面向終端的AMP Linux聯結器的基本故障排除指南

目錄

簡介

本文描述解決效能問題的基本方法 於 思科高級惡意軟體防護 (AMP) 對於 終端Linux聯結器.

必要條件

需求

思科建議您瞭解以下主題：

- AMP端點版
- Linux/Unix基於的作業系統

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Red Hat Enterprise Linux (RHEL) /社群企業作業系統(Cent)OS)版本6.10 和7.7
- AMP端點版Linux 聯結器 版本 1.11.1

有關與Linux操作系統相容的AMP版本的完整清單，請參閱本文。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

AMP聯結器會掃描機器上的所有活動檔案（那些移動、複製和/或修改自己的檔案），除非明確要求不要， 如果在聯結器處於活動狀態時運行過多的進程和操作，這必然會帶來效能問題，這會導致CPU使用率高、速度減慢，有時還會導致軟體無法運行或運行緩慢。此外，AMP聯結器可能基於檔

案的雲信譽阻止檔案，這有時可能是錯誤的（誤報）。 解決這兩個問題的方法是 這些路徑和進程；如果出現誤報、與效能無關的問題或效能問題似乎無法通過本指南解決，建議提出票證支援。

基本效能問題故障排除流程如下：

- 重現問題時收集調試捆綁包。
- 運行AMP支援工具
- 檢視相關檔案
- 根據需要新增排除項

疑難排解

如何收集調試捆綁包

調試捆綁包是包含聯結器上詳細調試資訊（如掃描日誌）的zip檔案。此捆綁包對於解決與面向終端的AMP聯結器相關的大多數問題至關重要。要收集調試捆綁包，請按照從面向終端的AMP Linux聯結器收集診斷資料中提供的步驟操作。

Amp支援工具收集哪些資訊，然後運行調試捆綁包？

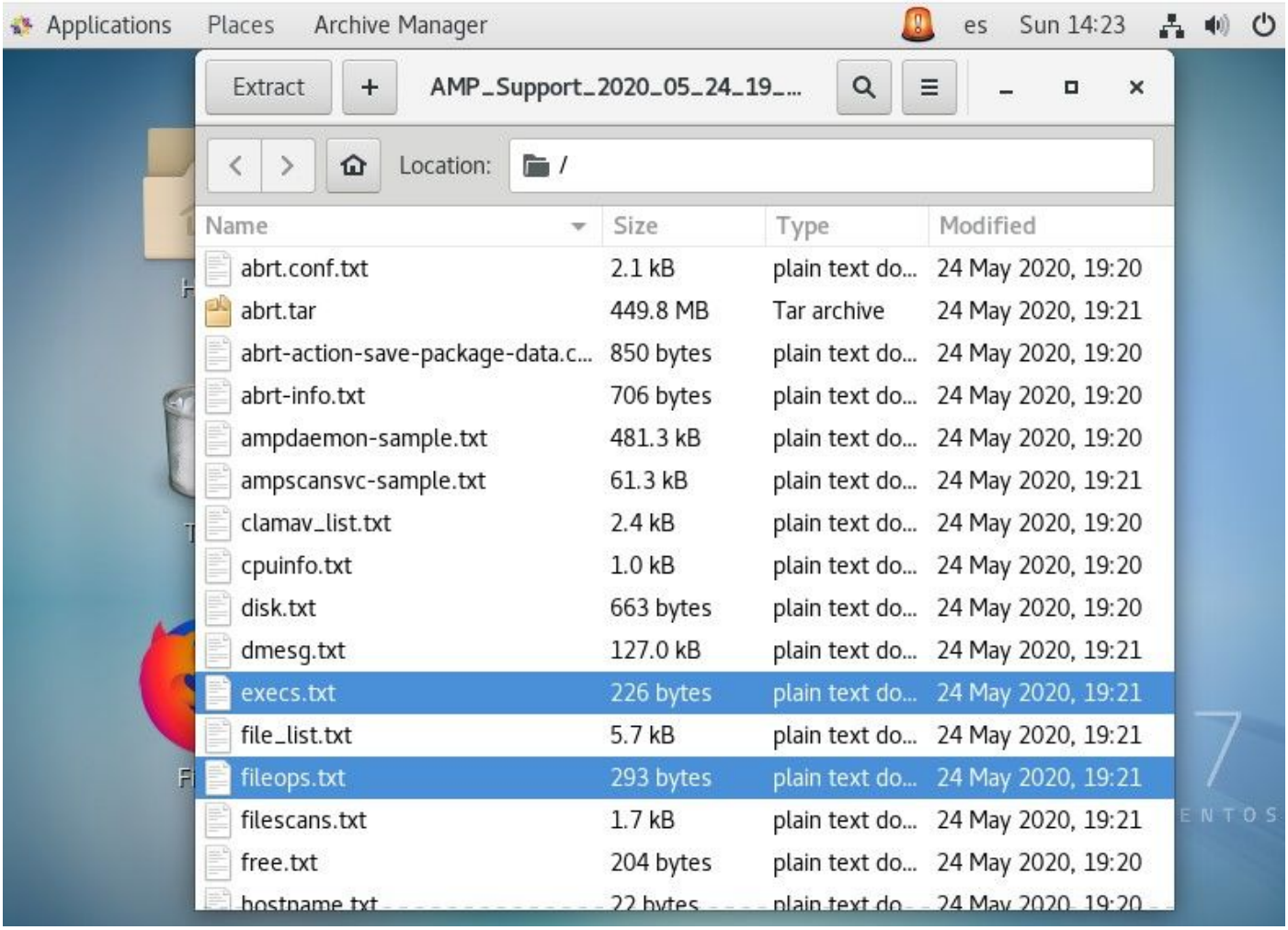
調試捆綁包流程輸入顯示 *ampsupport會運行一些log-collection命令，如下圖所示。*

```
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
```

