Guía de FireAMP a las exclusiones en Windows

Contenido

Introducción

Este documento proporciona una guía de consulta en cómo encontrar detectó los archivos y describe un proceso para excluirlos. Cuando usted ejecuta Cisco AMP para los puntos finales (también conocidos como FireAMP) en un ordenador, usted puede ser que experimente el problema de rendimiento en una aplicación o en el ordenador sí mismo. Esto pudo ocurrir debido a las operaciones, a la paginación, o a meter en diario de lectura/grabación excesiva. Esto puede causar los problemas con las aplicaciones que requieren los asideros de archivo exclusivos, tales como programa para de aplicación de base de datos o de la información.

> **Caution**: La exclusión reduce su área de cobertura. Cuando usted excluye una carpeta o un archivo, FireAMP no analiza dentro de esa carpeta. Para evitar la exclusión de los archivos excesivos, usted debe ser específico siempre que sea posible.

Cómo encontrar los archivos detectados

Cuando usted quiere excluir los archivos, usted puede tomar un acercamiento amplio o escribir una exclusión muy específica con un comodín para cubrir apenas un archivo afectado. Este documento comienza con una identificación básica de los directorios de Microsoft Windows.

Archivos de C:\Program

La mayor parte de las aplicaciones están instaladas en este directorio. Esta carpeta es a menudo la fuente para la actividad de archivo en el sistema y es el foco primario. Cisco estará en el puesto de observación para las aplicaciones de base de datos y el otro software del programa de antivirus así como propietario o interno.

Datos de C:\Program

Este directorio se utiliza a veces para ocultar o para salvar los archivos temporales. En esta carpeta, usted puede ser que note muchas actividades que son dependientes en las aplicaciones.

C:\Users

Este directorio acomoda las diversas carpetas de usuario, tales como escritorio, documentos, descargas, y appdata. La carpeta del appdata se utiliza universal para los archivos temporales, los archivos de la ojeada de Internet, historial, y así sucesivamente.

> **Caution**: Debido al número de archivos y de datos que se descarguen en este directorio, usted debe tener cuidado cuando usted especifica una exclusión, e intenta ser tan específico como sea posible hacer juego los archivos “seguros”.

C:\Windows

Este directorio tiene los archivos del sistema. Usted no necesita generalmente excluir mucho de este directorio mientras que es manejado por el conjunto predeterminado de la exclusión. Usted puede ser que quiera excluir esta carpeta para ocultar, tal como almacenamiento en memoria inmediata para los archivos del registro del administrador de configuración (SCCM) y de Windows de System Center.

Tipos soportados de la exclusión

Amenaza: Éste es el nombre de una amenaza que no quarantined. Ningún archivo que accione un nombre determinado de la amenaza no quarantined. Un ejemplo es `Win.Malware.PDF`

Ruta: Esto es una ubicación del sistema del archivo único. Aquí usted puede utilizar una trayectoria específica tal como `C:\Program Files\Cisco`, o usted puede utilizar la lista especial constante de elemento ID (CSIDL).

> **Note**: Un CSIDL es una variable incorporada que es reconocida por el Windows y puede ser útil en los escenarios donde una trayectoria podría residir en diversas letras de la unidad. Un ejemplo es `CSIDL_PROGRAM_FILES \ Cisco`. Este ejemplo cubre `C:\Program Files\Cisco` y `D:\Program Files\Cisco`. Trabajo de CSIDLs solamente en las exclusiones de la trayectoria. Refiera a la documentación de Windows para una lista completa de CSIDLs disponible.

Comodín: Este tipo debe ser utilizado siempre que deseen a un comodín (*) dentro de la exclusión. Por ejemplo: `C:\Program Files\Cisco\ *.tmp`

Extensión de archivo: Esto es una exclusión simple para una extensión de archivo del tipo de archivo. Un ejemplo es `.txt`.

Cuándo excluir

Síntoma

Si usted ejecuta FireAMP y experimenta los problemas de rendimiento con el sistema o con una aplicación específica, ésta podría ser una indicación de la falta de respuesta a la entrada de usuario, del rendimiento lento de un proceso automatizado, de las caídas, o de los errores. La aplicación visualiza a veces un error específico.

Verificación

Para determinar los archivos o los directorios se exploran que y cómo con frecuencia, siga los siguientes pasos:

Paso 1: El primer paso es generar el paquete de diagnóstico y extraerlo. Esto es un archivo 7zip y requiere una aplicación extraerla.

