ESA 메시지 처리 결정

목차

[소개](#)
[사전 요구 사항](#)
[메시지 추적](#)
[Findevent 명령](#)
[Grep 명령](#)
[예](#)

소개

이 문서에서는 Cisco ESA(Email Security Appliance)의 다양한 명령에서 검색한 메일 로그가 포함된 메시지의 속성을 확인하는 방법에 대해 설명합니다.

사전 요구 사항

이 문서의 정보는 다음을 기반으로 합니다.

- ESA
- 모든 버전의 AsyncOS

메시지 추적

AsyncOS for Email Version 6.0 이상을 실행하는 경우 특정 메시지에 발생한 상황을 확인하는 가장 효과적인 방법은 Monitor(모니터) 탭에서 Message Tracking(메시지 추적) 페이지를 사용하는 것입니다.이를 통해 사용이 간편한 웹 인터페이스에서 다양한 옵션을 사용하여 검색할 수 있습니다.

이전 버전을 실행하거나 문제 해결을 위해 모든 로그 행을 수집해야 하는 경우 다음 섹션에 자세히 설명된 대로 **grep** 또는 **findevent** 명령을 사용합니다.

Findevent 명령

AsyncOS for Email 버전 5.1.2 이상이 있는 경우 CLI **findvent** 명령을 사용하면 특정 메시지를 더 쉽게 검색할 수 있습니다.**Findevent**를 사용하면 봉투, 봉투 수신자 또는 메시지 Subject로 검색할 수 있습니다.이 작업은 경우에 관계없이 수행할 수 있습니다.메시지를 찾으면 해당 메시지와 관련된 모든 로그 라인을 반환할 수 있습니다.인수 없이 **findevent**를 실행하면 프로세스를 안내하기 위해 마법사가 실행됩니다.항상 **help** 명령을 사용하여 짧은 형식을 배울 수 있습니다.

```
> help findevent
```

```
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```
첫 번째 양식은 이름이 지정된 log_name 내에서 특정 봉투(from, subject 또는 envelope)를 검색하고 일치하는 메시지 ID(MID)를 나열합니다.대/소문자를 구분하지 않는 검색에 -i 플래그를 사용할 수 있습니다.

두 번째 양식은 지정된 MID에 대한 모든 로그 라인을 표시합니다.

이전 버전이 있는 경우 CLI **grep** 명령을 사용하여 동일한 작업을 수행할 수 있습니다.그러나 grep 명령을 사용하려면 ESA가 메시지 이벤트를 로깅하는 방법에 대한 자세한 정보가 필요합니다.

Grep 명령

메일 로그를 검색할 때의 첫 번째 과제는 메시지를 찾는 것입니다.발신자, 수신자 또는 제목을 검색하는 경우 이 작업을 수행할 수 있습니다.메시지를 찾은 후에는 메일 로그가 어떻게 구성되는지 이해하는 것이 중요합니다.Content Security 메일 로그 이벤트에는 약어가 제공됩니다.가장 중요한 이벤트는 ICID, MID, RID 및 DCID입니다.

수신 연결 ID(ICID):원격 호스트가 어플라이언스에 대한 연결을 설정하면 해당 연결에 ICID가 할당됩니다.하나의 ICID가 많은 MID를 생성할 수 있습니다.

> **참고:ICID 0**은 자체에서 삽입된 메시지를 정의합니다.실제로 ICID 또는 DCID 뒤의 숫자 0은 디바이스의 로컬 루프 주소에 열려 있거나 해당 디바이스에서 시작되는 세션을 나타냅니다.

중간:연결이 설정되면 성공한 각 SMTP(Simple Mail Transfer Protocol) **메일 수신:**새 MID를 생성합니다.단일 MID는 많은 RID를 생성할 수 있습니다.

받는 사람 ID(RID):각 수신자(받는 사람:참조:또는 숨은 참조에서 RID를 가져옵니다.RID는 소프트 바운스(연결 오류)가 있고 전달을 다시 시도하면 여러 DCID만 생성합니다.

배달 연결 ID(DCID):동일한 대상 도메인으로 이동하는 각 수신자는 수신 시스템의 한도까지 동일한 DCID를 받습니다.따라서 메시지의 수신자가 모두 동일한 도메인으로 이동할 경우 모든 RID에 대해 하나의 DCID가 있습니다.대신 각 RID가 별도의 도메인으로 이동하면 일대일 상관관계가 발생합니다.

> **참고:DCID 0**은 보내지 않은 메시지를 정의합니다.실제로 ICID 또는 DCID 뒤의 숫자 0은 디바이스의 로컬 루프 주소에 열려 있거나 해당 디바이스에서 시작되는 세션을 나타냅니다.

일반적으로 메시지를 찾으면 MID가 표시됩니다.그런 다음 MID에 만족하고 ICID 및 RID를 결정합니다.ICID를 사용하여 발신자에 대한 SBRS(SenderBase Reputation Score)를 확인할 수 있습니다.RID와 DCID를 함께 사용하면 ESA가 전달을 시도할 때 발생한 상황을 확인할 수 있습니다.

> **참고:**MID, ICID 및 DCID가 있으면 메시지의 원본이 가장 오래된 메일 로그보다 오래되지 않은 경우 한 **grep**에서 해당 메시지의 모든 행을 검색할 수 있습니다.

예

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

1. 메시지 제목 검색:

```
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'
```

이렇게 하면 제목에 **테스트**가 포함된 여러 일치가 생성됩니다.메시지는 오후 3시 42분 경에 전송되었으므로 다음 검색에 해당 MID를 사용할 수 있습니다.

다음은 이 질문에 대한 몇 가지 중요한 사항입니다.

이 검색을 대/소문자를 구분하지 않도록 하시겠습니까?[Y]>
이 질문에 **예**로 대답하면, 대소문자를 구분하지 않고 항목을 찾습니다.

로그를 미닫으시겠습니까?[N]>
이 질문에 **예**로 답하면 새 항목이 생성되면 해당 항목만 찾습니다.일부 로그 파일은 검색되지 않습니다.모든 로그를 검색하려면 No를 선택합니다.

출력을 페이징하시겠습니까?[N]>
이 질문에 **예**로 답하면 한 번에 한 페이지씩 항목이 표시됩니다.이 기능은 일반 검색을 수행해야 하고 많은 항목을 검색해야 하는 경우에 유용합니다.이렇게 하면 항목이 화면에서 스크롤되지 않습니다.

2. MID 검색:

```
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
```

MID 항목은 메시지가 처리되는 방식에 대한 자세한 정보를 제공합니다.MID 항목은 ICID 및 DCID도 참조합니다.수신 연결에 대해 자세히 알아보려면 ICID에 대해 grep를 참조하십시오 .ESA가 전달을 시도할 때 발생한 상황에 대해 자세히 알아보려면 DCID에 **대해** grep를 참조하십시오.

3. 메시지가 전달된 위치를 확인하려면 DCID를 검색합니다.

```
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
```

메시지가 **192.168.0.199** 인터페이스에서 포트 25를 통해 IP 주소 **10.1.112**를 사용하는 호스트로 전달되었습니다.

전달을 시도하지 않았지만 메시지가 전달을 **위해 대기된** 경우 시스템이 대상 서버와의 통신에 문제가 있음을 나타냅니다.수신자 호스트의 상태가 **Down**인지 확인하고, 주문 IP가 목적지 도메인에 대한 SMTP 경로 또는 퍼블릭 MX 레코드와 일치하는지 확인하기 위해 CLI에서 호스트 상태를 사용할 수 있습니다.