

高CPUのmacOS AMP診断バンドルの分析

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[トラブルシューティング](#)

[別のウイルス対策がマシンにインストールされているかどうかを確認します](#)

[特定のアプリケーションの使用中にCPUの使用率が高くなっていることを特定する](#)

[分析のための診断バンドルの取得](#)

[エンドポイントのデバッグレベル](#)

[AMPコマンドラインインターフェイス\(CLI\)のデバッグレベル](#)

[ポリシーのデバッグレベル](#)

[他のアンチウイルスソリューションからAMPを除外する](#)

[問題を再現し、診断バンドルを収集する](#)

[高いCPUパフォーマンスの分析](#)

[関連情報](#)

概要

このドキュメントでは、macOSデバイスのエンドポイントのパブリッククラウド向けAdvanced Malware Protection(AMP)から診断バンドルを分析し、高いCPU使用率をトラブルシューティングする手順について説明します。

著者 : Cisco TACエンジニア、Uriel Torres、編集 : Yeraldin Sanchez

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コンソールでの基本的なナビゲーション
- MAC端末のナビゲーション

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。

- AMP for Endpointsコンソール5.4.20200512
- macOS Catalinaバージョン10.15.4

- AMPコネクタ1.12.3.738

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 Connectorは、明示的に指示されない限り、マシン上のすべてのアクティブなファイル（移動、コピー、変更するファイル）をスキャンします。これは、Connectorの実行中に実行され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場合があります、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除外することです。

