Remoção do esconderijo e dos arquivos históricos de FireAMP em Windows

Índice

Introdução

Este documento fornece algumas encenações que exigem uma remoção dos arquivos da base de dados em FireAMP para valores-limite e descreve um procedimento apropriado para removê-los quando necessário. O FireAMP para valores-limite mantém um registro de suas detecções e disposições do arquivo recente nos arquivos da base de dados. Em certos casos, um engenheiro de suporte da Cisco pôde pedir que você remova alguns dos arquivos da base de dados a fim pesquisar defeitos uma edição.

> **aviso:** Você pode remover um arquivo da base de dados somente se instruído pelo Suporte técnico de Cisco.

Arquivos da base de dados para o esconderijo e a história

Propósito

Os arquivos da base de dados do esconderijo mantêm as disposições conhecidas para arquivos. Os arquivos da base de dados de história seguem todas as detecções do arquivo de FireAMP, junto com nomes do arquivo de origem e valores SHA256.

Quando você adiciona uma lista do bloco a uma política e atualiza o conector, o comportamento para um arquivo dado não muda imediatamente. Isto é porque o esconderijo tem identificado já que o arquivo não é malicioso. Como tal, não será mudado nem será cancelado por sua lista do bloco. A disposição muda quando o esconderijo está expirado pelo tempo em sua política e uma

consulta nova está executada - primeiramente contra suas lista e subseqüentemente contra a nuvem.

Razões para a remoção

Se os arquivos da base de dados do base de dados e do esconderijo da história são removidos de um diretório, são frescos recreado quando o serviço de FireAMP reinicia. Em certos casos pôde ser necessário remover estes arquivos do diretório de FireAMP. Por exemplo, se você quer testar uma detecção feita sob encomenda simples ou uma lista do bloco do aplicativo para um arquivo dado.

Épossível que um base de dados poderia se tornar corrompido, que o torne incapaz de abrir ou ver as detecções em um base de dados. Alternativamente, se o base de dados é corrompido em um sistema pode causar erros dentro do serviço do conector de FireAMP tal como a incapacidade começar o conector ou a degradação do desempenho de sistema total. Nestes exemplos você pôde querer cancelar os arquivos históricos do conector de modo que você pudesse evitar questões relacionadas ao desempenho da corrupção e poder capturar logs novos para o diagnóstico.

Identifique os arquivos da base de dados

Em Microsoft Windows, estes arquivos são ficados tipicamente em C:\Program Files\Sourcefire\fireAMP ou em C:\Program Files\Cisco\AMP.

