Guía básica de solución de problemas de AMP para terminales Conector Linux

Contenido

Introducción

Este documento describe una manera básica de resolver problemas de rendimiento encendido la protección frente a malware avanzado de Cisco (AMP) para Terminales Conector Linux.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- AMP para terminales
- Linux/UnixSistemas operativos basados en

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Red Hat Enterprise Linux (RHEL) / Sistema operativo empresarial comunitario (CentSO) versiones 6.10 y 7.7
- AMP para terminales Linux Conector versión 1.11.1

Para obtener una lista completa de versiones AMP compatibles con sistema operativo Linux, consulte [este artículo](#).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

El conector de AMP analiza todos los archivos activos (aquellos que se mueven, copian y/o modifican) de una máquina a menos que se les indique explícitamente que no lo hagan, esto inevitablemente conlleva problemas de rendimiento si se ejecutan demasiados procesos y operaciones mientras el conector está activo, lo que conduce a un uso elevado de la CPU, ralentizaciones y, en algunos casos, software que no se ejecutará o ejecutará lentamente. Además, el conector de AMP puede bloquear los archivos en función de su reputación en la nube, que en ocasiones puede ser erróneo (falso positivo). La solución a ambos problemas es excluir estos trayectos y procesos; en el caso de falsos positivos, problemas no relacionados con el rendimiento o problemas de rendimiento que no parecen resolverse a través de esta guía, se recomienda aumentar el soporte de notificaciones.

El flujo de solución de problemas de rendimiento básico es el siguiente:

- Recopile un paquete Debug mientras se reproduce el problema.
- Ejecute la herramienta de soporte de AMP
- Revisar los archivos pertinentes
- Añadir exclusiones según sea necesario

Troubleshoot

Cómo recopilar un paquete de depuración

Un paquete de depuración es un archivo zip que contiene información detallada de depuración (como registros de escaneo) en el conector. Este paquete es esencial para solucionar la mayoría de los problemas relacionados con el conector de AMP para terminales. Para recopilar un paquete de depuración, siga los pasos proporcionados en Recopilación de Datos de Diagnóstico de AMP para Terminales Conector Linux.

¿Qué información recopila la herramienta de soporte amp y luego se ejecuta un paquete Debug?

La entrada del proceso de debug bundle muestra que el *ampsupport ejecuta algunos comandos log-collection, como se muestra en la imagen.*

