エンドポイント用AMPからの診断データの収集 Linuxコネクタ

内容

概要

このドキュメントでは、AMP For Endpoints Linux Connectorから診断ファイルを生成する手順について説明します。Linux Connectorで技術的な問題が発生した場合は、シスコテクニカルサポートエンジニアが診断ファイルで利用可能なログメッセージを分析する必要があります。

診断ファイルの生成

このコマンドを使用すると、Linuxコマンドラインインターフェイス(CLI)から診断ファイルを直接生成できます。

```
/opt/cisco/amp/bin/ampsupport
```

これにより、デスクトップに。7zファイルが作成されます。このファイルをCisco Technical Assistance Center(TAC)に提供して、詳細な分析を行うことができます。

デバッグ モード

コネクタのデバッグモードは、ロギングに詳細な情報を提供します。コネクタの問題をより詳細に把握できます。このセクションでは、コネクタでデバッグモードを有効にする方法について説明します。

> **警告**：デバッグモードは、シスコがこのデータを要求する場合にのみ有効にしてください。デバッグモードを長く有効にすると、ディスク領域を非常に迅速に埋め込むことができ、ファイルサイズが大きすぎるためにサポート診断ファイルがコネクターログを収集するのを防ぐ場合があります。

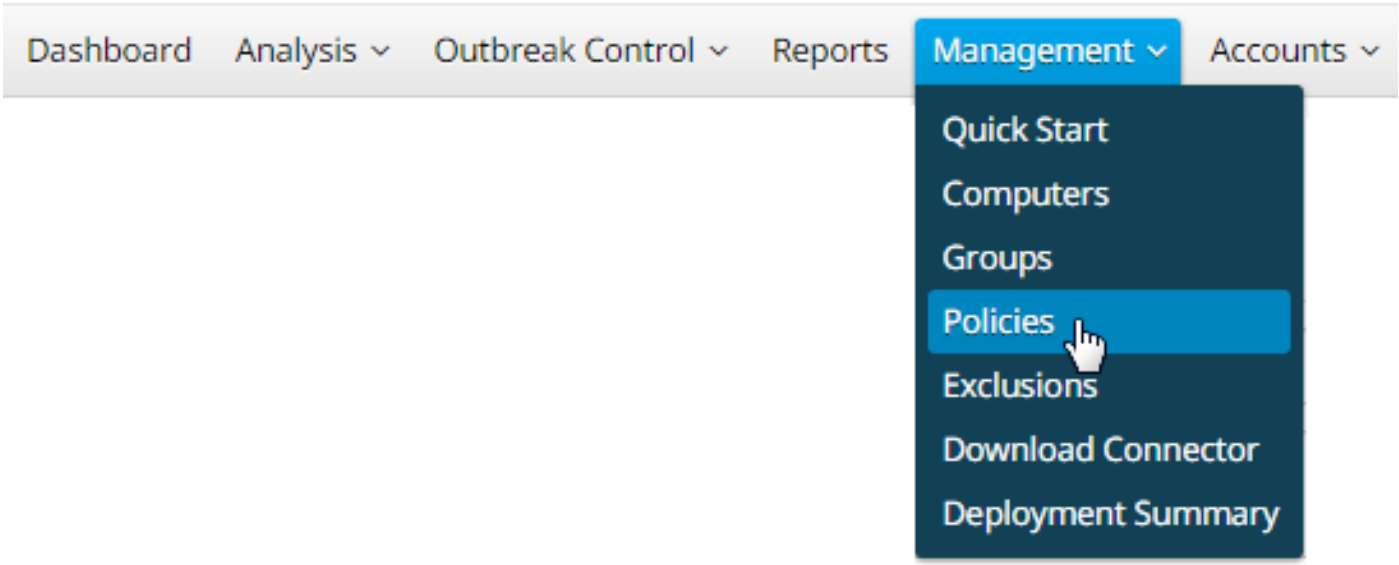
AMPコンソールの使用

デバッグ モードの有効化

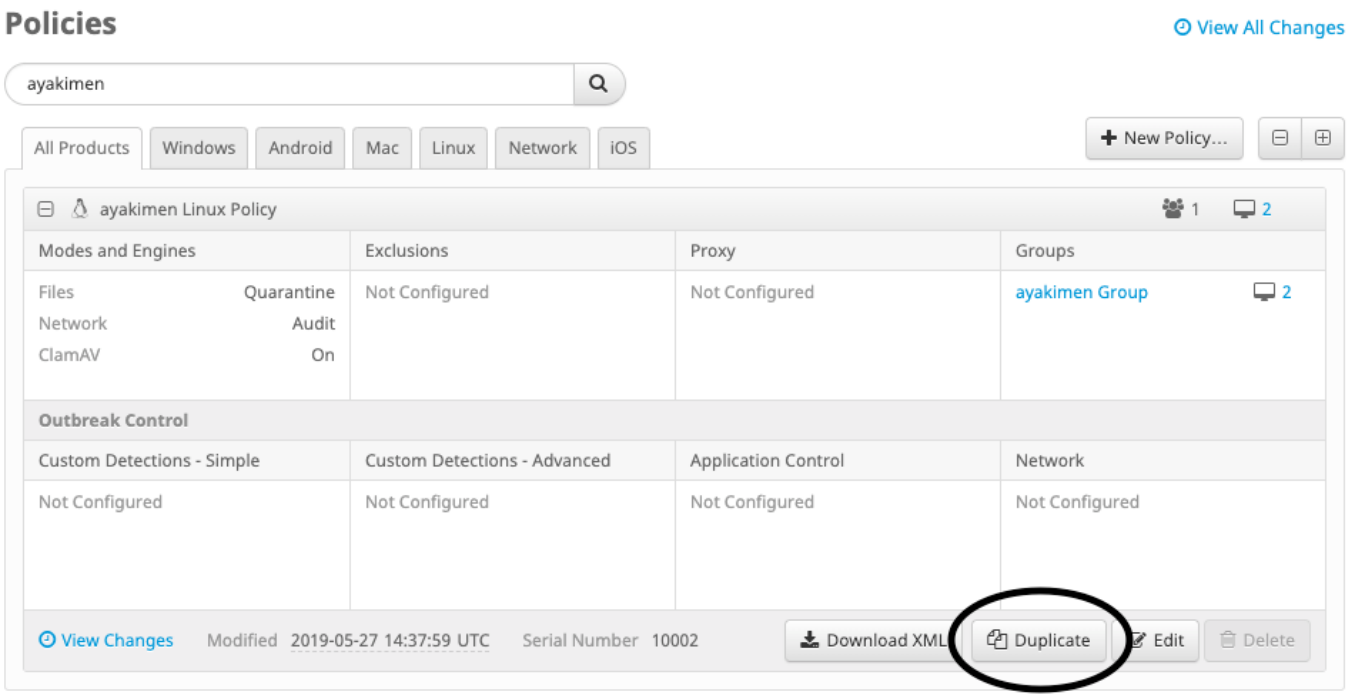
ステップ5 ~ 7で現在のポリシーでデバッグモードを有効にするか、次のすべてのステップでデバッグモードで新しいポリシーを作成できます。

ステップ1:AMPコンソールにログインします。

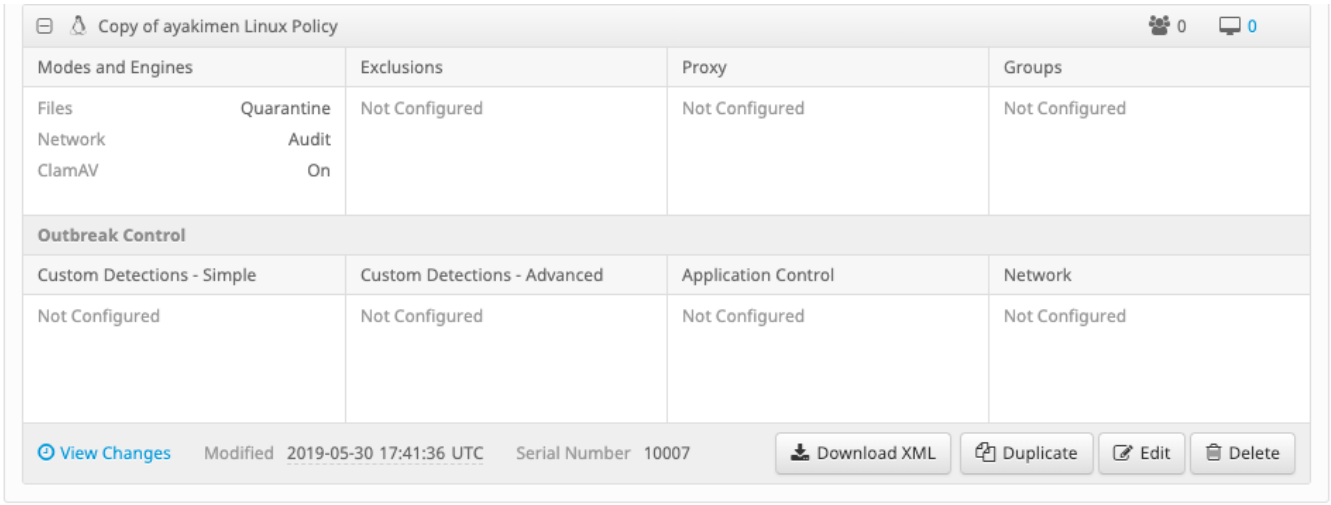
ステップ2:[管理(**Management)] > [ポリシー(Policies)]を選択します。**



