메시지가 격리에서 릴리스되면 로깅된 위치는 어디입니까?

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance) 또는 Cisco SMA(Security Management Appliance)에서 격리에서 릴리스된 메시지의 속성을 확인하기 위해 메일 로그를 보는 방법에 대해 설명합니다.

메시지가 격리에서 릴리스되면 로깅된 위치는 어디입니까?

ESA에서 ISQ(IronPort Spam Quarantine), 정책 격리 또는 기타 사용자 지정 격리에서 메시지를 릴리스하면 해당 작업 및 관련 이벤트가 IronPort Text Mail Logs(mail_logs) 파일에 보고됩니다.로그 항목은 원래 MID와 연결됩니다.

이를 추적하는 가장 좋은 방법은 격리된 원본 메시지의 *From*, *To* 또는 *Subject*를 가져오는 것입니다.그런 다음 로그에서 해당 항목을 검색하여 격리에서 해제되었는지 확인한 다음 최종 메일 서버가 이를 수락했는지 또는 반송했는지 확인합니다.

예: 발신자 "spam@test.com"에 대한 메일 로그 검색:

```
> 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>
```

메시지 ID(MID) 및 DCID(Delivery Connection ID)에 주의를 기울여야 합니다.

이 특정 MID가 전체 mail_logs 또는 메시지 추적에서 스팸 격리로 전송된 것을 확인할 수 있습니다.

```
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
```

릴리스되면 ISQ에서 릴리스된 메시지에서 찾을 항목의 예는 다음과 같습니다.

```
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
```

이 예에서는 메시지가 릴리스되고 인터페이스(192.168.0.199)이 ESA의 리스너로, 최종 전송 엔드 메일 서버로 (192.168.0.200)에 연결됩니다.

스팸 격리 로그(euq_logs)를 보면 릴리스 작업에 다음이 표시됩니다.

```
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.
```

마찬가지로, 원본 메시지가 정책 격리로 격리되고 릴리스된 경우 다음 예와 비슷한 결과가 표시됩니다.

```
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
```

정책 격리에서 메시지가 정책 격리에서 릴리스되고 인터페이스(192.168.0.199)이 ESA의 리스너로 최종 전송 엔드 메일 서버로 연결(192.168.0.200)됩니다.

관련 정보

- Cisco Email Security Appliance – 엔드 유저 가이드
- MID(Message ID), ICID(Injection Connection ID) 또는 DCID(Delivery Connection ID)란 무엇입니까?
- 기술 지원 및 문서 – Cisco Systems