在ESA中配置CEF日誌條目和CEF標頭

目錄

簡介

本檔案介紹思科安全電子郵件閘道(SEG)的通用事件格式(CEF)日誌條目和標頭的設定。

必要條件

需求

思科建議瞭解以下主題：

- 思科安全電子郵件閘道/電子郵件安全裝置(SEG/ESA)
- 內容過濾器知識
- 日誌訂閱知識

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 電子郵件安全裝置版本14.3

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

整合的事件日誌將每個消息事件彙總到單個日誌行中。使用此日誌型別可以減少傳送到安全資訊和事件管理(SIEM)供應商或應用程式進行分析的資料（日誌資訊）位元組數。日誌採用大多數SIEM供

應商廣泛使用的CEF日誌消息格式。

新增CEF日誌條目和CEF標頭以提供跟蹤和組織郵件事件的額外資訊。

設定

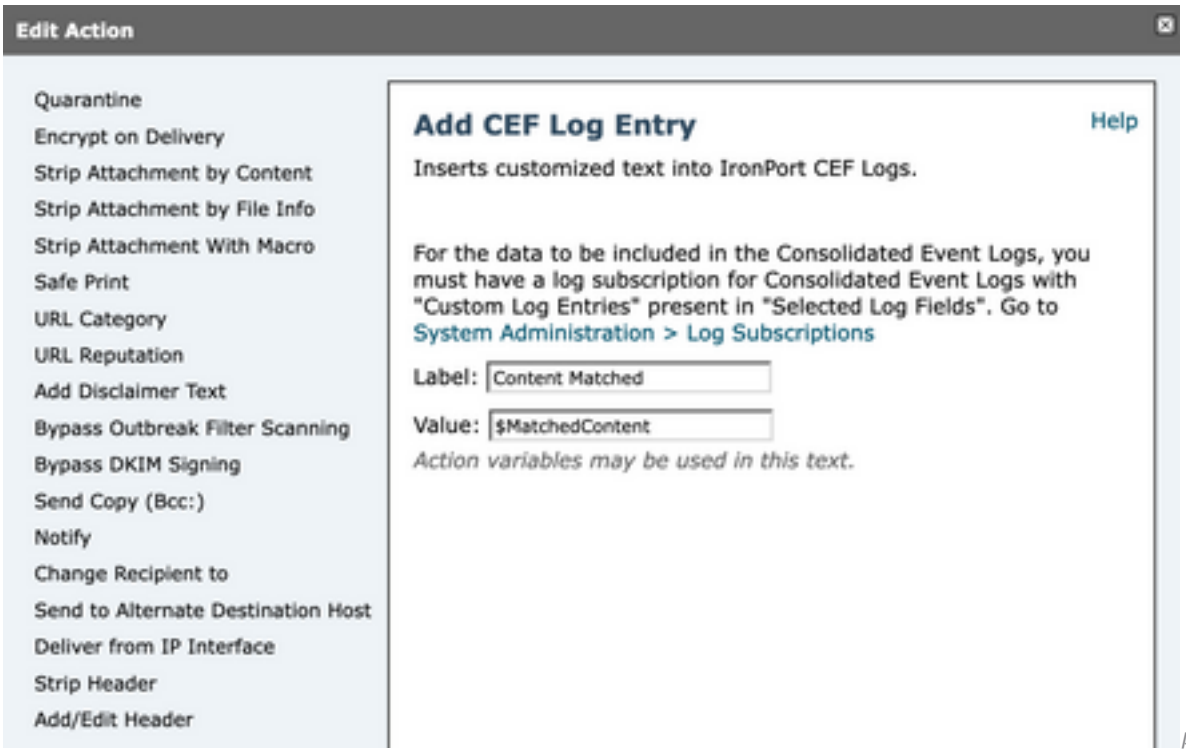
CEF日誌條目

新增傳入/傳出內容過濾器

首先，在ESA上建立內容過濾器：

1. 轉到 **Mail Policies > Incoming/Outgoing content filters**
2. 點選 **Add Filter**
3. 為過濾器命名
4. 新增所需條件
5. 點選 **Add Action**
6. 選擇 **Add CEF Log Entry**
7. 命名標籤並使用 **Action Variables** 用於值框
8. **Submit and Commit**

