Rimozione della cache e dei file di cronologia di FireAMP in Windows

Sommario

Introduzione

In questo documento vengono presentati alcuni scenari che richiedono la rimozione di file di database in FireAMP for Endpoints e viene descritta una procedura appropriata per la rimozione di tali file quando necessario. FireAMP for Endpoints conserva una registrazione delle sue recenti rilevazioni ed eliminazioni di file nei file di database. In alcuni casi, un tecnico dell'assistenza Cisco potrebbe chiedere di rimuovere alcuni file del database per risolvere un problema.

> **Avviso:** È possibile rimuovere un file di database solo su istruzione del supporto tecnico Cisco.

File di database per cache e cronologia

Scopo

I file del database della cache mantengono le disposizioni note per i file. I file del database cronologico rilevano tutti i rilevamenti di file FireAMP, oltre ai nomi dei file di origine e ai valori SHA256.

Quando si aggiunge un elenco di blocco a un criterio e si aggiorna il connettore, il comportamento di un determinato file non cambia immediatamente. La cache ha già rilevato che il file non è dannoso. Pertanto, non verrà modificato o sostituito dall'elenco Blocca. La disposizione cambia quando la cache è scaduta ogni volta nel criterio e viene eseguita una nuova ricerca, prima negli elenchi e successivamente nel cloud.

Motivi della rimozione

Se i file del database di cronologia e del database di cache vengono rimossi da una directory, verranno ricreati al riavvio del servizio FireAMP. In alcuni casi potrebbe essere necessario rimuovere questi file dalla directory FireAMP. Ad esempio, se si desidera verificare un semplice rilevamento personalizzato o un elenco di applicazioni bloccate per un determinato file.

Èpossibile che un database risulti danneggiato e pertanto non sarà possibile aprire o visualizzare i rilevamenti in un database. In alternativa, se il database è danneggiato su un sistema, è possibile che si verifichino errori nel servizio FireAMP Connector, ad esempio l'impossibilità di avviare il connettore o il peggioramento delle prestazioni complessive del sistema. In questi casi è possibile cancellare i file di cronologia dal connettore in modo da evitare problemi relativi alle prestazioni e poter acquisire nuovi registri per la diagnosi.

Identificare i file di database

In Microsoft Windows questi file si trovano in genere in C:\Program Files\Sourcefire\fireAMP o C:\Program Files\Cisco\AMP.

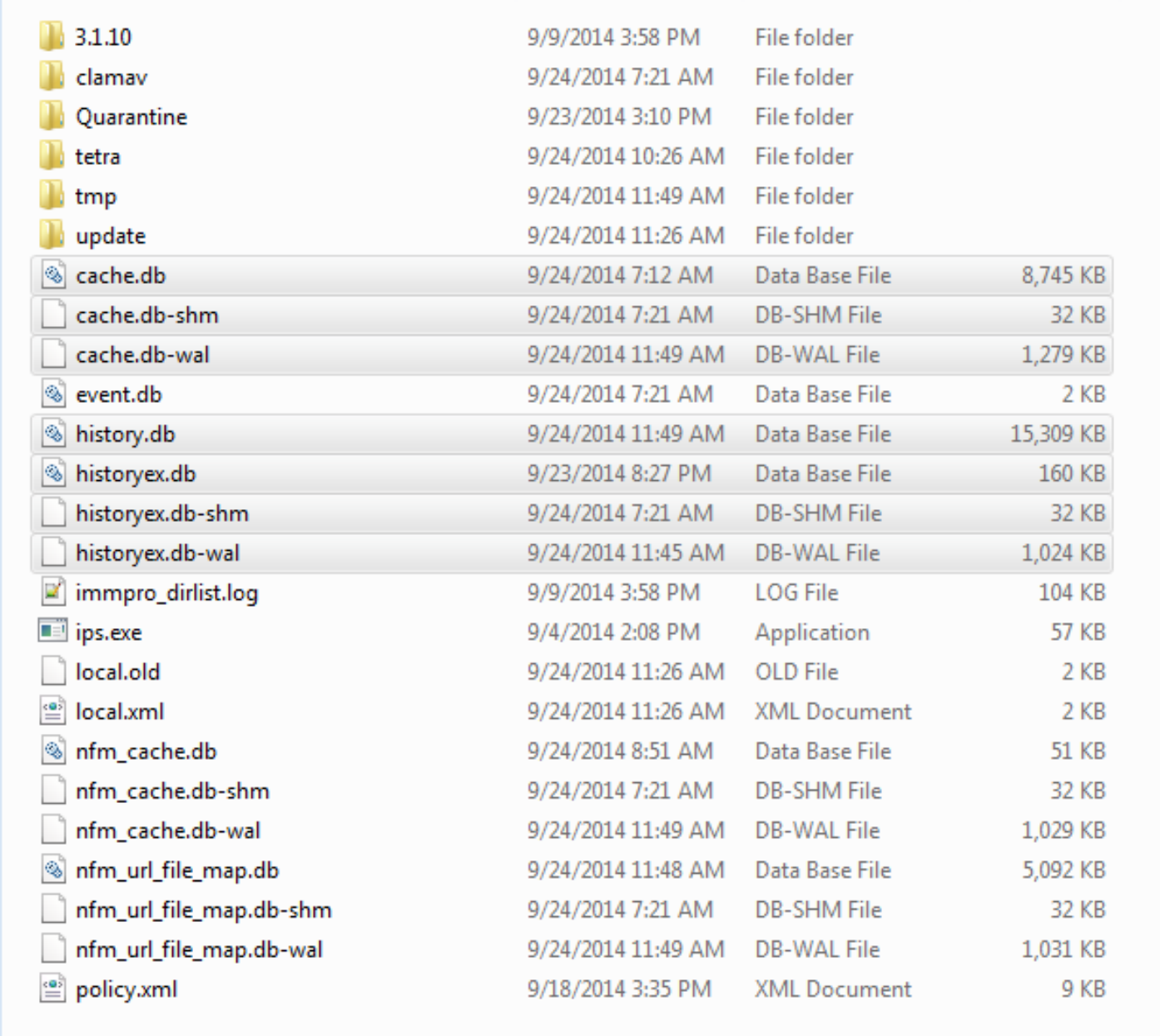
Nome dei file di database della cache:

```
cache.db
cache.db-shm
cache.db-wal
```

