郵件從隔離區釋放時，該郵件記錄到何處？

目錄

簡介

本文說明如何檢視郵件日誌，以確定從思科郵件安全裝置(ESA)或思科安全管理裝置(SMA)隔離區釋放的郵件的處理情況。

郵件從隔離區釋放時，該郵件記錄到何處？

在ESA上，當您從IronPort垃圾郵件隔離區(ISQ)、策略隔離區或其他自定義隔離區釋放郵件時，該操作和相關事件將在IronPort文本郵件日誌(mail_logs)檔案中報告。日誌條目與原始MID關聯。

跟蹤此資訊的最佳方式是獲取被隔離的原始郵件的*發件人*、*收件人*或*主題*。接下來，在日誌中搜尋該郵件，檢視它是否已從隔離區釋放，然後檢視最終郵件伺服器是接受還是將其退回。

例如，搜尋發件人"spam@test.com"的郵件日誌：

```
> grep -i "spam@test.com" mail_logs
Wed Aug 13 12:59:36 2014 Info: MID 1357 ICID 10152 From: <spam@test.com>
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: mailfrom identity spam@test.com None
Wed Aug 13 12:59:57 2014 Info: MID 1357 ready 185 bytes from <spam@test.com>
```

您需關注郵件ID(MID)和傳遞連線ID(DCID)。

我們可以從完整的mail_logs或郵件跟蹤中看到此特定的MID已傳送到垃圾郵件隔離區：

```
Wed Aug 13 12:59:29 2014 Info: New SMTP ICID 10152 interface Management
(192.168.0.199) address 75.111.22.123 reverse dns host spam.test.com verified yes
Wed Aug 13 12:59:29 2014 Info: ICID 10152 RELAY SG RELAY_SG match 75.111.22.123
SBRS not enabled
Wed Aug 13 12:59:36 2014 Info: Start MID 1357 ICID 10152
Wed Aug 13 12:59:36 2014 Info: MID 1357 ICID 10152 From: <spam@test.com>
Wed Aug 13 12:59:40 2014 Info: MID 1357 ICID 10152 RID 0 To: <end_user@domain.com>
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: helo identity postmaster None
Wed Aug 13 12:59:42 2014 Info: MID 1357 SPF: mailfrom identity spam@test.com None
Wed Aug 13 12:59:57 2014 Info: MID 1357 SPF: pra identity None headers None
Wed Aug 13 12:59:57 2014 Info: MID 1357 Message-ID '<9afe3f$1ad@my_esa.domain.com>'
Wed Aug 13 12:59:57 2014 Info: MID 1357 Subject 'This is spam?'
Wed Aug 13 12:59:57 2014 Info: MID 1357 ready 185 bytes from <spam@test.com>
Wed Aug 13 12:59:57 2014 Info: MID 1357 matched all recipients for per-recipient
```

```
policy DEFAULT in the outbound table
Wed Aug 13 12:59:58 2014 Info: MID 1357 interim verdict using engine: CASE
spam positive
Wed Aug 13 12:59:58 2014 Info: MID 1357 using engine: CASE spam positive
Wed Aug 13 12:59:58 2014 Info: ISQ: Tagging MID 1357 for quarantine
Wed Aug 13 12:59:58 2014 Info: MID 1357 interim AV verdict using Sophos CLEAN
Wed Aug 13 12:59:58 2014 Info: MID 1357 antivirus negative
Wed Aug 13 12:59:58 2014 Info: MID 1357 Outbreak Filters: verdict negative
Wed Aug 13 12:59:58 2014 Info: MID 1357 DLP no violation
Wed Aug 13 12:59:58 2014 Info: MID 1357 queued for delivery
Wed Aug 13 13:00:02 2014 Info: RPC Delivery start RCID 161 MID 1357 to local IronPort
Spam Quarantine
Wed Aug 13 13:00:08 2014 Info: ISQ: Quarantined MID 1357
Wed Aug 13 13:00:08 2014 Info: RPC Message done RCID 161 MID 1357
Wed Aug 13 13:00:08 2014 Info: Message finished MID 1357 done
Wed Aug 13 13:05:11 2014 Info: ICID 10152 close
```

