

附件的ESA日誌檔名配置示例

目錄

[簡介](#)

[必要條件](#)

[設定](#)

簡介

本檔案介紹如何記錄通過思科電子郵件安全裝置(ESA)的附件的檔名。

必要條件

本文中的資訊係根據以下軟體和硬體版本：

- ESA
- AsyncOS的所有版本

設定

附註：在AsyncOS版本7.x及更高版本中，如果至少安裝了一個過濾器來檢查檔案資訊（檔名、副檔名、檔案型別、內容掃描），則自動記錄附件。有關詳細資訊，請參閱AsyncOS中的使用手冊或聯機幫助。

此解決方案可用於早期的AsyncOS版本。

1. 建立一個包含所有附件檔名的新標題。
2. 使用`logconfig > logheaders`將該標頭的值記錄到`mail_log`。

以下是記錄包含附件的郵件的檔名的過濾器：

```
add_filenames_header:
if (attachment-filename == "^.*$") {
insert-header ("X-fn", "$filenames");
```

「`^.*$`」註冊可確保檔名中至少有一個字元的附件。對於沒有附件的郵件，此值為`false`，因此只記錄附件。

附註：電子郵件中「附件」的定義存在爭議。通常，第一個文本/純文字檔案和文本/HTML部分被視為「正文」。有關附件內容的詳細資訊，請參閱使用手冊。

以下是`mail_logs`中顯示的內容示例：

```
Fri Sep 15 13:49:39 2006 Info: Start MID 98 ICID 146
Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 From: <joe@example.com>
```

Fri Sep 15 13:49:39 2006 Info: MID 98 ICID 146 RID 0 To: <carl@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 Message-ID '<9151349.VSREACRQ@example.com>'
Fri Sep 15 13:49:39 2006 Info: MID 98 Subject '1:49 pm'
Fri Sep 15 13:49:39 2006 Info: MID 98 ready 20670 bytes from <joe@example.com>
Fri Sep 15 13:49:39 2006 Info: MID 98 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Fri Sep 15 13:49:39 2006 Info: MID 98 antivirus negative
Fri Sep 15 13:49:39 2006 Info: MID 98 queued for delivery
Fri Sep 15 13:49:39 2006 Info: Delivery start DCID 64 MID 98 to RID [0]
Fri Sep 15 13:49:41 2006 Info: Message done DCID 64 MID 98 to RID [0] [('X-fn',
'Encoding.txt')]
Fri Sep 15 13:49:41 2006 Info: MID 98 RID [0] Response '2.0.0 OK 1158353381
r66si9145992pye'
Fri Sep 15 13:49:41 2006 Info: Message finished MID 98 done

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）。