Guide de dépannage de base pour le connecteur Linux AMP for Endpoints

Contenu

Introduction

Ce document décrit une méthode de base de dépannage des problèmes de performances sur Cisco Advanced Malware Protection (AMP) pour Connecteur Linux de terminaux.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Components Used

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

- Red Hat Enterprise Linux (RHEL) / Système d'exploitation d'entreprise communautaire (CentOS) versions 6.10 et 7.7
- AMP pour terminaux Linux Connecteur version 1.11.1

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

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 votre réseau

est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Le connecteur AMP analyse tous les fichiers actifs (ceux qui se déplacent, se copient et/ou se modifient eux-mêmes) sur une machine, sauf indication explicite contraire, cela entraîne inévitablement des problèmes de performances si un trop grand nombre de processus et d'opérations s'exécutent pendant que le connecteur est actif, ce qui entraîne une utilisation élevée du CPU, des ralentissements et dans certains cas des logiciels qui ne s'exécutent pas ou ne s'exécutent pas lentement. En outre, le connecteur AMP peut bloquer des fichiers en fonction de leur réputation dans le cloud, ce qui peut parfois être erroné (faux positif). La solution à ces deux problèmes est d'exclure ces voies et processus ; dans le cas de problèmes faux positifs, non liés aux performances ou de problèmes de performances qui ne semblent pas être résolus par le biais de ce guide, il est recommandé d'augmenter le support des billets.

Le flux de dépannage des problèmes de performances de base est le suivant :

- Collecter un bundle de débogage pendant la reproduction du problème.
- Exécuter l'outil de support AMP
- Examiner les fichiers pertinents
- Ajouter des exclusions si nécessaire

Dépannage

Comment collecter un bundle de débogage

Un bundle de débogage est un fichier zip qui contient des informations de débogage détaillées (comme les journaux d'analyse) sur le connecteur. Cette offre groupée est essentielle pour résoudre la plupart des problèmes liés au connecteur AMP for Endpoints. Pour collecter un bundle de débogage, suivez les étapes fournies sur Collection de données de diagnostic d'AMP for Endpoints Linux Connector.

Quelles informations l'outil de support amp recueille-t-il pour qu'un bundle de débogage soit exécuté ?

L'entrée du processus de débogage indique que *ampsupport exécute certaines commandes log-collection, comme l'illustre l'image.*

