Grundlegender Fehlerbehebungsleitfaden für AMP für Endgeräte Linux Connector

Inhalt

Einführung

Dieses Dokument beschreibt eine grundlegende Methode zur Behebung von Leistungsproblemen. auf Cisco Advanced Malware Protection (AMP) für Linux-Connector für Endgeräte.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- AMP für Endgeräte
- Linux/UnixBetriebssysteme

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Red Hat Enterprise Linux (RHEL) / Community Enterprise Operating System (Cent)BS) Versionen 60,10 und 77
- AMP für Endgeräte Linux Anschluss Version 1,11,1

Eine vollständige Liste der kompatiblen AMP-Versionen mit Linux-Betriebssystem finden Sie in diesem Artikel.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Der AMP-Connector scannt alle aktiven Dateien (die sich selbst verschieben, kopieren und/oder ändern) auf einem Computer, es sei denn, dies wird ausdrücklich untersagt. Dies führt unweigerlich zu Leistungsproblemen, wenn zu viele Prozesse und Abläufe ausgeführt werden, während der Connector aktiv ist. Dies führt zu einer hohen CPU-Auslastung, Verlangsamungen und in einigen Fällen zu Software, die nicht ausgeführt wird oder langsam läuft. Darüber hinaus blockiert der AMP-Connector möglicherweise Dateien basierend auf ihrer Cloud-Reputation, was manchmal falsch (falsch positiv) sein kann. Die Lösung für beide Probleme ist, diese Pfade und Prozesse; Bei Fehlalarmen, nicht leistungsbezogenen Problemen oder Leistungsproblemen, die nicht über diesen Leitfaden gelöst zu werden scheinen, wird empfohlen, die Ticketunterstützung zu erhöhen.

Die Fehlerbehebung für grundlegende Leistungsprobleme verläuft wie folgt:

- Sammeln Sie ein Debug-Paket, während das Problem reproduziert wird.
- Führen Sie das AMP-Support-Tool aus
- Überprüfen der entsprechenden Dateien
- Nach Bedarf Ausschluss hinzufügen

Fehlerbehebung

Sammeln eines Debugpakets

Ein Debugpaket ist eine ZIP-Datei, die detaillierte Debuginformationen (z. B. Scan-Protokolle) auf dem Anschluss enthält. Dieses Paket ist zur Fehlerbehebung bei den meisten Problemen mit dem AMP für Endgeräte-Anschluss unerlässlich. Um ein Debug-Paket zu sammeln, gehen Sie wie in der Sammlung von Diagnosedaten von AMP für Endgeräte Linux Connector beschrieben vor.

Welche Informationen werden vom AMP-Support-Tool erfasst, wenn ein Debug-Paket ausgeführt wird?

Die Prozesseingabe des Debugpakets zeigt, dass die *ampsupport führt einige Protokollauflistungsbefehle aus, wie im Bild gezeigt.*

