Détermination de disposition de message ESA

Contenu

Introduction

Ce document décrit comment déterminer la disposition d'un message avec les logs de messagerie récupérés de diverses commandes sur l'appliance de sécurité du courrier électronique de Cisco (ESA).

Conditions préalables

Les informations dans ce document sont basées en fonction :

- ESA
- Toutes les versions d'AsyncOS

Cheminement de message

Si vous exécutez AsyncOS pour la version 6.0 ou ultérieures d'email, la plupart de façon efficace de déterminer ce qui est arrivée à un message particulier est d'utiliser le message dépistant la page de l'onglet de moniteur. Ceci te permet pour rechercher avec un grand choix d'options dans une interface web facile à utiliser.

Si vous exécutez une version plus ancienne ou devez recueillir toutes les lignes de log pour dépannage des buts, utilisez le **grep** ou les commandes **findevent** comme détaillé dans les sections suivantes.

Commande de Findevent

Si vous avez AsyncOS pour la version 5.1.2 ou ultérieures d'email, la commande **findevent** CLI le rend plus simple pour rechercher un message spécifique. **Findevent** vous permet de le rechercher par l'enveloppe de, le destinataire d'enveloppe, ou le sujet de message. Ceci peut être aussi bien fait indépendamment du cas. Une fois que vous trouvez votre message, vous pouvez renvoyer chaque ligne de log concernant ce message. Si vous exécutez **findevent** sans des arguments, il

lance un assistant afin de vous guider par le processus. En tant que toujours, vous pouvez employer la commande d'**aide** afin d'apprendre la forme courte :

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

La première forme conduit un rechercher une enveloppe de, un sujet, ou une enveloppe spécifique à dans le log_name Désigné et répertorie les id de message (MIDS) cette correspondance. - Je diminue peux être utilisé pour des recherches sensibles non dossier.

La deuxième forme affiche toutes les lignes de log pour le MID donné.

Si vous avez une version plus ancienne, la commande de **grep** CLI peut être utilisée afin d'accomplir la même chose. Cependant, l'utilisation de la commande de **grep** exige la connaissance plus détaillée de la façon dont des événements de message de log d'ESAs.

Commande de Grep

Le premier défi quand vous recherchez des logs de messagerie est de trouver votre message. Vous pouvez faire ceci si vous recherchez l'expéditeur, le destinataire, ou pour le sujet. Une fois que vous avez trouvé votre message, il est important de comprendre comment les logs de messagerie sont organisés. Des événements de log de messagerie de sécurité du contenu sont donnés des acronymes. Les événements les plus importants sont ICID, MID, SE DÉBARRASSENT, et DCID.

ID de connexion d'injection (ICID) : Quand un serveur distant établit une connexion à l'appliance, cette connexion est assignée un ICID. Un ICID peut engendrer beaucoup le MIDS.

> **Note**: **ICID 0** définit un message qui a été injecté de lui-même. En fait, le chiffre 0 après qu'un ICID ou un DCID se rapporte à des sessions ouvertes à ou de l'adresse de boucle locale du périphérique.

MID : Une fois qu'une connexion est établie, chaque **messagerie** réussie de Protocole SMTP (Simple Mail Transfer Protocol) **de :** la commande crée un nouveau MID. Un MID simple peut engendrer beaucoup se débarrasse.

ID réceptif (DÉBARRASSÉ) : Chaque destinataire (à : Cc : ou Bcc obtient DÉBARRASSÉ. Débarrasse seulement le frai plusieurs DCIDs s'il y a un rebond doux (erreur de connexion) et la livraison reattempted.

ID de connexion de la livraison (DCID) : Chaque destinataire qui va au même domaine de destination reçoit le même DCID jusqu'aux limites du système de réception. Ainsi si les receipients de l'des messages tous vont au même domaine, puis il y a un DCID pour le tout les se débarrasse. Si à la place, chacun DÉBARRASSÉ va à un domaine distinct, alors il y a une corrélation linéaire.

> **Note**: **DCID 0** définit un message qui n'a été jamais envoyé. En fait, le chiffre 0 après qu'un ICID ou un DCID se rapporte à des sessions ouvertes à ou de l'adresse de boucle locale du périphérique.

Généralement, quand vous trouvez votre message, vous trouvez son MID. Puis vous grep pour le MID et déterminez l'ICID et VOUS DÉBARRASSEZ. Avec l'ICID, vous pouvez déterminer le score de réputation de SenderBase (SBRS) pour l'expéditeur. Avec DÉBARRASSÉ et puis le DCID, vous pouvez déterminer ce qui s'est produit quand l'ESA a tenté la livraison.

> **Note**: Une fois que vous avez le MID, l'ICID, et le 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 log de messagerie plus ancien.

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

Exemple

1. Recherchez le sujet de message :

```
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'
```

Ceci a généré plusieurs correspondances qui ont contenu le **test** dans le sujet. Le message a été envoyé approximativement à 3:42pm, ainsi vous pouvez utiliser ce MID pour la prochaine recherche.

Voici quelques points impotant à noter au sujet des questions :

Voulez-vous que cette recherche soit-elle ne distinguant pas majuscules et minuscules ? [Y] **>**
Si vous répondez **oui à** cette question, elle trouve des entrées indépendamment du cas.

Voulez-vous suivre les logs ? [N] **>**
Si vous répondez **oui à** cette question, elle trouve seulement de nouvelles entrées pendant qu'elles sont générées. Il ne recherche pas tous les fichiers journal. Choisissez **aucun** afin de

rechercher tous les logs.

Voulez-vous paginer la sortie ? [N] **>**
Si vous répondez **oui à** cette question, elle affiche des entrées une page à la fois. C'est utile si vous devez faire une recherche générale et la compter récupérer beaucoup d'entrées. Ceci arrête les entrées de faire défiler hors fonction de l'affichage.

2. Recherchez le 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
```

Notez que les MI entrées fournissent plus d'informations au sujet de le comment le message est traité. Les MI entrées mettent en référence également l'ICID et le DCID. Si vous voulez connaître plus la connexion entrante, **grep** pour l'ICID. Si vous voulez connaître plus ce qui s'est produit quand le l'ESA a tenté la livraison, **grep** pour le DCID.

3. Afin de déterminer où le message a été fourni, recherchez le 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
```

Notez que le message a été fourni de l'interface de **192.168.0.199 à l'**hôte avec l'adresse IP **10.1.1.112** au-dessus du port 25.

Si la livraison n'était pas tentée, mais le message **était aligné pour la livraison**, il indique que le système pourrait avoir la difficulté dans ses transmissions avec le serveur cible. Vous pouvez employer le **hoststatus du** CLI afin de voir si le statut de l'hôte réceptif est **en baisse** et pour vérifier que la correspondance commandée IPS vos artères de SMTP pour le domaine de destination ou les enregistrements MX de public, comme applicable.