# 如何搜尋和檢視ESA上的郵件日誌？

## 目錄



## 簡介

本文檔介紹如何搜尋顯示ESA（郵件安全裝置）如何處理郵件的日誌條目。

## 如何搜尋和檢視ESA上的郵件日誌？

您可以搜尋日誌，以收集有關來自您感興趣的此IP地址的電子郵件的*發件*人和收件人主題的更多資訊。

日誌的名稱為*mail_logs*。您可以在**系統管理>日誌訂閱> mail_logs**中看到此資訊。

有多種方法可以訪問這些日誌。

1. 通過Web瀏覽器。 轉至**系統管理>日誌訂閱**。對於mail_logs，按一下mail_logs右側的ftp連結。如果出現錯誤，請轉到**Network > IP interface**，選擇您通常可以訪問ESA的介面，然後開啟FTP/埠21服務。
2. 在命令列中： 使用ssh客戶端（如Putty），通過埠22/ssh登入到ESA裝置的CLI。在命令列中，使用**grep**搜尋IP。您需要輸入與裝置的mail_logs關聯的#，然後輸入要搜尋的模式，即。192.168.1.1或joe@example.com。對於接下來的三個問題，請按enter鍵並保持預設值。完成搜尋可能需要一些時間。返回輸出後，您可以搜尋ICID或MID。
   ```
   grep "ICID 123456" mail_logs
   ```
   輸出返回後，您可以搜尋MID
   ```
   grep "MID 78901234" mail_logs
   ```
   您應該能夠從MID檢視*自*、*至*、*主*題。您應該能夠從ICID檢視IP地址和HAT發件人組。
3. 另一種方法是，將mail_logsftp到本地電腦(Desktop)，並使用您自己的檔案/文本編輯器搜尋IP地址。