ESA メッセージ破棄の判別

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス（ESA）のさまざまなコマンドから取得されるメール ログによるメッセージの処理を決定する方法について説明します。

前提条件

このドキュメントの情報は、次のハードウェアに基づくものです。

- ESA
- AsyncOS のすべてのバージョン

メッセージ トラッキング

AsyncOS for Email バージョン 6.0 以降を実行する場合、特定のメッセージがどうなるかを判断する最も効果的な方法は、[Monitor] タブから [Message Tracking] ページを使用することです。これにより、使いやすい Web インターフェイスのさまざまなオプションを使って検索することができます。

これよりも古いバージョンを実行している場合、または、トラブルシューティングのためにすべての ログ行を収集する必要がある場合は、次のセクションで詳しく説明する **grep** コマンドや **findevent** コマンドを使用します。

Findevent コマンド

AsyncOS for Email バージョン 5.1.2 以降である場合は、CLI の **findevent** コマンドを使用すると、特定のメッセージを簡単に検索できます。 **Findevent** ではエンベロープ送信者、エンベロープ受信者、メッセージの件名で検索することができます。 大文字と小文字に関係なく検索することもできます。 メッセージを見つけたら、そのメッセージに関連した ログ行に戻ることができます。 引数を使用せずに **findevent** を実行した場合、処理のガイドを行うウィザードが起動します。短縮形式を知るために、通常どおり、**help コマンド**を使用できます。

```
> help findevent
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```

最初の形式では指定した log_name 内で特定のエンベロープ送信者、件名、エンベロープ受信者を検索し、それに一致するメッセージ ID (MID) をリストします。 -i フラグは大文字と小文字を区別しない検索に使用できます。

2 番目の形式は、指定した MID のすべてのログ行を表示します。

古いバージョンを使用している場合は、CLI の **grep コマンド**を使用して同じことを行うことができます。 ただし、**grep コマンド**を使用するには、ESA がメッセージ イベントを記録する方法についてより詳しい知識が必要です。

Grep コマンド

メール ログを検索するときの最初の難所は、目的のメッセージを見つけることです。 送信者、受信者、または件名を検索する場合は、これが可能です。 メッセージが見つかったら、メール ログがどのように構成されているかを理解することが重要です。 コンテンツ セキュリティのメール ログ イベントには頭字語が与えられます。 最も重要なイベントは ICID、MID、RID、および DCID です。

インジェクション接続 ID (ICID) リモート ホストがアプライアンスへの接続を確立すると、その接続には ICID が割り当てられます。 1 つの ICID から多くの MID を生成できます。

> **注: ICID 0** は、自身が挿入したメッセージを定義します。 実際には、後ろに数字 0 が付いた ICID や DCID は、デバイスのローカル ループ アドレスとやり取りするために開かれたセッションを意味します。

MID : 接続が確立されると、Simple Mail Transfer Protocol (SMTP) が正常に実行されるたびに **mail from:** コマンドにより、新しい MID が作成されます。 1 つの MID から多くの RID を生成できます。

受信者 ID (RID) : 各受信者 (To: Cc: または Bcc) は 1 つの RID を取得します。 RID が複数の DCID を生成するのは、ソフト バウンス (接続エラー) があり、配信が再試行される場合のみです。

配信接続 ID (DCID) : 同じ宛先ドメインになる各受信者は、受信するシステムの上限まで同じ DCID を受け取ります。 そのため、あるメッセージの受信者全員が同じドメインの場合、すべての RID に対して 1 つの DCID が割り当てられます。 そうではなく、各 RID が別々のドメインになる場合は、1 対 1 の関係になります。

> **注: DCID 0** は、送信されなかったメッセージを定義します。 実際には、後ろに数字 0 が付いた ICID や DCID は、デバイスのローカル ループ アドレスとやり取りするために開かれたセッションを意味します。

通常、メッセージが見つかったら、MID がわかります。 その後、grep を使用して MID を検索し、ICID と RID を判定します。 ICID で、送信者の SenderBase レピュテーション スコア (SBRS) を確認できます。 RID およびその後の DCID で、ESA が配信を試行したときに何か起こったのか確認できます。

注: メッセージの最初が最も古いメール ログよりも古くなければ、MID、ICID、DCID がわかれば 1 回の **grep** でそのメッセージのすべての行を検索できます。

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

例

1. メッセージの件名の検索：

```
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'
```

これにより、件名に **test** が含まれている複数の一致が生成されました。 メッセージは 3:42 pm 頃に送信されたので、次の検索には MID を使用できます。

質問については注意すべき重要なポイントがいくつかあります。

Do you want this search to be case insensitive? (この検索で大文字小文字を区別しますか？) [Y]>
この質問に「**Yes**」と答えると、大文字小文字に関係なく、エントリが検索されます。

Do you want to tail the logs? (ログの最後を表示しますか？) [N]>
この質問に「**Yes**」と答えると、新しく生成されたエントリだけが検索されます。 ログ ファイル全部は検索されません。 すべてのログを検索するには、「No」を選択します。

Do you want to paginate the output? (出力をページングしますか？) [N]>
この質問に「**Yes**」と答えると、一度に 1 ページのエントリが表示されます。 これは一般的な検索を実行する必要があり、多くのエントリ取得が予想される場合に便利です。 こうすることにより、エントリでディスプレイがスクロールされていくのを防ぐことができます。

2. MID 検索：

```
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 のエントリは、メッセージの処理方法についてより詳しい情報を提供することに注意してください。 MID のエントリは ICID および DCID も参照します。 着信接続についてより詳しい情報を知るには、ICID に対して grep を実行します。 ESA が配信を試行したときに何が起こったかについてより詳しい情報を知るには、CDIC に対して grep を実行します。

3. メッセージがどこに配信されたかを特定するには、DCID を検索します。

```
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
```

このメッセージは **192.168.0.199** インターフェイスから、ポート 25 を介して IP アドレスが 10.1.1.112 のホストに配信されたことがわかります。

配信は試行されなかったにもかかわらず、メッセージが**配信のためにキューに置かれた**場合は、システムで宛先サーバとの通信に問題があることを示します。 CLI で **hoststatus** を使用し、受信者のホストのステータスが **[Down]** であるかどうかを調べ、順番が付けられた IP が宛先ドメインの SMTP ルートか、パブリック MX レコード（該当する場合）の SMTP ルートのどちらに一致するのか検証できます。