將ESA配置為跳過上傳未知MIME型別檔案到檔案分析伺服器

目錄

簡介

本文檔介紹跳過將未知MIME型別檔案（應用程式/二進位制八位數流）上傳到Cisco ESA中的檔案分析伺服器的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- ESA中的高級惡意軟體防護(AMP)如何工作。
- 檔案MIME型別的基本知識。

思科建議您：

- 已安裝物理或虛擬ESA。
- 許可證已啟用或已安裝。
- 安裝精靈已完成。

- 對ESA命令列介面(CLI)的管理訪問。

採用元件

本文檔適用於AsyncOS 15.5.1、15.0.2及更高版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

MIME型別

媒體型別(也稱為多用途網際網路郵件延伸功能(MIME)型別)可用來辨識檔案、檔案或位元組集合的字元和結構。MIME型別的規範在Internet工程任務組(IETF) RFC 6838中建立並統一。

只要MIME實作知道如何處理字元集，無法辨識的「text」子型別就必須視為子型別「plain」。同時指定無法辨識的字元集的無法辨識的子型別必須視為「application/octet-stream」。

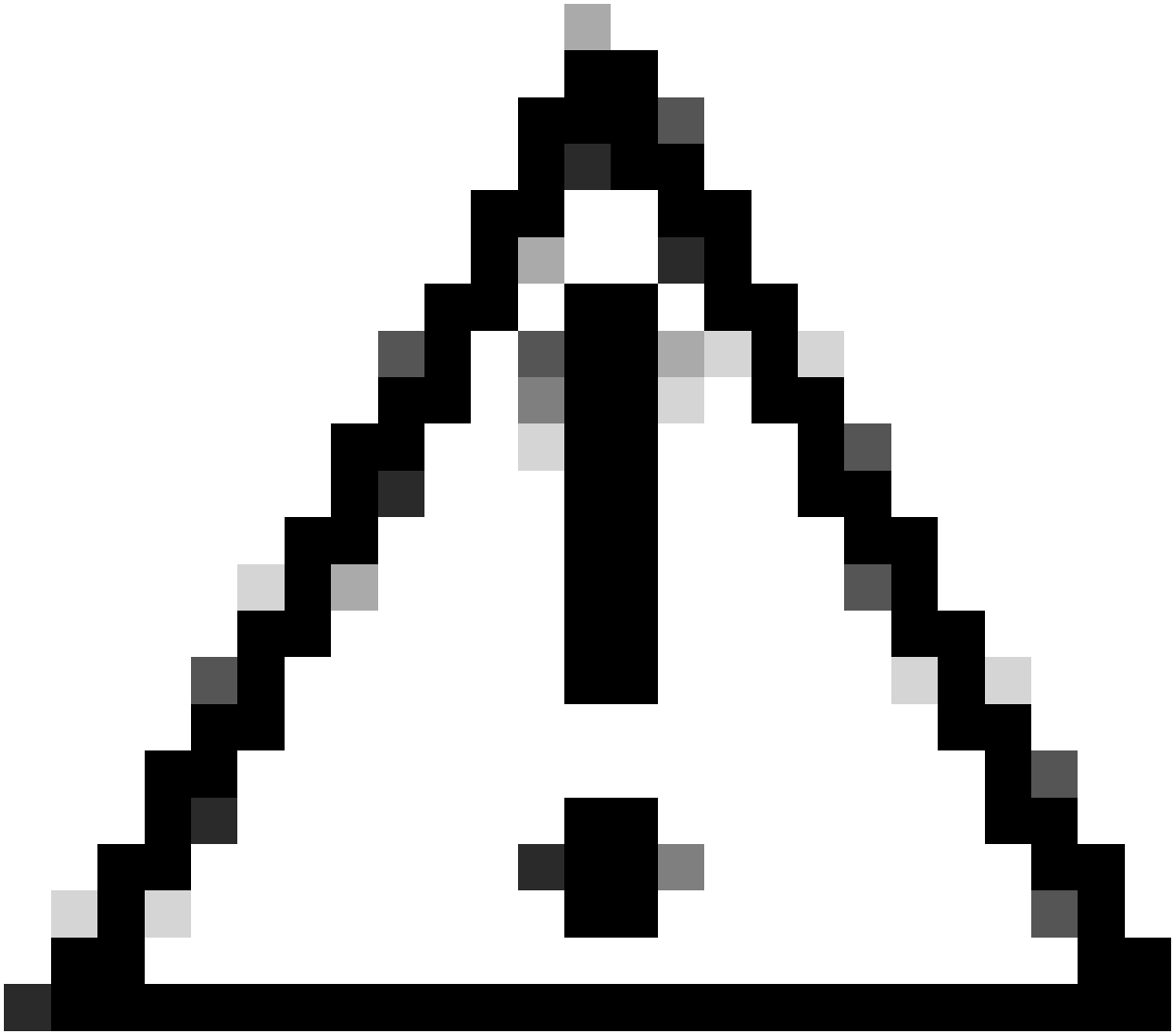
有關詳細資訊，請參閱RFC 2046 -多用途Internet郵件擴展(MIME)第2部分：媒體型別

ESA裝置超出上傳限制

如果已啟用檔案分析服務，且信譽服務沒有有關該檔案的資訊，並且檔案滿足可分析檔案的條件，則郵件將被隔離，檔案將被傳送進行分析。如果您尚未將裝置配置為在傳送附件以供分析時隔離郵件，或者未傳送檔案以供分析，則會將郵件釋放給使用者。