トラブルシューティングのパフォーマンスの問題のフローを図に示します。



トラブルシュート

このセクションでは、設定のトラブルシューティングに役立つ情報を説明します。

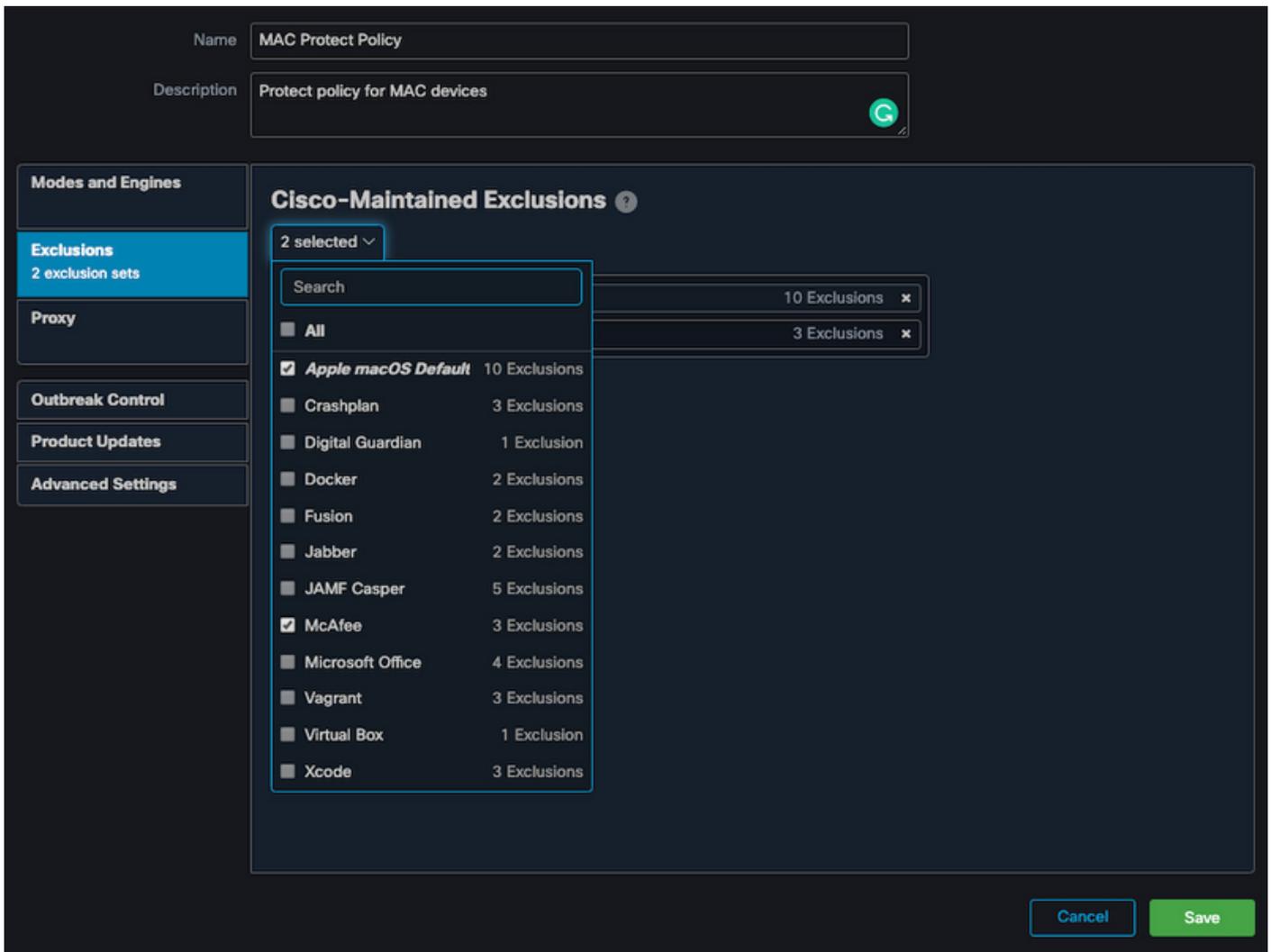
別のウイルス対策がマシンにインストールされているかどうかを確認します

ヒント：使用されているソフトウェアがリストに含まれている場合は、シスコが管理する除外項目を使用してください。これらの除外項目は、アプリケーションの新しいバージョンに追加できます。

AMPコンソールの[Cisco maintained exclusions]セクションで使用可能なリストを表示するには、次の手順を実行します。

- [Management] > [Policies] に移動します。
- ポリシーを検索し、[Edit]をクリックします。
- ポリシーの[設定]ウィンドウで、[除外]をクリックします。