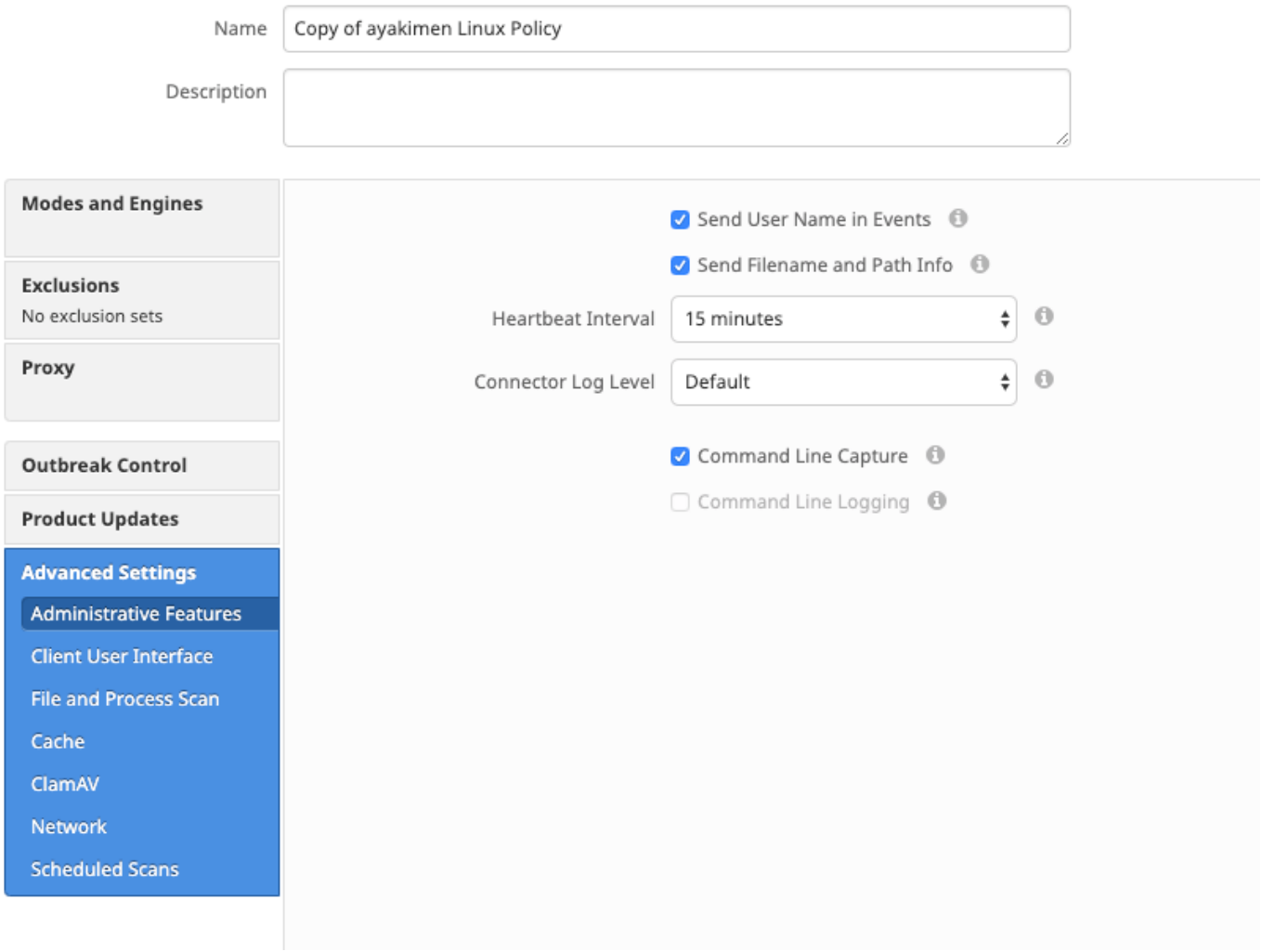
ステップ3：エンドデバイスまたはコンピュータに適用されているポリシーを見つけ、[Policy]をクリックします。[Policy]ウィンドウが展開されます。[Duplicate] **をクリックします。**