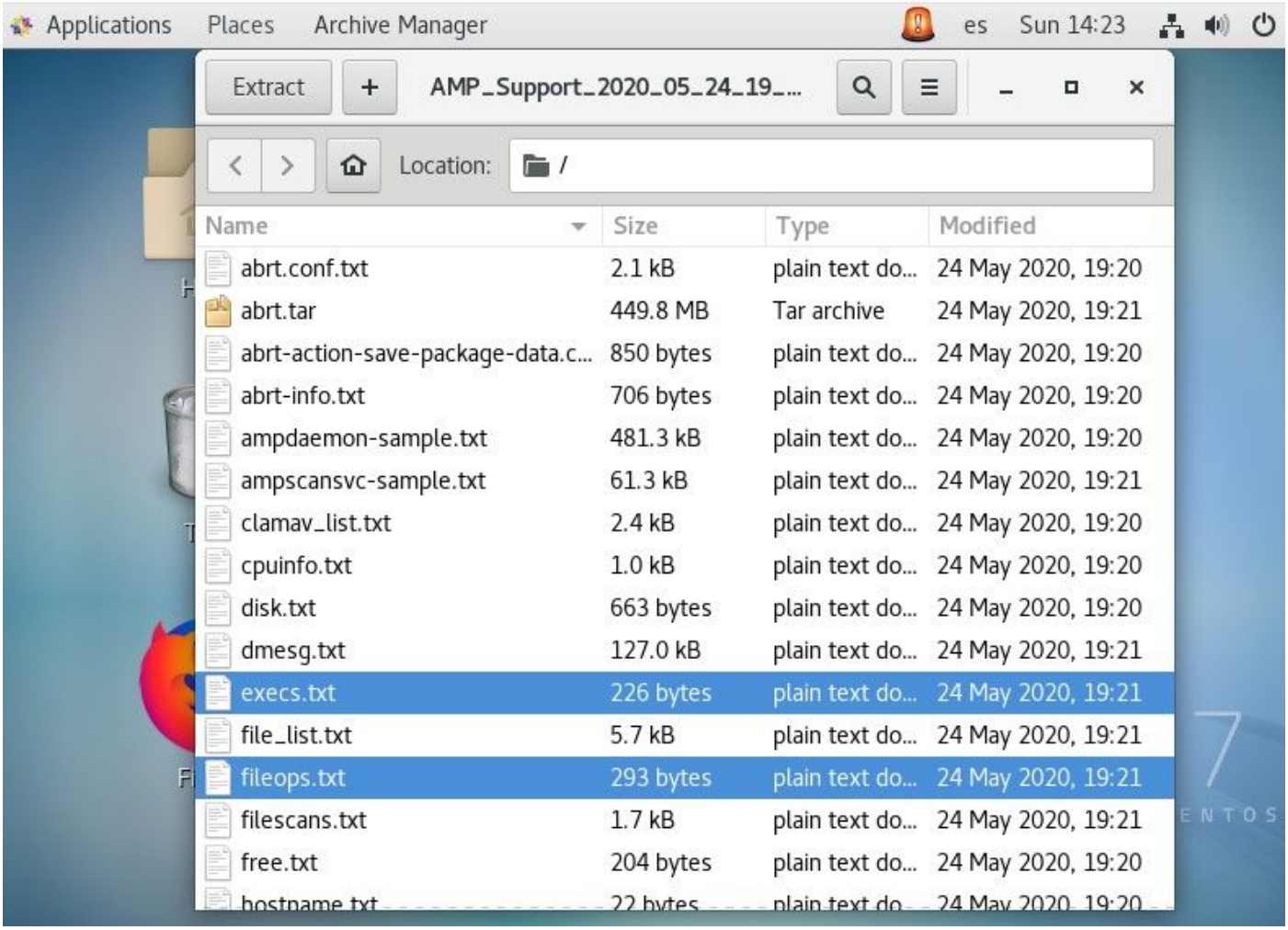
```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: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

chemins et processus affectés

L'offre Linux AMP for Endpoints Debug porte a pléthore d'informations utiles, cependant, à des fins de dépannage des performances de base, il n'y a que quelques fichiers à consulter, fileops.txt, fiescans.txt et Execs.txt, comme le montre l'image.



Le fichier texte des opérations de fichiers (fichiers) sert d'outil principal de dépannage des performances. il répertorie toutes les opérations actives en cours sur votre point d'extrémité pendant que le connecteur s'exécute. Il s'agit des chemins à ajouter au jeu d'exclusions de stratégie si cela est jugé nécessaire/sûr.

Il se lit comme suit :

- <Numéros analysés sur le chemin d'accès exécuté pendant l'exécution du processus de collecte de l'offre groupée> /<Chemin analysé>

Analyse l'exemple :

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

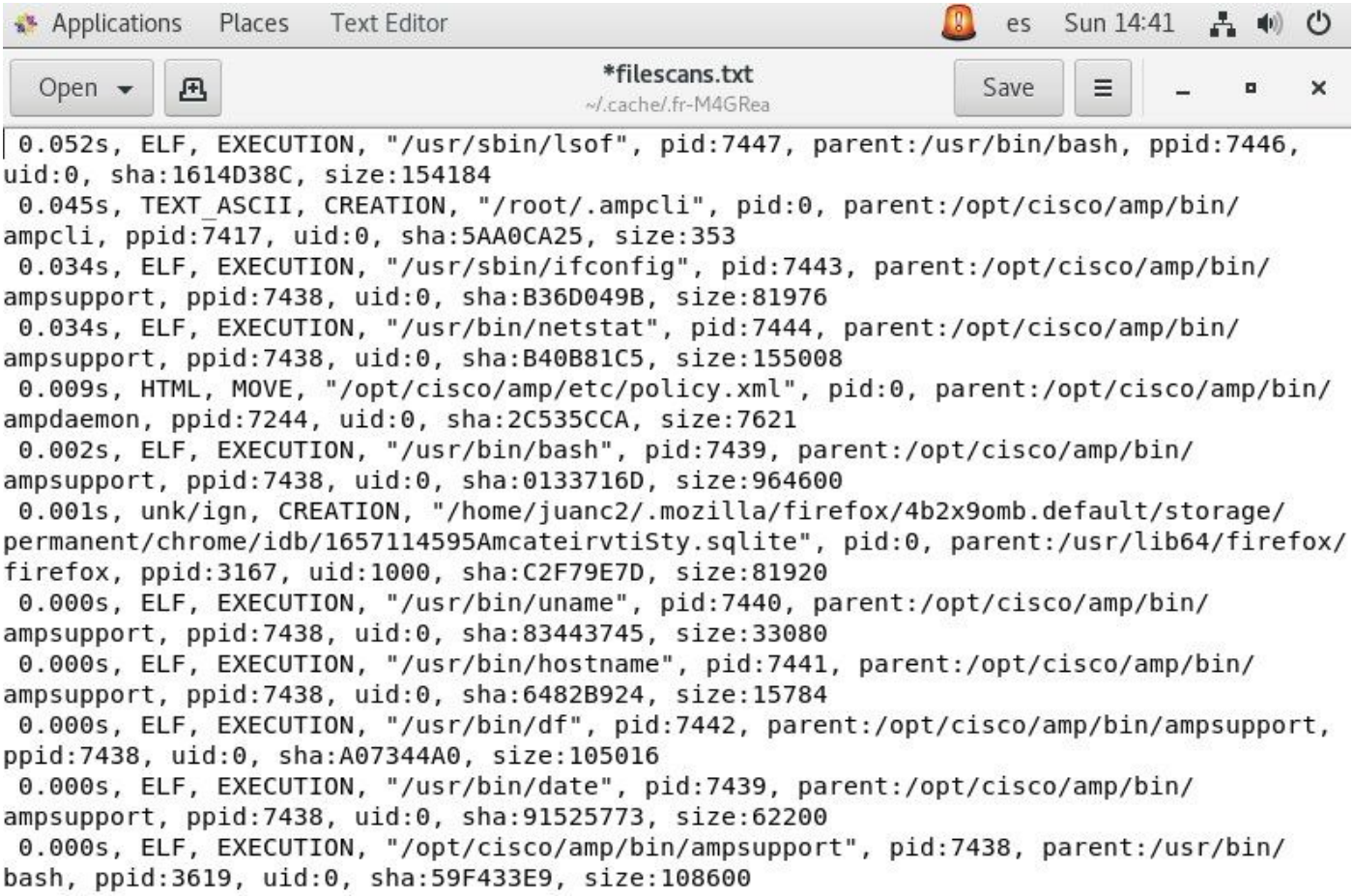
Le fichier texte Analyse les fichiers (filescan) répertorie tous les processus qui s'exécutent pendant que le connecteur collecte les informations de débogage.

Il se lit ainsi :

- <Temps d'exécution> , <Type de fichier>, <Type d'opération>, <Chemin du processus>, <Chemin du processus parent> , <ID du processus>, <ID du processus parent> , <Signature SHA (et non SHA256)> <Taille du fichier>

Le fichier texte File Execution (Execs) répertorie toutes les commandes Linux utilisées par les processus actifs sur le connecteur pendant que le connecteur collectait l'ensemble.

> **Avertissement** : Les chemins d'accès répertoriés ici ne doivent pas être exclus de la stratégie AMP, car il s'agit de binaires (/bin) et de binaires système (/sbin) que tous les processus utilisent. Cependant, cette liste peut être utile pour essayer de comprendre quelles actions sont exécutées par les différents processus qui s'exécutent sur l'ordinateur cible.



Une fois identifié, le chemin d'accès doit être exclu via la stratégie. Veuillez suivre les Méthodes Recommandées pour les exclusions d'AMP pour les terminaux.

Les exclusions de processus gérées par les connecteurs Mac et Linux sont également ajoutées via la politique, cependant, la méthode diffère légèrement : Exclusions de processus dans macOS et Linux.

Une fois les exclusions ajoutées, testez et surveillez si le problème persiste. Contactez l'assistance TAC AMP.