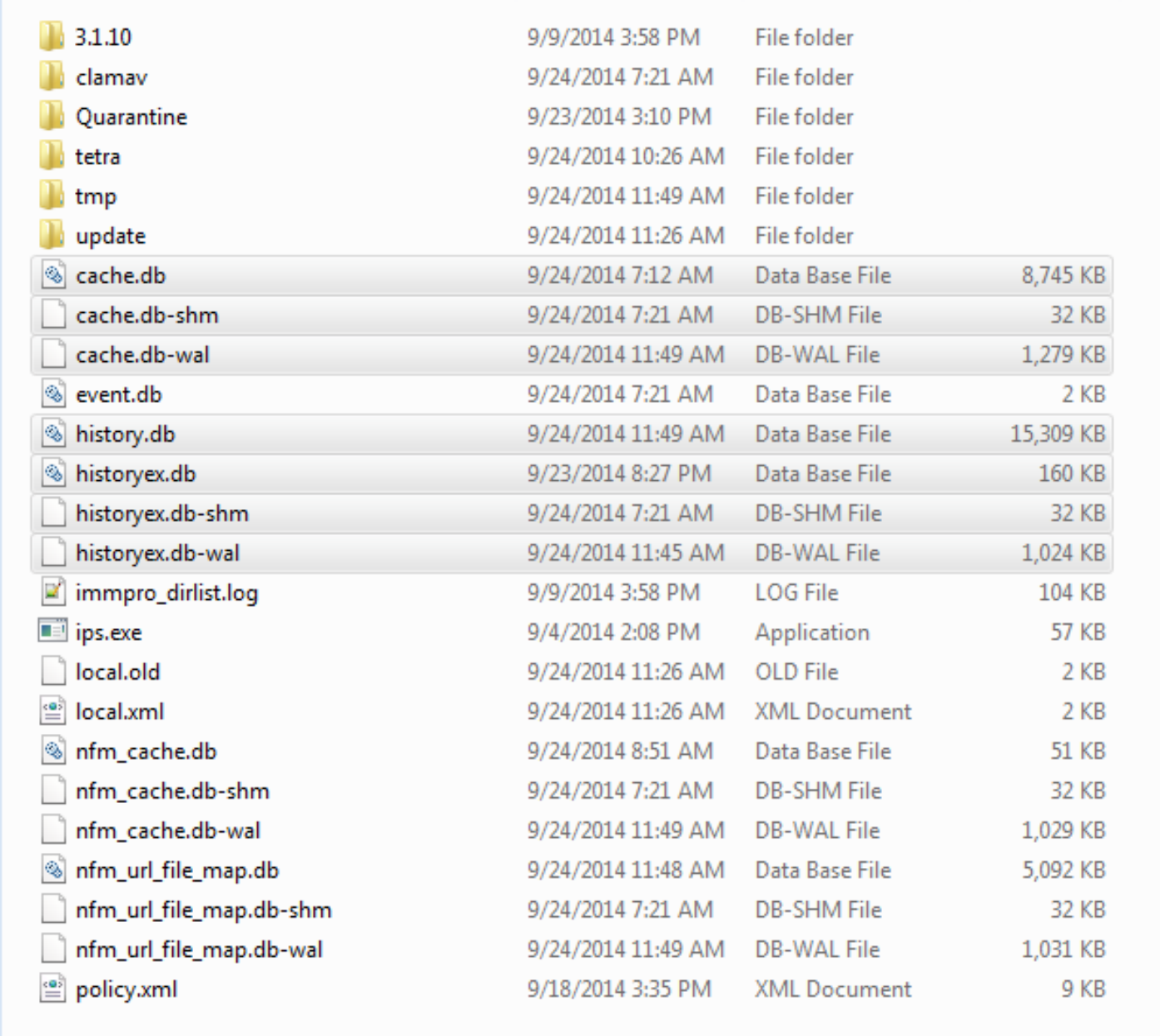
O nome dos arquivos da base de dados do esconderijo é:

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

O nome dos arquivos da base de dados da história é:

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

Este tiro de tela mostra os arquivos no explorador do arquivo de 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

Procedimento para remover os arquivos da base de dados

Passo 1: Pare o serviço do conector de FireAMP

Você pode parar maneiras do serviço do conector de FireAMP as várias:

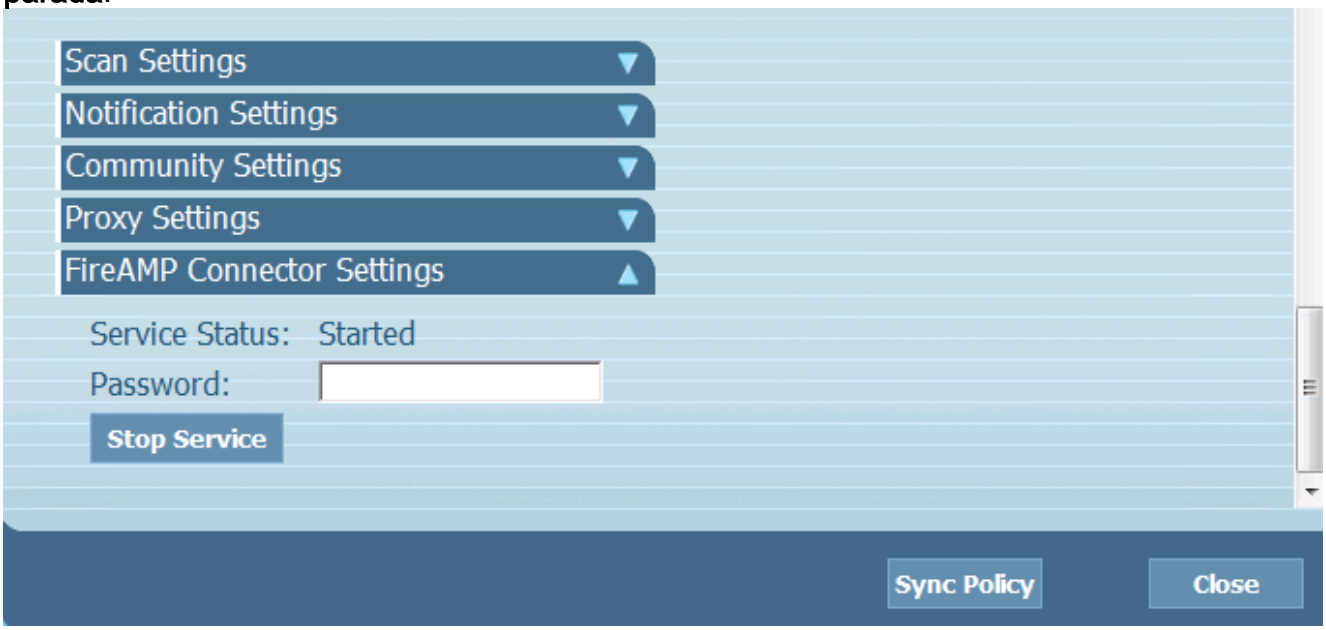
- Interface do utilizador (UI) do serviço do conector de FireAMP
- Console de serviços de Windows
- O comando prompt do administrador