發佈後，下面是從ISQ發佈的消息中查詢內容的示例：

```
Wed Aug 13 13:02:14 2014 Info: Start MID 1359 ICID 0 (ISQ Released Message)
Wed Aug 13 13:02:14 2014 Info: ISQ: Reinjected MID 1357 as MID 1359
Wed Aug 13 13:02:14 2014 Info: MID 1359 ICID 0 From: <spam@test.com>
Wed Aug 13 13:02:14 2014 Info: MID 1359 ICID 0 RID 0 To: <end_user@domain.com>
Wed Aug 13 13:02:14 2014 Info: MID 1359 Subject '[SPAM] This is spam?'
Wed Aug 13 13:02:14 2014 Info: MID 1359 ready 1445 bytes from <spam@test.com>
Wed Aug 13 13:02:14 2014 Info: MID 1359 queued for delivery
Wed Aug 13 13:02:14 2014 Info: New SMTP DCID 165 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Aug 13 13:02:15 2014 Info: Delivery start DCID 165 MID 1359 to RID [0]
Wed Aug 13 13:02:15 2014 Info: Message done DCID 165 MID 1359 to RID [0]
Wed Aug 13 13:02:15 2014 Info: MID 1359 RID [0] Response '2.0.0 Ok: queued as
33B7380356'
Wed Aug 13 13:02:15 2014 Info: Message finished MID 1359 done
Wed Aug 13 13:02:20 2014 Info: DCID 165 close
```

在本示例中，消息被釋放，並且介面(192.168.0.199)是ESA上的偵聽器，連線到(192.168.0.200)作為最終傳送端郵件伺服器。

當您檢視垃圾郵件隔離區日誌(euq_logs)時，釋放操作會顯示以下資訊：

```
Wed Aug 13 13:02:14 2014 Info: ISQ: Releasing MID [1357] for all
Wed Aug 13 13:02:14 2014 Info: ISQ: Delivering released MID 1357 (skipping
work queue)
Wed Aug 13 13:02:14 2014 Info: ISQ: Corpus status: 0
Wed Aug 13 13:02:15 2014 Info: ISQ: Released MID 1357 to end_user@domain.com
Wed Aug 13 13:02:15 2014 Info: ISQ: Deleting MID [1357] for all
Wed Aug 13 13:02:15 2014 Info: ISQ: Deleted MID 1357 for all
Wed Aug 13 13:02:15 2014 Info: ISQ: Cleared 8192 bytes (MIDs 1, for all
recipients) from database. Current bytes=0.
```

同樣，如果原始郵件已隔離到策略隔離區，然後被釋放，您會看到與以下示例類似的消息：

```
Wed Aug 13 13:09:27 2014 Info: MID 1361 released from quarantine "Policy" (manual)
t=29
Wed Aug 13 13:09:27 2014 Info: MID 1361 released from all quarantines
Wed Aug 13 13:09:27 2014 Info: MID 1361 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Wed Aug 13 13:09:27 2014 Info: MID 1361 interim AV verdict using Sophos CLEAN
Wed Aug 13 13:09:27 2014 Info: MID 1361 antivirus negative
Wed Aug 13 13:09:27 2014 Info: MID 1361 queued for delivery
```

```
Wed Aug 13 13:09:27 2014 Info: New SMTP DCID 169 interface 192.168.0.199 address
192.168.0.200 port 25
Wed Aug 13 13:09:27 2014 Info: Delivery start DCID 169 MID 1361 to RID [0]
Wed Aug 13 13:09:27 2014 Info: Message done DCID 169 MID 1361 to RID [0]
Wed Aug 13 13:09:27 2014 Info: MID 1361 RID [0] Response '2.0.0 Ok: queued
as C702980356'
Wed Aug 13 13:09:27 2014 Info: Message finished MID 1361 done
Wed Aug 13 13:09:32 2014 Info: DCID 169 close
```

從策略隔離區中，郵件從策略隔離區釋放，並且介面(192.168.0.199)是ESA上的偵聽器，連線到(192.168.0.200)作為最終的傳遞終端郵件伺服器。

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 什麼是消息ID(MID)、注入連線ID(ICID)或傳遞連線ID(DCID)?
- 技術支援與文件 - Cisco Systems