對ESA中的「無法掃描的類別=消息錯誤，無法掃描的原因=歸檔錯誤：超過未歸檔檔案的總大小限制」錯誤進行故障排除

目錄

簡介

本文描述如何對郵件安全裝置(ESA)中的錯誤「無法掃描的類別=郵件錯誤，無法掃描的原因=存檔錯誤：超過未存檔檔案的總大小限制」進行故障排除。

必要條件

需求

思科建議您瞭解以下主題：

- ESA
- 思科進階惡意軟體防護

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- ESA AsyncOS 11.1.2-023。
- ESA AsyncOS 12.0.0-419。

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。

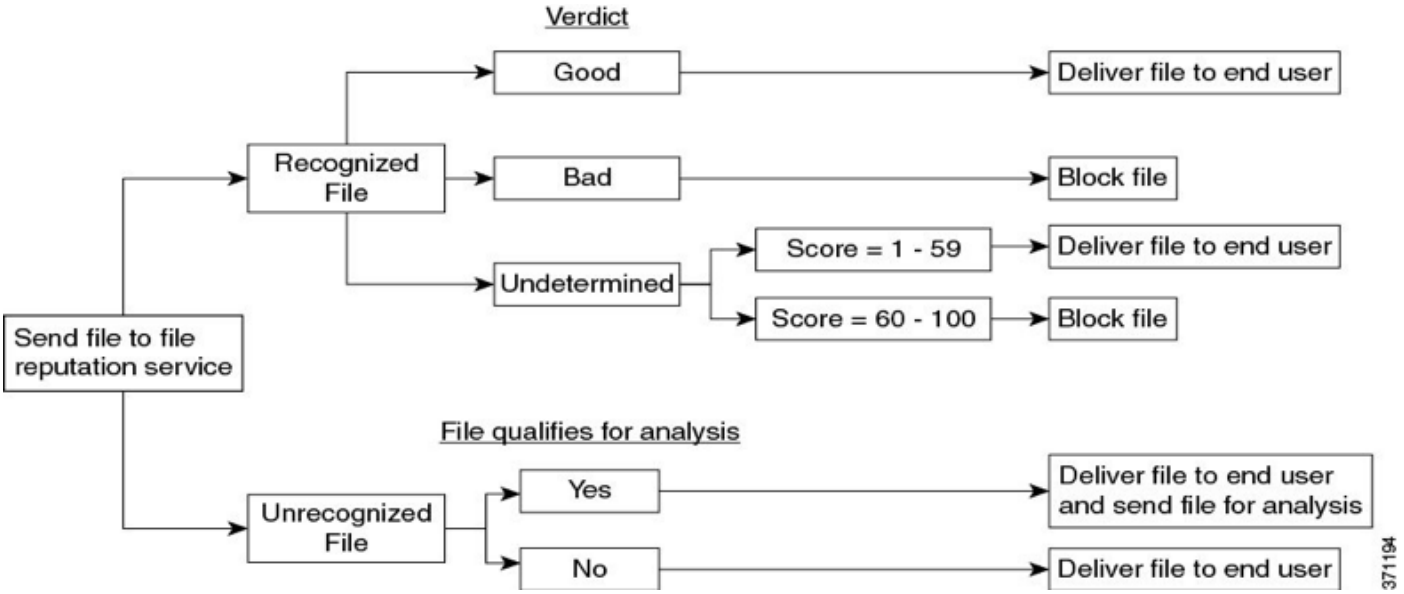
背景資訊

當帶有附件的郵件到達管道中的AMP時，ESA會嘗試解析郵件中的附件並檢查郵件信頭(檢查是否符合RFC 2045)。 即使郵件不完全符合，ESA仍會盡最大努力分析附件。

下一步是檢查附件是否為歸檔檔案，如果是，ESA會嘗試將其解包，它會考慮多個因素以確定壓縮檔案大小，以確保附件是合法的，而不是zip檔案。

如果找不到檔案信譽，並且檔案符合分析標準，則會將其隔離並上傳到沙盒。

然後，ESA會開啟與AMP伺服器的連線並上傳檔案，然後等待判定更新，如下圖所示：



ESA根據以下情況做出判斷：

- 如果提取的檔案之一為惡意檔案，則檔案信譽服務會針對壓縮檔案或歸檔檔案返回判定為Malicious。
- 如果壓縮檔案或存檔檔案是惡意檔案，並且提取的所有檔案都是乾淨的，則檔案信譽服務會針對壓縮檔案或存檔檔案返回惡意判定結果。
- 如果任何提取檔案的判定結果未知，則選擇傳送提取的檔案進行檔案分析（如果已配置且支援檔案型別進行檔案分析）。
- 如果任何提取的檔案或附件的判定風險較低，則不會傳送該檔案進行檔案分析。
- 如果檔案解壓縮後提取失敗，然後將其壓縮或存檔檔案，則檔案信譽服務會針對壓縮或存檔檔案返回Unscannable判定結果。請記住，在此場景中，如果提取的某個檔案是惡意檔案，檔案信譽服務會針對壓縮檔案或存檔檔案返回一個「惡意」判定結果（惡意判定優先於「無法掃描」判定結果）。

