Guía de Ajuste del Rendimiento de Conector Mac de Terminal Seguro

Contenido

Introducción

¿Por qué necesitamos sintonizar?

Cada vez que se crea, mueve, copia o ejecuta un archivo en un terminal Mac, se envía un evento para ese archivo desde el sistema operativo al conector Mac de punto final seguro. El evento hace que el conector analice ese archivo. El proceso de análisis generalmente implica el hash del archivo en cuestión y ejecutarlo a través de diferentes motores de análisis tanto en el equipo como en la nube. Es importante reconocer que este acto de hashing sí consume ciclos de CPU.

Cuantas más operaciones y ejecuciones de archivos se produzcan en un punto final determinado, más ciclos de CPU y recursos de E/S necesitará el conector para el hash. Hay varias funciones que se han agregado al conector para reducir la sobrecarga. Por ejemplo, si se ha analizado previamente un archivo que se está creando, moviendo o copiando, el conector utilizará un resultado almacenado en caché. Sin embargo, en el caso de algunos eventos, como los que se ejecutan en los que la seguridad es primordial, todos los eventos se analizan por completo mediante el conector. Esto significa que las aplicaciones o los procesos que propagan múltiples ejecuciones repetitivas de procesos secundarios -especialmente durante un período breve- pueden causar problemas de rendimiento. Encontrar y excluir aplicaciones que ejecutan repetidamente procesos secundarios a una velocidad mayor que una vez por segundo puede reducir significativamente el uso de la CPU y aumentar la duración de la batería en los portátiles.

Las operaciones de archivos, como la creación y los movimientos, generalmente tienen menos impacto que los ejecutados, pero las escrituras de archivos excesivas y la creación temporal de archivos pueden ocasionar problemas similares. Una aplicación que escribe con frecuencia en un archivo de registro o que genera varios archivos temporales puede hacer que el terminal seguro consuma muchos ciclos de CPU con análisis innecesarios y puede crear mucho ruido para el motor de punto final seguro. Distinguir partes ruidosas de aplicaciones legítimas es un paso muy importante para mantener un terminal productivo y seguro.

El propósito de este documento es ayudar a distinguir las operaciones del archivo (crear, mover y copiar) y ejecuta que tendrán un efecto negativo en el rendimiento del demonio y desperdiciarán los ciclos de CPU. La identificación de estas rutas de acceso de directorio y archivo le permitirá crear y mantener los conjuntos de exclusión adecuados para su organización.

Puede agregar listas de exclusión precreadas a las políticas que mantiene Cisco para

proporcionar una mejor compatibilidad entre el conector de terminal seguro y el antivirus, la seguridad u otro software. Estas listas están disponibles en la página Exclusiones de la consola como Exclusiones Mantenidas por Cisco.

Tipos de ajuste

Hay tres tipos de opciones de ajuste de exclusión disponibles:

1. **Ajuste previo a la instalación: esto se puede hacer antes de instalar el conector Mac de terminal seguro. Le dará la apariencia más limpia de la aplicación y de las rutas más transitadas de su máquina. Sin embargo, es un proceso muy ruidoso y requiere que el usuario haga un buen análisis y agregación por su cuenta.**
2. **Ajuste de herramientas de soporte**: esto se puede hacer después de instalar el conector Mac y se puede realizar en cualquier terminal sin binarios adicionales. Realiza un análisis limitado y es perfecto para identificar aplicaciones problemáticas.
3. **Ajuste Procmon** - Este proceso también requiere que el conector esté instalado, pero también requiere el uso del binario Procmon, nuestra herramienta de ajuste personalizada. Se trata esencialmente de una versión más sofisticada de la función de ajuste de la herramienta de soporte. Este método requiere la mayor cantidad de configuración; sin embargo, proporciona los mejores resultados.

1. Ajuste previo a la instalación

El ajuste previo a la instalación es la forma más básica de ajuste y se realiza principalmente a través de la línea de comandos en una sesión de terminal.

