エンドポイント用AMPの基本的なトラブルシューティングガイドLinuxコネクタ

内容

概要

このドキュメントでは、パフォーマンスの問題をトラブルシューティングする基本的な方法について説明します 日付： Cisco Advanced Malware Protection (AMP) を参照 エンドポイント Linuxコネクタ.

前提条件

要件

次の項目に関する知識があることが推奨されます。

- AMP for Endpoints
- Linux/Unix – ベースのオペレーティングシステム

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Red Hat Enterprise Linux (RHEL) /コミュニティエンタープライズオペレーティングシステム(Cent)OS)バージョン6.10 および7.7
- AMP For Endpoints Linux コネクタ version 1.11.1

Linux OSと互換性のあるAMPバージョンの完全なリストについては、この記事を参照してください。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

AMPコネクタは、明示的に指示されていない限り、マシン上のすべてのアクティブなファイル（移動、コピー、または修正を行うファイル）をスキャンします。 コネクタがアクティブな状態で実行するプロセスや操作が多すぎると、パフォーマンスの問題が発生し、CPUの使用率が高くなり、速度が低下したり、ソフトウェアが低速になったりする場合があります。さらに、AMPコネクタはクラウドのレピュテーションに基づいてファイルをブロックする可能性があります。これは誤っている（誤検出）可能性があります。 両方の問題の解決策は、 これらのパスとプロセスを示します このガイドでは解決できないような誤検出、パフォーマンスに関連しない問題、またはパフォーマンスの問題の場合は、チケットのサポートを増やすことを推奨します。

基本的なパフォーマンス問題のトラブルシューティングの流れは次のとおりです。

- 問題の再現中にデバッグバンドルを収集します。
- AMPサポートツールの実行
- 関連ファイルを確認します
- 必要に応じて除外を追加

トラブルシュート

デバッグバンドルの収集方法

デバッグバンドルは、コネクタ上の詳細なデバッグ情報（スキャンログなど）を含むzipファイルです。このバンドルは、AMP for Endpointsコネクタに関連するほとんどの問題のトラブルシューティングに不可欠です。デバッグバンドルを収集するには、「AMP for Endpoints Linux Connectorからの診断データの収集」に記載されている手順に従ってください。

