Retiro del caché y de los archivos del historial de FireAMP en Windows

Contenido

Introducción

Este documento proporciona algunos escenarios que requieran un retiro de los archivos de base de datos en FireAMP para los puntos finales y describe un procedimiento adecuado para quitarlos cuando sea necesario. El FireAMP para los puntos finales mantiene un expediente de sus detecciones y disposiciones del archivo reciente en los archivos de base de datos. En ciertos casos, un ingeniero de soporte de Cisco pudo pedir que usted quite algunos de los archivos de base de datos para resolver problemas un problema.

> Advertencia: Usted puede quitar un archivo de base de datos solamente si es dado instrucciones por el Soporte técnico de Cisco.

Archivos de base de datos para el caché y el historial

Propósito

Los archivos de base de datos del caché mantienen las disposiciones sabidas para los archivos. Los archivos de base de datos de historial siguen todas las detecciones del archivo de FireAMP, junto con los nombres del archivo de origen y los valores SHA256.

Cuando usted agrega una lista del bloque a una directiva y pone al día el conector, el comportamiento para un archivo dado no cambia inmediatamente. Esto es porque el caché ha identificado ya que el archivo no es malévolo. Como tal, no será cambiada ni será reemplazada por su lista del bloque. La disposición cambia cuando el caché se expira por el tiempo en su

directiva y se realizan las nuevas operaciones de búsqueda - primero contra sus listas y posteriormente contra la nube.

Razones del retiro

Si los archivos de base de datos de la base de datos y del caché del historial se quitan de un directorio, están frescos reconstruido cuando el servicio de FireAMP recomienza. En seguro lo encajona pudo ser necesario quitar estos archivos del directorio de FireAMP. Por ejemplo, si usted quiere probar una detección de encargo simple o una lista del bloque de la aplicación para un archivo dado.

Es posible que una base de datos podría llegar a ser corrupta, que le hace incapaz de abrir o de ver las detecciones en una base de datos. Alternativamente, si la base de datos es corrupta en un sistema puede causar los errores dentro del servicio del conector de FireAMP tal como la incapacidad para comenzar el conector o la degradación del funcionamiento general del sistema. En estos casos usted puede ser que quiera borrar los archivos del historial del conector de modo que usted pueda evitar los asuntos relacionados con el rendimiento de la corrupción y poder capturar los nuevos registros para la diagnosis.

Identifique los archivos de base de datos

En Microsoft Windows, estos archivos se establecen típicamente en C:\Program Files\Sourcefire\fireAMP o C:\Program Files\Cisco\AMP.