図に示すように、現在マシンにインストールされているソフトウェアに従ってエンドポイントに必要なものを選択し、ポリシーを保存します。



特定のアプリケーションの使用中にCPUの使用率が高くなっていることを特定する

潜在的な除外の特定に役立つ問題を複製できる場合は、1つのアプリケーションまたはいくつかの実行されている間に問題が発生したかどうかを特定します。

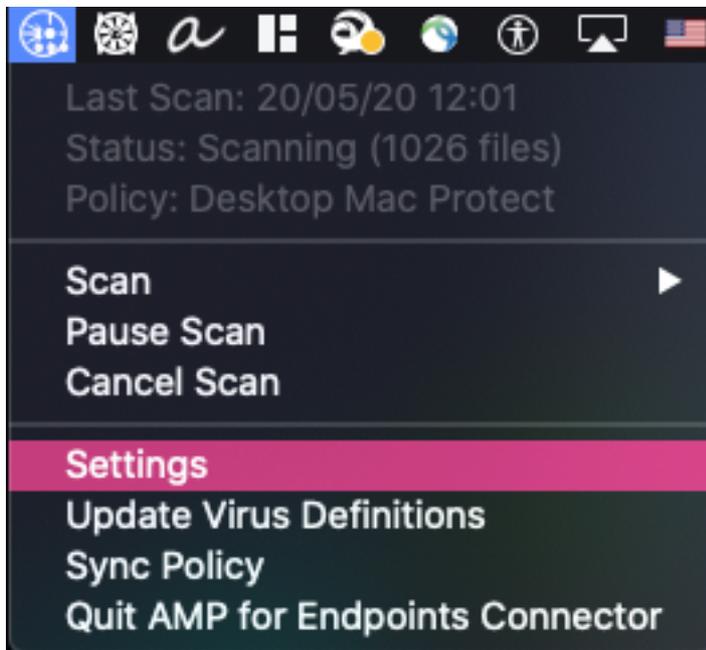
分析のための診断バンドルの取得

有用な診断バンドルを収集するには、デバッグログレベルを有効にする必要があります。

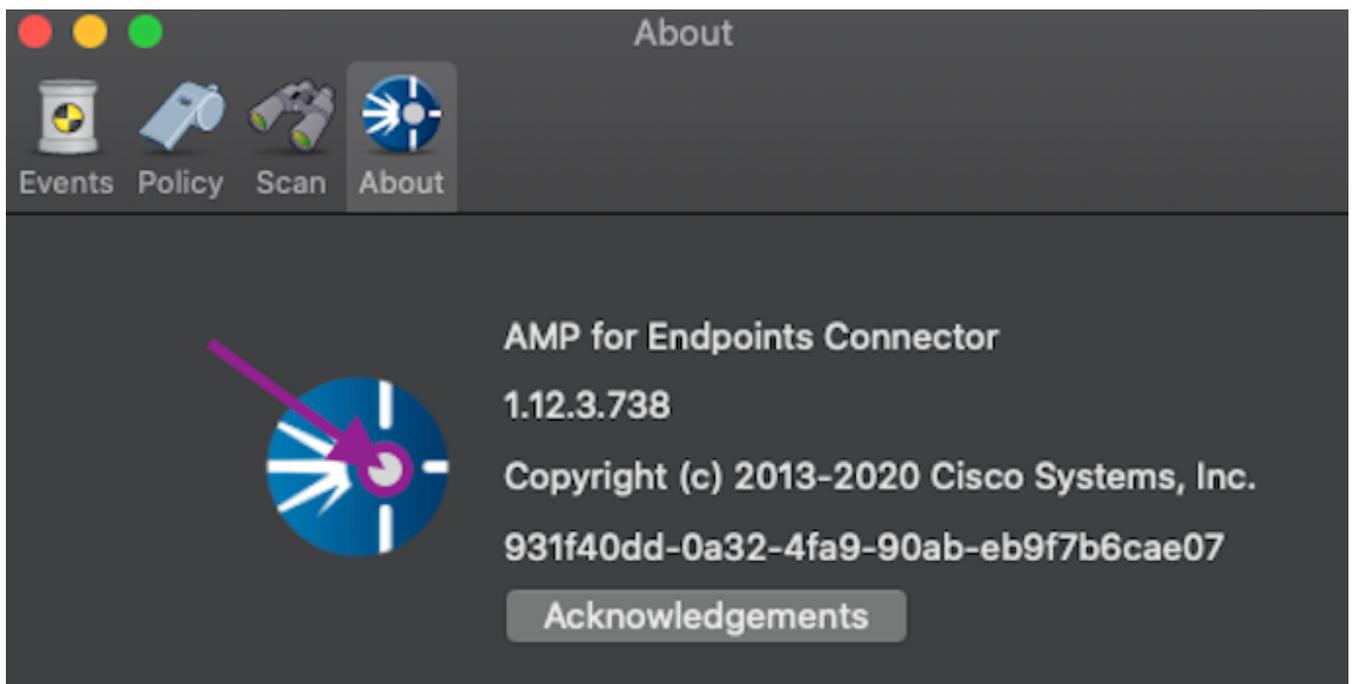
エンドポイントのデバッグレベル

問題を複製してエンドポイントにアクセスできる場合は、診断バンドルをキャプチャする最良の手順を次に示します。

- MACメニューバーで、[AMP]アイコンをクリックします。
- 図に示すように[設定]セクションに移動します。



- 設定ウィンドウで、[バージョン情報]に移動します。
- デバッグモードを有効にするには、図に示すように、AMPロゴの内側をクリックします。



AMPコネクタがデバッグモードであることを示すポップアップ

次のポリシーハートビート間隔まで、デバッグログレベルを有効にします。

AMPコマンドラインインターフェイス(CLI)のデバッグレベル

- ターミナルを開く
- `/opt/cisco/amp/bin/`に移動します。
- `ampcli`を実行します。
`./ampcli`
- AMP CLIでデバッグモードを有効にします。
`ampcli>debuglevel 1`