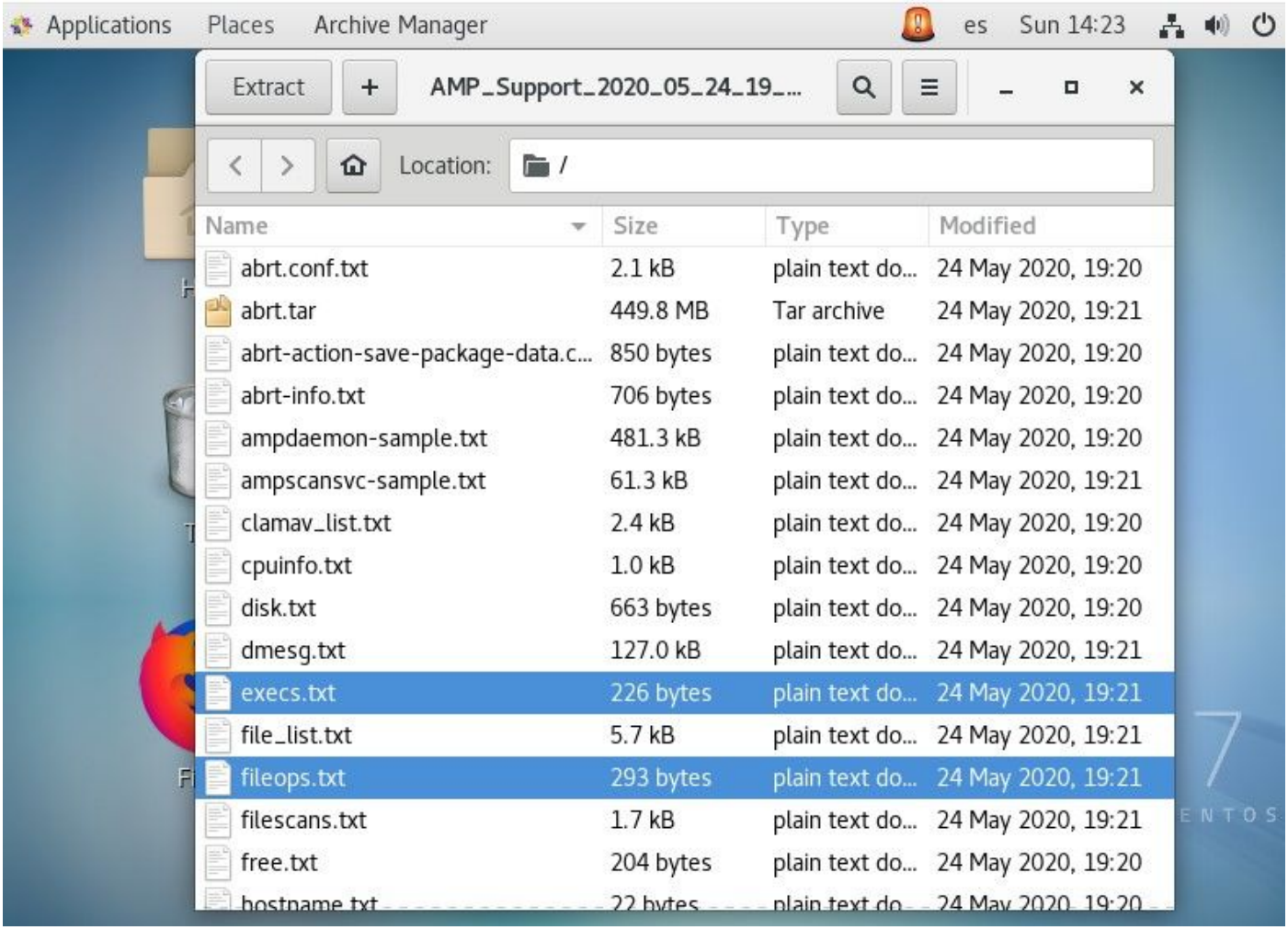
```
top -b -n5 -d2 -H -p `pidof ampdaemon | tr ' ' ,` -p `pidof ampscansvc | tr ' ' ,`
[ -e 'abrt-cli' ] && abrt-cli list -d
[ -d '/var/spool/abrt' ] && for dir in $(find /var/spool/abrt/*/ -type d -maxdepth 1);
do echo -e "
Crash: ${dir}"; echo -e "
Kernel: $(cat "${dir}/kernel")"; echo -e "
Count: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

Lesen grundlegender Linux-Bündelprotokolle, um die betroffenen Pfade und

Prozesse zu identifizieren

Das Debug-Paket für Linux AMP für Endgeräte wird mitgeliefert. eine Fülle nützliche Informationen, aber für die grundlegende Behebung von Leistungsproblemen gibt es nur wenige Dateien zu überprüfen, wie im Bild gezeigt: fileops.txt, fiescans.txt und Execs.txt.



Die Textdatei File Operations (fileops) fungiert als wichtigstes Tool zur Behebung von Leistungsproblemen. Es listet alle aktuell aktiven Vorgänge auf Ihrem Endpunkt auf, während der Connector ausgeführt wird. Dies sind die Pfade, um die Festlegung von Richtlinien auszuschließen, wenn dies für notwendig/sicher erachtet wird.

Es erhält folgende Fassung:

- <Bei Ausführung des Paketerfassungsprozesses durchgeführte Nummernprüfungen für den Pfad> /<gescannter Pfad>

Scans Beispiel:

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

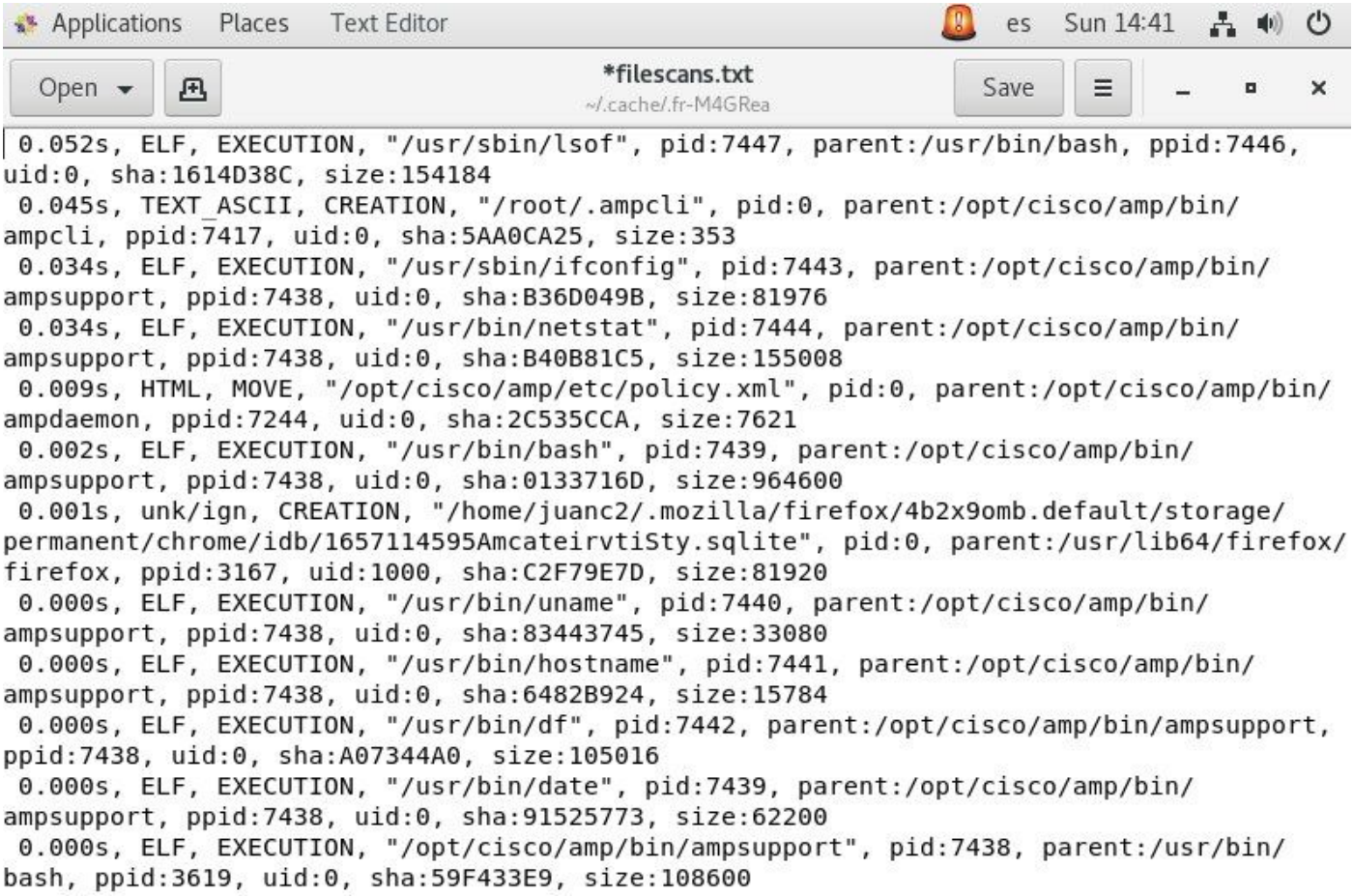