Para el nuevo mac de OS X El Capitan, deberá iniciar primero para recuperar el modo (command-r) mientras inicia y desactiva la protección para dtrace:

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

Para inspeccionar las ejecuciones de archivos más frecuentes, ejecute lo siguiente:

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

Esto generalmente mostrará qué aplicaciones se ejecutan una y otra vez. Muchas aplicaciones de aprovisionamiento ejecutarán secuencias de comandos o binarios en intervalos cortos para mantener las políticas de software de la empresa. Cualquier solicitud que se considere ejecutada a un ritmo superior a una vez por segundo o ejecutada varias veces en ráfagas cortas debe considerarse un buen candidato para la exclusión.

Para inspeccionar qué operaciones de archivo son más frecuentes, ejecute el siguiente comando:

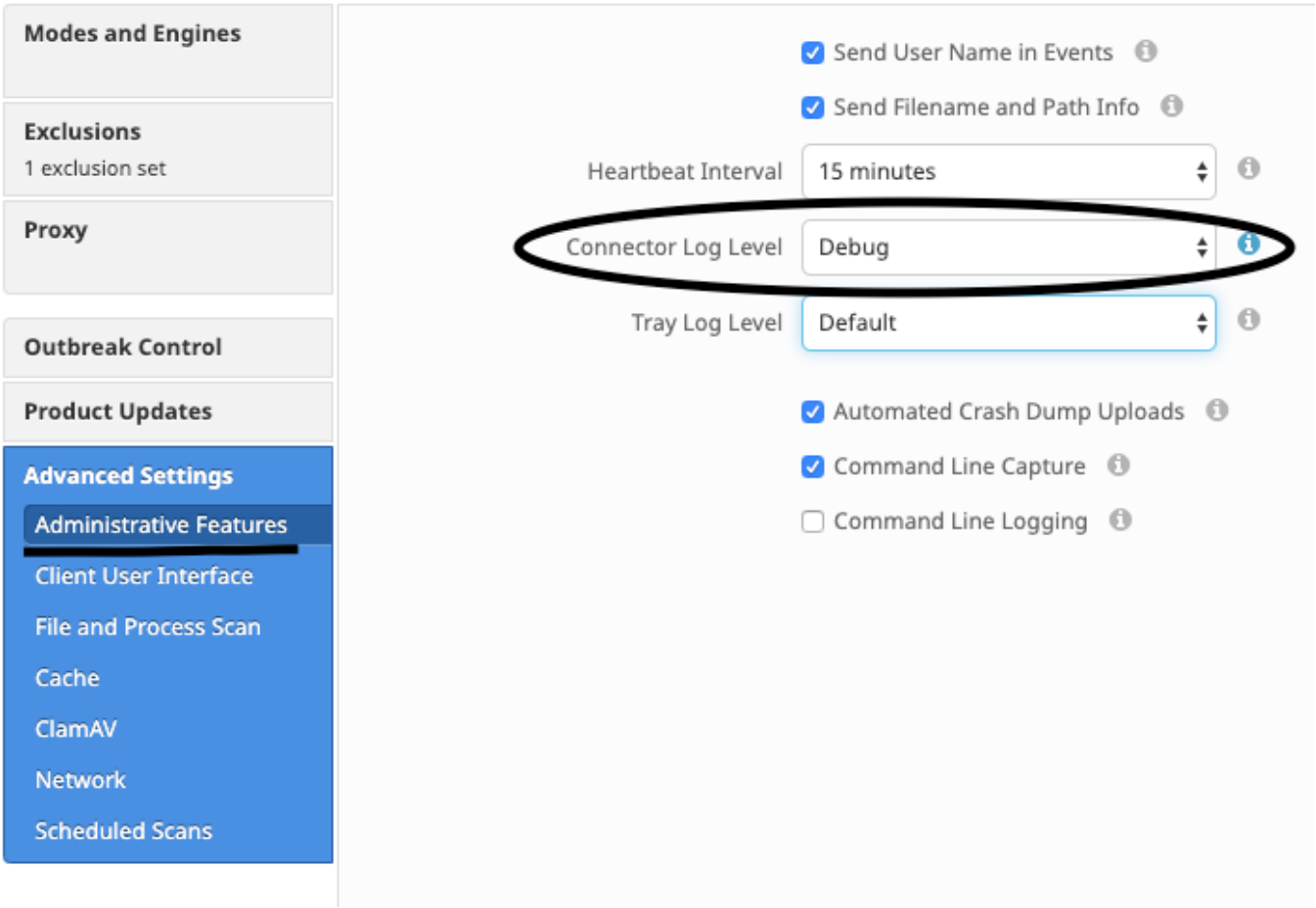
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

Verá inmediatamente qué archivos se están escribiendo a la mayoría. A menudo, se escribirán archivos de registro en los que se ejecutan aplicaciones, se copian archivos de software de copia de seguridad o se escriben aplicaciones de correo electrónico que escriben archivos temporales. Además de esto, una buena regla general es que cualquier cosa con una extensión de archivo de registro o diario debe considerarse un candidato de exclusión adecuado.