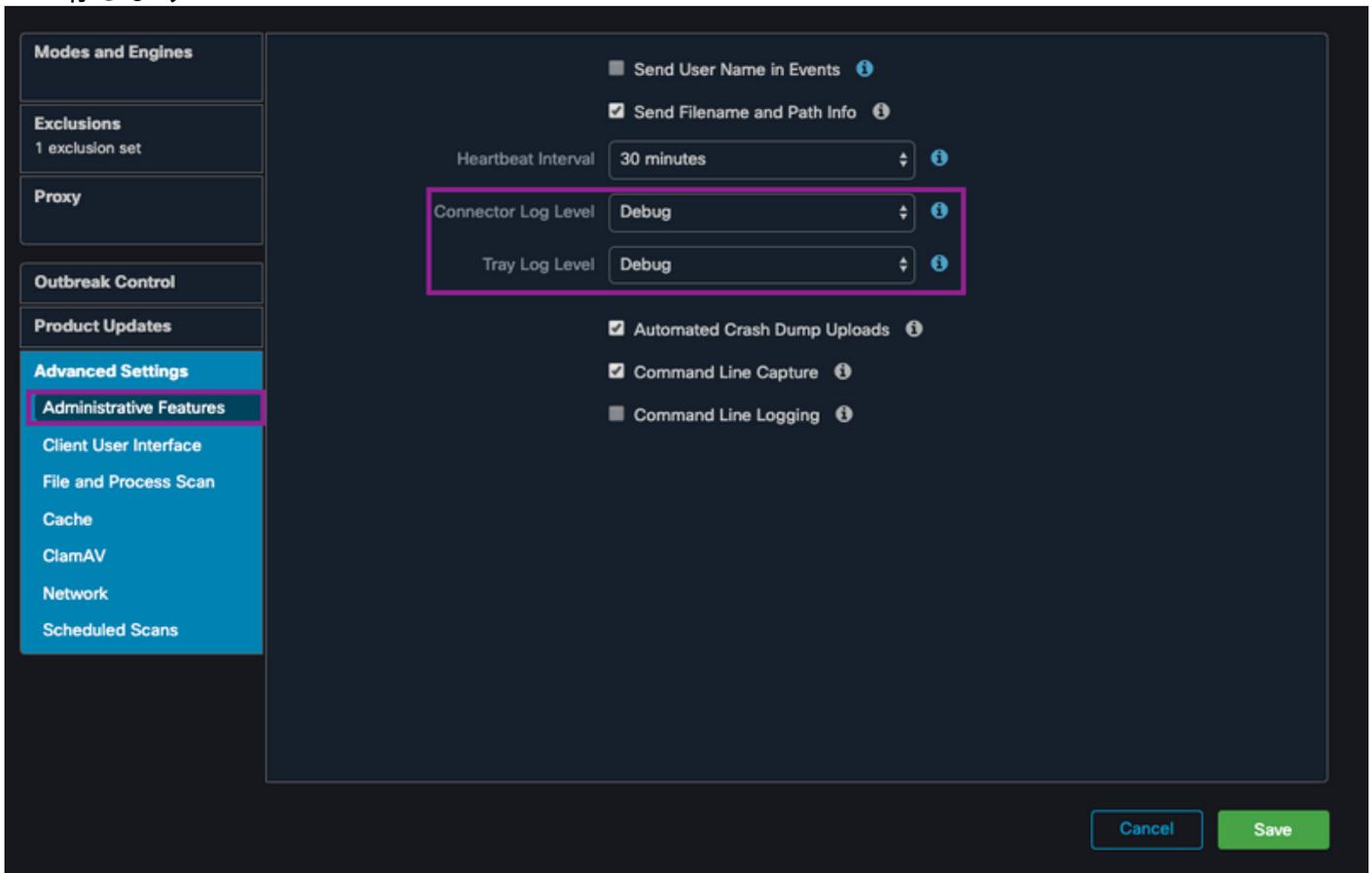
このプロセスは、次のポリシーハートビート間隔までデバッグログレベルを有効にします。