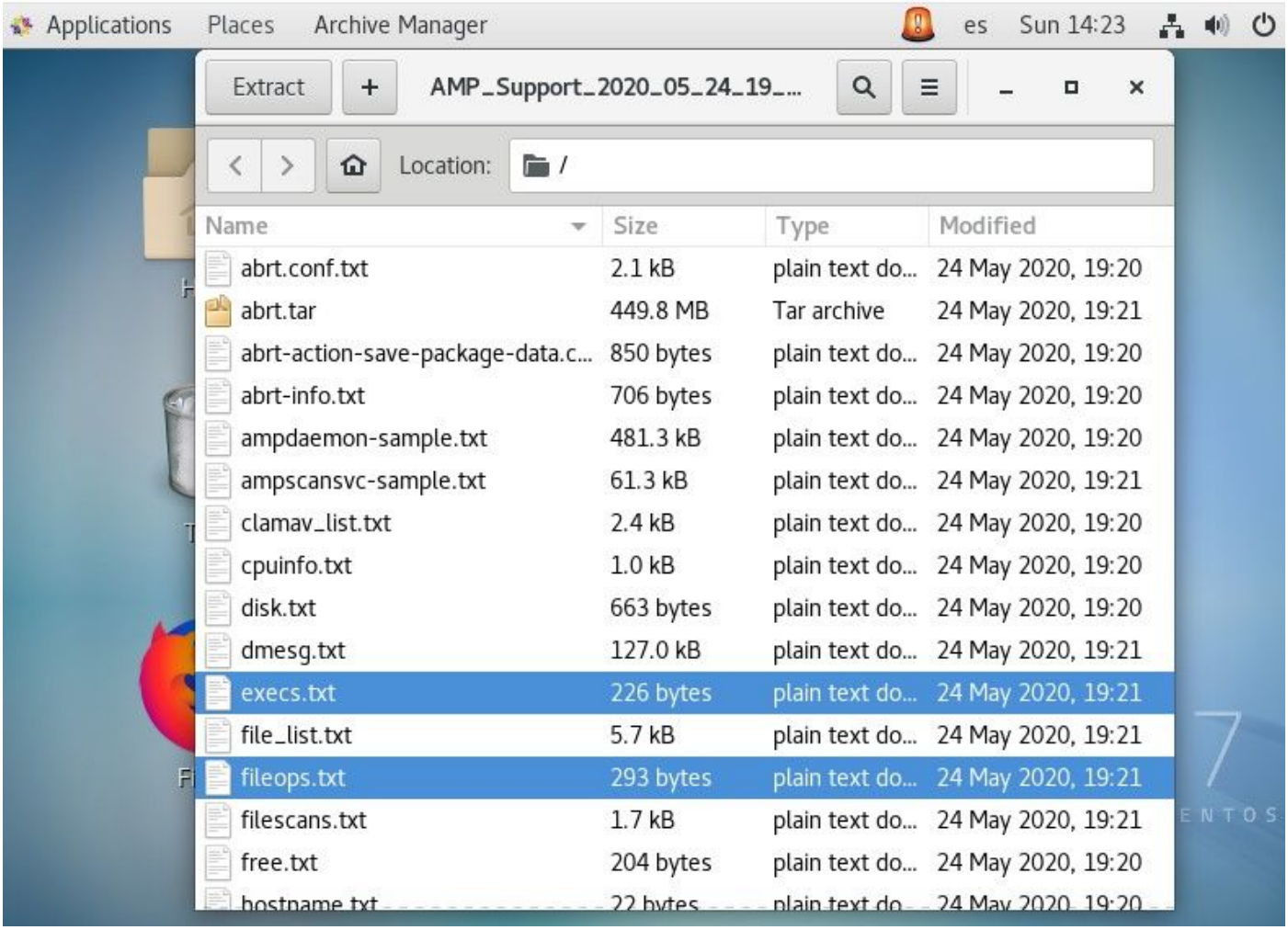
```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: $(cat "${dir}/count")";echo -e "
Executable: $(cat "${dir}/executable")"; echo -e "
Uid: $(cat "${dir}/uid")";echo -e "
Reason: $(cat "${dir}/reason")"; echo -e "
Package: $(cat "${dir}/package")"; done
find: warning: you have specified the -maxdepth option after a non-option argument -typ
e, but options are not positional (-maxdepth affects tests specified before it as well
as those specified after it).  Please specify options before other arguments.

cat: /var/spool/abrt/oops-2020-05-18-18:21:09-10472-0//executable: No such file or dire
ctory
[ -e '/etc/abrt/abrt.conf' ] && cat '/etc/abrt/abrt.conf'
[ -e '/etc/abrt/abrt-action-save-package-data.conf' ] && cat '/etc/abrt/abrt-action-sav
e-package-data.conf'
cat /proc/slabinfo
```

Cómo leer los registros básicos del paquete Linux para identificar los trayectos y

procesos afectados

El paquete de depuración de AMP para terminales de Linux transporta a plétora de información útil, sin embargo, para propósitos básicos de resolución de problemas de rendimiento, sólo hay unos pocos archivos que revisar, fileops.txt, fiescans.txt y execs.txt, como se muestra en la imagen.



El archivo de texto File Operations (fileops) funciona como la principal herramienta de solución de problemas de rendimiento. muestra todas las operaciones activas actuales en su terminal mientras se ejecuta el conector. Estas son las rutas para agregar al conjunto de exclusión de políticas si se considera necesario/seguro.

El texto es el siguiente:

- <Los escaneos numéricos realizados en la trayectoria realizada mientras se ejecuta el proceso de recopilación de paquetes> /<Ruta explorada>

Ejemplo de análisis:

- 1 /homet/user/.mozila/Firefox/

El archivo de análisis de archivos (los archivos pueden) muestra todos los procesos que se ejecutan mientras el conector recopila información de depuración.