2. Herramienta de soporte Ajuste

Habilitación del Registro de Debug

El demonio del conector debe ponerse en modo de registro de depuración antes de comenzar a ajustar el archivo de soporte. Esto se realiza a través de la [consola de terminal seguro], a través de la configuración de políticas del conector en *Management -> Policies*. Seleccione la política, edite la política y vaya a la sección *Funciones administrativas* de la barra lateral *Configuración avanzada*. Cambie la configuración *de nivel de registro del conector* a **Depurar**.



Siguiente, guarde su política. Una vez guardada la política, asegurarse de que se ha sincronizadoronizado a laconector. Ejecute el comando cconector en este modo para al menos 15-20 minutos antes de continuar con el resto de los ajustes.

NOTE: Una vez finalizada la adaptación, no olvidarse de cambiar el *Nivel de registro del conector* configuración **Predeterminado** de modo que la cconector ejecutar in su más eficientes y modo efectivo.

Herramienta de soporte en ejecución

Este método implica el uso de la herramienta Support Tool, una aplicación instalada con el conector Mac de punto final seguro. Se puede acceder a él desde la carpeta Aplicaciones haciendo doble clic en /Applications->Cisco Secure Endpoint->Support Tool.app. Esto generará un paquete de soporte completo que contiene archivos de diagnóstico adicionales.

Un alternativa, y más rápido, el método es ejecutar el línea de comandos siguiente desde a

Terminal sesión:

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

Esto resultará en un archivo de soporte mucho más pequeño que contiene solamente los archivos de ajuste relevantes.

De cualquier manera que elija ejecutarlo, Support Tool generará un archivo zip en su escritorio que contiene dos archivos de soporte de ajuste: fileops.txt y execs.txt. fileops.txt contiene una lista de los archivos creados y modificados con más frecuencia en el equipo. execs.txt contendrá la lista de los archivos ejecutados con mayor frecuencia. Ambas listas se ordenan por recuento de escaneo, lo que significa que las rutas exploradas más frecuentemente aparecen en la parte superior de la lista.

Deje el conector ejecutándose en modo Debug durante un período de 15-20 minutos y, a continuación, ejecute la herramienta de soporte. Una buena regla general es que cualquier archivo o ruta de acceso con un promedio de 1000 visitas o más durante ese tiempo son buenos candidatos para ser excluidos.

Creación de Exclusiones de Ruta, Comodín, Nombre de Archivo y Extensión de Archivo

Una forma de comenzar con las reglas de exclusión de rutas es encontrar las rutas de acceso de archivos y carpetas más exploradas de fileops.txt y, a continuación, considerar la creación de reglas de exclusión para esas rutas. Una vez descargada la política, monitoree el nuevo uso de CPU. Puede tardar entre 5 y 10 minutos después de que se actualice la política antes de que observe la caída del uso de la CPU, ya que podría tardar el demonio en ponerse al día. Si todavía está viendo problemas, vuelva a ejecutar la herramienta para ver qué rutas nuevas observa.

- Una buena regla general es que cualquier cosa con una extensión de archivo de registro o diario debe considerarse un candidato de exclusión adecuado.

