Determinazione della disposizione del messaggio ESA

Sommario

Introduzione

In questo documento viene descritto come determinare la disposizione di un messaggio con i log di posta recuperati da diversi comandi di Cisco Email Security Appliance (ESA).

Prerequisiti

Le informazioni fornite in questo documento si basano su:

- ESA
- Tutte le versioni di AsyncOS

Verifica messaggi

Se si esegue AsyncOS for Email Version 6.0 o versioni successive, il modo più efficace per determinare il problema che si è verificato a un determinato messaggio è utilizzare la pagina Verifica messaggio della scheda Monitor. In questo modo è possibile eseguire ricerche con una varietà di opzioni in un'interfaccia Web di facile utilizzo.

Se si esegue una versione precedente o è necessario raccogliere tutte le righe di registro per la risoluzione dei problemi, utilizzare i comandi **grep** o **findevent** come descritto nelle sezioni successive.

Comando Findevent

se si dispone di AsyncOS for Email Version 5.1.2 o versioni successive, il comando **findevent della** CLI semplifica la ricerca di un messaggio specifico. **Findevent** consente di eseguire la ricerca in base alla busta di, al destinatario della busta o all'oggetto del messaggio. Ciò può essere fatto indipendentemente dal caso. Una volta trovato il messaggio, è possibile restituire tutte le righe di

registro relative al messaggio. Se si esegue **findevent** senza argomenti, viene avviata una procedura guidata che consente di eseguire in modo semplificato il processo. Come sempre, è possibile utilizzare il comando **help** per ottenere informazioni sulla forma breve:

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

La prima maschera esegue la ricerca di una busta specifica da, oggetto o busta all'interno del nome_log specificato ed elenca gli ID messaggio (ID messaggio) corrispondenti. Il flag -i può essere utilizzato per ricerche che non fanno distinzione tra maiuscole e minuscole.

La seconda maschera visualizza tutte le righe di log per il MID specificato.

Se si ha una versione precedente, è possibile usare il comando **grep** della CLI per ottenere la stessa cosa. Tuttavia, l'uso del comando **grep** richiede una conoscenza più dettagliata di come le ESA registrano gli eventi dei messaggi.

Comando Grep

La prima sfida quando si esegue una ricerca nei log di posta è trovare il messaggio. È possibile eseguire questa operazione se si cerca il mittente, il destinatario o l'oggetto. Dopo aver trovato il messaggio, è importante comprendere come sono organizzati i log di posta. Agli eventi del registro di posta di Protezione contenuto vengono assegnati degli acronimi. Gli eventi più importanti sono ICID, MID, RID e DCID.

ID connessione iniezione (ICID): Quando un host remoto stabilisce una connessione con l'accessorio, a tale connessione viene assegnato un ICID. Un ICID può generare molti MID.

> **Nota: ICID 0** definisce un messaggio inserito da se stesso. Infatti, il numero 0 dopo un ICID o DCID si riferisce alle sessioni aperte dall'indirizzo del loop locale del dispositivo o verso di esso.

MID: Una volta stabilita una connessione, ogni messaggio SMTP (Simple Mail Transfer Protocol) inviato correttamente **da:** crea un nuovo MID. Un singolo MID può generare molti RID.

ID destinatario (RID): Ogni destinatario (A: Cc o Ccn ottiene un RID. I RID generano più DCID solo se si verifica un soft bounce (errore di connessione) e viene eseguito un nuovo tentativo di recapito.

ID connessione recapito (DCID): Ogni destinatario che si reca allo stesso dominio di destinazione riceve lo stesso DCID fino ai limiti del sistema ricevente. Pertanto, se i destinatari di un messaggio appartengono tutti allo stesso dominio, sarà disponibile un unico DCID per tutti i RID. Se invece ogni RID viene assegnato a un dominio separato, esiste una correlazione uno-a-uno.

> **Nota: DCID 0** definisce un messaggio che non è mai stato inviato. Infatti, il numero 0 dopo un ICID o DCID si riferisce alle sessioni aperte dall'indirizzo del loop locale del dispositivo o verso di esso.

In genere, quando si trova un messaggio, è possibile trovarne il MID. Quindi si consiglia di

utilizzare il MID e di determinare l'ICID e il RID. L'ICID consente di determinare il punteggio SBRS (SenderBase Reputation Score) del mittente. Con il RID e poi il DCID, è possibile determinare cosa è successo quando l'ESA ha tentato la consegna.

> **Nota:** Una volta ottenuto il MID, l'ICID e il DCID, è possibile recuperare tutte le righe del messaggio in un solo **grep**, se l'origine del messaggio non è precedente al log di posta meno recente.

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

Esempio

1. Cerca oggetto del messaggio:

```
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'
```

Sono state generate diverse corrispondenze contenenti il **test** nell'oggetto. Il messaggio è stato inviato alle 15.42 circa, quindi puoi utilizzare quel MID per la ricerca successiva.

Ecco alcuni punti importanti da notare riguardo le domande:

Non si desidera distinguere tra maiuscole e minuscole nella ricerca? [S]>
Se si risponde **Sì** a questa domanda, verranno trovate le voci indipendentemente dalla distinzione tra maiuscole e minuscole.

Eseguire la coda dei registri? [N]>
Se si risponde **Sì** a questa domanda, verranno trovate solo le nuove voci generate. Non esegue la ricerca in tutti i file di registro. Scegliere **No** per eseguire la ricerca in tutti i log.

Impaginare l'output? [N]>

Se si risponde **Sì** a questa domanda, verranno visualizzate le voci una pagina alla volta. Ciò è utile se è necessario eseguire una ricerca generale e si prevede di recuperare molte voci. In questo modo si interrompe lo scorrimento delle voci all'esterno dello schermo.

2. Cerca MID:

```
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
```

Si noti che le voci MID forniscono ulteriori informazioni sulla modalità di elaborazione del messaggio. Le voci MID fanno riferimento anche all'ICID e al DCID. Per ulteriori informazioni sulla connessione in ingresso, **utilizzare** l'ICID. Se si desidera saperne di più su cosa è successo quando l'ESA ha tentato la consegna, **grep** per il DCID.

3. Per determinare la destinazione del messaggio, cercare il DCID.

```
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
```

Notare che il messaggio è stato consegnato dall'interfaccia **192.168.0.199** all'host con indirizzo IP **10.1.1.12** sulla porta 25.

Se il recapito non è stato tentato, ma il messaggio è stato **accodato per il recapito**, è possibile che il sistema abbia difficoltà nelle comunicazioni con il server di destinazione. È possibile usare **hoststatus** dalla CLI per verificare se lo stato dell'host del destinatario è **Inattivo** e per verificare che gli IP ordinati corrispondano alle route SMTP per il dominio di destinazione o ai record MX pubblici, a seconda del caso.