AMP para la guía del ajuste del rendimiento del conector del mac de los puntos finales

Contenido

Introducción

Editado por: Alex Yakimenko, ingeniero de software

¿Por qué necesitamos ajustar?

Un archivo se crea cada vez, movido, copiado, o ejecutado en un punto final del mac un evento para ese archivo se envía del sistema operativo al conector del mac AMP. El evento da lugar a ese archivo que es analizado por el conector. El proceso del análisis implica generalmente el desmenuzar del archivo en la pregunta y el funcionamiento él a través de diversos motores del análisis en el ordenador y en la nube. Es importante reconocer que este acto del picado consume los ciclos de la CPU.

Más operaciones del archivo y ejecutan que ocurren en un punto final dado, más ciclos de la CPU y los recursos entrada-salida el conector requerirá para desmenuzar. Hay varias características que se han agregado al conector para reducir los gastos indirectos. Por ejemplo, si un archivo que era creado, movido, o copiado se ha analizado previamente, el conector utilizará un resultado ocultado. Sin embargo, en el caso de algunos eventos por ejemplo ejecuta donde está suprema la Seguridad, todos los eventos siempre son analizados completamente por el conector. Esto significa que las aplicaciones o los procesos que propagan las ejecuciones repetidores múltiples de los procesos hijo - especialmente durante un período corto - pueden causar los problemas de rendimiento. Encontrando y excluyendo las aplicaciones que repetidor ejecutan los procesos hijo a una tarifa mayor que una vez por segundo pueda reducir perceptiblemente su tiempo de vida de la batería del USO de la CPU y del aumento en las laptopes.

Las operaciones del archivo por ejemplo crean y los movimientos tienen generalmente menos impacto que ejecutan, pero el archivo excesivo escribe y la creación del archivo temporal puede dar lugar a los problemas similares. Una aplicación que escribe a un archivo del registro con frecuencia, o una que genera los archivos temporales múltiples puede hacer el AMP consumir muchos ciclos de la CPU con el análisis innecesario y puede crear mucho ruido para la parte AMP. La distinción de las aplicaciones legítimas de las partes de ruidosas es un paso muy importante en mantener un punto final productivo y seguro.

El propósito de este documento es ayudar a distinguir las operaciones del archivo (cree, muévase, y copia) y ejecuta que tendrán un efecto negativo en los ciclos de la CPU del funcionamiento y de la basura de la daemon. La identificación esta archivo y los trayectos del

directorio permitirá que usted cree y mantener la exclusión apropiada fija para su organización.

Usted puede agregar las listas PRE-creadas de la exclusión a sus directivas que sean sean mantenidas por Cisco para proporcionar una mejor compatibilidad entre el AMP para el conector de los puntos finales y antivirus, Seguridad, o otro software. Estas listas están disponibles en la página de las exclusiones en la consola como exclusiones Cisco-mantenidas.

Tipos de ajustar

Hay tres clases de exclusión que ajustan las opciones disponibles:

1. **Instale previamente ajustar – esto se puede hacer antes de instalar el conector del mac AMP. Le dará la mirada más limpia en la cual la aplicación y las trayectorias están las más ocupadas en su máquina. Sin embargo, es un proceso muy ruidoso y requiere al usuario hacer un bit justo del análisis y de la agregación en sus los propio.**
2. Support tool (Herramienta de soporte) **ajustando** – esto puede ser hecha después de que el conector del mac esté instalado y se pueda realizar en cualquier punto final sin el binaries adicional. Realiza una mirada limitada detrás y es grande para identificar las aplicaciones molestas.
3. **El ajustar de Procmon** – este proceso también requiere el conector ser instalado, pero también requiere el uso del binario de Procmon, nuestra herramienta del ajuste personalizado. Es esencialmente una versión más sofisticada Support tool (Herramienta de soporte) de la característica que ajusta. Este método requiere la cantidad más grande de configuración; sin embargo, proporciona los mejores resultados.

1. Instale previamente ajustar

Instale previamente ajustar es la mayoría del formato básico de ajustar y se hace sobre todo a través de la línea de comando en una sesión terminal.

