Guida alla risoluzione dei problemi di base per il connettore Linux di AMP for Endpoints

Sommario

Introduzione

In questo documento viene descritto un metodo di base per risolvere i problemi relativi alle prestazioni on Cisco Advanced Malware Protection (AMP) per Endpoint Linux Connector.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- AMP for Endpoints
- Linux/UnixSistemi operativi

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Red Hat Enterprise Linux (RHEL) / Sistema Operativo Aziendale Della Community (Cent)OS) versioni 6.10 e 7.7
- AMP For Endpoints Linux Connettore version 1.11.1

Per un elenco completo delle versioni compatibili di AMP con il sistema operativo Linux, fare riferimento a questo articolo.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Il connettore AMP esegue la scansione di tutti i file attivi (quelli che si spostano, si copiano e/o si modificano da soli) su una macchina a meno che non sia esplicitamente indicato di non farlo, ciò causa inevitabilmente problemi di prestazioni se vengono eseguiti troppi processi e operazioni mentre il connettore è attivo, con conseguente elevato utilizzo della CPU, rallentamenti e in alcuni casi software che non verrà eseguito o eseguito lentamente. Inoltre, il connettore AMP può bloccare i file in base alla loro reputazione cloud, che a volte può essere errata (falso positivo). La soluzione a entrambi i problemi consiste nell'escludere tali percorsi e processi; in caso di problemi falsi positivi, non correlati alle prestazioni o problemi di prestazioni che non sembrano essere risolti tramite questa guida, è consigliabile aumentare il supporto ticket.

Il flusso di risoluzione dei problemi relativi alle prestazioni di base è il seguente:

- Raccogliere un bundle di debug durante la riproduzione del problema.
- Eseguire lo strumento di supporto AMP
- Esaminare i file pertinenti
- Aggiungere esclusioni in base alle esigenze

Risoluzione dei problemi

Come raccogliere un bundle di debug

Un bundle di debug è un file zip che contiene informazioni di debug dettagliate (come i log di scansione) sul connettore. Questo pacchetto è essenziale per risolvere la maggior parte dei problemi relativi al connettore AMP for Endpoints. Per raccogliere un bundle di debug, seguire i passaggi forniti in Raccolta di dati diagnostici da AMP for Endpoints Linux Connector.

Quali informazioni vengono raccolte dallo strumento di supporto amp e viene eseguito un bundle di debug?

L'input del processo del bundle di debug indica che *ampsupport esegue alcuni comandi di raccolta dei log, come mostrato nell'immagine.*