ポリシーのデバッグレベル

エンドポイントにアクセスできないか、問題が一貫して再現されない場合は、ポリシーでデバッグログレベルを有効にする必要があります。

ポリシーでデバッグログレベルを有効にするには、次のコマンドを実行します。

- [Management] > [Policies]に移動します。
- ポリシーを検索し、[Edit]をクリックします
- [Advanced Settings] > [Administrative Features]に移動します。
- 図に示すように、[Connector Log Level]と[Tray Log Level]を[Debug]に設定し、ポリシーを保存します



注意：ポリシーからデバッグモードが有効になっている場合、すべてのエンドポイントがこの設定を受信します。

注：エンドポイントのポリシーを同期して、デバッグモードを確認します。

他のアンチウイルスソリューションからAMPを除外する

ユーザガイドによると、MAC用AMPコネクタと互換性を持たせるには、次のディレクトリとファイル、ディレクトリ、および実行可能ファイルをウイルス対策製品で除外する必要があります。除外するディレクトリは次のとおりです。

- /Library/Application Support/Cisco/AMP for Endpoints Connector
- /opt/cisco/amp

問題を再現し、診断バンドルを収集する

デバッグレベルを設定したら、システムでHigh CPUの状態が発生するまで待つか、以前に特定した条件を手動で再現してから、診断バンドルを収集します。

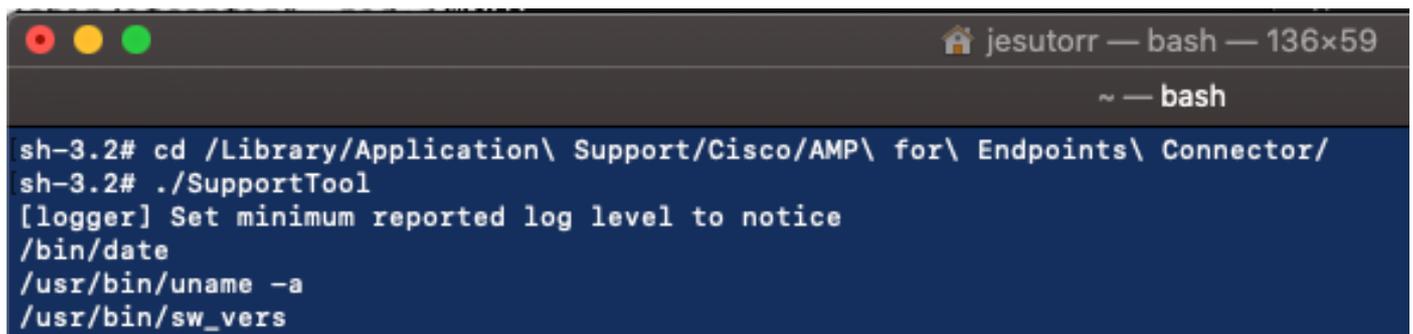
デバッグバンドルを収集するには、次の手順を実行します。

- ターミナルを開きます。
- スーパーユーザレベルにアクセスし、[/Library/Application Support/Cisco/AMP for Endpoints Connector]に移動します。

```
cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
```

