Basic Troubleshooter Guide voor AMP voor Endpoints Linux-connector

Inhoud

Inleiding

Dit document beschrijft een eenvoudige manier om problemen met de prestaties van de probleemoplossing te definiëren aan Cisco Advanced Malware Protection (AMP) voor Endpoints Linux-connector.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Advanced Malware Protection voor endpoints
- Linux/UnixOp gebaseerde besturingssystemen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Red Hat Enterprise Linux (RHEL) / Enterprise Operating System (Cent)OS) versies 6.10 en 7.7
- Advanced Malware Protection voor endpoints Aansluiting versie 1.11.1

Zie dit artikel voor een compleet overzicht van compatibele AMP-versies met Linux Operating System.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

De AMP-connector scant alle actieve bestanden (bestanden die zich verplaatsen, kopiëren en/of wijzigen) op een machine tenzij expliciet wordt aangegeven dat dit niet het geval is, dat onvermijdelijk prestatiekwesties met zich meebrengt als er te veel processen en bewerkingen worden uitgevoerd terwijl de connector actief is, wat leidt tot een hoog CPU-gebruik, vertragingen en in sommige gevallen tot software die niet langzaam werkt of werkt. Bovendien kan de AMP-connector bestanden blokkeren op basis van hun cloudreputatie, die soms onjuist (fout-positief) kan zijn. De oplossing voor beide kwesties is het uitsluiten van deze wegen en processen; In het geval van fout-positieve, niet-prestatiegerelateerde problemen of prestatiekwesties die niet lijken te zijn opgelost via deze gids, wordt aangeraden om de ticketondersteuning te verhogen.

De stroom van problemen met basisprestaties bij het oplossen van problemen is als volgt:

- Verzamel een debug bundel terwijl het probleem is gereproduceerd.
- Voer het AMP-ondersteuningsgereedschap uit
- Bekijk de corresponderende bestanden
- Voeg eventuele uitsluitingen toe indien nodig

Problemen oplossen

Het verzamelen van een debug-bundel

Een debug-bundel is een zip-bestand dat gedetailleerde debug-informatie (zoals scanlogbestanden) op de connector bevat. Deze bundel is essentieel om problemen op te lossen bij de meeste problemen die te maken hebben met de Advanced Malware Protection voor endpoints. Om een debug-bundel te verzamelen volgt u de stappen die zijn meegeleverd bij het verzamelen van diagnostische gegevens van AMP voor Endpoints Linux-connector.

Welke informatie verzamelt het poststeungereedschap dan een debug bundel?

