面向终端的AMP Linux连接器基本故障排除指南

目录

简介

本文档介绍排除性能问题的基本方法 在 思科高级恶意软件防护 (AMP) 对于 终端Linux连接器。

先决条件

要求

Cisco 建议您了解以下主题：

- 面向终端的 AMP
- Linux/Unix基于的操作系统

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Red Hat Enterprise Linux (RHEL) /社区企业操作系统（美分）OS)版本6.10 和7.7
- 面向终端的AMP Linux 连接器 version 1.11.1

有关与Linux操作系统兼容的AMP版本的完整列表，请参[阅本文](#)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

AMP连接器扫描计算机上的所有活动文件（移动、复制和/或修改自己的文件），除非明确要求不要， 如果连接器处于活动状态时运行了太多进程和操作，势必会带来性能问题，这会导致CPU利用率高、速度慢，在某些情况下，还会导致软件无法运行或运行缓慢。此外，AMP连接器可能会根据其云信誉阻止文件，这有时可能是错误的（误报）。 解决这两个问题的方法是排除 这些路径和流程；如果误报、非性能相关问题或性能问题似乎无法通过本指南解决，建议提高票证支持。

排除基本性能问题的流程如下：

- 在重现问题时收集调试捆绑包。
- 运行AMP支持工具
- 查看相关文件
- 根据需要添加排除项

故障排除

如何收集调试捆绑包

调试捆绑包是包含连接器上的详细调试信息（如扫描日志）的zip文件。此捆绑包对于解决与面向终端的AMP连接器相关的大多数问题至关重要。要收集调试捆绑包，请按照从面向终端的AMP的终端Linux连接器收集诊断数据上提供的步骤操作。

运行调试捆绑包后，amp支持工具会收集什么信息？

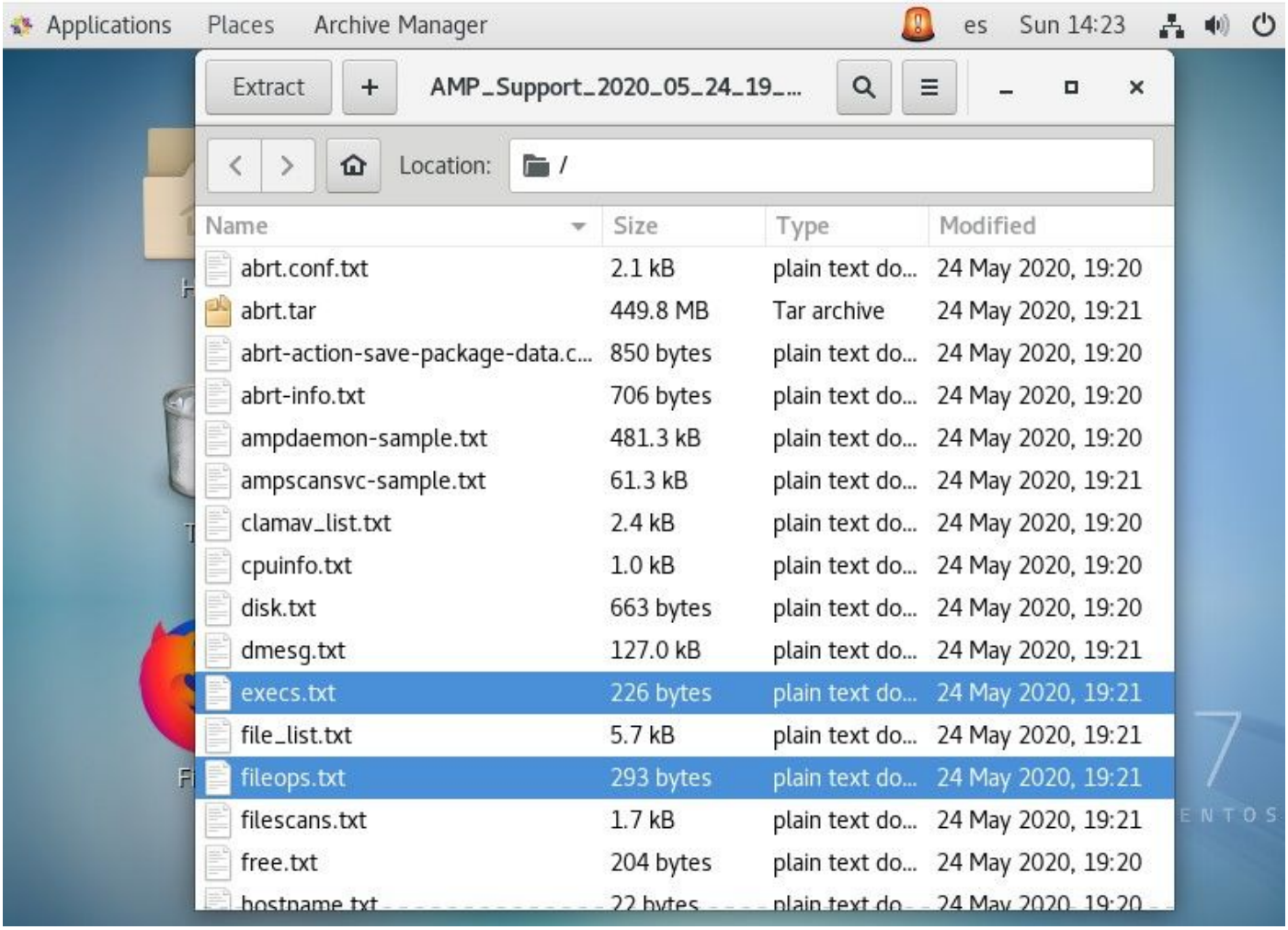
调试捆绑进程输入显示 *ampsupport运行一些log-collection命令，如图所示。*

```
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
```

