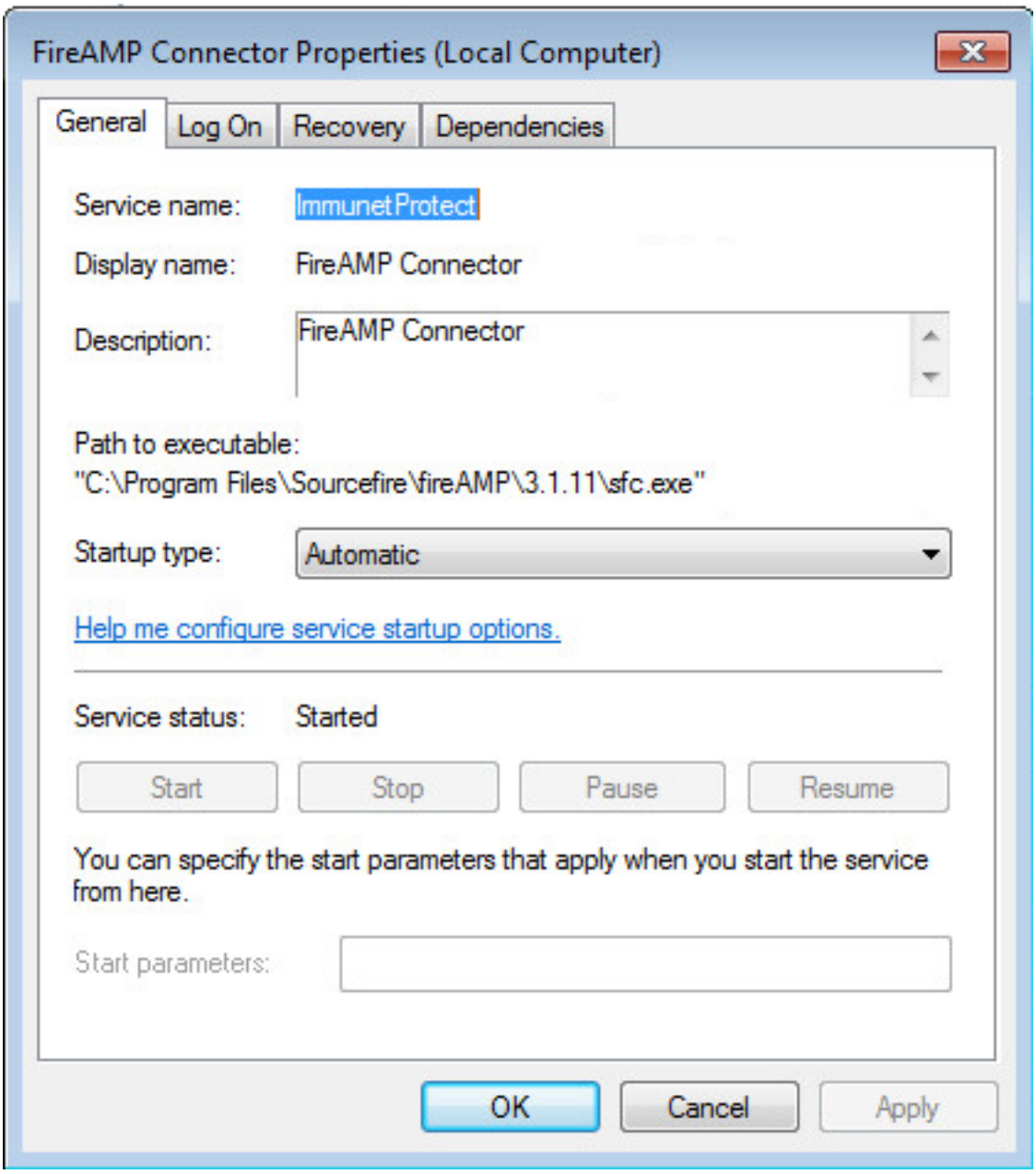
Motivi di una fermata

Di seguito sono riportati alcuni scenari in cui è possibile arrestare il servizio del connettore FireAMP o disinstallare FireAMP:

1. Arrestare il servizio per rimuovere i file di database danneggiati o i file di registro obsoleti.
2. Disinstallare FireAMP a causa di un errore, di un danneggiamento o di un'installazione incompleta.
3. Sostituire il file policy.xml per diagnosticare i problemi di connettività.