Il nome dei file del database della cronologia è:

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

In questa schermata vengono mostrati i file in Esplora file di Windows:



3.1.10	9/9/2014 3:58 PM	File folder	
clamav	9/24/2014 7:21 AM	File folder	
Quarantine	9/23/2014 3:10 PM	File folder	
tetra	9/24/2014 10:26 AM	File folder	
tmp	9/24/2014 11:49 AM	File folder	
update	9/24/2014 11:26 AM	File folder	
cache.db	9/24/2014 7:12 AM	Data Base File	8,745 KB
cache.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
cache.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,279 KB
event.db	9/24/2014 7:21 AM	Data Base File	2 KB
history.db	9/24/2014 11:49 AM	Data Base File	15,309 KB
historyex.db	9/23/2014 8:27 PM	Data Base File	160 KB
historyex.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
historyex.db-wal	9/24/2014 11:45 AM	DB-WAL File	1,024 KB
immpro_dirlist.log	9/9/2014 3:58 PM	LOG File	104 KB
ips.exe	9/4/2014 2:08 PM	Application	57 KB
local.old	9/24/2014 11:26 AM	OLD File	2 KB
local.xml	9/24/2014 11:26 AM	XML Document	2 KB
nfm_cache.db	9/24/2014 8:51 AM	Data Base File	51 KB
nfm_cache.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
nfm_cache.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,029 KB
nfm_url_file_map.db	9/24/2014 11:48 AM	Data Base File	5,092 KB
nfm_url_file_map.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
nfm_url_file_map.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,031 KB
policy.xml	9/18/2014 3:35 PM	XML Document	9 KB

Procedura di rimozione dei file di database

Passaggio 1: Arresta il servizio FireAMP Connector

Èpossibile arrestare il servizio FireAMP Connector in diversi modi:

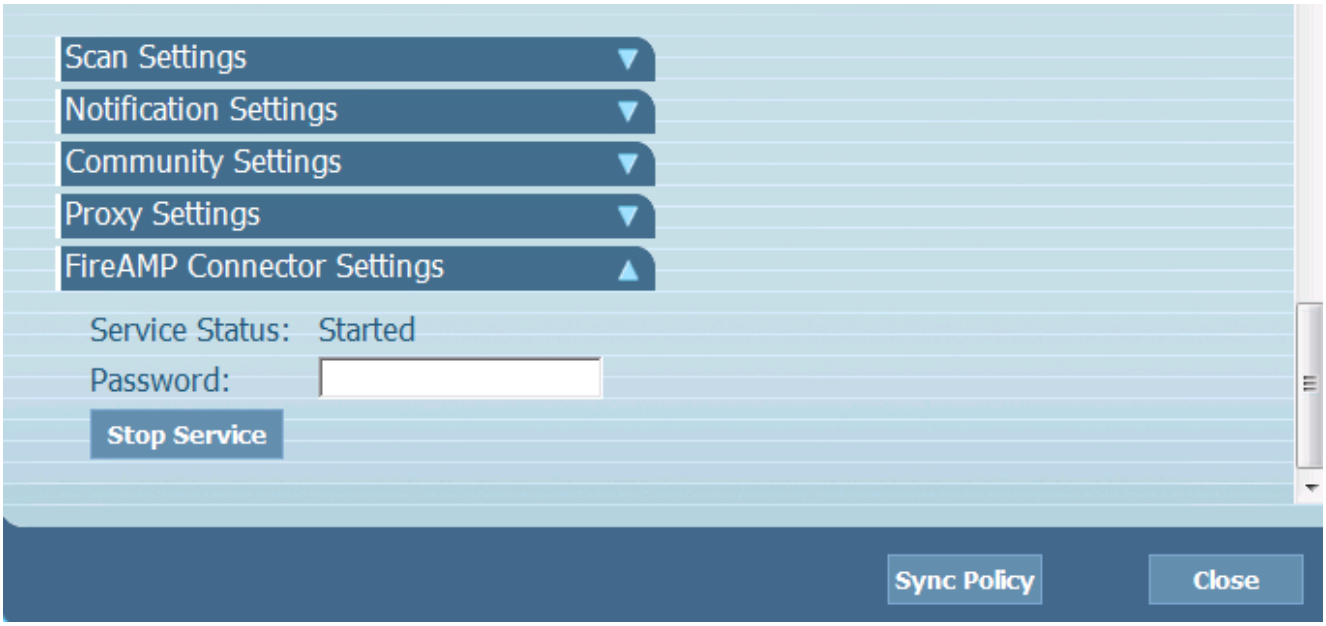
- Interfaccia utente del servizio FireAMP Connector
- Console Servizi Windows
- Prompt dei comandi dell'amministratore

Interfaccia utente

> **Nota:** Se la protezione del connettore è abilitata, è necessario utilizzare l'interfaccia utente per interrompere il servizio FireAMP Connector.

1. Aprire l'interfaccia utente dall'area di notifica e fare clic su **Impostazioni**.

2. Scorrere fino alla parte inferiore ed espandere **Impostazioni connettore FireAMP**.
3. Nel campo Password, immettere la password di protezione del connettore. Fare clic su **Arresta servizio**.

