De base dépannez le guide pour l'AMP pour le connecteur de Linux de points finaux

Contenu

Introduction

Ce document décrit une méthode simple de dépanner des problèmes de performance sur la protection de malware avancée par Cisco (AMP) pour le connecteur de Linux de points finaux.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- AMP pour les points terminaux
- Linux/systèmes d'exploitation basés sur Unix

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Linux rouge d'entreprise de chapeau (RHEL)/de système d'exploitation entreprise de la Communauté versions 6.10 et 7.7 (CentOS)
- AMP pour la version 1.11.1 de connecteur de Linux de points finaux

Pour une liste complète de versions compatibles d'AMP avec le système d'exploitation Linux, référez-vous à cet article.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est en ligne, assurez-vous

de bien comprendre l’incidence possible des commandes.

Informations générales

Le connecteur d'AMP analyse tous les actifs (ceux qui se déplace, copient et/ou se modifient) sur un ordinateur à moins qu'ait explicitement dit pas à, cela apporte inévitablement des questions d'interprétations si trop de processus et d'exécutions fonctionnent tandis que le connecteur est en activité, qui mène à l'utilisation du CPU élevé, aux défilements ralentis et dans certains cas au logiciel qui ne fonctionneront pas ou fonctionneront lentement. En outre, le connecteur d'AMP peut bloquer des fichiers basés sur leur réputation de nuage, qui peut quelques fois être erronée (faux positif). La solution aux deux questions est d'exclure ces chemins et processus ; dans le cas du faux positif, des questions liées non représentation ou des problèmes de performance qui ne semblent pas être résolus par l'intermédiaire de ce guide, il est recommandé pour soulever le support de ticket.

L'écoulement de dépanner les problèmes de performance de base est comme suit :

- Collectez un paquet de débogage tandis que la question est reproduite.
- Exécutez l'outil d'assistance d'AMP
- Examinez les fichiers pertinents
- Ajoutez les exclusions comme nécessaires

Dépanner

Comment collecter un paquet de débogage

Un paquet de débogage est un fichier zip qui contient les informations détaillées de débogage (comme des logs de balayage) sur le connecteur. Ce paquet est essentiel pour dépanner la plupart de problème lié à l'AMP pour le connecteur de points finaux. Pour collecter un paquet de débogage, suivez les étapes données sur la collecte de données diagnostiques d'AMP pour le connecteur de Linux de points finaux.

Quelles informations l'outil d'assistance d'Ampère collecte-il alors un paquet de débogage est-il exécuté ?

L'entrée de traitement de paquet de débogage prouve que l'*ampsupport* exécute quelques commandes de log-collecte, suivant les indications de l'image.