In der Datei Dateiprüfungen (DateienScan) Text werden alle Prozesse aufgelistet, die ausgeführt werden, während der Connector die gesammelten Debuginformationen erfasst.

Er lautet als solcher:

- <Ausführungszeit> , <Dateityp>, <Betriebstyp>, <Prozesspfad>, <Parent Process path>, <Prozess-ID>, <Parent Process ID>, <SHA-Signatur (Nicht SHA256)> <Dateigröße>

Die Textdatei File Execution (Execs) listet alle Linux-Befehle auf, die von aktiven Prozessen auf dem Connector verwendet werden, während der Connector das Paket gesammelt hat.

> **Warnung**: Die hier aufgeführten Pfade dürfen in der AMP-Richtlinie nicht ausgeschlossen werden, da es sich um Binärdateien (/bin) und Systembinaries (/sbin) handelt, die von allen Prozessen verwendet werden. Diese Liste kann jedoch nützlich sein, um zu versuchen, zu verstehen, welche Aktionen von den verschiedenen Prozessen ausgeführt werden, die auf dem Zielcomputer ausgeführt werden.



Sobald Pfad identifiziert ist, muss er über Richtlinie ausgeschlossen werden. Befolgen Sie die Best Practices für AMP für Endgeräte-Ausschlüsse.

Prozessausschlüsse, die von den Mac- und Linux-Anschlüssen behandelt werden, werden in ähnlicher Weise über Richtlinien hinzugefügt. Die Methode unterscheidet sich jedoch geringfügig: Prozessausschlüsse in MacOS und Linux.

Nach dem Hinzufügen von Ausschlüssen können Sie testen und überwachen, ob das Problem weiterhin besteht. Wenden Sie sich an den AMP TAC-Support.