如何读取基本Linux捆绑包日志以识别受影响的路径和进程

面向终端的Linux AMP调试捆绑包承载 a 太多 但是，为了进行基本性能故障排除，只有几个文件需要查看，如图所示，fileops.txt、fiescans.txt和execs.txt。



文件操作（文件操作）文本文件用作主要的性能故障排除工具。它列出连接器运行时终端上当前所有活动操作。这些路径可添加到策略排除集（如果认为必要/安全）。


```
      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
```

如下所示：

- <捆绑包收集进程运行时对路径执行的数量扫描> /<路径扫描>

扫描示例：

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

文件扫描(filescan)文本文件列出连接器收集调试信息时运行的所有进程。

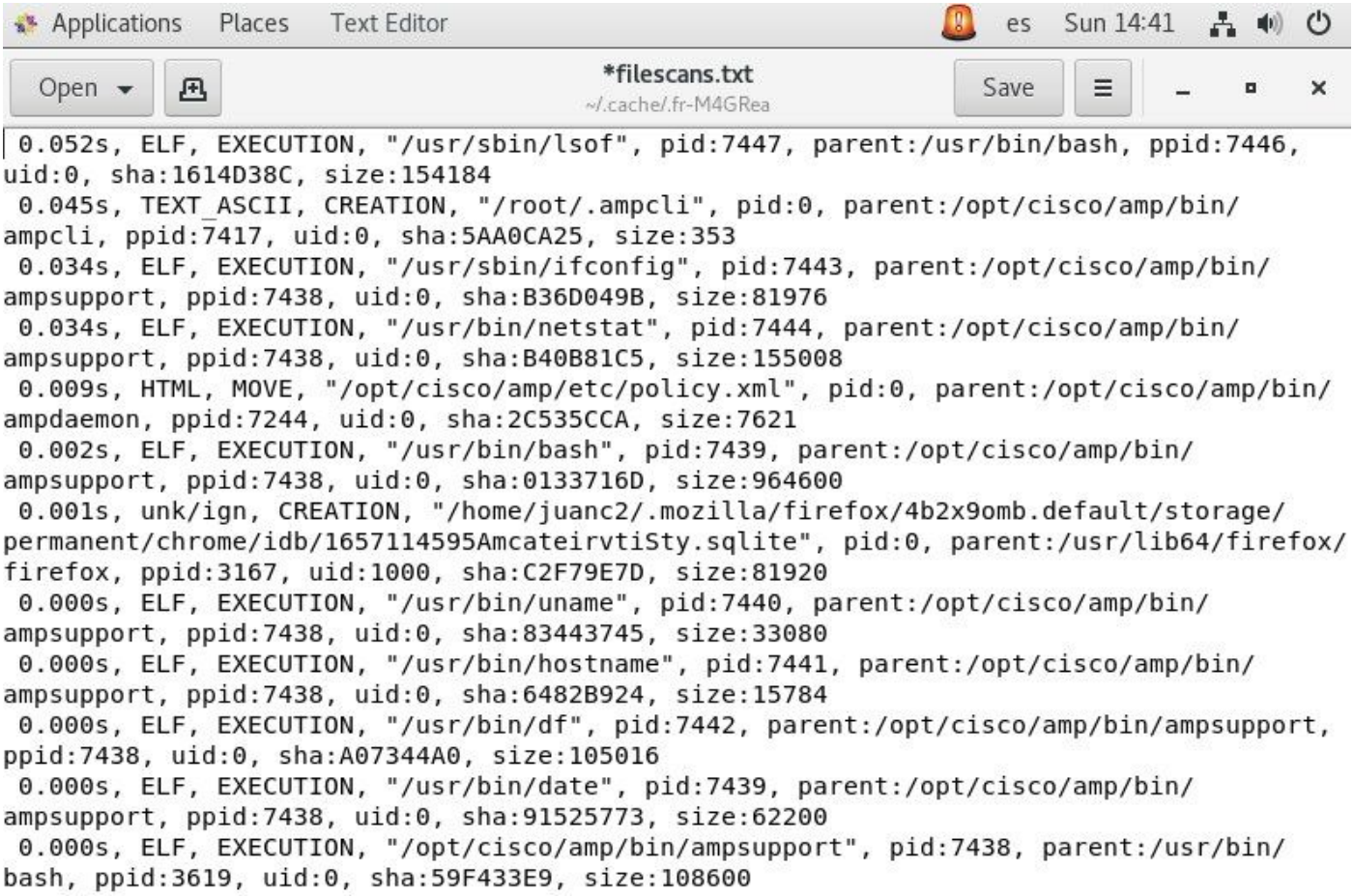

```
      1 /usr/sbin/lsof
      1 /usr/sbin/ifconfig
      1 /usr/bin/uname
      1 /usr/bin/netstat
      1 /usr/bin/hostname
      1 /usr/bin/df
      1 /usr/bin/date
      1 /usr/bin/bash
      1 /opt/cisco/amp/bin/ampsupport
```

它读起来如下：

- <执行时间> 、 <文件类型> 、 <操作类型> 、 <进程路径> 、 <父进程路径> 、 <进程ID> 、 <父进程ID> 、 <SHA签名（非SHA256）> <文件大小>

文件执行(execs)文本文件列出连接器上活动进程收集捆绑包时使用的所有Linux命令。

> 警告:此处列出的路径不能排除在AMP策略中，因为这些是所有进程都使用的二进制文件(/bin)和系统二进制文件(/sbin)，但是，此列表可能有助于尝试了解目标计算机上运行的不同进程执行哪些操作。



一旦确定，路径将通过策略排除，请遵循适用于终端排除的AMP的最佳实践。

Mac和Linux连接器处理的进程例外项也通过策略添加，但方法略有不同： macOS和Linux中的 Process Exclusions。

添加排除项后，测试并监控问题是否仍然存在。联系AMP TAC支持。