セキュアエンドポイントMacコネクタパフォーマンスチューニングガイド

内容

概要

調整が必要な理由

Macエンドポイントでファイルを作成、移動、コピー、または実行するたびに、そのファイルのイベントがオペレーティングシステムからセキュアエンドポイントMacコネクタに送信されます。このイベントにより、そのファイルがコネクタによって分析されます。通常、分析プロセスには、問題のファイルをハッシュし、コンピュータとクラウドの両方で異なる分析エンジンを介してファイルを実行することが含まれます。このハッシュ処理はCPUサイクルを消費することを認識することが重要です。

特定のエンドポイントで実行されるファイル操作と実行が多いほど、コネクタがハッシュ処理に必要とするCPUサイクルとI/Oリソースが多くなります。オーバーヘッドを減らすために、コネクタに追加された機能がいくつかあります。たとえば、作成、移動、またはコピーされたファイルが以前に解析された場合、コネクタはキャッシュされた結果を使用します。ただし、セキュリティが最も重要な実行などのイベントの場合、すべてのイベントは常にコネクタによって完全に分析されます。つまり、子プロセスの複数の繰り返し実行を伝播するアプリケーションやプロセスは、特に短期間でパフォーマンスの問題を引き起こす可能性があります。1秒に1回の割合で繰り返し子プロセスを実行するアプリケーションを見つけて除外すると、CPU使用率が大幅に低下し、ラップトップのバッテリ寿命が向上します。

createやmoveなどのファイル操作は、通常は実行ほど影響を受けませんが、過剰なファイル書き込みや一時ファイルの作成は、同様の問題を引き起こす可能性があります。ログファイルに頻繁に書き込むアプリケーション、または複数の一時ファイルを生成するアプリケーションは、Secure Endpointが不要な分析で大量のCPUサイクルを消費し、Secure Endpointバックエンドに大きなノイズを発生させる可能性があります。正当なアプリケーションのノイズの多い部分を区別することは、生産性が高く安全なエンドポイントを維持するための非常に重要なステップです。

このドキュメントの目的は、ファイル操作（作成、移動、およびコピー）を区別し、実行を実行することで、デーモンのパフォーマンスとCPUサイクルの浪費に悪影響を及ぼすことです。これらのファイルおよびディレクトリパスを特定すると、組織に適した除外セットを作成および維持できます。

事前作成された除外リストをポリシーに追加して、シスコが保持する除外リストを保持することで、セキュアエンドポイントコネクタとウイルス対策、セキュリティ、またはその他のソフトウ

ェアとの互換性を向上させることができます。これらのリストは、コンソールの[Exclusions]ページで[Cisco-Maintained Exclusions]として使用できます。

チューニングのタイプ

除外チューニングオプションには、次の3種類があります。

1. インストール前の調整:**これは、セキュアエンドポイントMacコネクタをインストールする前に実行できます。**マシンで最も混雑しているアプリケーションとパスを最もクリーンに見ることができます。しかし、これは非常にノイズの多いプロセスであり、ユーザは独自に公平な分析と集約を行う必要があります。
2. **サポートツールの調整**:これはMacコネクタのインストール後に行うことができ、追加のバイナリなしで任意のエンドポイントで実行できます。限定的なルックバックを行い、面倒なアプリケーションを特定するのに最適です。
3. **Procmon Tuning**:このプロセスでは、コネクタをインストールする必要がありますが、Procmonバイナリを使用する必要があります。これはカスタムチューニングツールです。これは、基本的により高度なサポートツールチューニング機能です。この方法では、最大量の設定が必要です。ただし、最適な結果が得られます。

1.インストール前の調整

インストール前の調整はチューニングの最も基本的な形式で、主にターミナルセッションのコマンドラインを使用して行われます。

OS X El Capitanの新しいmacの場合は、起動時に回復モード(command-r)を起動し、dtraceの保護を無効にする必要があります。

```
csrutil enable --without dtrace
```

