不明なMIMEタイプのファイルのファイル分析サーバへのアップロードをスキップするためのESAの設定

内容

はじめに

このドキュメントでは、Cisco ESAのFile Analysis Serverへの不明なMIMEタイプファイル（アプリケーション/オクテットストリーム）のアップロードをスキップする手順について説明します。

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。

- ESAでの高度なマルウェア防御(AMP)の動作
- ファイルのMIMEタイプに関する基本的な知識

Cisco では次の前提を満たす推奨しています。

- インストールされている物理または仮想ESA。
- ライセンスの有効化またはインストール
- セットアップウィザードが完了しました。

- ESAコマンドラインインターフェイス(CLI)への管理アクセス。

使用するコンポーネント

このドキュメントは、AsyncOS 15.5.1、15.0.2以降のリリースに適用されます。

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、クリアな（デフォルト）設定で作業を開始しています。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。

MIMEタイプ

メディアタイプは、Multipurpose Internet Mail Extensions(MIME)タイプとも呼ばれ、ドキュメント、ファイル、またはバイトのコレクションの文字と構造を識別するために使用されます。MIMEタイプの仕様は、Internet Engineering Task Force（IETF；インターネット技術特別調査委員会）RFC 6838で確立され、統一されています。

認識されない「text」のサブタイプは、MIME実装が文字セットの処理方法を知っている限り、サブタイプ「plain」として扱う必要があります。認識されない文字セットを指定する認識されないサブタイプは、「アプリケーション/オクテット – ストリーム」として扱われる必要があります。

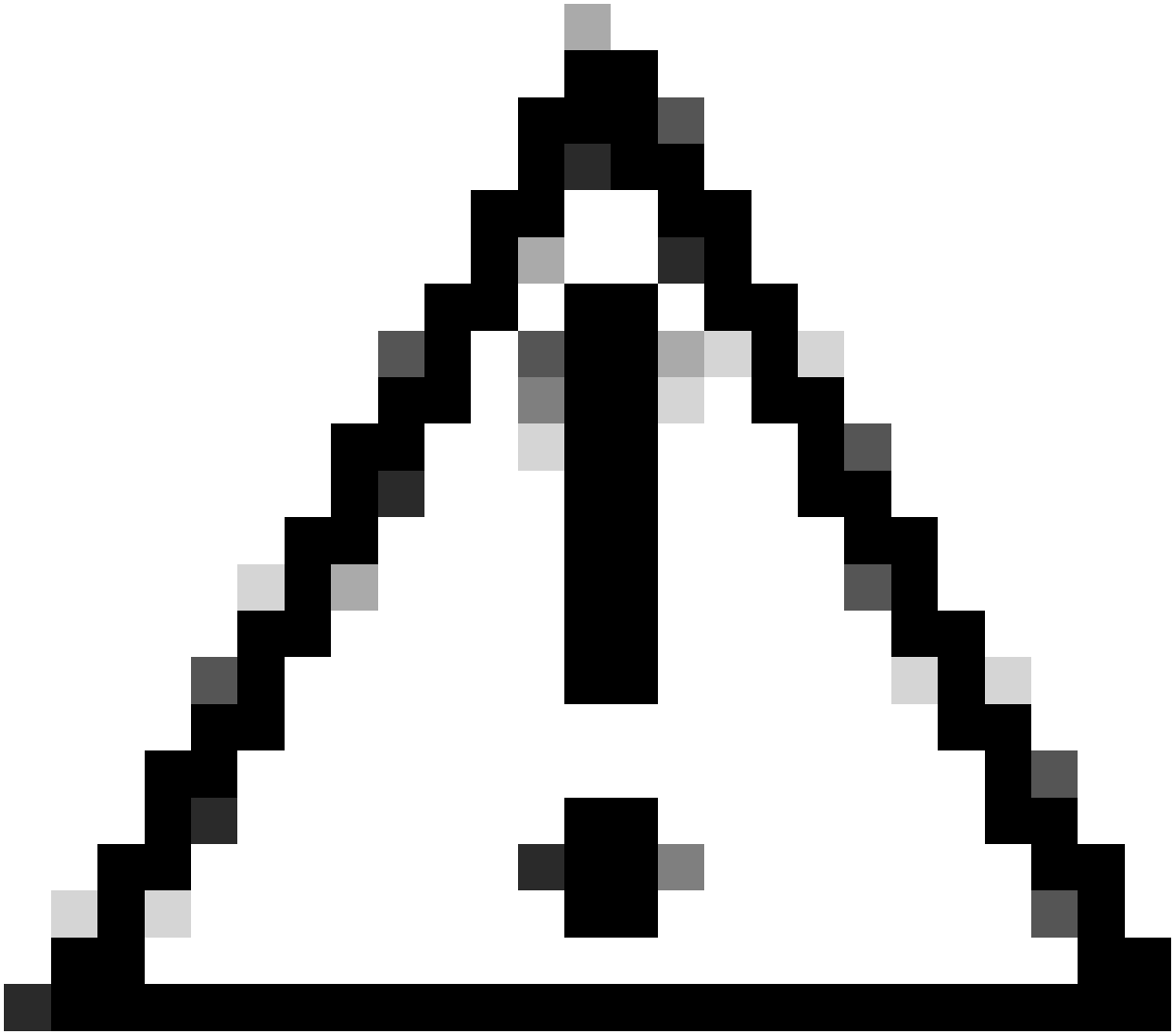
詳細については、『RFC 2046 - Multipurpose Internet Mail Extensions (MIME) Part 2: Media Types』を参照してください。