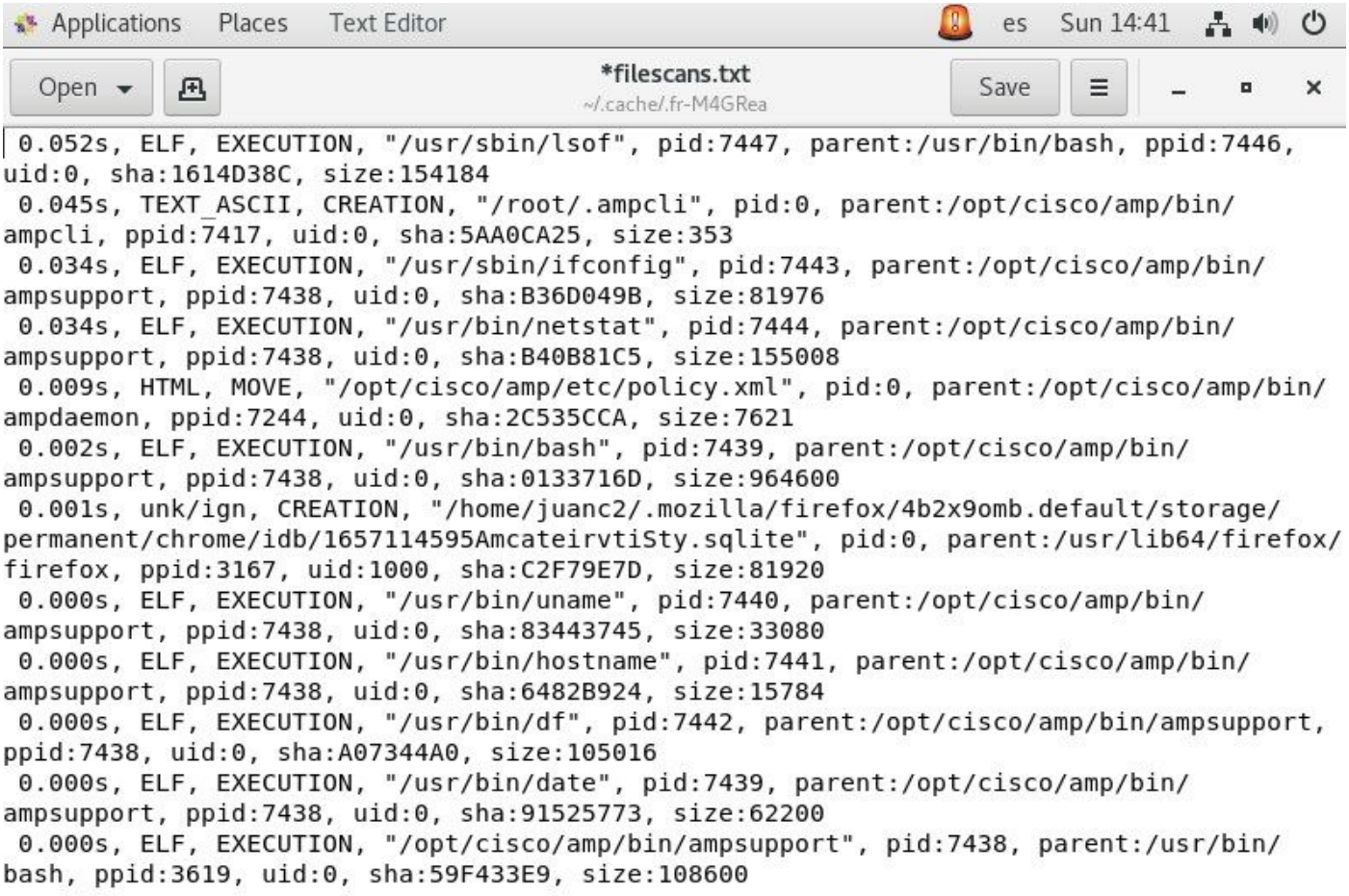
Dice así:

- <Execution time> , <File Type>, <Operation type>, <Process path>, <Parent process path> , <Process ID>, <Parent Process ID> , <SHA Signature (Not SHA256)> <File Sze>

El archivo de texto File Execution (execs) enumera todos los comandos Linux utilizados por los procesos activos en el conector mientras el conector recopilaba el paquete.

> **Advertencia**: Las trayectorias enumeradas aquí no deben excluirse en la política de AMP, ya que son binarios (/bin) y binarios del sistema (/sbin) que utiliza todo el proceso; sin embargo, esta lista puede resultar útil para intentar comprender qué acciones se realizan en los

diferentes procesos que se ejecutan en la máquina de destino.



Una vez identificada, la ruta se excluirá mediante la política, siga las Prácticas recomendadas para AMP para las exclusiones de terminales.

Las exclusiones de procesos manejadas por los conectores Mac y Linux se agregan de manera similar a través de la política, sin embargo, el método difiere ligeramente: Exclusiones de procesos en MacOS y Linux.

Una vez agregadas las exclusiones, pruebe y supervise si el problema persiste. Póngase en contacto con el servicio de asistencia del TAC de AMP.