- サポートツールを実行するには、次のコマンドを使用します。

```
./SupportTool
```



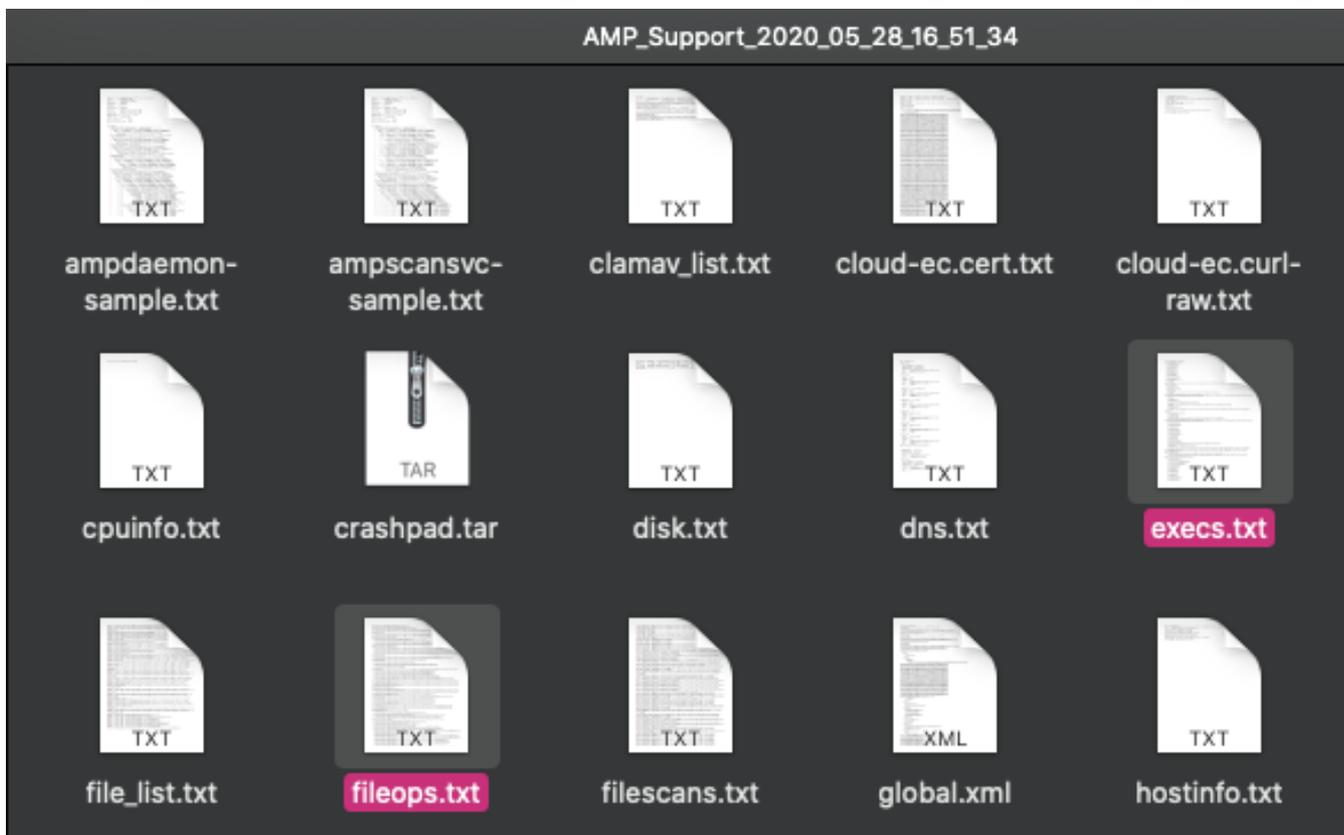
```
jesutorr — bash — 136x59
~ — bash
sh-3.2# cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
sh-3.2# ./SupportTool
[logger] Set minimum reported log level to notice
/bin/date
/usr/bin/uname -a
/usr/bin/sw_vers
```

デバッグバンドルは、.zipファイル拡張子としてDesktopフォルダに保存されます。

高いCPUパフォーマンスの分析

デバッグ診断バンドルは、分析を開始するためにデスクトップに保存されています。

- 診断バンドルの圧縮解除
- 確認するファイルは2つあります ファイル操作 : fileops.txtファイルの実行 : execs.txt



- fileops.txtは、トラブルシューティングの主要なパフォーマンスツールとして機能します。コネクタの実行中に、エンドポイントで現在有効な操作がすべて一覧表示されます。次のように読み取られます。