Arresta servizio mediante proprietà connettore

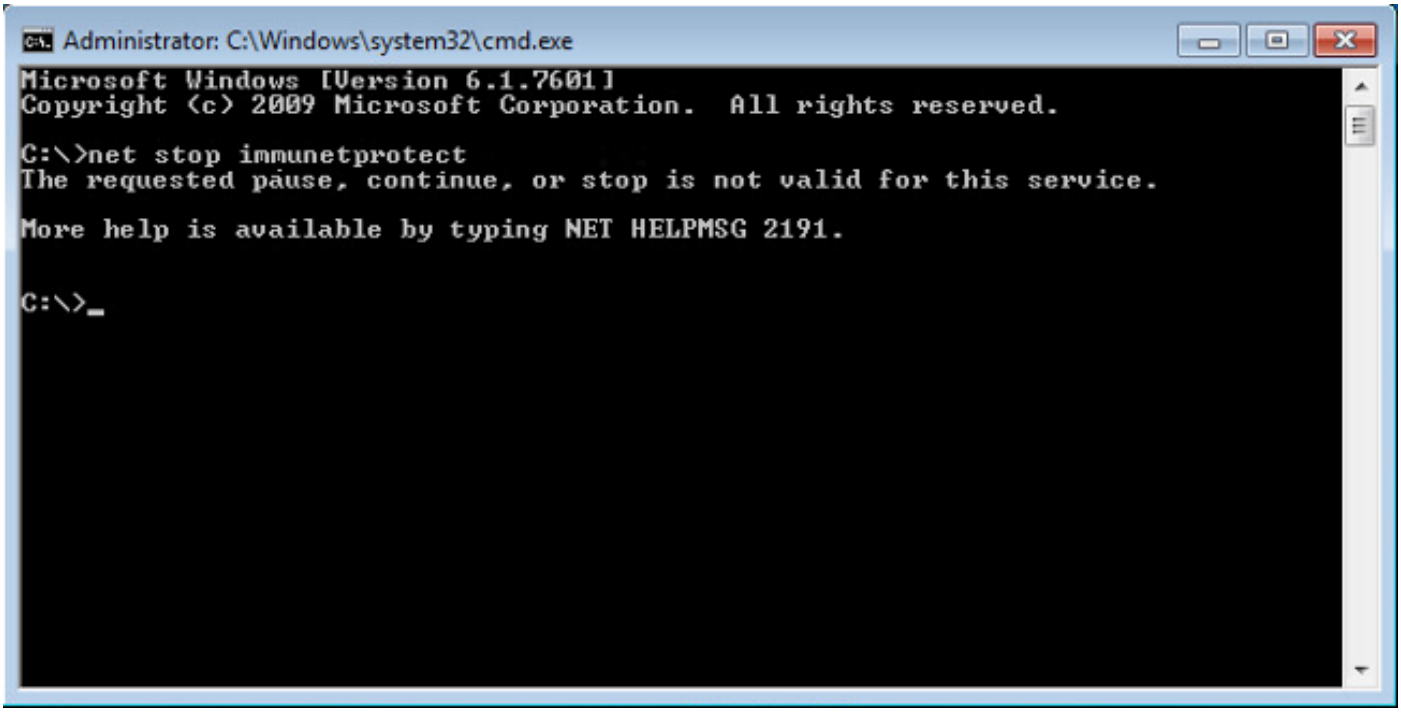
Non sarà possibile interrompere il servizio utilizzando la finestra **Proprietà connettore FireAMP** se la funzione **Protezione connettore** è abilitata. I pulsanti per la gestione del servizio sono disattivati come segue:



Arresta servizio tramite CLI

Quando si tenta di arrestare un servizio mentre la funzione di protezione del connettore è attivata, viene visualizzato un messaggio di errore simile al seguente:

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



Nella versione 4.3.0+ il servizio sfc.exe può essere arrestato con il comando "sfc.exe -k password", dove 'password' è la password definita nel criterio.