如需詳細資訊，請參閱使用者指南。 思科安全郵件網關AsyncOS 15.0使用手冊- GD（常規部署）-檔案信譽過濾和檔案分析[思科安全郵件網關] -思科

我們引入了一個新的CLI命令，以解決由於ESA提交過多的檔案供檢查，檔案提交配額有限而過早達到最大上傳容量的裝置問題。此增強功能已經從15.5.1版開始實施，並且正在合併到15.0.2維護版本(MR)及後續版本中。



注意：為了增強安全性，我們強烈建議按照建議上傳所有檔案。但是，如果您認為對於特定檔案型別必須繞過此步驟，則所提供的命令可讓選項自行決定是否跳過此步驟。請謹慎行事，瞭解其中可能涉及的風險。

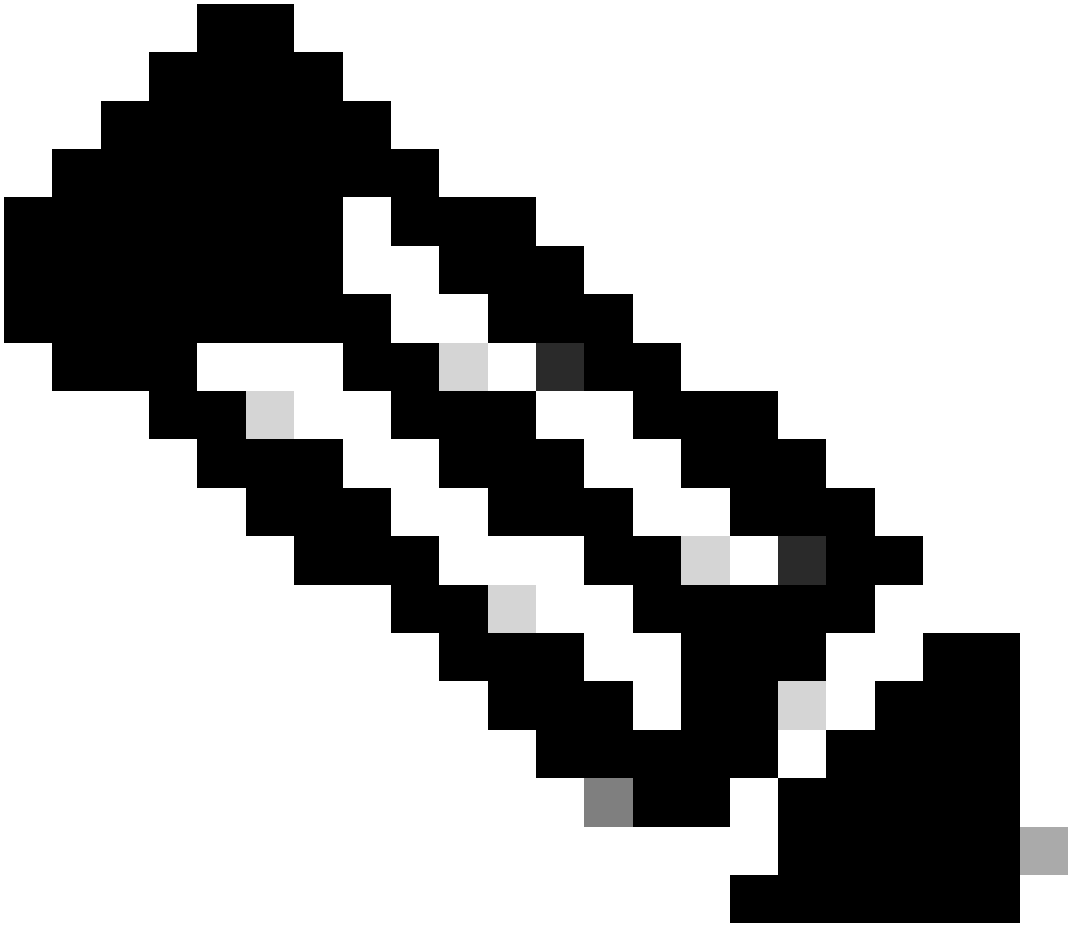
排除要上傳至檔案分析的應用程式/八位元資料流MIME型別

若要排除要上傳至檔案分析伺服器進行掃描的應用程式/八位元資料流MIME型別，請使用以下步驟：

步驟 1.登入到CLI。

步驟2.運行ampconfig 命令

步驟 3. 鍵入unknownmimeoverride，然後按Enter



注意：unknownmimeoverride是隱藏命令。

步驟 4.鍵入N回覆「Do you want to send unknown mime for analysis only if them extensions are selected？」[N]>「

步驟 5.按Enter退出嚮導。

步驟 6.提交更改

```
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
```

連結的缺陷和改進

由於以下功能要求和缺陷，引入了這一新功能：

- 上傳至File Analysis的HTML和八位元資料流檔案中的行為變更，會讓客戶感到困惑。思科漏洞ID CSCwh61317
- 即使未選擇檔案型別，也會將p7s檔案上載到檔案分析。思科漏洞ID CSCwh70476

參考資料

思科安全郵件網關AsyncOS 15.0使用手冊- GD（常規部署）-檔案信譽過濾和檔案分析[思科安全郵件網關] -思科

RFC 2046：多用途網際網路郵件延伸(MIME)第2部分：媒體型別

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。