ESAアプライアンスがアップロード制限を超えました

ファイル分析サービスを有効にしていても、レピュテーションサービスにファイルに関する情報がなく、ファイルが分析可能なファイルの基準を満たしている場合、メッセージを隔離して、ファイルを分析用に送信できます。分析のために添付ファイルが送信されたときにメッセージを検疫するようにアプライアンスが設定されていない場合、またはファイルが分析のために送信されない場合、メッセージはユーザにリリースされます。

詳細については、ユーザガイドを参照してください。 AsyncOS 15.0 for Cisco Secure Email Gatewayユーザガイド – GD（一般導入）– ファイルレピュテーションフィルタリングおよびファイル分析[Cisco Secure Email Gateway] – シスコ

ESAがインスペクションのために過剰なファイルを送信したために、ファイル送信クォータが早期に最大アップロードキャパシティに達してしまうという問題を解決するために、新しいCLIコマンドが導入されました。この機能拡張は、バージョン15.5.1から実装されており、15.0.2メンテナンスリリース(MR)以降のバージョンにも組み込まれています。



注意：セキュリティを強化するために、すべてのファイルを推奨どおりにアップロードすることを強くお勧めします。ただし、特定のファイルタイプに対してこの手順をバイパスすることが重要であると考えられる場合は、提供されるコマンドを使用して、任意でバイパスを実行するオプションを有効にします。関連する潜在的なリスクを理解し、注意して進めてください。