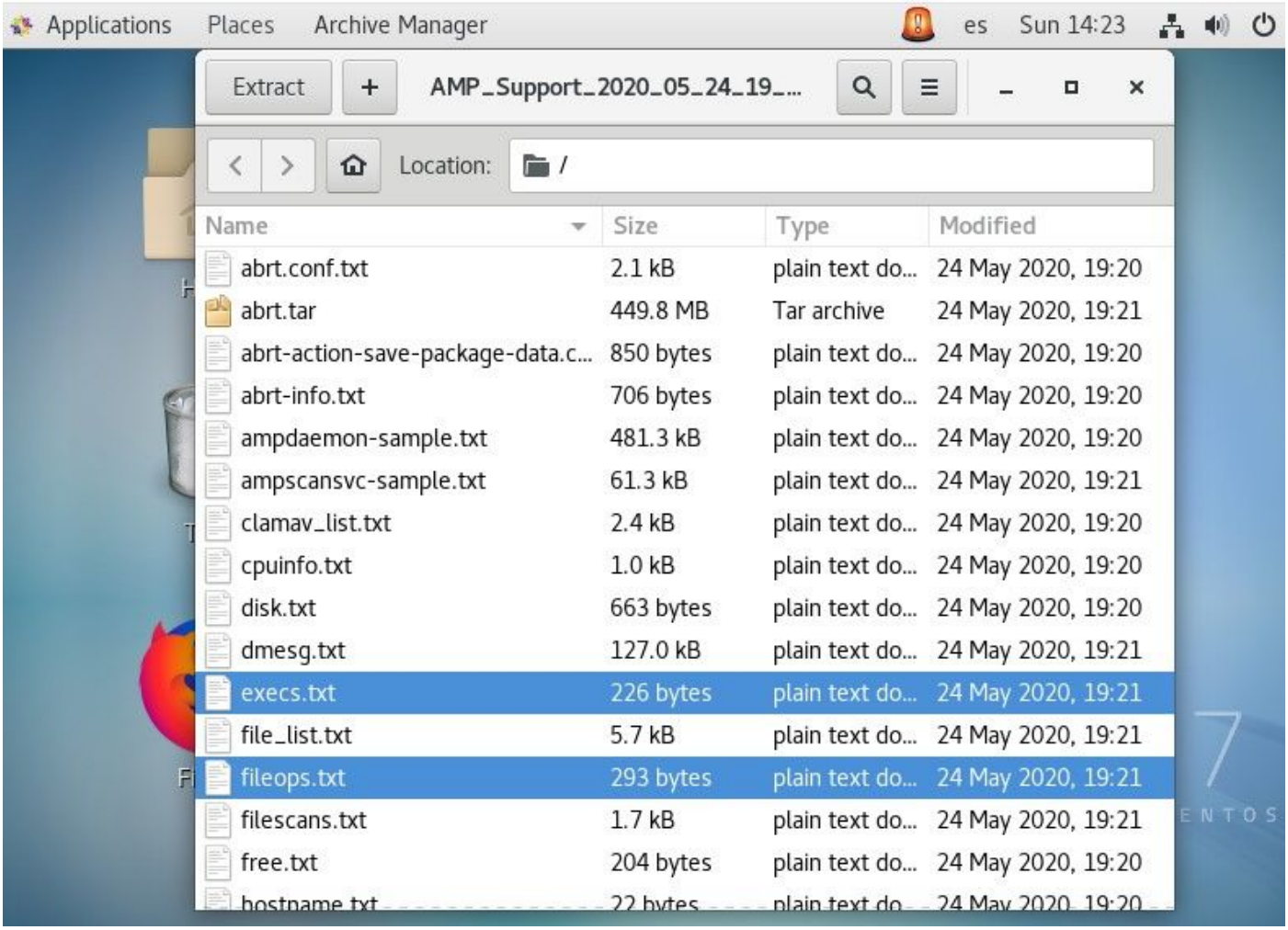
```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: $(cat "${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
```

Come leggere i registri di base del bundle Linux per identificare i percorsi e i

processi interessati

Il bundle di debug di Linux AMP for Endpoints a pletora di informazioni utili, tuttavia, per la risoluzione dei problemi relativi alle prestazioni di base, è possibile esaminare solo alcuni file, fileops.txt, fiescans.txt ed excs.txt, come mostrato nell'immagine.



Il file di testo Operazioni file (fileops) funge da strumento principale per la risoluzione dei problemi relativi alle prestazioni. durante l'esecuzione del connettore, vengono elencate tutte le operazioni attualmente attive sull'endpoint. Percorsi da aggiungere al set di esclusione dei criteri se ritenuto necessario/sicuro.

Si legge come segue:

- <Numero di scansioni eseguite sul percorso durante l'esecuzione del processo di raccolta del bundle> /<Percorso analizzato>

Esempio di analisi:

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

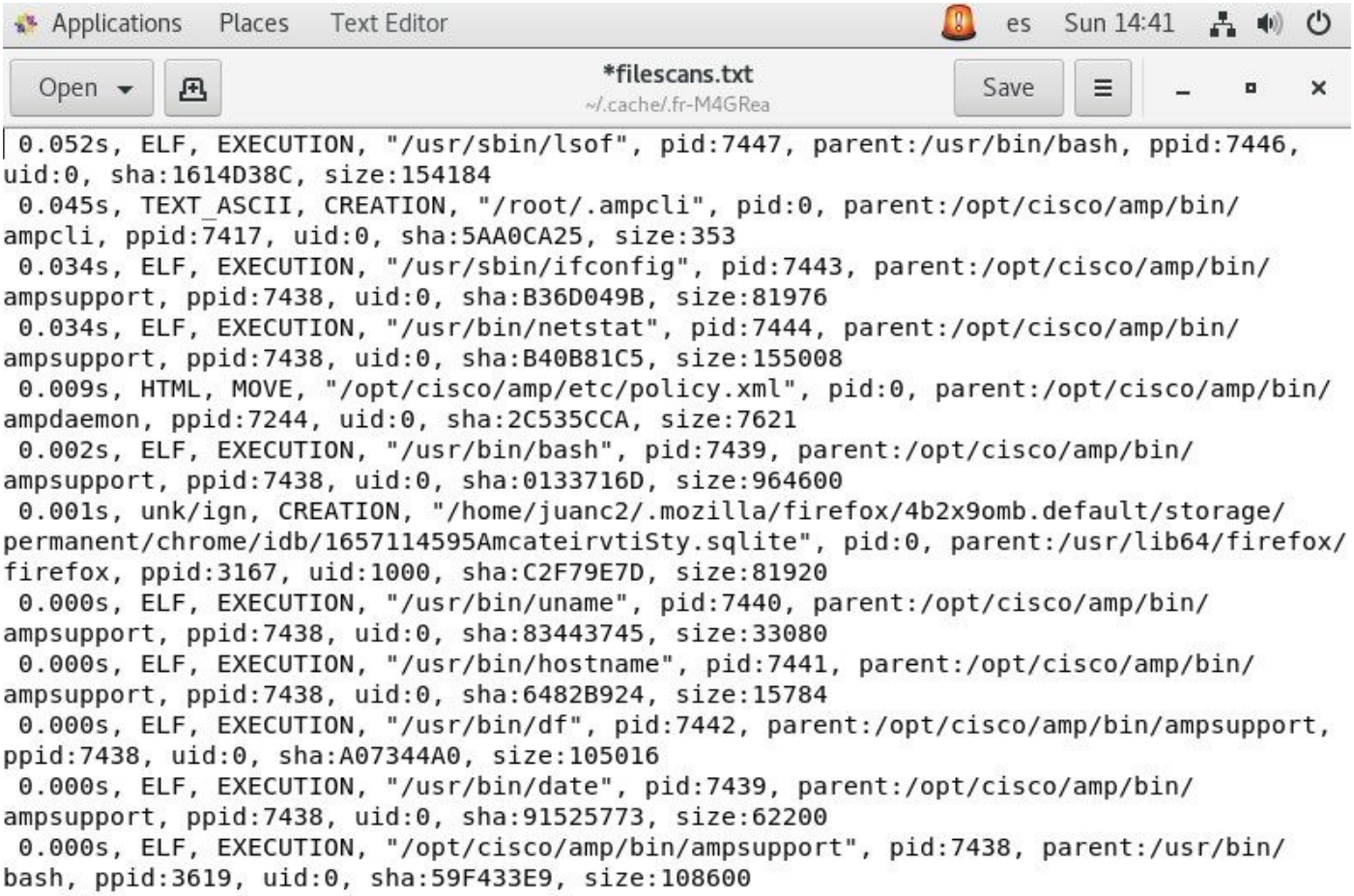
Il file di testo Scansioni file (filescan) elenca tutti i processi in esecuzione durante la raccolta delle informazioni di debug da parte del connettore.

Si legge così:

- <Tempo di esecuzione> , <Tipo file>, <Tipo operazione>, <Percorso processo>, <Percorso processo padre> , <ID processo>, <ID processo padre> , <Firma SHA (non SHA256)> <Dimensione file>

Il file di testo Esecuzione file (excs) elenca tutti i comandi Linux utilizzati dai processi attivi sul connettore durante la raccolta del bundle da parte del connettore.

> Avviso: i percorsi elencati non devono essere esclusi dai criteri AMP, poiché si tratta di binari (/bin) e binari di sistema (/sbin) utilizzati da tutti i processi. Tuttavia, questo elenco può risultare utile per capire quali azioni vengono eseguite dai diversi processi in esecuzione sul computer di destinazione.



Una volta identificato, il percorso deve essere escluso tramite criteri, seguire le best practice per AMP for Endpoint Exclusions.

Le esclusioni dei processi gestite dai connettori Mac e Linux vengono aggiunte in modo simile tramite criteri, tuttavia il metodo differisce leggermente: Esclusioni dei processi in macOS e Linux.

Una volta aggiunte le esclusioni, verificare e monitorare se il problema persiste. Contattare il supporto TAC AMP.