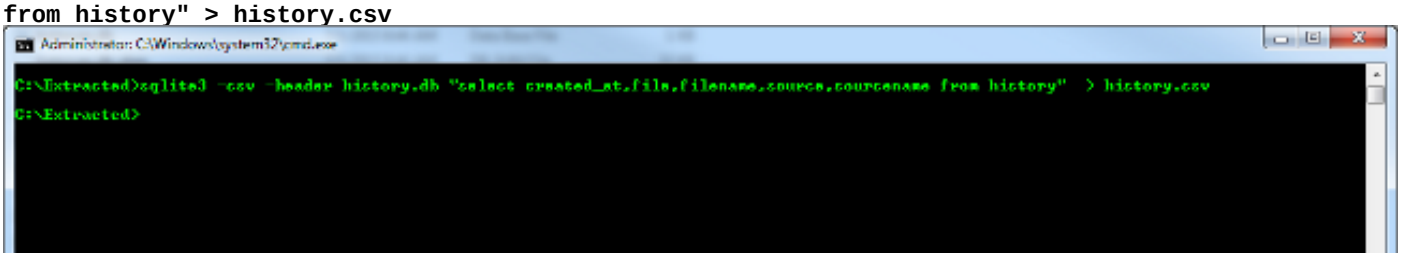
Paso 2: El segundo paso es acceder el `archivo history.db del` archivo de diagnóstico.

`El archivo history.db` es un archivo de base de datos de SQLite que no pierde de vista todo el FireAMP detectó los archivos. Cada fila incluye la disposición, el nombre del archivo, el archivo SHA, el archivo de origen, y la fuente SHA. La fuente es el archivo que creó/accedió el archivo sí mismo. Esto nos deja ver cómo la aplicación se comportó y lo que lo hizo.

En este ejemplo, el comando SQLite3 se utiliza para convertir la base de datos del historial en un archivo del Comma Separated Value (CSV).

- Descargue el binario precompilado SQLite3 para su sistema operativo.
- Extraiga el paquete de diagnóstico de FireAMP con una aplicación tal como 7zip.
- Navegue a la carpeta de diagnóstico extraída y encuentre el `archivo history.db` dentro del C_ `\ de los archivos de programa \ Sourcefire \ fireAMP \ directorio`.
- Dentro de una terminal o de un comando prompt, llame el binario SQLite3 que usted descargó y proporcione el `archivo history.db` con este comando. (Este comando lo asume que SQLite3 está en una ubicación especificada en sus variables de entorno para su sistema operativo, o necesita ser colocado dentro de la carpeta de diagnóstico.)

```
sqlite3 -csv -header history.db "select created_at,file,filename,source,sourcename
from history" > history.csv
```



Usted no verá la confirmación o la hará salir si el comando es acertado.

Si el comando falló, esté seguro que usted ha especificado la ubicación del binario SQLite3. Si usted ve cualesquiera otros mensajes con respecto al `history.db clasifiar`, usted puede ser que necesite borrar los cuatro archivos del historial del equipo del host afectado mientras que se para el servicio, que permite que genere un conjunto fresco de los archivos la próxima vez que el servicio se comienza.

Paso 3: Una vez archivo CSV se ha generado le puede abrirlo con su aplicación de hoja de cálculo preferida. Las aplicaciones tales como Microsoft Excel pudieron permitir que usted convierta archivo CSV a una tabla, que no le prohibe filtrar/clase. Revise la documentación de Microsoft para que cómo utilice Excel.

Las columnas primarias a utilizar son:

- **nombre de fichero**: Este campo muestra que el archivo es analizado por FireAMP.
- **sourcename**: Este campo muestra el proceso o ejecutable que asido la manija (read/write y así sucesivamente). Estos datos se utilizan para determinar si los archivos son manejados por una aplicación confiada en o de otra manera.
- **created_at**: Éste es el grupo fecha/hora en el evento para la detección del archivo.