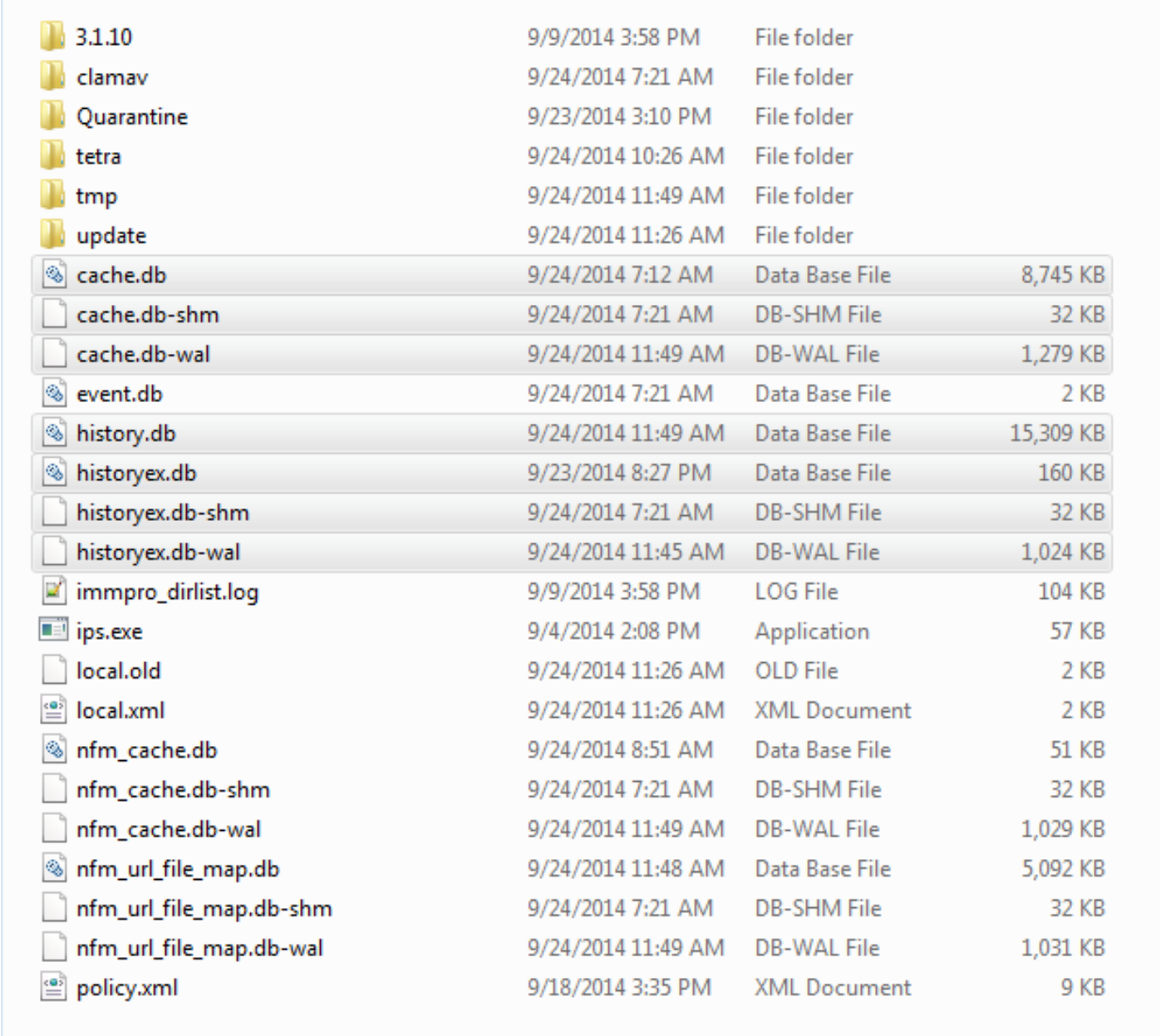
El nombre de los archivos de base de datos del caché es:

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

El nombre de los archivos de base de datos del historial es:

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

Este tiro de pantalla muestra los archivos en el explorador del archivo 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

Procedimiento para quitar los archivos de base de datos

Paso 1: Pare el servicio del conector de FireAMP

Usted puede parar las distintas maneras del servicio del conector de FireAMP:

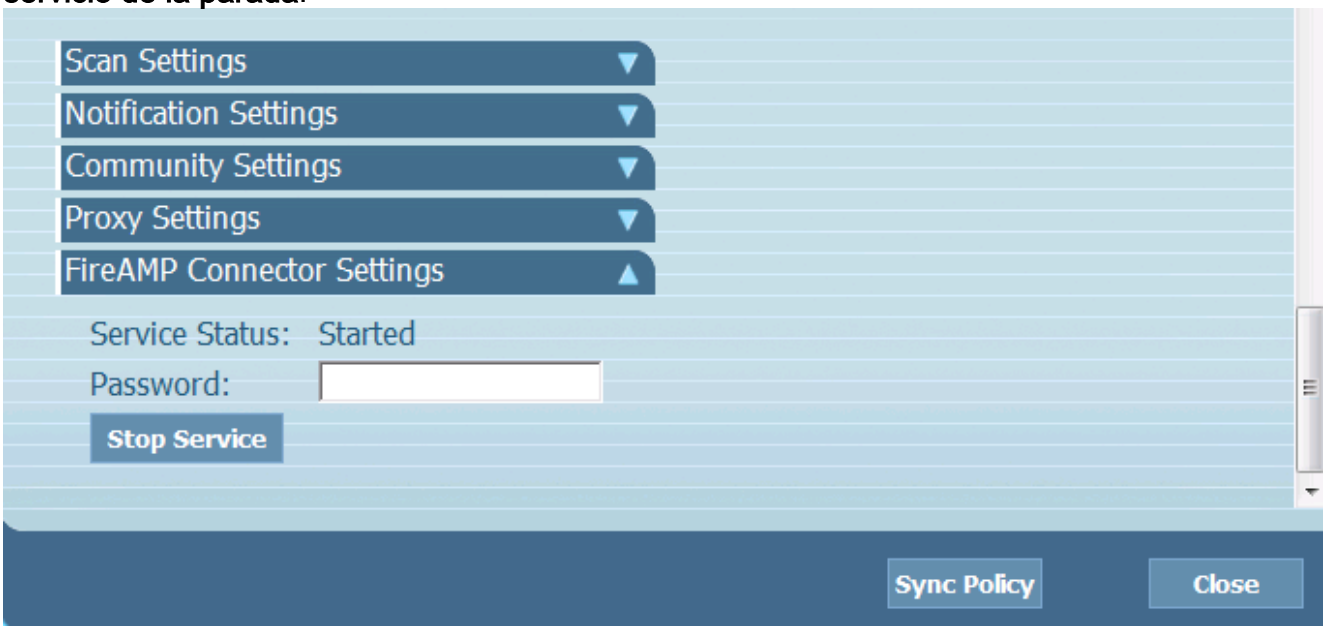
- Interfaz de usuario (UI) del servicio del conector de FireAMP
- Consola de servicio de Windows
- El comando prompt del administrador

