ESA報文處置確定

目錄

簡介

本文說明如何使用從思科電子郵件安全裝置(ESA)上的各種命令中檢索到的郵件日誌來確定郵件的處理方式。

必要條件

本檔案中的資訊是根據：

- ESA
- AsyncOS的所有版本

郵件跟蹤

如果運行AsyncOS for Email 6.0或更高版本，則確定特定郵件發生情況的最有效方法是使用「監視器」頁籤中的「郵件跟蹤」頁。這允許您在易於使用的Web介面中使用各種選項進行搜尋。

如果運行的是較舊版本或者需要收集所有日誌行以進行故障排除，請使用**grep**或**findevent**命令，如下一節中所述。

Findevent命令

如果您有適用於電子郵件版本5.1.2或更高版本的AsyncOS，則CLI **findevent**命令可簡化搜尋特定郵件的過程。**Findevent**允許您按信封發件人、信封收件人或郵件主題進行搜尋。這也可以實現，不管發生什麼情況。找到您的消息後，您可以返回與該消息相關的每個日誌行。如果運行不帶引數的**findevent**，它將啟動嚮導以引導您完成該過程。您可以一如既往使用**help**命令來學習短形式：

```
> help findevent
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```

第一個表單在命名的log_name內搜尋從、主題或信封到的特定信封，並列出匹配的郵件ID(MID)。-i標誌可用於不區分大小寫的搜尋。

第二個窗體顯示給定MID的所有日誌行。

如果您使用的是較舊版本，則可使用CLI **grep**命令來完成相同任務。但是，使用**grep**命令需要有關ESA如何記錄消息事件的更詳細知識。

Grep命令

搜尋郵件日誌時的第一個挑戰就是查詢郵件。如果搜尋發件人、收件人或主題，則可以執行此操作。找到郵件後，必須瞭解郵件日誌的組織方式。內容安全郵件日誌事件以縮寫形式指定。最重要的事件是ICID、MID、RID和DCID。

注入連線ID(ICID):當遠端主機建立與裝置的連線時，該連線會被分配一個ICID。一個ICID可以生成多個MID。

> **附註**：**ICID 0定**義從自身注入的消息。事實上，ICID或DCID後面的數字0是指向裝置本地環路地址開放或從裝置本地環路地址開啟的會話。

MID:建立連線後，每個成功的簡單郵件傳輸協定(SMTP)郵件**均來自：**命令建立一個新的MID。單個MID可以生成多個RID。

收件人ID(RID):每個收件人(收件人：抄送：或者Bcc獲得RID。RID只在存在軟退回（連線錯誤）且重新嘗試傳送時產生多個DCID。

傳送連線ID(DCID):到達同一目標域的每個接收者都收到相同的DCID，直到接收系統的限制。因此，如果一個消息的接收者都轉到同一個域，則所有RID都有一個DCID。相反，如果每個RID轉到單獨的域，則存在一對一關聯。

> **附註**：**DCID 0定**義了從未傳送過的消息。事實上，ICID或DCID後面的數字0是指向裝置本地環路地址開放或從裝置本地環路地址開啟的會話。

通常，當您找到您的消息時，會找到其MID。然後您會尋找MID並確定ICID和RID。使用ICID，您可以確定發件人的SenderBase信譽得分(SBRS)。通過RID和DCID，您可以確定ESA嘗試傳送時發生了什麼情況。

> **附註**：一旦您擁有MID、ICID和DCID，您就可以檢索該消息的所有行，如果消息來源不早於您最早的郵件日誌，則其格式為**grep**。

```
example.com> grep -e " MID 11123" -e " ICID 11092" -e " DCID 23349" mail_logs
```

範例

1. 搜尋郵件主題：

```
example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> test
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Mon Jan 23 10:25:03 2006 Info: SMTP listener testpairlist starting
Tue Jan 24 12:10:15 2006 Info: Message aborted MID 8 Dropped by filter
'testdrop'
Tue Jan 31 23:55:38 2006 Info: MID 32 Subject 'testmsgquarantine'
Wed Feb 1 00:23:59 2006 Info: MID 62 Subject 'testmsgquarantine'
Wed Feb 1 00:27:48 2006 Info: MID 64 Subject 'testmsg2'
Wed Feb 1 22:30:37 2006 Info: MID 80 Subject 'test zip'
Wed Feb 1 22:37:51 2006 Info: MID 83 Subject 'FW: test zip'
Wed Feb 1 22:41:50 2006 Info: MID 84 Subject 'FW: test zip'
Fri Feb 3 15:17:47 2006 Info: MID 94 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
```

這生成了多個匹配項，其中包含主題中的**test**。郵件大約在下午3:42傳送，因此您可使用該MID進行下一次搜尋。

以下是關於這些問題的一些重要注意事項：

是否希望此搜尋不區分大小寫？[Y]>
如果對此問題回答**Yes**，則無論大小寫都會查詢條目。

是否要跟蹤日誌？[N]>
如果對此問題回答**Yes**，則僅在生成新條目時查詢這些條目。它不會搜尋所有日誌檔案。選擇**否**以搜尋所有日誌。

是否要對輸出進行分頁？[N]>
如果對此問題回答**Yes**，則每次顯示一個頁條目。如果需要執行一般搜尋並期望檢索許多條目，這很有用。這將阻止條目從顯示中滾出。

2. 搜尋MID:

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> MID 96
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:41:43 2006 Info: Start MID 96 ICID 10394
Fri Feb 3 15:41:43 2006 Info: MID 96 ICID 10394 From: <bob@example.net>
Fri Feb 3 15:41:58 2006 Info: MID 96 ICID 10394 RID 0 To:
<nasir@example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Message-ID
```

```
<4o8836$30@mail.example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test'
Fri Feb 3 15:42:06 2006 Info: MID 96 ready 23 bytes from
<bob@example.net>
Fri Feb 3 15:42:06 2006 Info: MID 96 matched all recipients for
per-recipient policy DEFAULT in the outbound table
Fri Feb 3 15:42:06 2006 Info: MID 96 antivirus negative
Fri Feb 3 15:42:06 2006 Info: MID 96 queued for delivery
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: MID 96 RID [0] Response '2.6.0
<4o8836$30@mail.example.com> Queued mail for delivery'
Fri Feb 3 15:42:06 2006 Info: Message finished MID 96 done
```

請注意，MID條目提供了有關如何處理消息的更多資訊。MID條目還引用ICID和DCID。如果您想瞭解有關傳入連線的更多資訊，請grep for the ICID。如果您想進一步瞭解ESA嘗試傳送時發生了什麼情況，請grep獲取DCID。

3. 為了確定消息送達的位置，請搜尋DCID。

```
mail.example.com> grep
Currently configured logs:
16. "mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll
Enter the number of the log you wish to grep.
[]> 16
Enter the regular expression to grep.
[]> DCID 14
Do you want this search to be case insensitive? [Y]>
Do you want to tail the logs? [N]>
Do you want to paginate the output? [N]>
Fri Feb 3 15:42:06 2006 Info: New SMTP DCID 14 interface 192.168.0.199
address 10.1.1.112 port 25
Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0]
Fri Feb 3 15:42:11 2006 Info: DCID 14 close
```

請注意，此消息通過埠25從192.168.0.199介面傳送到IP地址為10.1.1.112的主機。

如果未嘗試傳送，但郵件已排隊等待傳送，則表示系統在與目標伺服器通訊時可能遇到困難。您可以在CLI中使用hoststatus來檢視收件人主機的狀態是否為Down，並驗證已排序的IP是否與目標域的SMTP路由或公共MX記錄（如果適用）匹配。