

Dépannez les emails sortants non désirés sur l'ESA des comptes compromis

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Dépannez](#)

[Contrôles de Workqueue](#)

[L'expéditeur ou le sujet des emails dans le Workqueue est connu](#)

[Contrôle de file d'attente de la livraison](#)

[Surveillance et action proactives](#)

[Informations connexes](#)

Introduction

Ce document décrit comment dépanner et corriger les files d'attente sur l'appliance de sécurité du courrier électronique (ESA) dans un événement qu'un compte d'utilisateur interne a été compromis et les emails unsolicited envoyés globalement.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations dans ce document sont basées sur AsyncOS 7.6 et plus tard pour l'ESA.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Dépannez

Il est recommandé de verrouiller en bas du compte qui envoie le Spam si on le connaît, autrement verrouillent en bas du compte une fois découvert par l'intermédiaire de l'enquête sur l'ESA.

Contrôles de Workqueue

Quand il y a un grand nombre d'emails dans le compteur de workqueue et le débit d'emails qui écrivent le système dépasse de loin le débit qui sortent du système, ceci indique qu'il y a une incidence sur le workqueue. Vous pouvez utiliser la commande de workqueue d'exécuter le contrôle.

```
C370.lab> workqueue status
```

```
Status as of: Thu Feb 06 12:48:02 2014 GMT
Status:      Operational
Messages:    48654
```

```
C370.lab> workqueue rate 5
```

Type Ctrl-C to return to the main prompt.

Time	Pending	In	Out
12:48:04	48654	48	2
12:48:09	48700	31	0

L'expéditeur ou le sujet des emails dans le Workqueue est connu

Afin d'enlever les emails qui affectent le workqueue, l'utilisation d'un filtre de message est recommandée. L'utilisation d'un filtre de message permettra à l'ESA à l'action ces emails au début du workqueue plutôt que l'extrémité afin d'assister la suppression des emails à un intervalle plus efficace.

Ce filtre peut être utilisé pour réaliser ceci :

```
C370.lab> filters
```

Choose the operation you want to perform:

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[> new
```

Enter filter script. Enter '.' on its own line to end.

```
FilterName:
if (mail-from == 'abc@abc1.com')
{
drop();
}
.
```

OR

```
FilterName:
if (subject == "^SUBJECT NAME$")
{
drop();
```

```
}  
.
```

Contrôle de file d'attente de la livraison

La commande de **tophosts** affichera les hôtes affectés par courant. Dans un environnement vivant vous verrez que l'hôte réceptif (file d'attente active en cours de la livraison) sera affecté avec un grand nombre de destinataire actif. Pour cette sortie, l'exemple est **impactedhost.queue**.

```
C370.lab> tophosts
```

```
Sort results by:
```

1. Active Recipients
 2. Connections Out
 3. Delivered Recipients
 4. Hard Bounced Recipients
 5. Soft Bounced Events
- ```
[1]> 1
```

```
Status as of: Thu Feb 06 12:52:17 2014 GMT
Hosts marked with '*' were down as of the last delivery attempt.
```

| # | Recipient Host            | Active Recip. | Conn. Out | Deliv. Recip. | Soft Bounced | Hard Bounced |
|---|---------------------------|---------------|-----------|---------------|--------------|--------------|
| 1 | <b>impactedhost.queue</b> | <b>321550</b> | <b>50</b> | <b>440</b>    | <b>75568</b> | <b>8984</b>  |
| 2 | the.euq.queue             | 0             | 0         | 0             | 0            | 0            |
| 3 | the.euq.release.queue     | 0             | 0         | 0             | 0            | 0            |

Si l'hôte affecté est un domaine réceptif peu familier où les informations supplémentaires sont exigées avant la suppression de tous les emails, les **showrecipients**, le **showmessage**, et les **deleterecipients** de commandes peuvent être utilisés. La commande de **showrecipients** affichera l'ID de message (MID), la taille de message, les tentatives de la livraison, l'expéditeur d'enveloppe, les récepteurs d'enveloppe, et le sujet de l'email.

```
C370.lab> showrecipients
```

```
Please select how you would like to show messages:
```

1. By recipient host.
  2. By Envelope From address.
  3. All.
- ```
[1]> 1
```

```
Please enter the hostname for the messages you wish to show.
```

```
> impactedhost.queue
```

Au cas où le MID suspecté dans la file d'attente de la livraison semblerait légitime, vous pouvez employer la commande de **showmessage** afin d'afficher la source de message avant que vous preniez n'importe quelle mesure.

```
C370.lab> showmessage
```

```
Enter the MID to show.
```

```
[ ]>
```

Une fois confirmé comme Spam, afin d'enlever ces emails, poursuivez et utilisez la commande

deleterecipient. La commande fournira trois options pour la suppression d'email outre de la file d'attente de la livraison ; Par l'expéditeur d'enveloppe, par l'hôte réceptif, ou tous les emails dans la livraison alignez.

```
C370.lab> deleterecipients
```

```
Please select how you would like to delete messages:
```

1. By recipient host.
2. By Envelope From address.
3. All.

```
[1]> 2
```

```
Please enter the Envelope From address for the messages you wish to delete.
```

```
[ ]>
```

Surveillance et action proactives

Sur la version 9.0+ AsyncOS sur l'ESA, nouvel une règle d'Header Repeats appelée de filtre de message par état est disponible.

Règle de répétitions d'en-tête

La règle de répétitions d'en-tête évalue pour rectifier si à un moment donné, nombre de messages spécifié :

- Avec le même sujet sont détectés pendant l'une dernière heure.
- Du même expéditeur d'enveloppe sont détectés pendant l'une dernière heure.
- en-tête-répétitions (<target>, <threshold> [, <direction>])

Les informations supplémentaires sur cette condition sont disponibles dans le guide de l'aide en ligne de votre périphérique.

Connectez-vous dans le CLI et déployez le filtre afin d'exécuter ces contrôle et action désirés. Un filtre d'exemple pour relâcher des emails ou pour informer un admin après un seuil est rencontré.

```
C370.lab> filters
```

```
Choose the operation you want to perform:
```

- NEW - Create a new filter.
- DELETE - Remove a filter.
- IMPORT - Import a filter script from a file.
- EXPORT - Export filters to a file
- MOVE - Move a filter to a different position.
- SET - Set a filter attribute.
- LIST - List the filters.
- DETAIL - Get detailed information on the filters.
- LOGCONFIG - Configure log subscriptions used by filters.
- ROLLOVERNOW - Roll over a filter log file.

```
[ ]> new
```

```
Enter filter script. Enter '.' on its own line to end.
```

```
FilterName:
```

```
if header-repeats('mail-from',1000,'outgoing')
```

```
{  
drop();  
}  
.
```

OR

```
FilterName:  
if header-repeats('subject',1000,'outgoing')  
{  
notify('admin@xyz.com');  
}  
.
```

[Informations connexes](#)

- [FOIRE AUX QUESTIONS ESA : Comment je vont-ils manuellement les destinataires clairs de la file d'attente d'email ?](#)
- [Support et documentation techniques - Cisco Systems](#)