

Quand un message est libéré de la quarantaine, où cela est connecté ?

Contenu

[Introduction](#)

[Quand un message est libéré de la quarantaine, où cela est connecté ?](#)

[Informations connexes](#)

Introduction

Ce document décrit comment visualiser la commande de logins de messagerie pour déterminer la disposition d'un message libéré de la quarantaine sur l'appliance de sécurité du courrier électronique de Cisco (ESA) ou l'appliance de Gestion de sécurité Cisco (SMA).

Quand un message est libéré de la quarantaine, où cela est connecté ?

Sur l'ESA, quand vous libérez un message de la quarantaine de la quarantaine (ISQ), de la stratégie de Spam d'IronPort, ou de toute autre quarantaine faite sur commande, que l'action et l'événement associé est signalé dans le fichier de logs de messagerie des textes d'IronPort (mail_logs). L'entrée de journal est affiliée avec le MID d'origine.

La meilleure manière d'approcher dépister ceci est vers le bas d'obtenir *de*, *à*, ou le *sujet du* premier message qui a été mis en quarantaine. Ensuite, recherchez-le dans le log pour voir s'il était libéré de la quarantaine, et puis pour voir si le serveur de messagerie d'extrémité la recevait ou la rebondissait.

L'exemple, recherchant la messagerie se connecte pour l'expéditeur « spam@test.com » :

```
> 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>
```

Vous voudrez prêter l'attention à l'ID de message (MID) et à l'ID de connexion de la livraison (DCID).

Nous pouvons voir que ce MID particulier a été envoyé à la quarantaine de Spam des pleins mail_logs, ou au cheminement de message :

```
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

```

Une fois que relâché, est ci-dessous un exemple de ce qu'à rechercher dans un message qui est relâché de l'ISQ :

```

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

```

Dans cet exemple, le message est libéré, et l'interface (192.168.0.199) est l'auditeur sur l'ESA, se connectant à (192.168.0.200) en tant que serveur de messagerie final d'extrémité de la livraison.

Quand vous regardez les logs de quarantaine de Spam (euq_logs), l'action de release affiche ce qui suit :

```

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.

De même, si le premier message avait mis en quarantaine à la quarantaine de stratégie, et alors libéré, vous verriez semblable à cet exemple :

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

De la quarantaine de stratégie, le message est libéré de la quarantaine de stratégie, et l'interface (192.168.0.199) est l'auditeur sur l'ESA, se connectant à (192.168.0.200) en tant que serveur de messagerie final d'extrémité de la livraison.

Informations connexes

- [Appliance de sécurité du courrier électronique de Cisco - Guides d'utilisateur](#)
- [Quel est un ID de message \(MID\), l'ID de connexion d'injection \(ICID\), ou l'ID de connexion de la livraison \(DCID\) ?](#)
- [Support et documentation techniques - Cisco Systems](#)