我們使用的文檔示例 **$MatchedContent** 操作變數，如下圖所示：



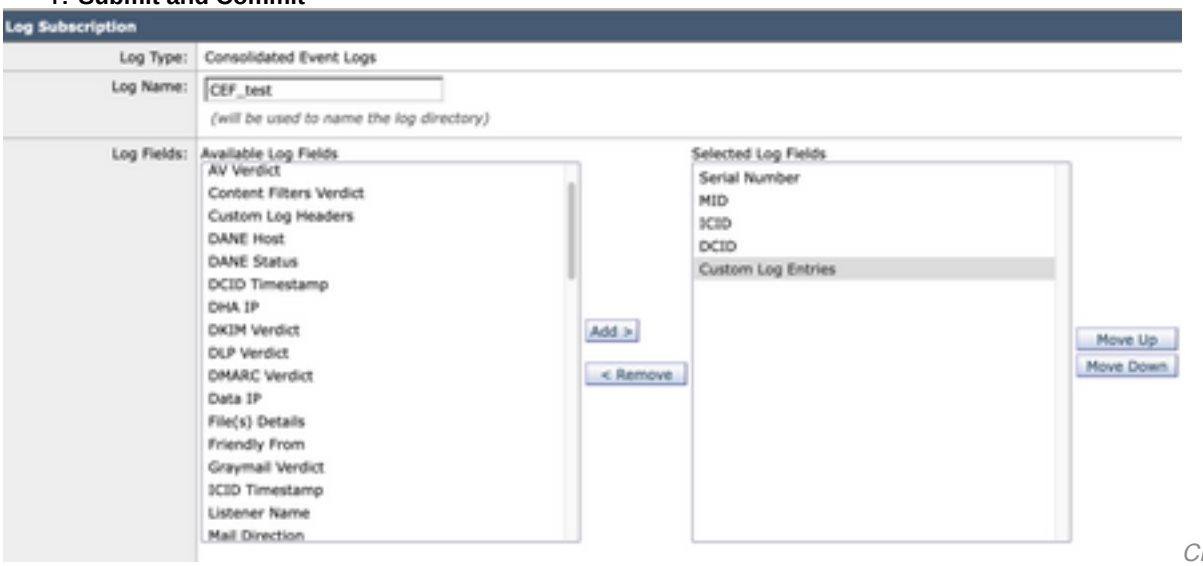
內容過濾器中的CEF日誌條目操作

在統一事件日誌訂閱中新增CEF日誌條目

接下來，建立或修改統一事件日誌訂閱，以新增以前建立的CEF日誌條目：

1. 轉到 **System Administration > Log Subscriptions**
2. 新增或選擇整合的事件日誌
3. 選擇 **Custom Log Entries** 然後按一下 **Add**