Para un mac más nuevo de OS x EL Capitan usted necesitará primero iniciar para recuperar el modo (comando r) mientras que inicia y inhabilita la protección para el dtrace:

```
csrutil enable --without dtrace
```

Para examinar que clasifían las ejecuciones sea el más frecuente ejecutan el siguiente:

```
$ sudo newproc.d | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

Esto mostrará generalmente qué aplicaciones se están ejecutando una y otra vez. Muchas aplicaciones del aprovisionamiento funcionarán con los scripts o ejecutarán el binaries en los intervalos cortos para mantener las políticas de software de la compañía. Cualquier ejecución vista aplicaciones a una tarifa mayor de una vez al segundo, o los tiempos múltiples ejecutados en las ráfagas breves, se considera un buen candidato a la exclusión.

Para examinar que clasifían las operaciones sea el más frecuente, funcionan con el siguiente comando:

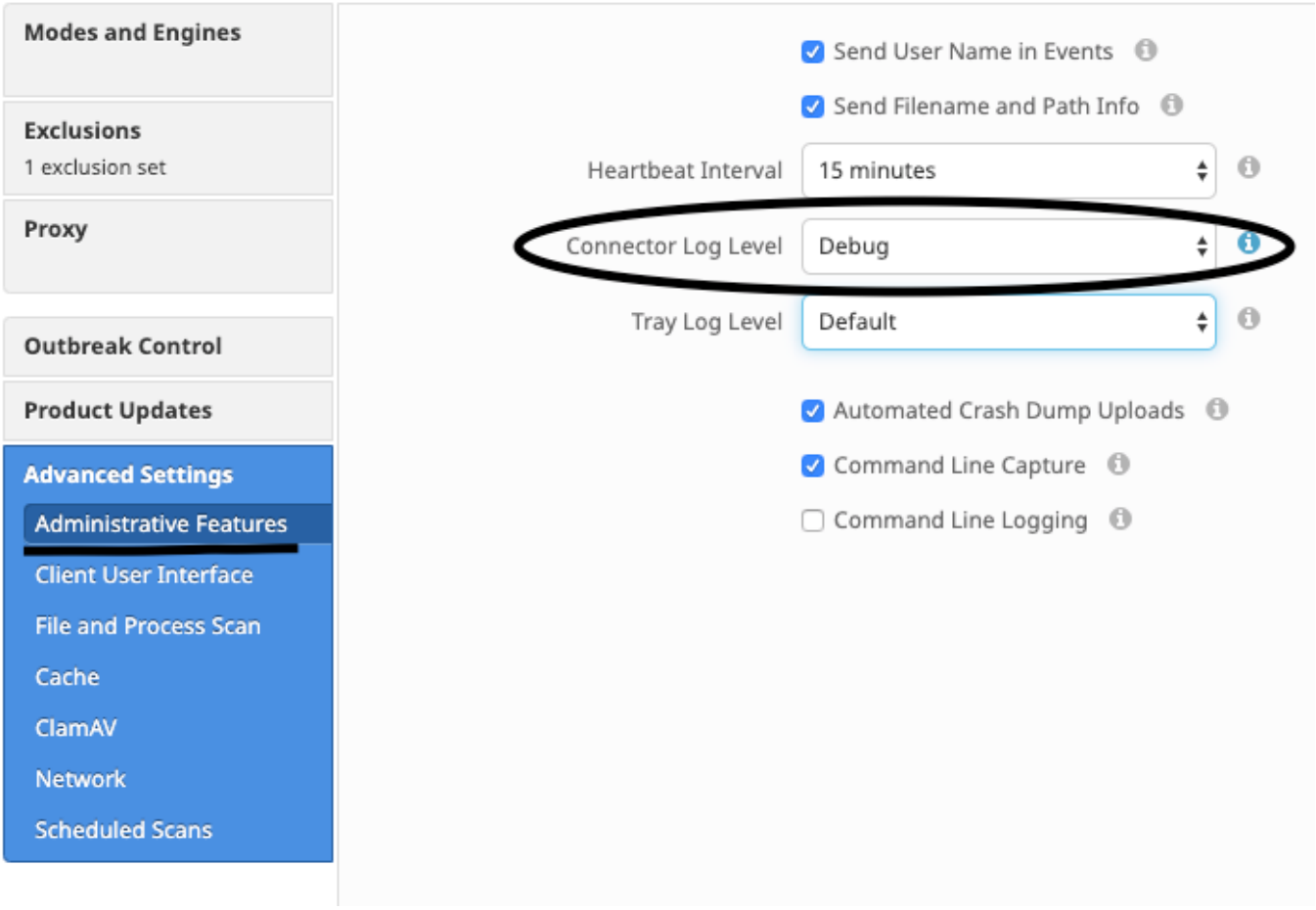
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

Usted verá inmediatamente qué archivos se están escribiendo la mayoría. Éste será a menudo archivos del registro que son escritos a ejecutar las aplicaciones, los archivos de copiado del software de backup, o las aplicaciones de correo electrónico que escriben los archivos temporales. Además de esto, una buena regla práctica es que cualquier cosa con una extensión del registro o de archivo de diario se debe considerar un candidato conveniente de la exclusión.

2. Support tool (Herramienta de soporte) ajustando

Habilitar el registro de debug

La daemon del conector necesita ser puesta en el modo del registro de debug antes de que comience ajustar del archivo del soporte. Esto se hace vía el AMP para la consola de los puntos finales, a través de las configuraciones de la directiva del conector en la *Administración - > las directivas*. Seleccione la directiva, edite la directiva, y vaya a la sección *administrativa de las características* bajo barra lateral *avanzada de las configuraciones*. Cambie la configuración del *nivel del registro del conector* **para hacer el debug de**.



Siguiente, salve su directiva. Una vez que se ha guardado su directiva, asegúrese que se haya sincronizado al conector. Funcione con el conector en este modo por lo menos 15-20 minutos antes de la continuación con el resto de ajustar.

NOTA: Cuando su ajustar es completo, no olvide cambiar la configuración del *nivel del registro del conector* de nuevo al **valor por defecto** de modo que el conector se ejecute en su modo de direccionamiento efectivo más eficiente y.

El ejecutarse Support tool (Herramienta de soporte)

Este método implica usar Support tool (Herramienta de soporte), una aplicación instalada con el conector del mac AMP. Puede ser accedido de la carpeta Applications haciendo doble clic en el >Cisco AMP->Support Tool.app de /Applications-. Esto generará un paquete de soporte completo que contiene los archivos de diagnóstico adicionales.

Una alternativa, y un más rápido, método es funcionar con la línea de siguiente comando de una sesión terminal:

```
sudo/Library/Application Support/Cisco/AMP for Endpoints Connector/SupportTool–x
```

Esto dará lugar a un archivo mucho más pequeño del soporte que contiene solamente los archivos que ajustan relevantes.

Cualquier manera que usted elige ejecutarla, Support tool (Herramienta de soporte) generará a archivo zip en su escritorio que contenga dos archivos del soporte que ajustan: fileops.txt y execs.txt. fileops.txt contiene una lista lo más frecuentemente de los archivos creados y modificados en su máquina. execs.txt contendrá la lista lo más frecuentemente de los archivos ejecutados. Ambas listas son clasificadas por la cuenta de la exploración, significando que lo más frecuentemente las trayectorias analizadas aparecen en la cima de la lista.

Deje el conector que se ejecuta en el modo del debug por un período minucioso 15-20, y después ejecute Support tool (Herramienta de soporte). Una buena regla práctica es que cualesquiera archivos o trayectoria que hagan un promedio de 1000 golpes o más durante ese tiempo son buenos candidatos que se excluirán.

Crear la trayectoria, el comodín, el nombre del archivo, y las exclusiones de la extensión de archivo

Una manera de conseguir comenzada con las reglas de la exclusión de la trayectoria está encontrando lo más frecuentemente las trayectorias analizadas del archivo y de la carpeta de fileops.txt y después de considerar crear las reglas de la exclusión para esas trayectorias. Una vez que se ha descargado la directiva, monitoree el nuevo USO de la CPU. Puede ser que tarde 5 a 10 minutos después de que la directiva es actualizada antes de que usted note el descenso del USO de la CPU como puede ser que tome tiempo para que alcance la daemon. Si usted todavía está viendo los problemas, funcione con la herramienta otra vez para ver qué nuevas trayectorias usted observa.

- Una buena regla práctica es que cualquier cosa con una extensión del registro o de archivo de diario se debe considerar un candidato conveniente de la exclusión.

Crear las exclusiones de proceso

NOTE: Process Exclusions on Mac can only be implemented for Mach-O files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts) or .app (Application Bundles).
Para las mejores prácticas con respecto a las exclusiones de proceso vea: AMP para los puntos finales: Exclusiones de proceso en MaOS y Linux

Un buen modelo que ajusta es primer identificando los procesos con un volumen alto de ejecuta de execs.txt, encuentra la trayectoria al ejecutable, y crea una exclusión para esta trayectoria. Sin embargo, hay algunos procesos que no deben ser incluidos, esto incluye:

- Programas de la utilidad generales - No se recomienda para excluir los programas de la utilidad generales (ex: usr/compartimiento/grep) sin explicar el siguiente. El usuario puede determinar lo que está llamando la aplicación el proceso, (ex: encuentre el proceso principal que está ejecutando el grep) y excluya el proceso principal. Esto se debe hacer si y solamente si, el proceso principal se puede hacer con seguridad en una exclusión de proceso. Si la exclusión del padre se aplica a los niños, después las llamadas a cualquier niño del proceso principal también serán excluidas.El usuario que está ejecutando el proceso puede ser determinado. (ex: si un proceso está siendo llamado en un volumen alto por el usuario “raíz”, una puede excluir el proceso, pero solamente para el usuario específicado 'raíz”, ésta permitirá que el AMP monitoree ejecuta de un proceso dado por cualquier usuario que no sea “raíz”).**NOTA: Las exclusiones de proceso son nuevas en las versiones 1.11.0 del conector y más nuevo. Debido a esto, los programas de la utilidad generales pueden ser se utilicen como exclusión de la trayectoria en las versiones 1.10.2 del conector y más viejo. Sin embargo, esta práctica se recomienda solamente cuando un equilibrio del funcionamiento es absolutamente necesario.**