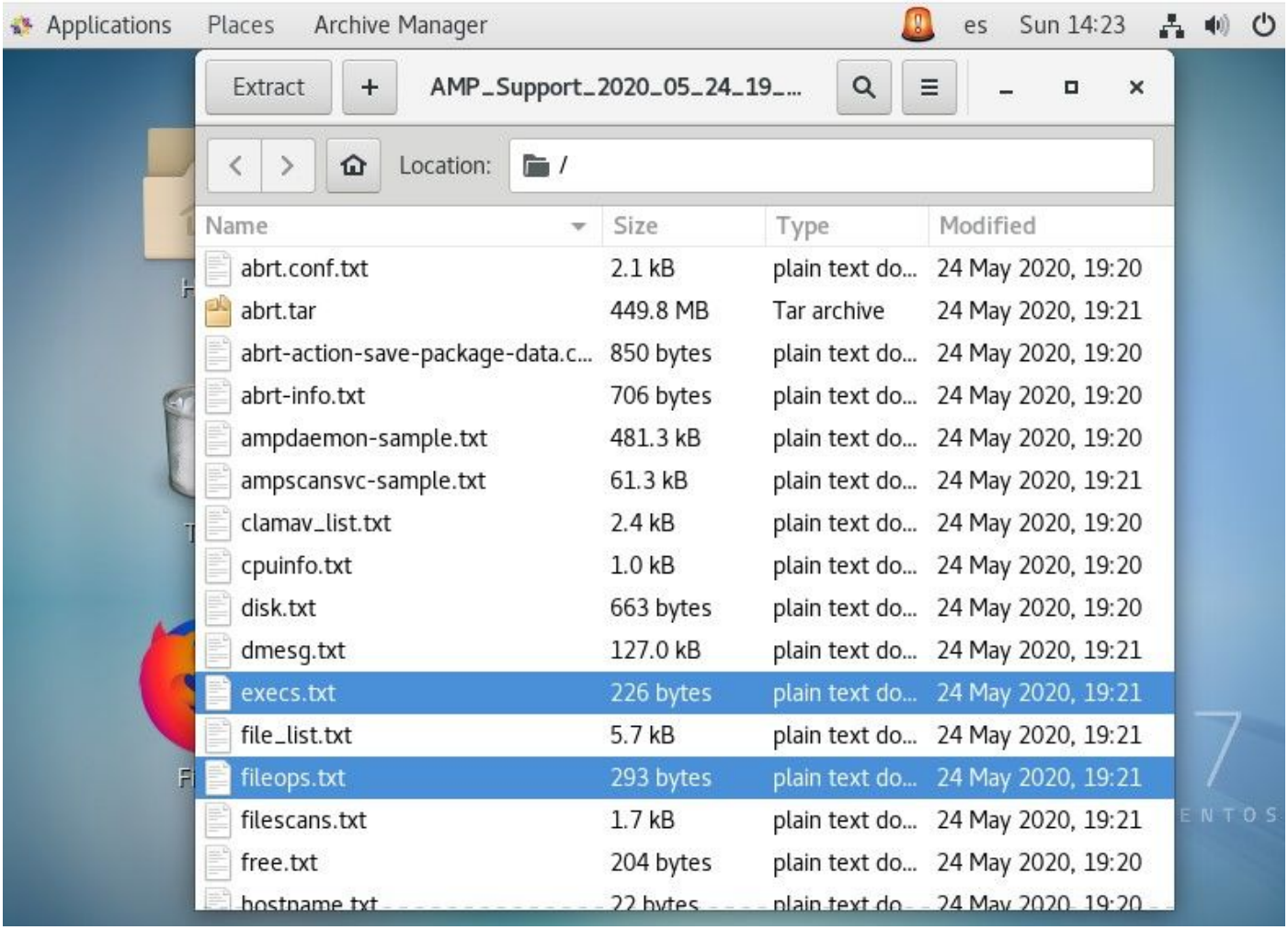
```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: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

Comment lire le paquet de base de Linux se connecte pour identifier les chemins et

les processus affectés

L'AMP de Linux pour le paquet de débogage de points finaux diffuse une pléthore des informations utiles, cependant, pour le dépannage de base de représentation, il y a seulement quelques fichiers à passer en revue, fileops.txt, fiescans.txt, et d'execs.txt, suivant les indications de l'image.



Le fichier texte d'exécutions de fichier (fileops) fonctionne comme outil principal de dépannage de représentation. il répertorie des exécutions actives en cours d'AI d'AI actuellement - sur votre point final tandis que le connecteur fonctionne. Ce sont les chemins à ajouter à l'exclusion de stratégie réglée si considéré nécessaires/coffre-fort.

On le lit comme suit :

- balayages de <Number exécutés sur le chemin exécuté tandis que scanned> du runs>/<Path de procédé de collecte de paquet

