# Come posso identificare e risolvere una situazione di loop postale sull'ESA?

## Sommario



## Introduzione

In questo documento viene descritto come identificare un loop di posta su Email Security Appliance (ESA).

## Premesse

I loop di posta possono essere indicati da messaggi con lo stesso Message-ID inseriti più di 3 volte. I loop di posta possono causare sintomi di CPU elevata, recapito lento e problemi di prestazioni complessive. Normalmente, gli ID dei messaggi immessi più di una volta indicano un ciclo continuo, ma a volte vengono inseriti più di una volta a causa di problemi, oppure potrebbe trattarsi di uno spammer disordinato che continua a inserire lo stesso messaggio di posta indesiderata con lo stesso Message-ID.

In genere, un loop di posta è causato da un problema dell'infrastruttura di posta elettronica che invia lo stesso messaggio o insieme di messaggi in tutta la rete dal server di posta al server di posta all'infinito.  Anche se questi messaggi possono rimanere intrattenuti in questo modo per molto tempo, non è una buona cosa né per la vostra larghezza di banda di rete né per i costi di elaborazione ESA sostenuti.

## Soluzione

Identificare un loop di posta, se si sospetta che questo possa essere il problema, di solito è abbastanza facile anche se è necessario fare la palla degli occhi.
Accedere all'interfaccia della riga di comando (CLI) del sistema ed eseguire uno di questi comandi o entrambi, a seconda dei vantaggi che si ottengono:

```
grep "Subject" mail_logs
grep "Message-ID" mail_logs
```

In particolare per la ricerca su ID-messaggio, se si vedono istanze ricorrenti dello stesso ID, allora si saprà che si ha un loop di posta.  In alcuni casi, tuttavia, questo non è sufficiente, in quanto uno

dei server di posta che recupera lo stesso messaggio potrebbe essere utile modificare o rimuovere l'intestazione Message-ID.  Se non si ottiene nulla identificabile con il controllo Message-ID procedere e provare il controllo Oggetto.

Supponendo che sia stato trovato il messaggio ciclico in base all'ID messaggio, si desidera trovare anche altre informazioni sul messaggio e sulla relativa connessione padre (ICID). Dato il Message-ID e un MID nella stessa riga di log, è possibile eseguire:

```
grep -e "MessageID_I_found" -e "MID 123456" mail_logs
```

Dato l'output risultante, è possibile trovare l'ICID e il DCID pertinenti ed eseguire:

```
grep -e "MessageID_I_found" -e "MID 123456" -e "ICID 1234567" -e "DCID 2345767" mail_logs
```

A questo punto, è necessario disporre della connessione completa, ovvero la transazione dei messaggi, e verificare l'origine e la destinazione del recapito, se tale operazione è già stata eseguita. Dopo aver identificato il messaggio ciclico, il passaggio successivo consiste nell'esaminarlo per risolvere il problema.  Senza risolvere la causa del loop, è probabile che questo messaggio e altri continuino a ripetersi o che il problema si ripresenti presto.

Creare un filtro messaggi simile al seguente:

```
loganddrop_looper:
if(header("Message-ID") == "MessageID_I_found") {
  archive("looper");
  drop();
}
```

Eseguire il commit della modifica ed eseguire questo comando per estrarre il messaggio:

```
tail looper
```

Con le informazioni che è possibile ottenere sul sistema remoto esaminando i log di posta, e altre informazioni che è possibile ottenere guardando il messaggio stesso, si dovrebbe essere in grado di determinare dove il vostro problema è.

## Come è possibile impedire che si verifichino loop di posta?

In ambienti complessi questo può essere difficile: capire come il flusso di posta nel tuo ambiente e come una nuova rete, sia su ESA che su un altro dispositivo, influirà su quel traffico è fondamentale. Una causa comune dei loop di posta in fuga è la rimozione dell'intestazione Received.  L'ESA rileva e interrompe automaticamente un loop di posta quando vede 100 intestazioni Ricevute in un messaggio, ma l'ESA consente la rimozione di questa intestazione, che spesso porta a un loop di posta errato.  A meno che non ci sia un *motivo veramente* valido per farlo, non spegnere l'intestazione Received o fare in modo che venga rimossa.

Di seguito è riportato un esempio di filtro che può aiutare a prevenire o correggere un loop di posta:

```
External_Loop_Count:
if (header("X-ExtLoop1")) {
 if (header("X-ExtLoopCount2")) {
```

```
   if (header("X-ExtLoopCount3")) {
     if (header("X-ExtLoopCount4")) {
       if (header("X-ExtLoopCount5")) {
         if (header("X-ExtLoopCount6")) {
           if (header("X-ExtLoopCount7")) {
             if (header("X-ExtLoopCount8")) {
               if (header("X-ExtLoopCount9")) {
                  notify ('joe@example.com');
                  drop();
               }
             else {insert-header("X-ExtLoopCount9", "from
                  $RemoteIP");}}
           else {insert-header("X-ExtLoopCount8", "from $RemoteIP");}}
         else {insert-header("X-ExtLoopCount7", "from $RemoteIP");}}
       else {insert-header("X-ExtLoopCount6", "from $RemoteIP");}}
     else {insert-header("X-ExtLoopCount5", "from $RemoteIP");}}
   else {insert-header("X-ExtLoopCount4", "from $RemoteIP");}}
 else {insert-header("X-ExtLoopCount3", "from $RemoteIP");}}
else {insert-header("X-ExtLoopCount2", "from $RemoteIP");}}
else {insert-header("X-ExtLoop1", "1"); }
```