Interface de usuário

> **Note**: Se você tem a proteção do conector permitiu-o deve usar o UI a fim parar o serviço do conector de FireAMP.

1. Abra o UI da bandeja e clique **ajustes**.

2. O rolo à parte inferior e expande **ajustes do conector de FireAMP**.
3. No campo de senha, incorpore a senha da proteção do conector. Clique o **serviço da parada**.

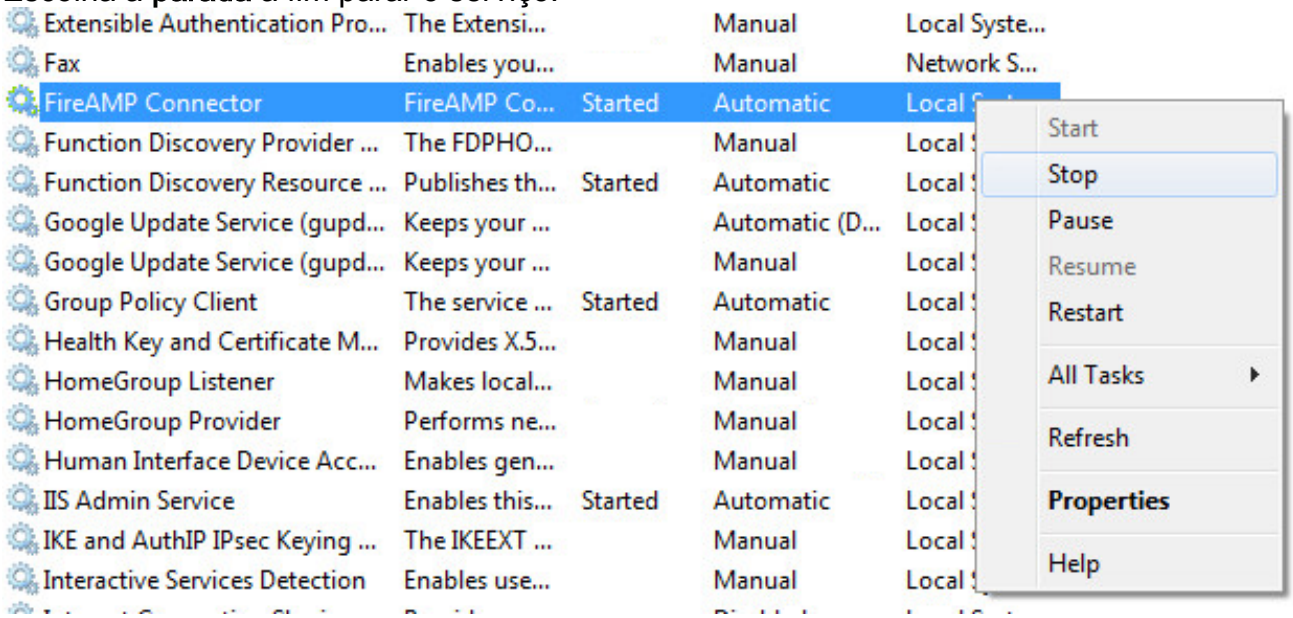


Console de serviços

> **Note**: A fim parar e enfiar serviços no console de serviços você precisa privilégios do administrado.