最も一般的なファイル実行を調べるには、次のコマンドを実行します。

```
$ sudo newproc.d | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

これは通常、繰り返し実行されているアプリケーションを示します。多くのプロビジョニングアプリケーションは、会社のソフトウェアポリシーを維持するために、スクリプトを実行するか、バイナリを短い間隔で実行します。1秒に1回より大きいレートで実行されているアプリケーション、または短いバーストで複数回実行されているアプリケーションは、除外の良い候補と見なされます。

最も一般的なファイル操作を調べるには、次のコマンドを実行します。

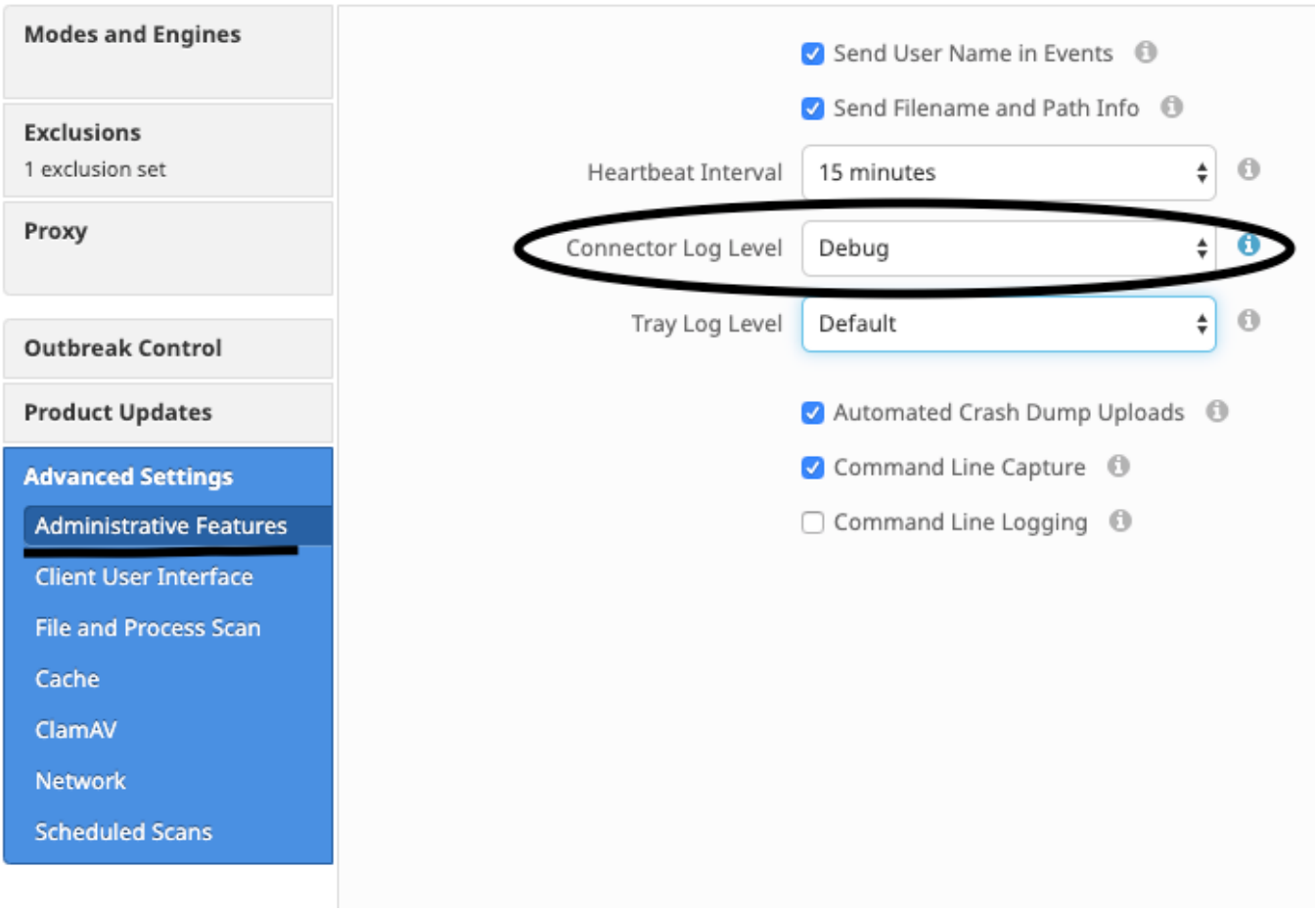
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

ほとんどのファイルに書き込まれているファイルがすぐに表示されます。多くの場合、これはアプリケーションの実行、バックアップソフトウェアのコピーファイル、または一時ファイルを書き込む電子メールアプリケーションによって書き込まれるログファイルです。これに加えて、ログファイル拡張子にlogまたはjournalを持つものは、適切な除外候補と見なすべきであるという目安が適切です。

2.サポートツール 調整

デバッグロギングの有効化

