什麼是 UNIX mbox（信箱）格式？

目錄

簡介

本文件說明 Unix 信箱 (mbox) 格式，以及此格式與思科電子郵件安全設備 (ESA) 相關的用途。

什麼是 UNIX mbox（信箱）格式？

當消息存檔並記錄到消息過濾器log()操作中時，AsyncOS使用UNIX mbox格式。「存檔郵件」是ESA上Ironport Anit-spam(IPAS)、防病毒（Sophos和McAfee）、高級惡意軟體防護(AMP)和灰色郵件的附加配置選項。

Mbox格式是ASCII格式的（即非二進位制）檔案格式，可以包含零個或多個郵件。消息在mbox檔案中串聯，並可根據檔案中的特定字串進行分隔。此格式與在RFC 2821相容郵件網關之間傳輸的消息完全相同。

mbox格式的每條消息都以一個以字串「From」開頭的行開頭（ASCII字元F、r、o、m和空格）。「自」行後跟多個欄位：envelope-sender、date和（可選）more data。

「發件人」字串後的第一個欄位是郵件的信封 — 發件人。根據建立mbox檔案的應用程式的不同，信封發件人可能以實際郵箱的形式存在，也可能以另一個字元或字串的形式存在。最常見的是，如果實際信封發件人不可用或未知，您會發現「 — 」（單字元短劃線）替換信封發件人。ESA插入的日期欄位採用標準的UNIX asctime()格式，長度始終為24個字元。在由非AsyncOS實現編寫的一些mbox檔案中，日期戳後會有進一步的資訊。這三個欄位由單個空格分隔。

以下是包含單一訊息的mbox檔案範例：

```
From Adam@Outside.COM Sun Oct 17 12:03:20 2004
Received: from mail.outside.com (192.35.195.200)
by smtp.alpha.com with ESMTP; 17 Oct 2004 12:03:20 -0700
X-IronPort-AV: i="3.85,147,1094454000";
v="EICAR-AV-Test'0'v";
d="scan'208"; a="86:adNrHT37924848"
X-IronPort-RCPT-TO: alan@mail.example.com
From: Adam@Outside.COM
To: Alan Alpha




--IronPort
Content-type: text/plain; format=flowed; charset=us-ascii
Content-transfer-encoding: 7bit
```

```
Blah blah blah blah blah
Blah blah blah blah blah
Blah blah blah blah blah
...
--IronPort
Content-type: text/plain
Content-transfer-encoding: 7bit
Content-disposition: inline

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-
FILE!$H+H*">X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

--IronPort--
```

在分析mbox格式的檔案時，最好不要在分隔消息的「自」行中讀取太多語義。由於許多不同的實用程式會寫入mbox檔案，因此這些行存在相當大的差異。但是，「發件人」行始終可以用作消息分隔符行，以可靠地指示已在mbox檔案中啟動新消息。總之，「From」消息分隔符之後的字串約有20種已知格式，通常很難解析它們。

「發件人」行後是RFC 2822格式的電子郵件，包含一系列郵件正文標題，後跟空白行，後跟其他郵件正文內容。

為確保消息正確分隔，以字串"From"開頭的行始終以單個">"開頭。 mbox檔案的各種不同變體以不同方式處理以「>From」開頭的行。在編寫mbox檔案的早期應用中，這些行本身沒有報價。AsyncOS日誌檔案將始終將「>」置於以一個或多個「>」字元開頭，後跟「From」的行之前。

以下是mbox檔案的示例，該檔案中包含一條包含起始字串「From」、「>From」和「>>>From」的郵件：

```
From jtrumbo@example1.com Sun Dec 12 12:27:33 2004
X-IronPort-RCPT-TO: trumbo@example1.com
From: jtrumbo@example1.com
To: trumbo@example2.com
Subject: Quote this, if you dare
Date: Sun, 12 Dec 2004 12:28:00 -0700

The following line is just From
>From A From Line

The following line has quoted >From
>>From A >From Line

The following line has many >>>>From
>>>>>From This line has 4 > characters before From

And this is the last line
```

mbox格式檔案中消息的結尾通常用空白行發訊號。但是，這並不總是存在（儘管AsyncOS確實會將其放置在那裡）。 分析mbox格式檔案時，您應該通過新消息的開頭（如果出現空行，則將其刪除）或檔案結尾來發出消息結尾的訊號。

mbox格式的另一個變體要求在消息頭內的「Content-Length」欄位中傳送消息的長度。該格式未使用「自」行報價。AsyncOS不使用此格式，也不插入「內容長度」欄位。