A fim parar o serviço do conector de FireAMP do console de serviços, termine estas etapas:

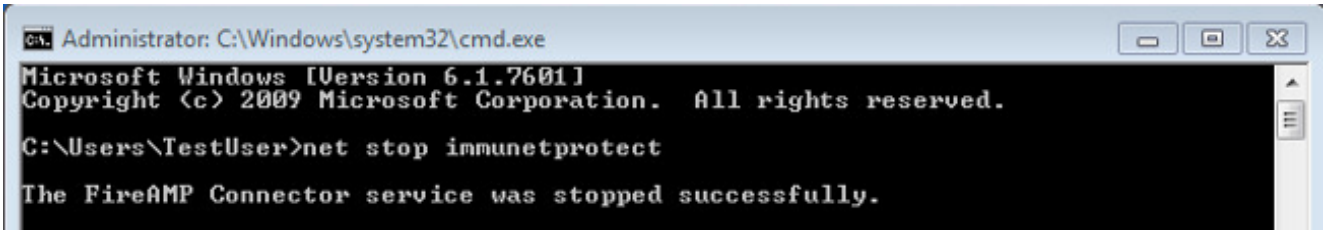
1. Navegue ao **menu de início**.
2. Incorpore **services.msc e** pressione-o entram**.** O console de serviços abre.
3. Selecione o serviço do **conector de FireAMP** e clicar com o botão direito o nome do serviço.
4. Escolha a **parada** a fim parar o serviço.



Comando prompt

A fim parar o serviço do conector de FireAMP do comando prompt de um administrador, termine estas etapas:

1. Navegue ao **menu de início**.
2. Incorpore **cmd.exe e** pressione-o entram**.** A janela imediata do **comando A** abre.
3. Incorpore o comando **líquido do immunetprotect da parada**. Se você tem a versão 5.0.1 ou mais recente, incorpore o **serviço wmic onde o "nome como "immunetprotect%"" startservice do atendimento** comanda pelo contrário. Este tiro de tela mostra um exemplo do serviço parado com
   sucesso:



Passo 2: Suprima dos arquivos da base de dados exigidos

Põe em esconderijo arquivos da base de dados

Uma vez que o serviço é parado você pode suprimir destes três arquivos de cache:

> **aviso:** Se você não suprime de todos os arquivos da base de dados relacionados do esconderijo pode criar pôr em esconderijo edições com o base de dados recreado. Como tal, o serviço pôde não começa ou você pôde experimentar o desempenho degradado do serviço.

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

Arquivos da base de dados da história

Uma vez que o serviço é parado, remova estes arquivos da base de dados da história:

> **aviso:** Se você não suprime de todos os arquivos da base de dados relacionados da história pode criar pôr em esconderijo edições com o base de dados recreado. Como tal, o serviço pôde não começa ou você pôde experimentar o desempenho degradado do serviço.