ampサポートツールが収集した情報のうち、デバッグバンドルが実行されているのはどれですか。

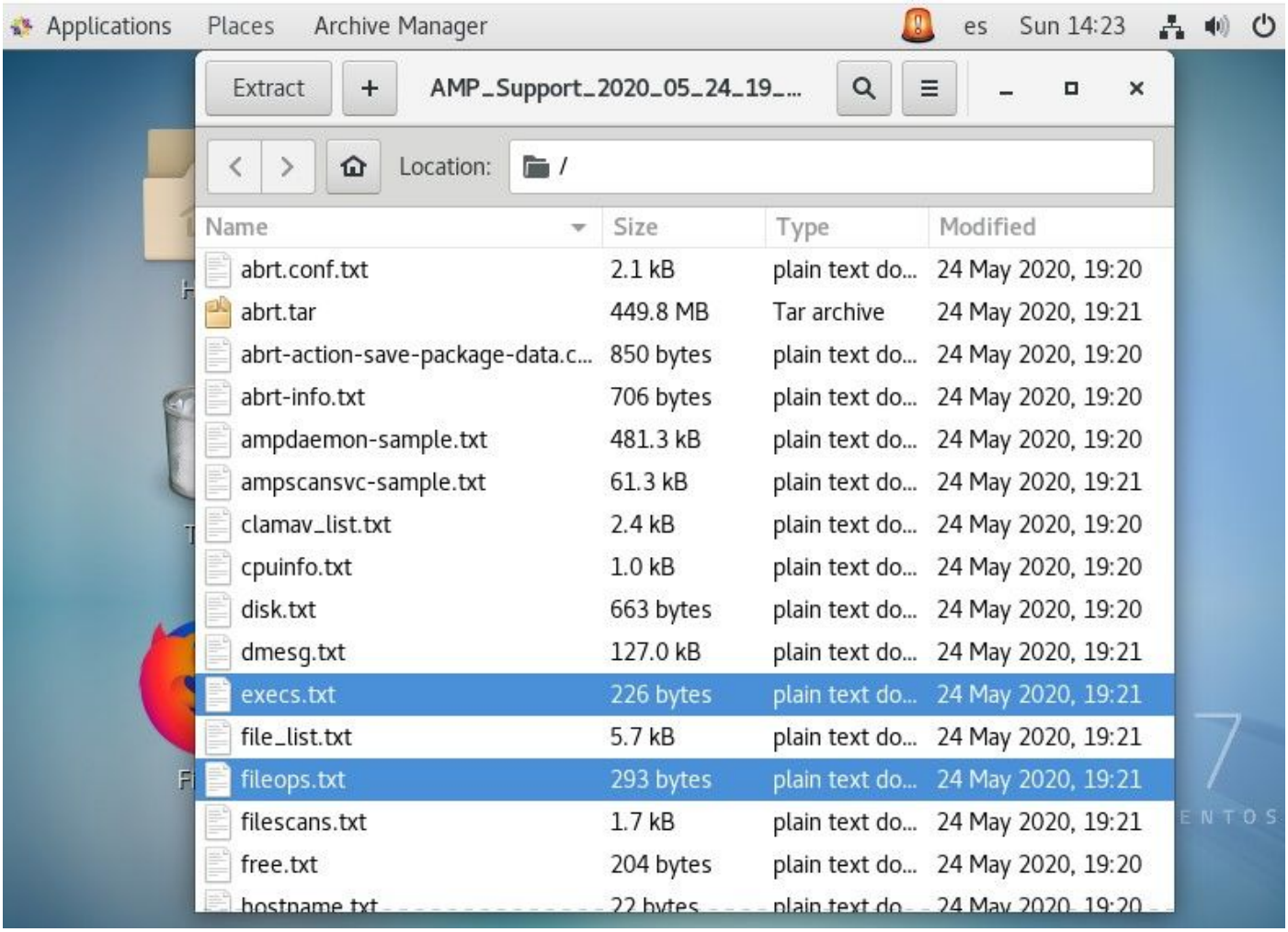
debug bundle processの入力は、 *ampsupportは、図に示すように、いくつかのlog-collectionコマンドを実行します。*

```
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
```

基本的なLinuxバンドルログを読み、影響を受けるパスとプロセスを特定する方法

エンドポイント向けLinux AMPデバッグバンドルは、 a 胸膜 ただし、基本的なパフォーマンスのトラブルシューティングを目的とした有用な情報については、次の図に示すように、確認するファイルは少数です。fileops.txt、fiescans.txt、およびexecs.txt。



ファイル操作(fileops)テキストファイルは、主なパフォーマンストラブルシューティングツールとして機能します。コネクタの実行中に、エンドポイント上で現在アクティブな操作がすべて一覧表示されます。これらは、必要/安全と判断された場合にポリシー除外セットに追加するパスです。