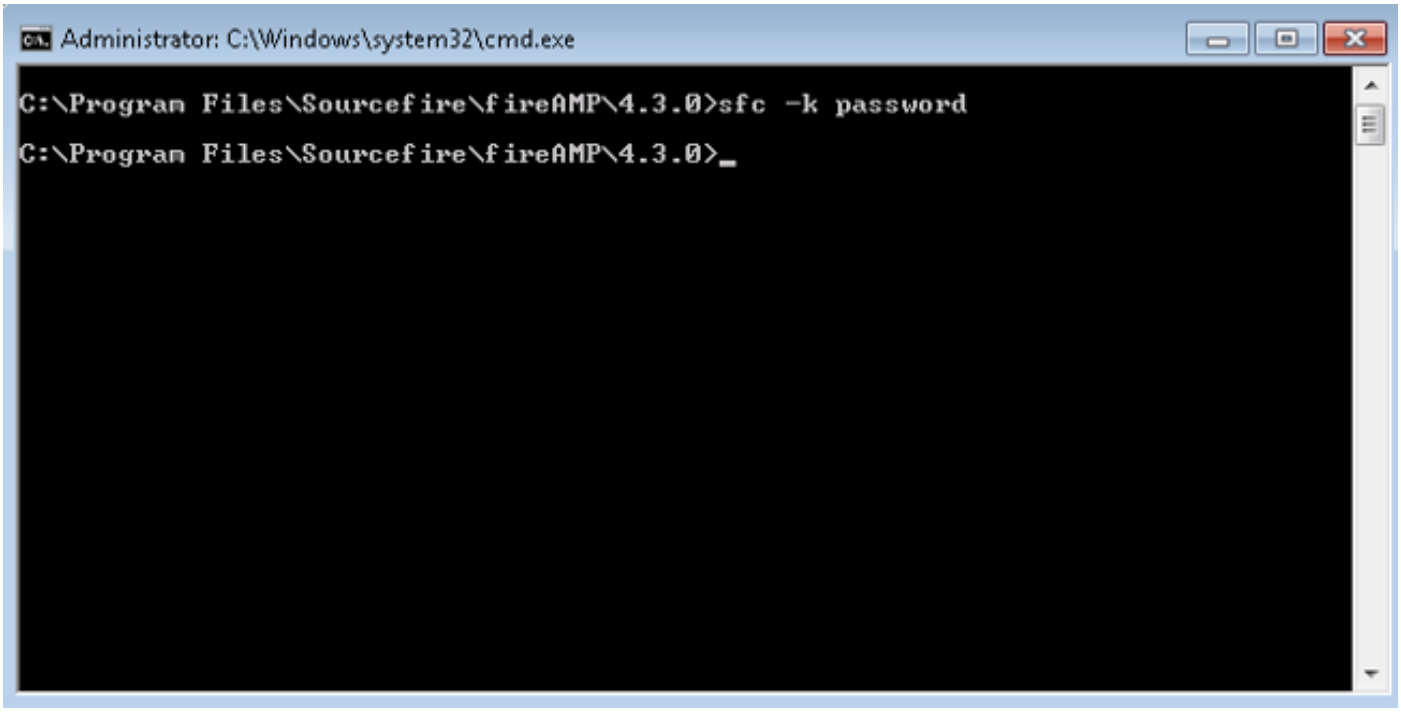
Soluzione

Arrestare il servizio utilizzando la riga di comando

Nota: questo comando funziona solo sulla versione 4.3.0 e successive del connettore FireAMP.

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

Sostituire la parola "password" con la password effettiva impostata nel criterio.



Arresta servizio mediante l'interfaccia utente

Èpossibile arrestare il servizio protetto da password dall'interfaccia utente.