détermination de la disposition des messages ESA

Table des matières

[Introduction](#)
[Conditions préalables](#)
[Suivi des messages](#)
[Commande Findevent](#)
[Grep, commande](#)
[Exemple](#)

Introduction

Ce document décrit comment déterminer la disposition d'un message avec les journaux de messagerie récupérés à partir de diverses commandes sur le dispositif de sécurité de la messagerie Cisco (ESA).

Conditions préalables

Les informations contenues dans ce document sont basées sur :

- ESA
- Toutes les versions d'AsyncOS

Suivi des messages

Si vous exécutez AsyncOS pour la version 6.0 ou ultérieure du courrier électronique, le moyen le plus efficace de déterminer ce qui est arrivé à un message particulier est d'utiliser la page Suivi des messages de l'onglet Surveillance. Vous pouvez ainsi effectuer des recherches à l'aide d'un grand nombre d'options dans une interface Web facile à utiliser.

Si vous exécutez une version plus ancienne ou que vous avez besoin de collecter toutes les lignes de journal à des fins de dépannage, utilisez les commandes grep ou findevent comme détaillé dans les sections suivantes.

Commande Findevent

Si vous disposez d'AsyncOS for Email Version 5.1.2 ou ultérieure, la commande CLI findevent simplifie la recherche d'un message spécifique. Findevent vous permet d'effectuer une recherche en fonction de l'enveloppe de, du destinataire de l'enveloppe ou de l'objet du message. Cela peut être fait quel que soit le cas aussi. Une fois que vous avez trouvé votre message, vous pouvez

renvoyer chaque ligne de journal correspondant à ce message. Si vous exécutez findevent sans argument, il lance un assistant afin de vous guider tout au long du processus. Comme toujours, vous pouvez utiliser la commande help afin d'apprendre la forme abrégée :

<#root>

>

help findevent

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

Le premier formulaire recherche une enveloppe spécifique à partir de, objet ou enveloppe dans le nom_journal nommé et répertorie les ID de message (MID) qui correspondent. L'indicateur -i peut être utilisé pour les recherches qui ne respectent pas la casse.

Le deuxième formulaire affiche toutes les lignes de journal pour le MID donné.

Si vous avez une version plus ancienne, la commande CLI grep peut être utilisée afin d'accomplir la même chose. Cependant, l'utilisation de la commande grep nécessite une connaissance plus détaillée de la façon dont les ESA consignent les événements de message.

Grep, commande

Le premier défi lorsque vous recherchez des journaux de messagerie est de trouver votre message. Vous pouvez le faire si vous recherchez l'expéditeur, le destinataire ou l'objet. Une fois que vous avez trouvé votre message, il est important de comprendre comment les journaux de messagerie sont organisés. Les événements du journal de messagerie de sécurité du contenu sont désignés par des acronymes. Les événements les plus importants sont ICID, MID, RID et DCID.

ICID (Injection Connection ID) : Lorsqu'un hôte distant établit une connexion à l'appliance, un ICID est affecté à cette connexion. Un ICID peut engendrer plusieurs MID.

> Remarque : ICID 0 définit un message qui a été injecté à partir de lui-même. En fait, le chiffre 0 après un ICID ou un DCID fait référence aux sessions ouvertes vers ou depuis l'adresse de boucle locale du périphérique.

MID : Une fois la connexion établie, chaque message SMTP (Simple Mail Transfer Protocol) provenant de : crée un nouveau MID. Un seul MID peut engendrer de nombreux RID.

ID du destinataire (RID) : Chaque destinataire (À : Cc : ou Cci obtient un RID. Les RID génèrent plusieurs DCID uniquement en cas de renvoi progressif (erreur de connexion) et de nouvelle tentative de remise.

ID de connexion de remise (DCID) : Chaque destinataire qui se dirige vers le même domaine de destination reçoit le même DCID jusqu'aux limites du système de réception. Donc, si les destinataires d'un message vont tous au même domaine, alors il y a un DCID pour tous les RID. Si, au lieu de cela, chaque RID va à un domaine séparé, alors il y a une corrélation un-à-un.

> Remarque : Le DCID 0 définit un message qui n'a jamais été envoyé. En fait, le chiffre 0 après un ICID ou un DCID fait référence aux sessions ouvertes vers ou depuis l'adresse de boucle locale du périphérique.

Généralement, lorsque vous trouvez votre message, vous trouvez son MID. Ensuite, vous effectuez un grep pour le MID et déterminez l'ICID et le RID. Avec l'ICID, vous pouvez déterminer le score de réputation SenderBase (SBRS) pour l'expéditeur. Avec le RID, puis le DCID, vous pouvez déterminer ce qui s'est passé lorsque l'ESA a tenté d'effectuer la livraison.

> Remarque : Une fois que vous avez MID, ICID et DCID, vous pouvez récupérer toutes les lignes pour ce message dans un grep, si l'origine du message n'est pas plus ancienne que votre journal de messagerie le plus ancien.

<#root>

example.com>

grep -e " MID 11123" -e " ICID 11092" -e " DCID 23349" mail_logs

Exemple

1. Recherchez l'objet du message :

<#root>

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'
```

Cela a généré plusieurs correspondances qui contenaient test dans le sujet. Le message a été envoyé vers 15h42. Vous pouvez donc utiliser ce MID pour la prochaine recherche.

Voici quelques points importants à noter à propos des questions :

- Voulez-vous que cette recherche ne respecte pas la casse ? [O]>
  Si vous répondez Oui à cette question, il trouve les entrées indépendamment de la casse.

- Voulez-vous suivre les journaux ? [N]>
  Si vous répondez Oui à cette question, il ne trouve les nouvelles entrées que lorsqu'elles sont générées. Il ne recherche pas tous les fichiers journaux. Choisissez No afin de rechercher tous les journaux.

- Voulez-vous paginer le résultat ? [N]>
  Si vous répondez Oui à cette question, les entrées s'affichent page par page. Ceci est utile si vous devez effectuer une recherche générale et vous attendre à récupérer de nombreuses entrées. Cela empêche les entrées de défiler hors de l'affichage.

2. Recherchez le MID :

<#root>

```
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
```

Notez que les entrées MID fournissent plus d'informations sur le traitement du message. Les entrées MID font également référence à l'ICID et au DCID. Si vous voulez en savoir plus sur la connexion entrante, grep pour l'ICID. Si vous voulez en savoir plus sur ce qui s'est passé quand l'ESA a tenté la livraison, grep pour le DCID.

3. Afin de déterminer où le message a été livré, recherchez le DCID.

<#root>

```
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
```

Notez que le message a été remis de l'interface 192.168.0.199 à l'hôte avec l'adresse IP 10.1.1.112 sur le port 25.

Si la remise n'a pas été tentée, mais que le message a été mis en file d'attente, cela indique que le système peut rencontrer des difficultés dans ses communications avec le serveur de destination. Vous pouvez utiliser hoststatus à partir de l'interface de ligne de commande afin de voir si l'état de l'hôte destinataire est Down et pour vérifier que les adresses IP commandées correspondent à vos routes SMTP pour le domaine de destination ou aux enregistrements MX publics, selon le cas.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.