コネクタのデーモンは、ファイルのチューニングをサポートする前に、デバッグログモードにする必要があります。この操作は、[*Management] -> [Policies*]でコネクタのポリシー設定を使用して、セキュアエンドポイントコンソールで行います。ポリシーを選択し、ポリシーを編集し、[詳細設定]サイドバーの下の*[管理*機能]セクションに*移動*します。コネクタの[ログ*レベル]の設定を*[デバッグ]に**変更します**。



次、 ポリシーを保存します。 ポリシーが保存されたら、、 同期されていることを確認します陳腐な cコネクタ c接続 このモードでは 少なくとも 続行する15 ~ 20分前 その他のチューニング.

注： チューニングが完了したら、 忘れる 変更 *コネクタログレベル* 設定に戻る **デフォルト** したがって c接続 実行 イン its 最も効率的で 有効モード。

サポートツールの実行

この方法では、サポートツール（セキュアエンドポイントMacコネクタがインストールされたアプリケーション）を使用します。Applicationsフォルダからアクセスするには、/Applications->Cisco Secure Endpoint->Support Tool.appをダブルクリックします。これにより、追加の診断ファイルを含む完全なサポートパッケージが生成されます。

1 つの 代替、 迅速に、 メソッドを実行する 次のコマンドライン 変更前 a 端末 session:

```
sudo/Library/Application Support/Cisco/AMP for Endpoints/SupportTool-x
```
これにより、関連するチューニングファイルのみを含むサポートファイルが大幅に小さくなります。

どちらの方法で実行するかを選択すると、サポートツールは次の2つのチューニングサポートファイルを含むzipファイルをデスクトップに生成します。fileops.txtおよびexecs.txtfileops.txtには、マシン上で最も頻繁に作成および変更されたファイルのリストが含まれています。execs.txtには、最も頻繁に実行されるファイルのリストが含まれます。両方のリストはスキャン数でソートされます。つまり、最も頻繁にスキャンされるパスがリストの先頭に表示されます。

コネクタをデバッグモードで15 ~ 20分間実行し、サポートツールを実行します。一般的に、その間に平均1000ヒット以上のファイルまたはパスが除外される候補であるのが適切です。

パス、ワイルドカード、ファイル名、およびファイル拡張子の除外の作成

パス除外ルールを使用する方法の1つは、filops.txtから最も頻繁にスキャンされるファイルおよびフォルダパスを見つけ、それらのパスの除外ルールを作成することを検討することです。ポリシーがダウンロードされたら、新しいCPU使用率を監視します。CPU使用率の低下に気付く前に、ポリシーが更新されてから5 ~ 10分後に、デーモンが追いつくのに時間がかかることがあります。それでも問題が発生する場合は、ツールを再度実行して、どの新しいパスが観察されるかを確認します。

- 良い目安は、ログファイル拡張子logまたはjournalを持つファイルは、適切な除外候補と見なされる必要があることです。

プロセス除外の作成

NOTE: Process Exclusions on Mac can only be implemented for Mach-O files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts) or .app (Application Bundles).
プロセス除外に関するベストプラクティスについては、次を参照してください。セキュアエンドポイント：macOSおよびLinuxでのプロセス除外

適切な調整パターンは、まずexecs.txtから大量の実行を持つプロセスを特定し、実行可能ファイルへのパスを見つけ、このパスの除外を作成することです。ただし、次のようなプロセスは含めないでください。

- 汎用ユーティリティプログラム：汎用ユーティリティプログラムを除外することは推奨されません(例：usr/bin/grep)を使用します。 ユーザは、プロセスを呼び出しているアプリケーション(例：grepを実行している親プロセスを検索し、親プロセスを除外します。これは、親プロセスを安全にプロセスの除外にできる場合にのみ行う必要があります。親の除外が子に適用される場合、親プロセスからのすべての子へのコールも除外されます。プロセスを実行しているユーザを確認できます。（例：ユーザー"root"によって大量にプロセスが呼び出されている場合、そのプロセスを除外できますが、指定したユーザー'root"に対してのみ許可されます。これにより、Secure Endpointは、"root"以外のユーザーによる特定のプロセスの実行を監視できます)。**注：プロセスの除外は、コネクタバージョン1.11.0以降で新しく追加されました。このため、一般的なユーティリティプログラムは、バージョン1.10.2以前のコネクタではパスの除外として使用できます。ただし、この方法は、パフォーマンスのトレードオフが絶対に必要な場合にのみ推奨されます。**

プロセスの除外では、親プロセスを見つけることが重要です。プロセスの親プロセスまたはユーザーが見つかると、特定のユーザーの除外を作成し、そのプロセス除外を子プロセスに適用できます。子プロセスは、プロセスの除外にできないノイズの多いプロセスを除外します。

親プロセスの識別

1. execs.txtから、大量のプロセス(例：/bin/rm にあります）。
2. サポートパッケージからampdaemon.logを開き、syslog.tarを解凍し、パス/Library/Logs/Cisco/ampdaemon.logに従います(デフォルトのオプションで生成されたサポートパッケージからではなくafullsupportパッケージでのみ利用可能)。
3. 除外するプロセスをampdaemon.logで検索します。プロセス実行を示すログ行を検索します(例：8月19 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]:デーモンRx:VNODE:EXECUTE X:6210 P:3296 PP:3200 U:502 [/bin/rm])。
4. 次のいずれかの方法を使用して、親プロセスを識別します。 除外するプロセスのパスに従う親プロセスパスを特定します(例：[/bin/rm] [*親プロセスのパス*])。ログに親プロセスパスが含まれていない場合は、ログ行のPPンから親プロセスIDを確認します(例：PP:3200)。
5. 親パスまたは親プロセスIDを使用して、手順3と4を繰り返し、現在の親プロセスの親を決定します。親プロセスが特定できない場合、または親プロセスID = 1(例：PP:1)。
6. プロセスツリーが認識されたら、除外する必要がある操作の大部分またはすべてをカバーし、アプリケーションを一意に識別するプログラムパス

を探します。これにより、別のアプリケーションによって実行される操作を意図せずに除外する可能性が最小限に抑えられます。

プロセスのユーザの特定

1. 上の「親プロセスの識別」のステップ1 ~ 3に従います。
2. 次のいずれかの方法を使用して、プロセスのユーザーを識別します。 ログ行のU：から指定されたプロセスのユID検索します(例：U:502)。[ターミナル]ウィンドウから、dsclコマンドを実行`list /Users UniqueID | grep #`、#はユIDです。次のような出力が表示されます：`Username 502`, `Username`は指定されたプロユーザです。
3. このユーザ名を[User]カテゴリのプロセス除外に追加すると、特定のプロセス除外に関して重要な除外の範囲を減らすことができます。 注：プロセスのユーザーがコンピューターのローカルユーザーであり、この除外は異なるローカルユーザーを持つ複数のコンピューターに適用する必要がある場合、プロセスの除外をすべてのユーザーに適用するには、ユーザーカテゴリを空白にしておく必要があります。