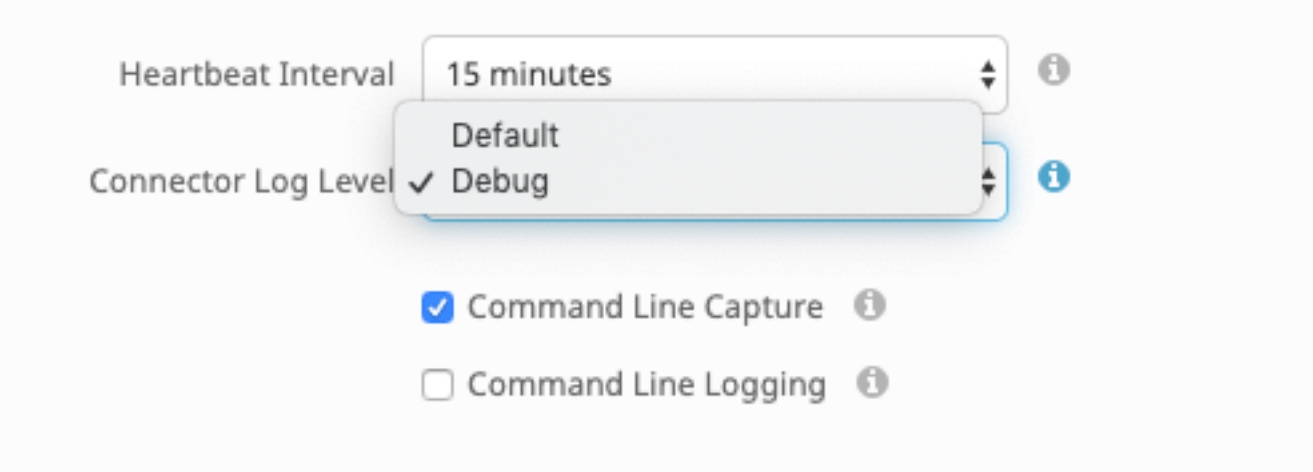
ステップ4:[**Duplicate**]をクリックすると、AMPコンソールがコピーされたポリシーで更新されます。



ステップ5:[Edit]をクリックし、[Advanced Settings]をクリックし、サイドバーから[Administrative Featuresement]をクリックします。



ステップ6:[Connector Log Level]で、ドロップダウンリストから[Debuggfrom]を選択します。



ステップ7:[Save]をクリックして変更を保存します。

ステップ8：新しいポリシーを保存した後、新しいポリシーを含むグループを作成または変更する必要があり、デバッグ情報を生成するエンドデバイスを追加する必要があります。

デバッグ モードの無効化

デバッグモードを無効にするには、デバッグモードを有効にした場合と同じ手順を実行しますが、[コネクタのログレベル]を[デフォルト]に変更します。

コマンドラインの使用

デバッグ モードの有効化

コンソールへの接続の問題が発生し、デバッグモードを有効にする場合は、CLIで次のコマンドを実行します。

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

次に出力を示します。

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

デバッグ モードの無効化

デバッグモードを無効にするには、次のコマンドを使用します。

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

サポートツール デバッグ中の調整

Connector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。これは、AMPコンソールで、[*Management*] -> [Policies]でコネクタのポリシー設定を*使用して行います*。ポリシーを編集し、[詳細設定]*タブの[管理*機能]セクション*に移動*

します。コネクタログ*レベルの設定*をデバッグに**変更します。**

次に、ポリシーを保存します。ポリシーが保存されたら、コネクタに同期されていることを確認します。このモードでコネクタを少なくとも15 ~ 20分間実行してから、残りのチューニングを続行します。

注：チューニングが完了したら、Connector Log LevelsettingをDefaultsoに変更して、Connectorが最も効率的かつ効果的なモードで実行されるようにしましょう。

サポートツールの実行

この方法では、サポートツール（AMP Macコネクタとともにインストールされるアプリケーション）を使用します。Applicationsフォルダからアクセスするには、/Applications->Cisco AMP->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 /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```
最初のオプションは、関連するチューニングファイルだけを含む、はるかに小さなサポートファイルになります。2つ目のオプションは、ログなど、プロセス除外の調整に必要な詳細情報を含む完全なサポートパッケージを提供します(Connectorバージョン1.11.0以降で利用可能)。

どちらの方法で実行しても、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~home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。これらはパス/ワイルドカードの除外に役立ちます。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。これらはプロセスの除外に役立ちます。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。

除外チューニング

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 Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).
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。 エンドポイント向けAMP: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"に対してのみ実行できます。これにより、AMP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、Connector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、コネクタバージ**

ョン1.10.2以前でパス除外として使用される可能性があります。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. 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:0)。「ターミナル」ウィンドウから、次のコマンドを実行します。 `getent passwd # | cut -d:-f1`。ここで#はユーザIDです。次のような出力が表示されます。`Username`は、Usernameは特定のプロセスのユーザです。
3. これは ユーザー名を[User]カテゴリのプロセス除外に追加すると、除外の範囲を減らすことができ、特定のプロセス除外では重要です。 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。

関連情報

- Windows 上で動作する FireAMP コネクタからの診断データの収集
- Mac OS上で動作するFireAMPコネクタからの診断データの収集
- テクニカル サポートとドキュメント – Cisco Systems