諸如csv、xml、txt等高度壓縮的檔案可能會超過硬編碼為ESA的最大檔案大小，壓縮演算法(如Lempel-Ziv*)會生成一個數字地*圖，計算整個文檔中的字元數量和位置，這樣會產生非常小的檔案大小。

另一方面，包含圖形、文本格式（如pdf、jpg、png）的檔案不是以相同方式壓縮的，因此它們幾乎保留原始檔案大小。

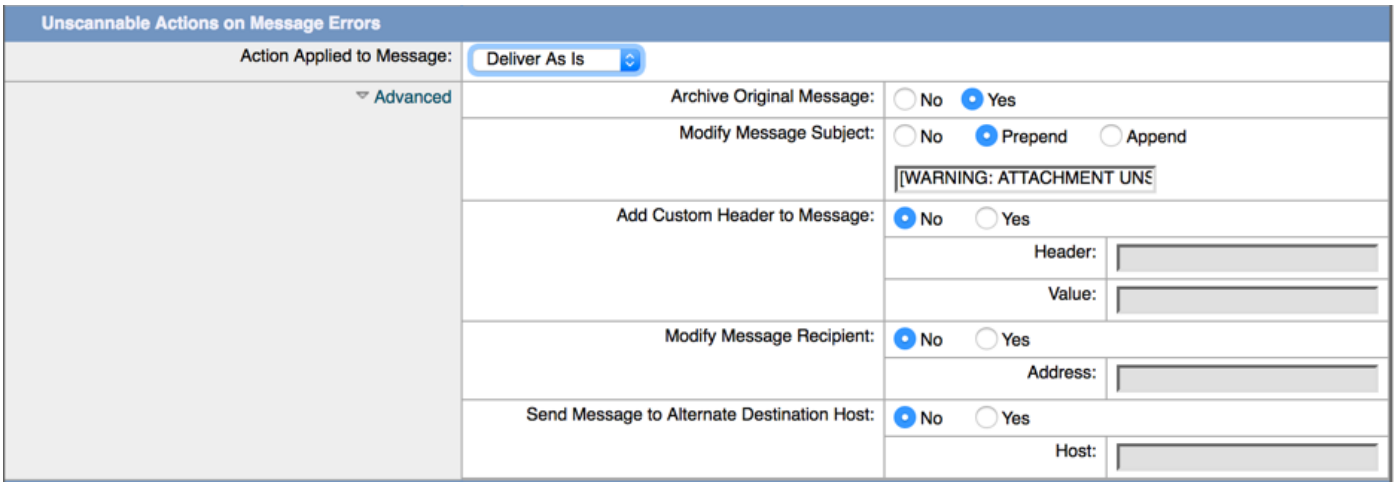
問題

當ESA收到附件中經過壓縮且超過最大壓縮比的電郵，並且ESA無法計算附件的檔案大小，則結果為以下錯誤日誌：

「Wed Feb 13 20:03:47 2019資訊： 無法掃描附件。檔名= 'ACTS截短ISO 88591 encod_NoSchema.XML.zip',MID = 226,SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f，不可掃描類別=消息錯誤，不可掃描原因=歸檔錯誤： 已超出未存檔檔案的大小總限制」

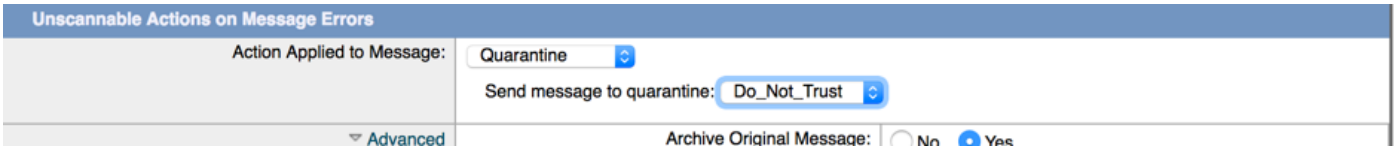
解決方案1

將無法掃描的消息預置到「Subject（主題）」中，以提醒使用者檔案未由AMP服務分析，如下圖所示。



解決方案2

隔離區無法掃描到策略病毒和爆發(PVO)隔離區，以進行進一步分析。如下圖所示。



相關資訊

- 思科郵件安全裝置AsyncOS 12.0使用手冊 — GD（常規部署）
- 啟用內容安全產品上的AMP(ESA/WSA)
- 驗證ESA上的檔案分析上傳
- 技術支援與文件 - Cisco Systems

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）。