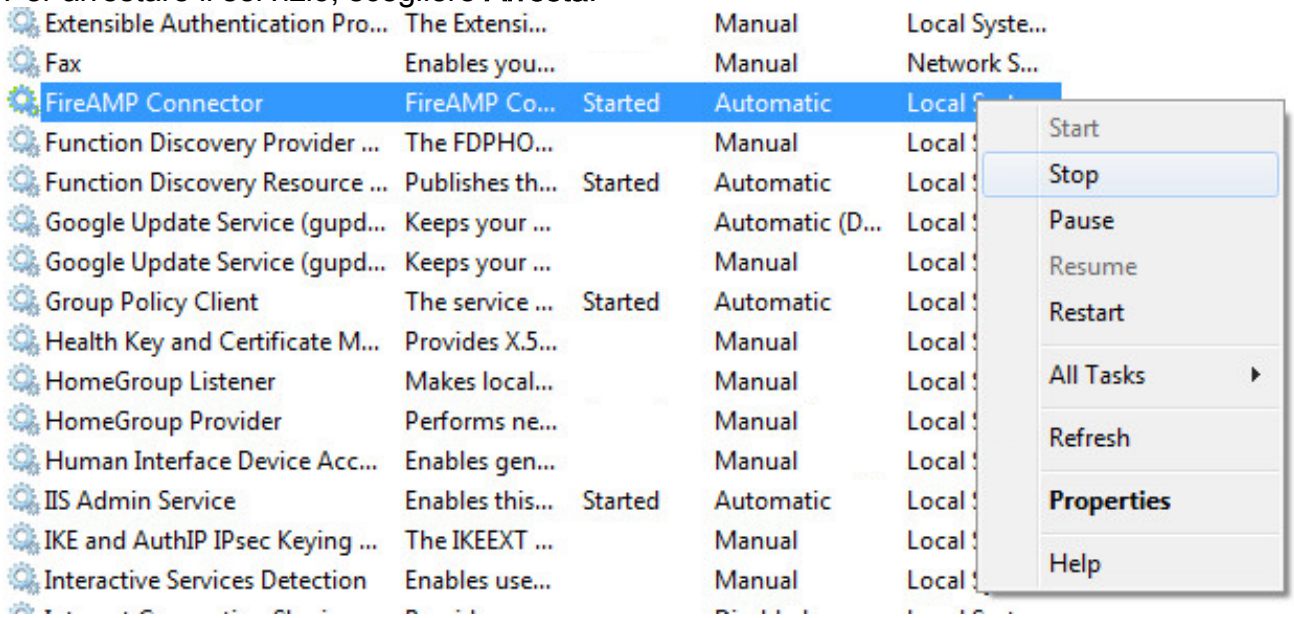


Console servizi

Nota: Per arrestare e avviare i servizi nella console dei servizi, è necessario disporre dei privilegi di amministratore.

Per interrompere il servizio FireAMP Connector dalla console dei servizi, attenersi alla seguente procedura:

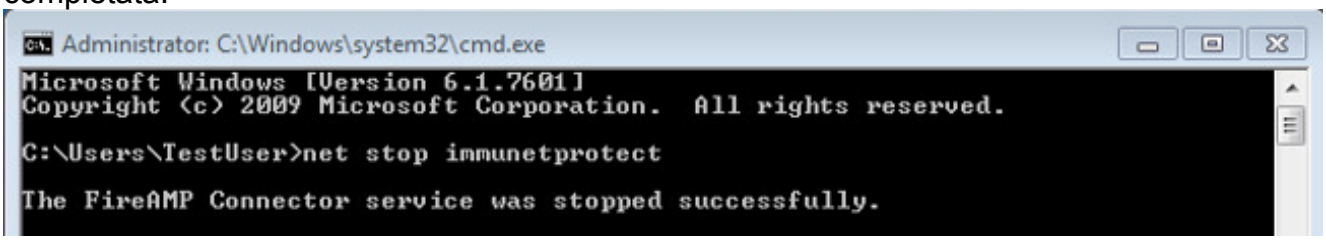
1. Passare al **menu Start**.
2. Immettere **services.msc** e premere **Invio**. Verrà visualizzata la console Servizi.
3. Selezionare il servizio **FireAMP Connector** e fare clic con il pulsante destro del mouse sul nome del servizio.
4. Per arrestare il servizio, scegliere **Arresta**.



Prompt dei comandi

Per interrompere il servizio FireAMP Connector dal prompt dei comandi di un amministratore, attenersi alla seguente procedura:

1. Passare al **menu Start**.
2. Immettere **cmd.exe** e premere **Invio**. Viene visualizzata una finestra del prompt dei comandi.
3. Immettere il comando **net stop immunetprotect**. Se si dispone della versione 5.0.1 o successiva, immettere il **servizio wmic dove "name like 'immunetprotect%'" chiama** invece il comando **startservice**. In questa schermata viene mostrato un esempio di interruzione del servizio
   completata:



Passaggio 2: Elimina i file di database necessari

Memorizza file di database nella cache

Una volta arrestato il servizio, è possibile eliminare i seguenti tre file di cache:

> **Avviso:** Se non si eliminano tutti i file di database della cache correlati, è possibile che si verifichino problemi di memorizzazione nella cache con il database ricreato. Di conseguenza, è possibile che il servizio non venga avviato o che le prestazioni del servizio risultino ridotte.

```
cache.db
cache.db-shm
cache.db-wal
```

File di database della cronologia

Una volta arrestato il servizio, rimuovere i seguenti file di database della cronologia:

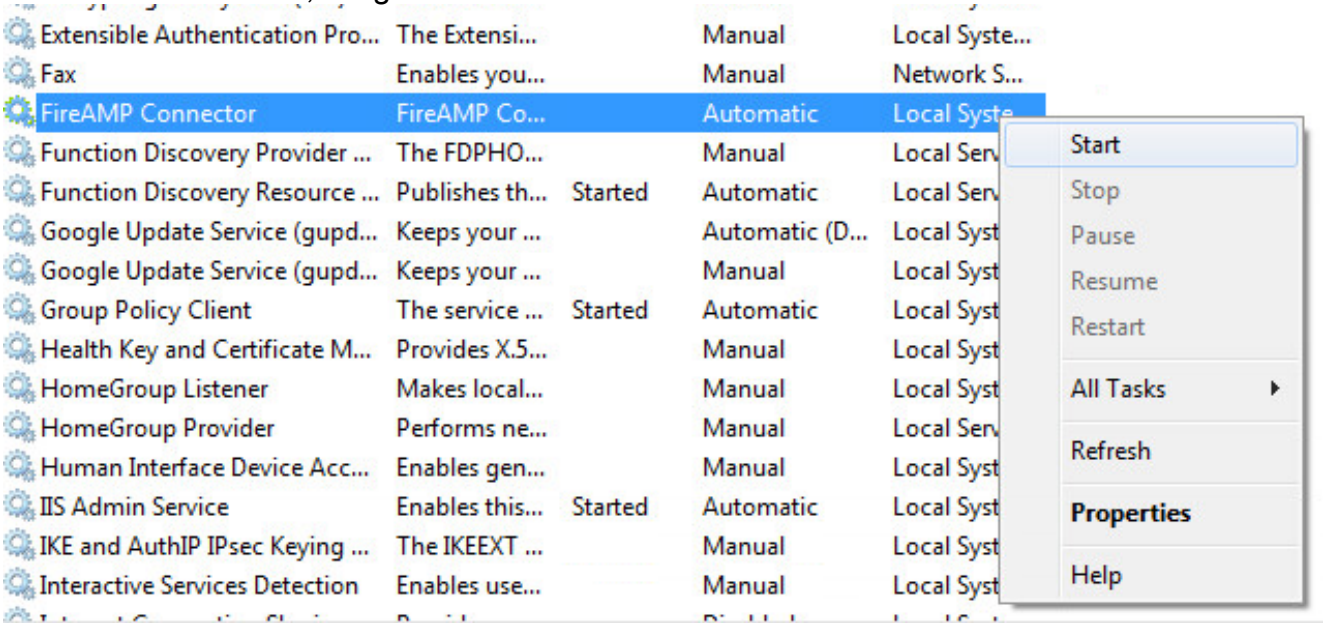
> **Avviso:** Se non si eliminano tutti i file di database della cronologia correlati, è possibile che si verifichino problemi di memorizzazione nella cache con il database ricreato. Di conseguenza, è possibile che il servizio non venga avviato o che le prestazioni del servizio risultino ridotte.

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

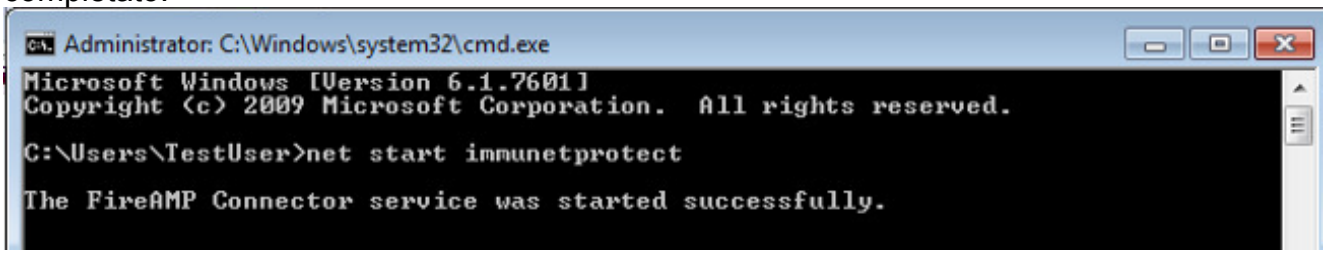
Passaggio 3: Avvia il servizio FireAMP Connector

Per avviare il servizio FireAMP Connector, attenersi alla seguente procedura:

1. Passare al **menu Start**.
2. Immettere **services.msc** e premere **Invio**. Verrà visualizzata la console Servizi.
3. Scegliere il servizio **FireAMP Connector** e fare clic con il pulsante destro del mouse sul nome del servizio.
4. Per avviare il servizio, scegliere **Avvia**.



In alternativa, al prompt dei comandi dell'amministratore è possibile immettere il comando **net start immunetprotect**. Se si dispone della versione 5.0.1 o successiva, immettere il **servizio wmic dove "name like 'immunetprotect%'" chiama** invece il comando **startservice**.In questa schermata viene mostrato un esempio di avvio del servizio completato:



Dopo il riavvio dei servizi, viene creato un nuovo set di file di database. In questo modo è possibile ottenere una nuova istanza del connettore FireAMP con elenchi di bianchi, elenchi di blocchi, esclusioni e così via.