Interfaz del usuario

> **Note**: Si usted tiene la protección del conector le habilitó debe utilizar el UI para parar el servicio del conector de FireAMP.

1. Abra el UI de la bandeja y haga clic las **configuraciones**.

2. Navegue a la parte inferior y amplíe las **configuraciones del conector de FireAMP**.
3. En el campo de contraseña, ingrese la contraseña de la protección del conector. Haga clic el **servicio de la parada**.

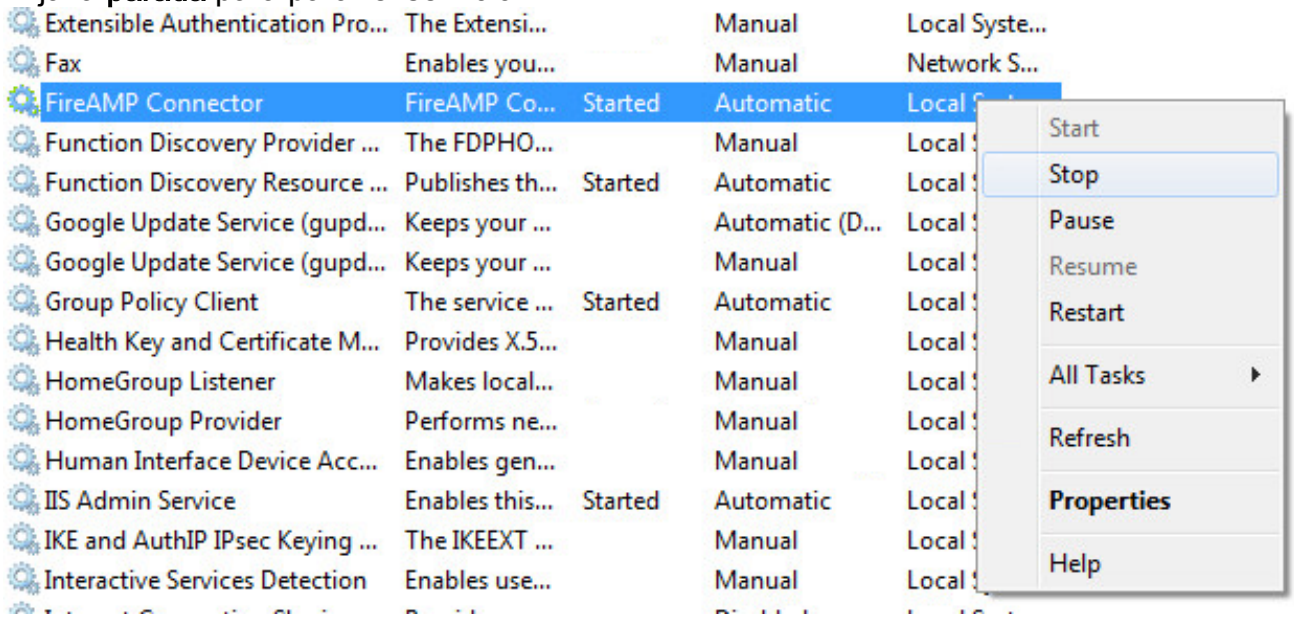


Consola de servicio

> **Note**: Para parar y comenzar los servicios en la consola de servicio usted necesita los privilegios de administrador.