Analyse l'exemple :

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

Le fichier texte (filescan) de balayages de fichier répertorie tous les processus qui fonctionnent tandis que le connecteur collectait les informations de débogage.

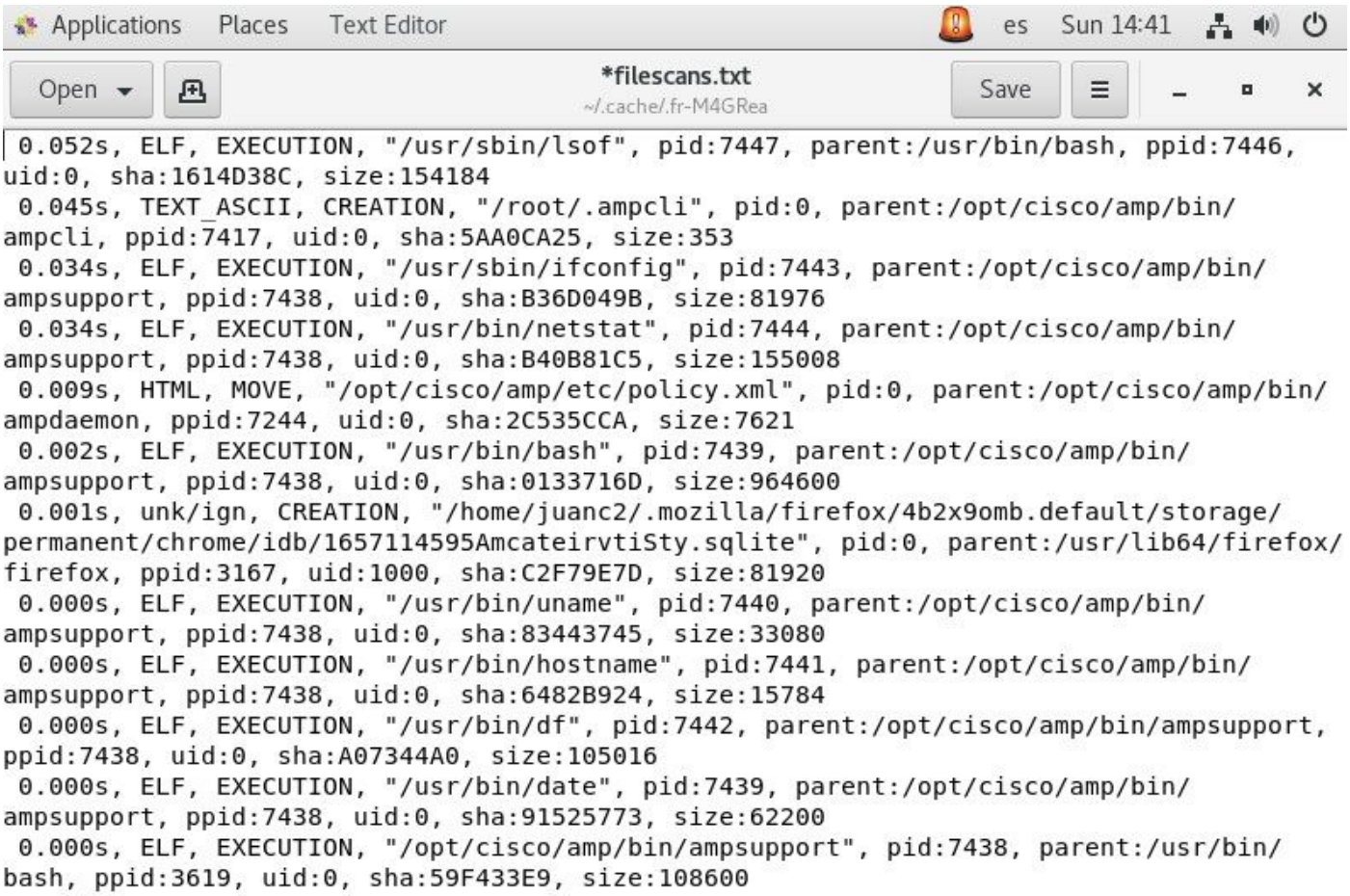
Il lit en tant que tels :

- time> de <Execution, Type> <File, type> de <Operation, path> de <Process, path> de processus <Parent, <Process ID>, PProcess <Parent ID>, signature <SHA (pas SHA256)> Sze> <File

Le fichier texte d'exécution de fichier (cadres) répertorie toutes les commandes de Linux utilisées par des processus actifs sur le connecteur tandis que le connecteur collectait le paquet.

Avertissement : Les chemins répertoriés ici ne doivent pas être exclus sur la stratégie

d'AMP, comme ce sont les binaires (/bin) et les binaires de système (/sbin) que tout le processus utilise, cependant, cette liste pourraient être livré utile à essayer pour comprendre quelles actions sont exécutées par les différents processus qui fonctionnent sur la machine cible.