Crear exclusiones de procesos

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 obtener información sobre las prácticas recomendadas en relación con las exclusiones de procesos, consulte:Terminal seguro: Exclusiones de procesos en MacOS y Linux

Un buen patrón de ajuste primero es identificar los procesos con un alto volumen de ejecuciones de execs.txt, encontrar la trayectoria al ejecutable y crear una exclusión para esta trayectoria. Sin embargo, hay algunos procesos que no deben incluirse, entre ellos:

- Programas generales de servicios públicos: no se recomienda excluir programas generales de servicios públicos (p. ej.: usr/bin/grep) sin tener en cuenta lo siguiente. El usuario puede determinar qué aplicación llama al proceso (p. ej.: busque el proceso primario que está ejecutando grep) y excluya el proceso primario. Esto se debe hacer si el proceso principal puede convertirse en una exclusión de proceso de manera segura, y sólo si lo hace si el proceso principal puede convertirse en una exclusión de proceso. Si la exclusión principal se aplica a los elementos secundarios, también se excluirán las llamadas a cualquier elemento secundario del proceso principal.Se puede determinar el usuario que está ejecutando el proceso. (p. ej.: si el usuario "root" llama a un proceso en un volumen alto, se puede excluir el proceso, pero sólo para el usuario 'root" especificado, esto permitirá que el terminal seguro monitoree los ejecutados de un proceso determinado por cualquier usuario que no sea "root").**NOTA: Las exclusiones de procesos son nuevas en las versiones 1.11.0 y posteriores del conector. Debido a esto, los programas de utilidad general se pueden utilizar como una exclusión de trayectoria en las versiones 1.10.2 y posteriores del conector. Sin embargo, esta práctica sólo se recomienda cuando es absolutamente necesario realizar un intercambio de resultados.**

Encontrar el proceso principal es importante para las exclusiones de procesos. Una vez que se encuentra el proceso principal y/o el usuario del proceso, el usuario puede crear la exclusión para un usuario específico y aplicar la exclusión del proceso a procesos secundarios, lo que a su vez excluirá los procesos ruidosos que no pueden convertirse en exclusiones del proceso.

Identificación del proceso principal

1. En execs.txt, identifique el proceso de gran volumen (p. ej.: /bin/rm).
2. Abra ampdaemon.log desde el paquete de soporte, descomprima syslog.tar y luego siga la ruta /Library/Logs/Cisco/ampdaemon.log (sólo disponible en un paquete de soporte completo, no de un paquete de soporte generado con las opciones predeterminadas).
3. Busque ampdaemon.log para que se excluya el proceso. Busque la línea de registro que muestra la ejecución del proceso (p. ej.: 19 de agosto 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]: Daemon Rx: VNODO:EJECUTAR X:6210 P:3296 PP:3200 U:502 [/bin/rm]).
4. Identifique el proceso principal mediante uno de los siguientes métodos: Identifique la ruta del proceso principal que puede seguir la ruta del proceso que se va a excluir (p. ej.: [/bin/rm] [*Ruta del proceso principal*]).Si el registro no incluye la ruta del proceso principal, identifique la ID del proceso principal de la sección `PP:` de la línea de registro (p: PP:3200).
5. Mediante la ruta principal o la ID de proceso principal, repita los pasos 3 y 4 para determinar el elemento primario del proceso principal actual. Continúe este proceso hasta que no se pueda determinar ningún padre o la ID de proceso principal = 1 (ej: PP:1).
6. Una vez conocido el árbol de procesos, busque la ruta del programa que cubre la mayoría o todas las operaciones que se deben excluir e identifique de forma única la aplicación. Esto minimiza la posibilidad de excluir involuntariamente las operaciones realizadas por otra aplicación.

Identificación del usuario del proceso

1. Siga los pasos 1-3 de Identificación del proceso principal desde arriba.
2. Identifique al usuario de un proceso utilizando uno de los siguientes métodos: Busque la ID de usuario del proceso dado desde `U:` en la línea de registro (p. ej.: U:502).Desde la ventana Terminal, ejecute el siguiente comando: `dscl . list /Users UniqueID | grep #`, donde #es la ID de usuario.Debería ver un resultado similar al de: `Nombre de usuario 502`, donde `Nombre de usuario` es el Usuario del proceso dado.
3. Este nombre de usuario se puede agregar a una exclusión de proceso en la categoría Usuario para reducir el alcance de la exclusión, que para ciertas exclusiones de proceso es importante. **NOTA: si el usuario de un proceso es el usuario local de la máquina y esta exclusión debe aplicarse a varios equipos con diferentes usuarios locales, la categoría Usuario debe dejarse en blanco para permitir que la Exclusión del proceso se aplique a todos los usuarios.**