Para parar el conector de FireAMP mantenga de la consola de servicio, completan estos pasos:

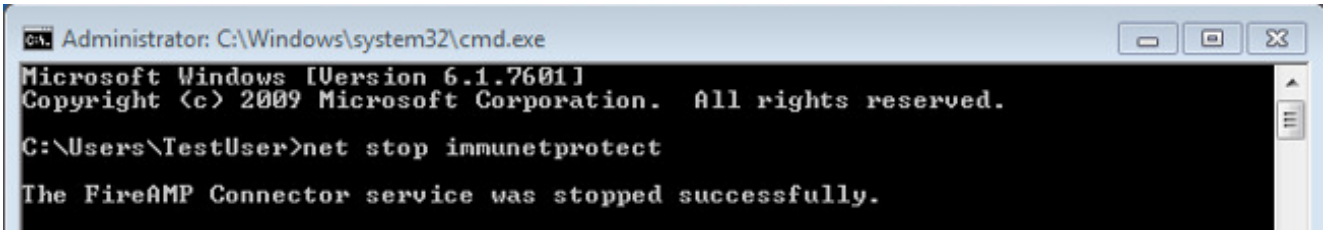
1. Navegue al **menú Inicio**.
2. Ingrese **services.msc y el** Presione ENTER**.** La consola de servicio se abre.
3. Seleccione el servicio del **conector de FireAMP** y haga clic con el botón derecho del ratón el nombre del servicio.
4. Elija la **parada** para parar el servicio.



Comando prompt

Para parar el conector de FireAMP mantenga del comando prompt de un administrador, completan estos pasos:

1. Navegue al **menú Inicio**.
2. Ingrese **cmd.exe y el** Presione ENTER**.** La ventana del prompt del **comando A** se abre.
3. Ingrese el comando **neto del immunetprotect de la parada**. Si usted tiene versión 5.0.1 o posterior, ingrese el **servicio wmic donde el "nombre como "el immunetprotect%"" startservice de la llamada** ordena en lugar de otro. Este tiro de pantalla muestra un ejemplo del servicio parado con éxito:



Paso 2: Borre los archivos de base de datos requeridos

Oculte los archivos de base de datos

Una vez que se para el servicio usted puede borrar estos archivos de tres cachés:

> Advertencia: Si usted no borra todos los archivos de base de datos relacionados del caché puede crear el almacenamiento en memoria inmediata de los problemas con la base de datos reconstruida. Como tal, el servicio pudo no poder comenzar o usted puede ser que experimente el rendimiento disminuido del servicio.

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

Archivos de base de datos del historial

Una vez que se para el servicio, quite estos archivos de base de datos del historial:

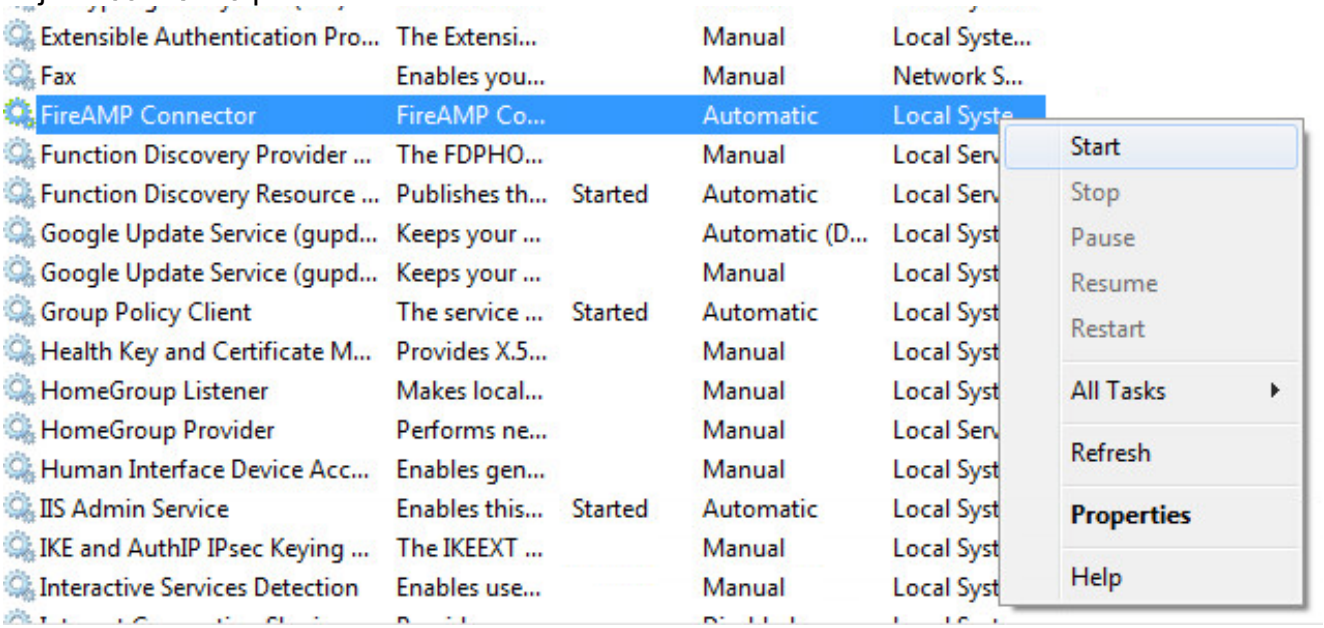
> Advertencia: Si usted no borra todos los archivos de base de datos relacionados del historial puede crear el almacenamiento en memoria inmediata de los problemas con la base de datos reconstruida. Como tal, el servicio pudo no poder comenzar o usted puede ser que experimente el rendimiento disminuido del servicio.

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

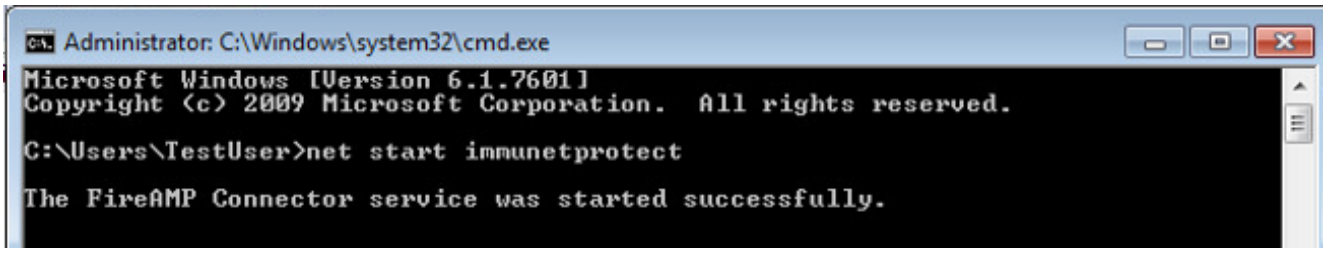
Paso 3: Comience el servicio del conector de FireAMP

Para comenzar el servicio del conector de FireAMP, complete estos pasos:

1. Navegue al **menú Inicio**.
2. Ingrese **services.msc y el** Presione ENTER**.** La consola de servicio se abre.
3. Elija el servicio del **conector de FireAMP** y haga clic con el botón derecho del ratón el nombre del servicio.
4. Elija el **comienzo** para comenzar el servicio.



Alternativamente, en el comando prompt del administrador usted puede ingresar el comando **neto del immunetprotect del comienzo**. Si usted tiene versión 5.0.1 o posterior, ingrese el **servicio wmic donde el "nombre como "el immunetprotect%"" startservice de la llamada** ordena en lugar de otro.Este tiro de pantalla muestra un ejemplo del servicio comenzado con éxito:



Después de que usted recomience los servicios un nuevo conjunto de los archivos de base de datos se crea. Esto debe ahora proveer de usted un caso fresco del conector de FireAMP con las listas blancas actuales, las listas del bloque, las exclusiones, y así sucesivamente.