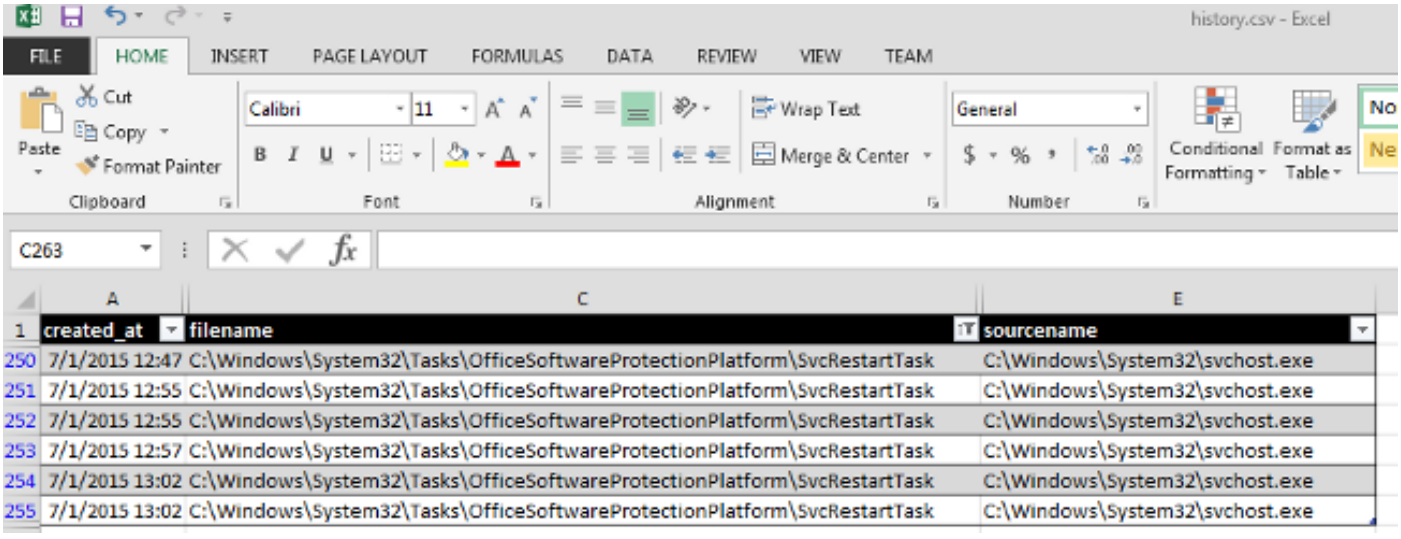
Troubleshooting

En este momento hay un par de opciones:

- Si usted acaba de experimentar el problema de rendimiento, usted puede clasificar la tabla por el **created_at** que es el grupo fecha/hora analizado y ver los eventos más recientes. Usted puede hojear las detecciones y el trabajo al revés para ver qué sucedió.
- Usted puede también buscar u hojear para las aplicaciones que se pudieron haber afectado recientemente por FireAMP.

Qué usted quiere buscar es algo como el mismo archivo que se analiza en varias ocasiones que pudo tener diversos valores SHA. Usted también quiere mirar el tipo de archivo para ver si ésta es conducta esperada.

En este ejemplo, el archivo se ha buscado para la “oficina”. Los resultados muestran a archivos que FireAMP analizó que tenido la palabra “oficina” en el nombre del archivo o la trayectoria. Usted puede también ver el proceso de la fuente que manejó el archivo correspondiente.



En este ejemplo, FireAMP analiza un archivo relacionado con Microsoft Office un servicio. Si

usted quiere excluir esto, usted podría crear una exclusión simple de la trayectoria tal como la que está mostrada aquí:

```
C:\Windows\System32\Tasks\OfficeSoftwareProtectionPlatform\SvcRestartTask
```

A veces, las exclusiones no son tan directas. Usted ve de vez en cuando la actividad como esto en otras áreas por ejemplo,

```
C:\Users\Username\Appdata\
```

Por ejemplo, diga allí es una aplicación de prueba esa los cachés al directorio del appdata con un nombre del archivo específico. Usted puede excluir algo con el nombre determinado.

```
C:\Users\Test\Appdata\Temp\cookies
C:\Users\Test\Appdata\Temp\cache
C:\Users\Test\Appdata\Temp\Test\testcachefile20150116.tmp
```

Este ejemplo excluye los archivos del caché para la aplicación de los temporeros. Sin embargo, usted no quiere excluir la carpeta temporal mientras que el caché de Internet clasifía como las descargas/las imágenes podrían residir en este directorio. Usted puede también estrechar abajo el directorio a la carpeta de la prueba, no obstante la aplicación pudo conectar con Internet también, o tiene otros archivos del caché que no dañen el funcionamiento ni podrían potencialmente estar abiertos arriesgar. Una placa comodín se utiliza para excluir esto.

```
C:\Users\Test\Appdata\Temp\Test\testcachefile*.tmp
```

Como usted ve, utilizaron a un comodín (*) para explicar cualquier cosa entre las cartas y el punto en el nombre del archivo. Este comodín excluye cualquier archivo que haga juego esta expresión. Éste es un ejemplo de cómo usted puede estrechar abajo las exclusiones para prevenir demasiado riesgo.

Usted puede también utilizar las placas comodín para los nombres de ruta completa. Aquí está un ejemplo similar;

```
C:\Users\Test\Appdata\Temp\Test\20150116\cache\testfilecache083022.tmp
C:\Users\Test\Appdata\Temp\Test\20150117\cache\testfilecache092533.tmp
C:\Users\Test\Appdata\Temp\Test\20150118\cache\testfilecache104431.tmp
```

Exclusiones del comodín - Las exclusiones se pueden hacer en una expresión del comodín donde la trayectoria y el nombre de fichero pueden ser expresados. Es decir, si el nombre de fichero es constante, después él es el mejor “obligan” al comodín a una trayectoria específica. Tan si AIM.exe existe siempre en C:\Program clasifía (x86)*\AIM.EXE miraría en cualquier sub-directório.

Después de que usted encuentre sus exclusiones deseadas de FireAMP, usted puede seguir los pasos enumerados en este artículo para implementarlos en su panel y realizar la prueba.

Versión 5.0+

En la versión 5.0+, las actividades de archivo se registran no más en `history.db`. Una nueva estructura para los archivos analizados y las trayectorias están situadas en historyex.db. Un script del `pitón`, no soportado por el Centro de Asistencia Técnica de Cisco (TAC), está disponible en la comunidad de CiscoSupport. En un entorno de Linux, el script puede convertir el

historyex.dbto un archivo del `Comma Separated Value` (CSV). Permite que usted revise las actividades para las exclusiones.

Documentos Relacionados

- Configure y maneje las exclusiones en FireAMP
- Repaso de las exploraciones de archivo en v5.0+
- Soporte Técnico y Documentación - Cisco Systems