Encontrar el proceso principal es importante para las exclusiones de proceso. Una vez encuentran el proceso principal y/o al usuario del proceso, el usuario pueden crear la exclusión para un usuario específico y aplicar la exclusión de proceso a los procesos hijo, que a su vez excluirán los procesos ruidosos que no se pueden ellos mismos hacer en las exclusiones de proceso.

Identifique el proceso principal

1. De execs.txt, identifique el proceso en grandes cantidades (ex: /bin/rm).
2. Abra ampdaemon.log del paquete de soporte, desabroche syslog.tar, después siga la trayectoria /Library/Logs/Cisco/ampdaemon.log (solamente disponible en el paquete del afullsupport, no de un paquete de soporte generado con las opciones predeterminadas).
3. Busque ampdaemon.log para que el proceso sea excluido. Encuentre la línea del registro que muestra la ejecución de proceso (ex: 19 de agosto 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]: Rx de la daemon: VNODE: EJECUTE EL [/BIN/RM] X:6210 P:3296 PP:3200 U:502).
4. Identifique el proceso principal usando uno de los métodos siguientes: Identifique la trayectoria de proceso principal que puede seguir la trayectoria del proceso que se excluirá (ex: [Parent Process path] del [/bin/rm]).Si el registro no incluye la trayectoria de proceso principal, identifique el proceso principal ID de los `PP:` sección de la línea del registro (ex: PP:3200).
5. Usando la trayectoria o el proceso principal ID del padre, relance los pasos 3 y 4 para determinar al padre del proceso principal actual. Continúe este proceso hasta que cualquier ningún padre pueda ser determinado, o el proceso principal ID= 1 (ex: PP:1).
6. Una vez que se sabe el árbol de proceso, busque la trayectoria del programa que cubre la mayoría o todas las operaciones que se deban excluir e identifiquen únicamente la aplicación. Esto minimiza la ocasión de involuntariamente excepto las operaciones realizadas por otra aplicación.

Identifique al usuario del proceso

1. Siga los pasos 1-3 de identificar el proceso principal desde arriba.
2. Identifique al usuario de un proceso usando uno el método siguiente: Encuentre la identificación del usuario del proceso dado de `U:` en la línea del registro (ex: U:502).De la ventana de terminal funcionada con el siguiente comando: `dscl. lista /Users UniqueID | grep #`, donde # está la identificación del usuario.Usted debe ver la salida similar a: `Nombre de usuario 502`, donde está el usuario el `nombre de usuario del` proceso dado.
3. Este nombre de usuario se puede agregar a una exclusión de proceso bajo categoría del usuario para reducir el alcance de la exclusión, que con certeza las exclusiones de proceso, son importantes. **NOTA: si el usuario de un proceso es el usuario local de la máquina, y esta exclusión debe aplicarse a las máquinas múltiples con diversos usuarios locales, la categoría del usuario se debe dejar en blanco para permitir que la exclusión de proceso se aplique a todos los usuarios.**