4. **Submit and Commit**



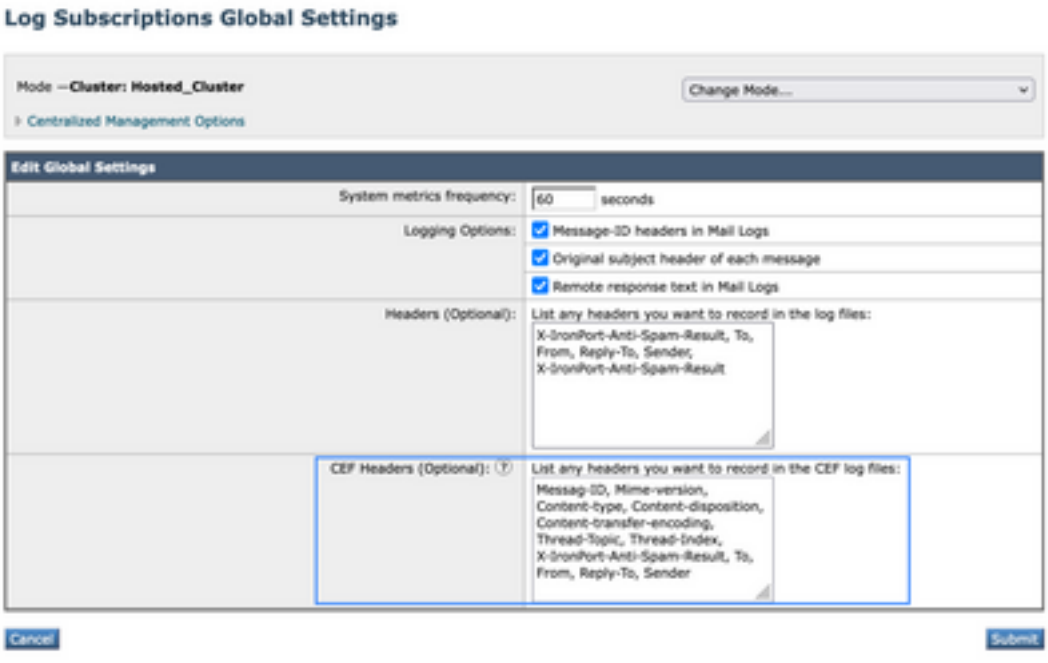
CEF日誌訂閱中的自定義日誌條目

CEF標頭

將CEF標頭新增到日誌中：

首先在ESA中新增CEF報頭

1. 轉到 **System Administration > Logs Subscription**
2. 點選 **Edit Settings** 在「全域性設定」下
3. 在CEF標頭下，列出要記錄的標頭
4. **Submit and Commit**



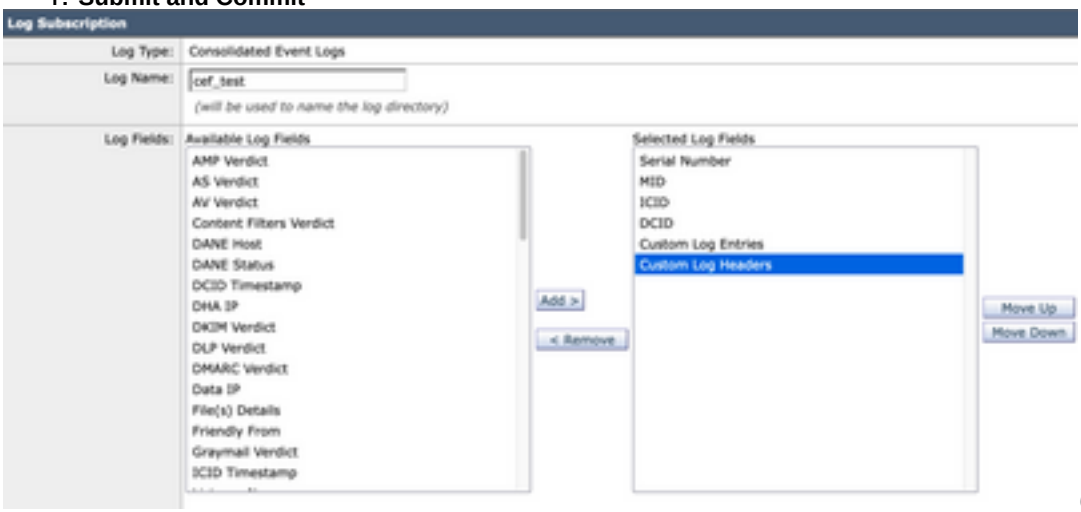
CEF報頭配置

在統一事件日誌訂閱中新增CEF日誌條目

接下來，建立或修改統一事件日誌訂閱，以新增以前記錄的CEF標頭：

1. 轉到 **System Administration > Logs Subscription**
2. 新增或選擇整合的事件日誌

3. 選擇 **Custom Log Entries** 然後按一下 **Add**
4. **Submit and Commit**



CEF日誌訂閱中的CEF日誌標頭

相關資訊

- 最終使用手冊ESA 14.3
- 發行說明ESA 14.3
- 技術支援 - 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）。