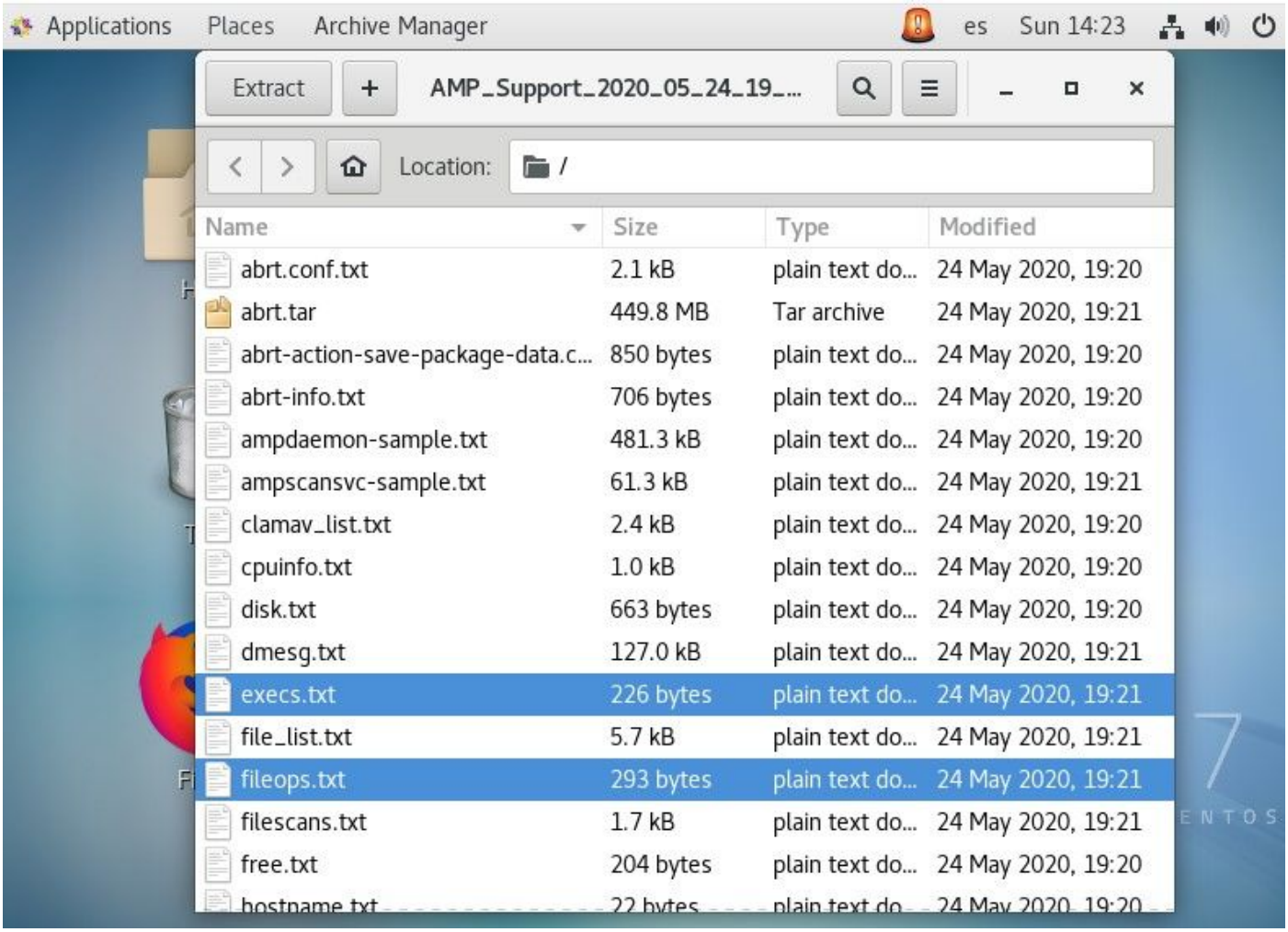
De debug-procesinvoer toont aan dat *ampsupport voert een aantal opdrachten voor logverzameling uit, zoals in de afbeelding.*

```
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
```

Hoe u de elementaire Linux-bundels leest om de getroffen paden en processen te identificeren

De Linux AMP voor Endpoints Debug Splitst a overvloed van nuttige informatie, echter, voor de doeleinden van het oplossen van problemen van basisprestaties zijn er slechts een paar te bekijken bestanden, fileops.txt, fiescans.txt, en execus.txt, zoals in de afbeelding getoond.



Het tekstbestand File Operations (bestanden) werkt als het belangrijkste gereedschap voor het oplossen van prestaties. het maakt een lijst van alle huidige actieve operaties op uw eindpunt terwijl de connector draait . Dit zijn de manieren om de beleidsuitsluiting te vergroten die is ingesteld als dit nodig/veilig wordt geacht.

Het wordt als volgt gelezen:

- <Number wordt gescand op het pad dat wordt uitgevoerd terwijl het bundelverzamelproces draait> /<Path gescand>

Een voorbeeld scannen:

- 1/homet/gebruiker/.mozila/Firefox/

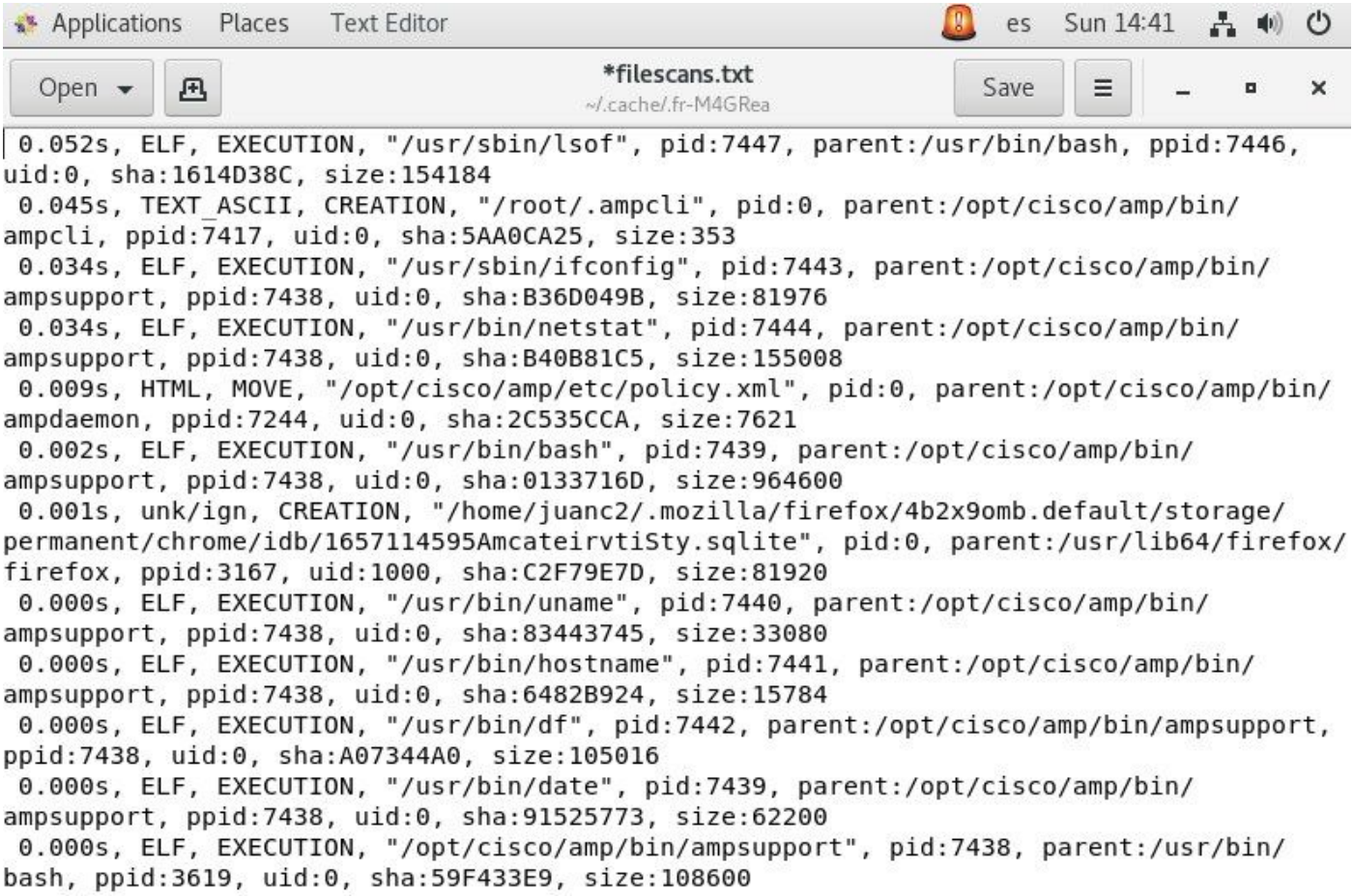
In het Tekstbestand Scans (bestanden) wordt een lijst weergegeven van alle processen die worden uitgevoerd terwijl de verzamelde connector informatie debug.

Het luidt als volgt:

- <Uitvoeringstijd>, <bestandstype>, <operatietype>, <Procespad>, <Parent-procespad>, <ProcesID>, <Parent-proces-ID>, <SHA-handtekening (niet SHA256)> <Bestandsgrootte>

Het tekstbestand File Performtion (EXS) maakt een lijst van alle Linux-opdrachten die door actieve processen op de connector worden gebruikt terwijl de connector de bundel verzamelde.

> **Waarschuwing**: de hier vermelde paden mogen niet worden uitgesloten van het AMP-beleid, omdat dit binaries (/bin) en system binaries(/sbin) zijn die alle processen gebruiken. Deze lijst kan echter nuttig zijn om te proberen te begrijpen welke acties worden uitgevoerd door de verschillende processen die op de doelmachine draaien.



Als Pad eenmaal geïdentificeerd is, moet Pad via het beleid worden uitgesloten, volgt u de best practices voor AMP voor uitsluitingen van endpoints.

Procesuitsluitingen die door de Mac- en Linux-connectors worden verwerkt, worden eveneens toegevoegd via het beleid, maar de methode verschilt enigszins: Procesuitsluitingen in macOS en Linux.

Zodra uitsluitingen zijn toegevoegd, test en controleer of het probleem blijft bestaan. Neem contact op met TAC-ondersteuning.