

瞭解使用AMP的ESA上的警報「達到上傳限制」

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[瞭解「已達到上傳限制」警報](#)

[如何檢查過去24小時內您的ESA上傳的樣本數量？](#)

[如何延伸上傳限制？](#)

[相關資訊](#)

簡介

本文描述當郵件安全裝置(ESA)配置為使用高級惡意軟體防護(AMP)功能掃描郵件時，會引發警報「達到上傳限制」。

必要條件

需求

思科建議您瞭解以下主題：

- [電子郵件安全裝置](#)
- [高級惡意軟體防護](#)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 執行軟體12.x的電子郵件安全裝置(ESA)

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

郵件安全裝置(ESA)使用高級惡意軟體防護(AMP)功能，該功能包含兩個主要功能：

- [檔案信譽](#)
- [檔案分析](#)

File Analysis將沙盒分析的郵件附件上傳到ThreatGrid雲伺服器。

瞭解「已達到上傳限制」警報

郵件跟蹤可以顯示高級惡意軟體防護(AMP)未掃描郵件，因為它們已達到上傳限制。

範例：

```
02 Dec 2019 14:11:36 (GMT +01:00) Message 12345 is unscannable by Advanced Malware Protection engine. Reason: Upload Limit Reached
```

在新的ThreatGrid樣本限制模型中，這些限制是每個組織允許裝置上傳以進行檔案分析的樣本數量。所有整合設備(WSA、ESA、CES、FMC等)以及面向終端的AMP都有權每天獲得200個樣本，無論裝置數量如何。

這是一個共用限制（不是每台裝置的限制），並且適用於2017年1月12日後購買的許可證。

附註：此計數器不是每天重置的，相反，它是按24小時滾動週期運行的。

範例：

在具有200個上傳樣本限制的4個ESA集群中，如果ESA1今天10:00上傳80個樣本，則從今天10:01到明天10:00（釋放前80個插槽），4個ESA（共用限制）中僅可上傳120個樣本。

如何檢查過去24小時內您的ESA上傳的樣本數量？

ESA:導航到Monitor > AMP File Analysis報告，然後檢查Files Uploaded for Analysis部分。

SMA：導航至Email > Reporting > AMP File Analysis報表，並檢查Files Uploaded for Analysis部分。

附註：如果AMP File Analysis報告未顯示準確資料，請檢視《使用手冊》中[Cloud Are Incomplete](#)中的[File Analysis Details](#)部分。

警告：如需其他資訊，請參閱[缺陷CSCvm10813](#)。

或者，您可以從CLI運行grep命令以統計上傳的檔案數。

必須在每台裝置上執行此操作。

範例：

```
grep "Dec 20.*File uploaded for analysis" amp -c  
grep "Dec 21.*File uploaded for analysis" amp -c  
可以使用PCRE正則表達來匹配日期和時間。
```

如何延伸上傳限制？

聯絡您的思科客戶經理或銷售工程師。

相關資訊

- [深入探討AMP和Threat Grid與思科電郵安全的整合](#)
- [檢驗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）。