如何讀取基本的Linux捆綁包日誌以確定受影響的路徑和進程

Linux AMP for Endpoints調試捆綁包攜帶 答 多胸蝶屬 但是，根據有用的資訊，要進行基本效能故障排除，只有幾個檔案需要檢視：fileops.txt、fiescans.txt和execs.txt，如下圖所示。



檔案操作（檔案）文本檔案用作主要的效能故障排除工具。它列出了聯結器運行時端點上的所有當前活動操作。如果認為必要/安全，則這些路徑將新增到策略排除集。


```
      1 /root/.ampcli
      1 /opt/cisco/amp/etc/policy.xml
      1 /home/juanc2/.mozilla/firefox/4b2x9omb.default/storage/permanent/chrome/idb/
3870112724rsegmnoittet-es.sqlite
      1 /home/juanc2/.mozilla/firefox/4b2x9omb.default/storage/permanent/chrome/idb/
1657114595AmcateirvtiSty.sqlite
```

內容如下：

- <運行捆綁包收集過程時對路徑執行的掃描次數> /<掃描的路徑>

掃描示例：

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

檔案掃描（檔案掃描）文本檔案列出在聯結器收集調試資訊時運行的所有進程。

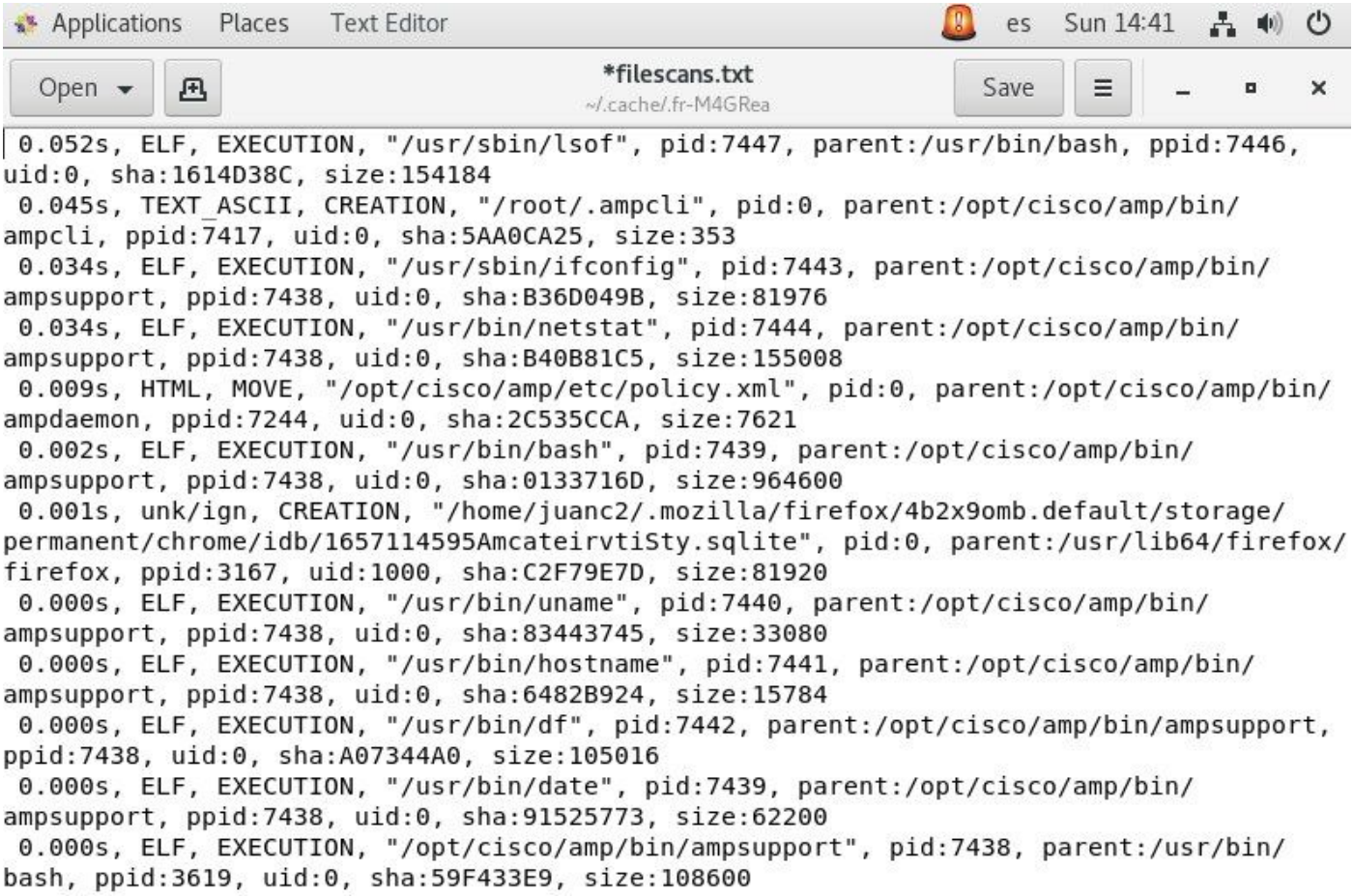

```
      1 /usr/sbin/lsof
      1 /usr/sbin/ifconfig
      1 /usr/bin/uname
      1 /usr/bin/netstat
      1 /usr/bin/hostname
      1 /usr/bin/df
      1 /usr/bin/date
      1 /usr/bin/bash
      1 /opt/cisco/amp/bin/ampsupport
```

其內容如下：

- <執行時間>、<檔案型別>、<操作型別>、<進程路徑>、<父進程路徑>、<進程ID>、<父進程ID>、<SHA簽名（非SHA256）> <檔案大小>

檔案執行(execs)文本檔案列出聯結器收集捆綁包時活動進程使用的所有Linux命令。

> **警告**：此處列出的路徑不能排除在AMP策略中，因為它們是所有進程使用的二進位制檔案(/bin)和系統二進位制檔案(/sbin)，但是，在嘗試瞭解目標電腦上運行的不同進程執行了哪些操作時，此清單可能會非常有用。



識別後，將通過策略排除路徑，請遵循適用於終端排除的AMP的最佳實踐。

Mac和Linux聯結器所處理的進程排除項同樣通過策略新增，但方法略有不同：MacOS和Linux中的進程排除項。

新增排除後，如果問題仍然存在，請進行測試和監控。聯絡AMP TAC支援。