メッセージが検疫から解放された場合は、ログのどこに記録されますか?

目次

概要

このドキュメントでは、Cisco Email Security Appliance（ESA）または Cisco Security Management Appliance（SMA）上の検疫から開放されたメッセージの処分を特定するためにメール ログを確認する方法について説明します。

メッセージが検疫から解放された場合は、ログのどこに記録されますか?

ESA 上で、IronPort Spam Quarantine（ISQ）、ポリシー検疫、またはその他のカスタム検疫からメッセージを解放すると、そのアクションと関連イベントが IronPort Text Mail Logs（mail_logs）ファイルで報告されます。 ログ エントリは元の MID で識別されます。

これを見つけ出すアプローチとして最善の方法は、検疫されていた元のメッセージの *From*、*To*、または *Subject* を探すことです。 次に、それを ログで検索して検疫から開放されたかどうかを確認し、エンド メール サーバがそれを受け入れたか、バウンスしたかを確認します。

送信者 "spam@test.com" のメール ログを検索する例：

```
> 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>
```

メッセージ ID（MID）と配信接続 ID（DCID）を中心に探してください。

この特定の MID がフル mail_logs またはメッセージ トラッキングからスパム検疫に送信されたことが確認できます。

```
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
```

解放後に、ISQ から解放されたメッセージで何を検索するかを示す例を以下に示します。

```
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
```

この例では、メッセージが解放され、インターフェイス（192.168.0.199）が、最終配信エンドメール サーバとして（192.168.0.200）に接続されている ESA 上のリスナーです。

Spam Quarantine Logs（euq_logs）を開くと、次のような解放アクションが表示されます。

```
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.
```

同様に、元のメッセージがポリシー検疫で検疫された後に解放された場合は、次の例のように表示されます。

```
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
```

メッセージがポリシー検疫から解放され、インターフェイス (192.168.0.199) が、最終配信エンド メール サーバとして (192.168.0.200) に接続されている ESA 上のリスナーです。

関連情報

- Cisco 電子メール セキュリティ アプライアンス - エンド ユーザ ガイド
- メッセージ ID (MID)、インジェクション接続 ID (ICID)、配信接続 ID (DCID) とは何か
- テクニカル サポートとドキュメント – Cisco Systems