<バンドルが収集されたときにパスで実行されたスキャン数> / <Path scanned>

```

fileops.txt
19 /Library/Application Support/Apple/ParentalControls/Users/jesutorr/2020/05/21-usage.data
18 /Users/jesutorr/Library/Application Support/Cisco/Unified Communications/Jabber/CSF/Config/dummy.phoneInfo
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyHistoryStats.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/SurveyEventActivityStats.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.Settings.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.GovernedChannelStates.json
17 /Users/jesutorr/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Floodgate/Outlook.CampaignStates.json

```

たとえば、homebrewアプリケーションがある場合、fileops.txtは次のアクティブな操作を示します。

```
639 /Users/jesutorr/Library/Bin/MyApplication/support/
```

```
460 /Users/jesutorr/Library/Bin/MyApplication/logs/
```

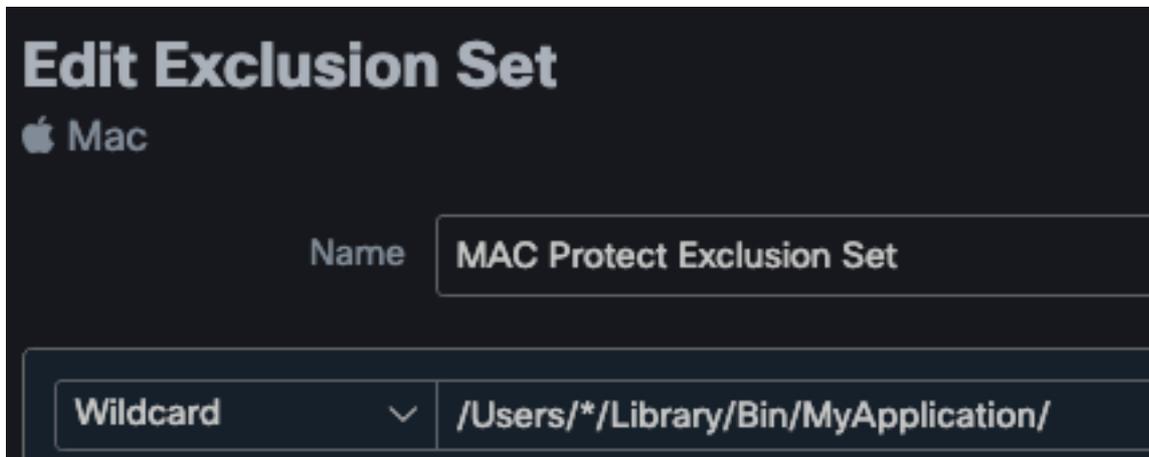
```
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```

```

fileops.txt — Edited
639 /Users/jesutorr/Library/Bin/MyApplication/support/
460 /Users/jesutorr/Library/Bin/MyApplication/logs/
219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/

```

- プロセスが特定されたら、除外を作成できます
- 除外を作成するには、
- AMPコンソールで、[Management] > [Exclusions]に移動します
- 除外セットを選択し、[Edit]をクリックします
- 除外は、図に示すように追加できます



- Execs.txtファイルには、コネクタがバンドルを収集している間に実行されるプロセスで使用されるすべてのコマンドが含まれています。ここに記載されているパスは、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、Execs.txtでは、実行されているメインプロセスを提供できません。

たとえば、Execs.txtファイルに次のログが表示されている場合です。

```
execs.txt — Edited
501 /bin/bash
96 /usr/bin/defaults
91 /usr/bin/stat
91 /usr/bin/tr
90 /usr/bin/cut
```

homebrewアプリケーションはbashを使用するため、アプリケーションが高CPUの原因であることを確認できます。

関連情報

- [エンドポイント向けAMP:macOSおよびLinuxでのプロセス除外](#)
- [AMP for Endpoints 除外対象のベストプラクティス](#)
- [テクニカル サポートとドキュメント – Cisco Systems](#)