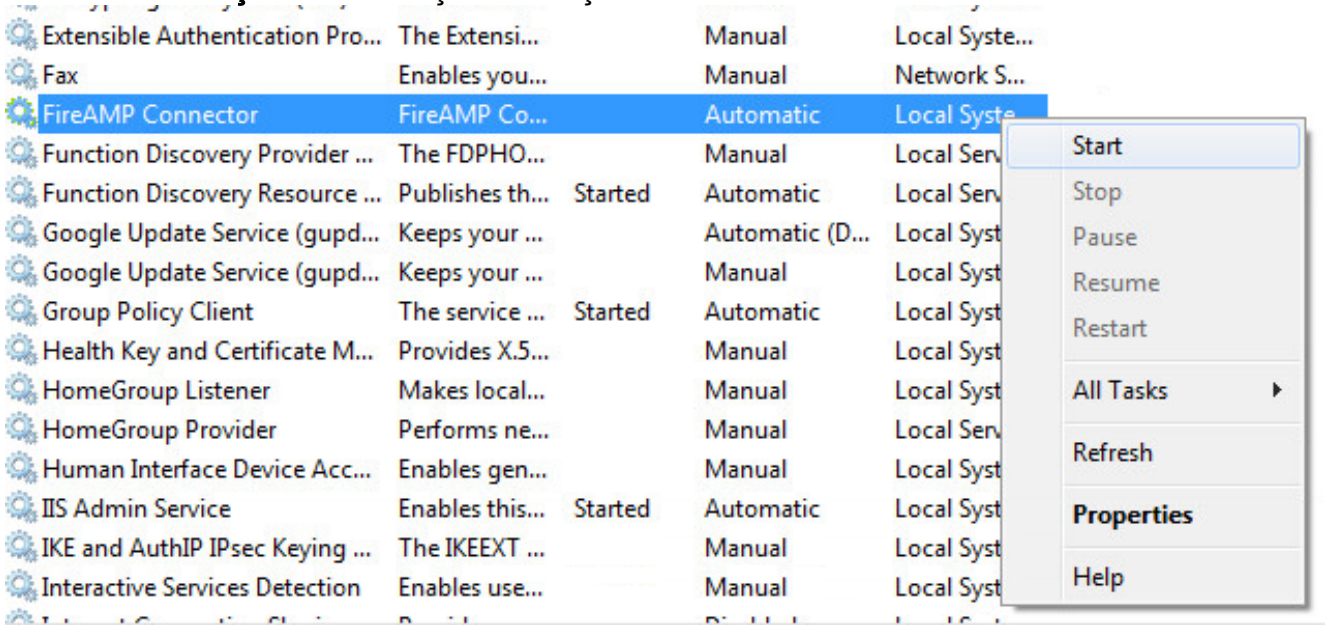
```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

Passo 3: Comece o serviço do conector de FireAMP

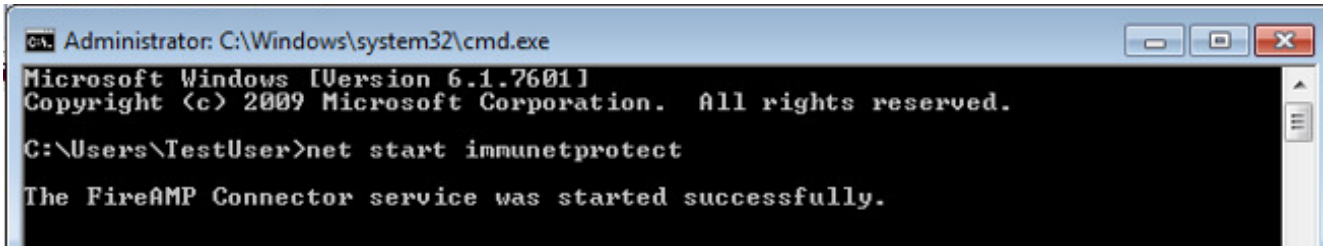
A fim começar o serviço do conector de FireAMP, termine estas etapas:

1. Navegue ao **menu de início**.

2. Incorpore **services.msc e** pressione-o entram. O console de serviços abre.
3. Escolha o serviço do **conector de FireAMP** e clicar com o botão direito o nome do serviço.
4. Escolha o **começo** a fim começar o serviço.



Alternativamente, no comando prompt do administrador você pode incorporar o comando **líquido do immunetprotect do começo**. Se você tem a versão 5.0.1 ou mais recente, incorpore o **serviço wmic onde o "nome como "immunetprotect%"" startservice do atendimento** comanda pelo contrário.Este tiro de tela mostra um exemplo do serviço começado com
sucesso:



Depois que você reinicia os serviços um grupo novo de arquivos da base de dados está criado. Isto deve agora fornecê-lo um exemplo fresco do conector de FireAMP com lista brancas atuais, lista do bloco, exclusões, e assim por diante.