次のように読まれます。

- <バンドル収集プロセスの実行中に実行されたパスに対して実行されたスキャン数> /<スキャンされたパス>

スキャンの例：

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

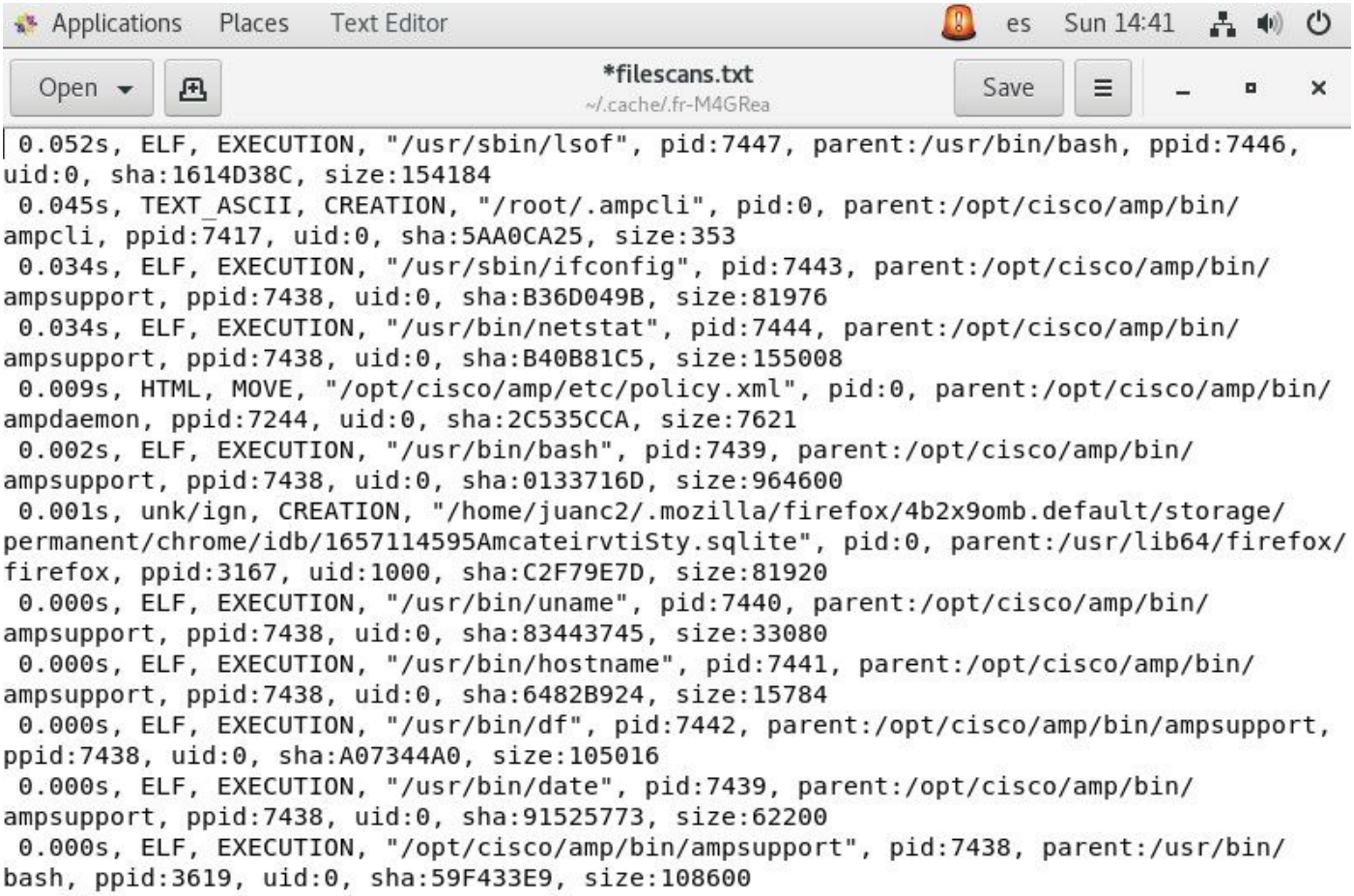
File Scans (filescan)テキストファイルには、コネクタがデバッグ情報を収集している間に実行したすべてのプロセスがリストされます。

次のように表示されます。

- <Execution time> 、 <File Type> 、 <Operation type> 、 <Process path> 、 <Parent process path> 、 <Process ID> 、 <Parent Process ID> 、 <SHA signature (Not SHA256)> <File Size>

File Execution(execs)テキストファイルには、コネクタがバンドルを収集している間に、コネクタ上のアクティブなプロセスによって使用されるすべてのLinuxコマンドがリストされます。

> **警告**：ここに示すパスは、すべてのプロセスが利用するバイナリ(/bin)およびシステムバイナリ(/sbin)であるため、AMPポリシーから除外しないでください。ただし、このリストは、ターゲットマシンで実行される異なるプロセスで実行されるアクションを理解する場合に役立ちます。



特定されたパスはポリシーによって除外されます。エンドポイントの除外に関するAMPのベストプラクティスに従ってください。

MacコネクタとLinuxコネクタで処理されるプロセス除外も同様にポリシーによって追加されますが、方法は少し異なります。MacOSとLinuxでのプロセス除外。

除外が追加されたら、問題が解決しない場合はテストし、モニタします。AMP TACサポートに連絡してください。