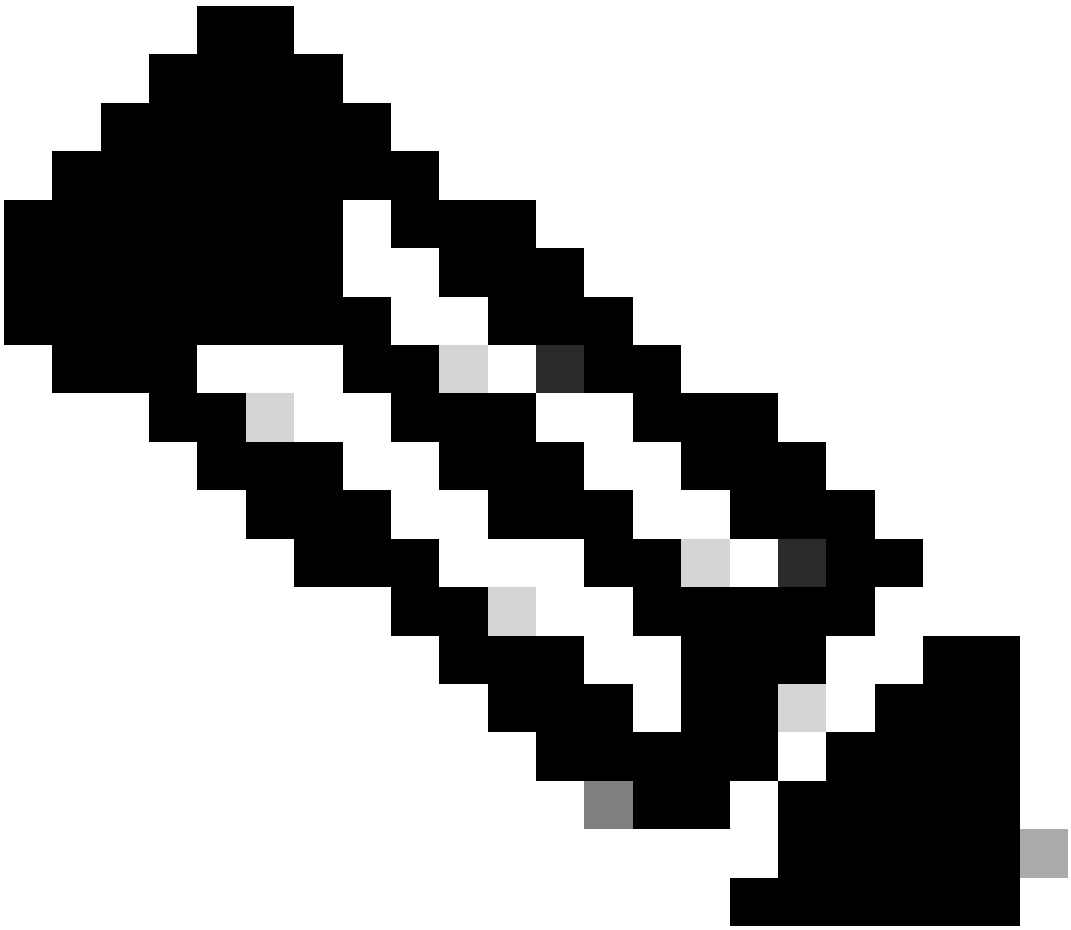
ファイル分析にアップロードするアプリケーション/オクテットストリームMIMEタイプの除外

スキャンのためにファイル分析サーバにアップロードするアプリケーション/オクテットストリームMIMEタイプを除外するには、次の手順を使用します。

ステップ 1：CLIにログインします。

手順2:ampconfigコマンドを実行する

ステップ 3： unknownmimeoverride と入力してEnterキーを押す。



注：unknownmimeoverrideは隠しコマンドです。

ステップ 4：「Do you want to send unknown mime for analysis only if their extensions are selected?」という質問に対する回答として「N」を入力します。[N]>"

ステップ 5：Enterキーを押してウィザードを終了します。

手順 6：変更を確定

```
ESA_CLI> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet
```

```
Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting
details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> unknownmimeoverride

Do you want to send unknown mime for analysis only if their extensions are selected? [Y]> N

ESA_CLI>  commit
```

リンクされた不具合と機能拡張

この新機能は、次の機能要求と不具合のために導入されました。

- ファイル分析にアップロードするHTMLおよびオクテットストリームファイルの動作が変化するため、お客様が混乱します。Cisco Bug ID CSCwh61317
- ファイルの種類が選択されていない場合でも、P7sファイルはファイル分析にアップロードされます。Cisco Bug ID CSCwh70476

参考資料

AsyncOS 15.0 for Cisco Secure Email Gatewayユーザガイド – GD（一般導入）– ファイルレピュテーションフィルタリングおよびファイル分析[Cisco Secure Email Gateway] – シスコ

RFC 2046 – 多目的インターネットメール拡張(MIME)パート2：メディアタイプ

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。