```
 0.052s, ELF, EXECUTION, "/usr/sbin/lsof", pid:7447, parent:/usr/bin/bash, ppid:7446,
uid:0, sha:1614D38C, size:154184
 0.045s, TEXT_ASCII, CREATION, "/root/.ampcli", pid:0, parent:/opt/cisco/amp/bin/
ampcli, ppid:7417, uid:0, sha:5AA0CA25, size:353
 0.034s, ELF, EXECUTION, "/usr/sbin/ifconfig", pid:7443, parent:/opt/cisco/amp/bin/
ampsupport, ppid:7438, uid:0, sha:B36D049B, size:81976
 0.034s, ELF, EXECUTION, "/usr/bin/netstat", pid:7444, parent:/opt/cisco/amp/bin/
ampsupport, ppid:7438, uid:0, sha:B40B81C5, size:155008
 0.009s, HTML, MOVE, "/opt/cisco/amp/etc/policy.xml", pid:0, parent:/opt/cisco/amp/bin/
ampdaemon, ppid:7244, uid:0, sha:2C535CCA, size:7621
 0.002s, ELF, EXECUTION, "/usr/bin/bash", pid:7439, parent:/opt/cisco/amp/bin/
ampsupport, ppid:7438, uid:0, sha:0133716D, size:964600
 0.001s, unk/ign, CREATION, "/home/juanc2/.mozilla/firefox/4b2x9omb.default/storage/
permanent/chrome/idb/1657114595AmcateirvtiSty.sqlite", pid:0, parent:/usr/lib64/firefox/
firefox, ppid:3167, uid:1000, sha:C2F79E7D, size:81920
 0.000s, ELF, EXECUTION, "/usr/bin/uname", pid:7440, parent:/opt/cisco/amp/bin/
ampsupport, ppid:7438, uid:0, sha:83443745, size:33080
 0.000s, ELF, EXECUTION, "/usr/bin/hostname", pid:7441, parent:/opt/cisco/amp/bin/
ampsupport, ppid:7438, uid:0, sha:6482B924, size:15784
 0.000s, ELF, EXECUTION, "/usr/bin/df", pid:7442, parent:/opt/cisco/amp/bin/ampsupport,
ppid:7438, uid:0, sha:A07344A0, size:105016
 0.000s, ELF, EXECUTION, "/usr/bin/date", pid:7439, parent:/opt/cisco/amp/bin/
ampsupport, ppid:7438, uid:0, sha:91525773, size:62200
 0.000s, ELF, EXECUTION, "/opt/cisco/amp/bin/ampsupport", pid:7438, parent:/usr/bin/
bash, ppid:3619, uid:0, sha:59F433E9, size:108600
```

Une fois qu'identifié, le chemin doit être exclu par l'intermédiaire de la stratégie, suivent s'il vous plaît des pratiques recommandées pour l'AMP pour des exclusions de point final.

Des exclusions de processus manipulées par les connecteurs de MAC et de Linux sont pareillement ajoutées par l'intermédiaire de la stratégie, cependant, la méthode diffère légèrement : Exclusions de processus dans le MaOS et le Linux.

Une fois que des exclusions sont ajoutées, testez, et surveillez si le problème persiste. Support de l'AMP TAC de contact.