Dépannage des courriers électroniques sortants indésirables

Table des matières

Introduction

Conditions préalables

- Composants utilisés

Dépannage

- Contrôles de file
- L'expéditeur ou l'objet des e-mails dans la file d'attente est connu
- QueueCheck de remise
- Surveillance et action proactives

Informations connexes

Introduction

Ce guide vous aide à enquêter et à résoudre les incidents où votre ESA envoie des e-mails sortants inattendus ou indésirables. Il décrit les étapes pratiques et les commandes permettant d'identifier la source et d'arrêter le comportement.

Conditions préalables

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Dépannage

Si vous savez quel compte envoie du spam, il est recommandé de verrouiller immédiatement ce compte. Si le compte n'est pas connu, effectuez une enquête à l'aide de l'ESA pour identifier le compte responsable, puis procédez au verrouillage.

Contrôles de file

Si vous observez un nombre élevé de courriers électroniques dans la file d'attente de travail et que le taux de courriers électroniques entrants dépasse de manière significative le taux de courriers sortants, cela indique un problème avec la file d'attente de travail. Vous pouvez utiliser la commande `workqueue` pour examiner l'état et les détails.

<#root>

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 l'objet des e-mails dans la file d'attente est connu

Si vous connaissez l'expéditeur ou l'objet des e-mails affectant la file d'attente de travail, il est recommandé d'utiliser un filtre de message. L'application d'un filtre de messages permet à l'ESA de traiter et d'agir sur ces e-mails plus tôt dans la file d'attente de travail, ce qui rend leur suppression plus efficace.

Pour ce faire, vous pouvez utiliser le filtre suivant :

<#root>

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 == 'user@example.com')
{
drop();
}
.
```

OR

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

Vérification de la file

La commande tophosts affiche les hôtes actuellement affectés. Dans un environnement actif, vous remarquerez peut-être qu'un hôte de destinataire (tel que example.com) a un grand nombre de destinataires actifs dans sa file d'attente de remise, ce qui indique un impact.

<#root>

```
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.

                                Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host              Recip.    Out     Recip.    Bounced    Bounced

1
```

example.com 321550 50 440 75568 8984

```
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 de destinataire inconnu et que vous avez besoin de plus d'informations avant de supprimer tous les e-mails, vous pouvez utiliser les commandes showRecipients, showmessage et deleterecipients. La commande show Recipients fournit des détails tels que l'ID de message (MID), la taille du message, le nombre de tentatives de remise, l'expéditeur de l'enveloppe, le ou les destinataires de l'enveloppe et l'objet de l'e-mail.

<#root>

```
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.
>
```

example.com

Si le MID suspecté dans la file d'attente de remise semble légitime, vous pouvez utiliser la commande showmessage afin d'afficher la source du message avant d'entreprendre toute action.

<#root>

```
C370.lab>
```

showmessage

```
Enter the MID to show.
[]>
```

123456789

Une fois que les e-mails sont confirmés comme spam, vous pouvez les supprimer à l'aide de la commande deleterecipientscommand. Cette commande offre trois options pour supprimer des e-mails de la file d'attente de remise : par expéditeur d'enveloppe, par hôte destinataire ou par tous les e-mails dans la file d'attente de remise.

<#root>

```
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.
[]>
```

user@example.com

Surveillance et action proactives

Règle des répétitions d'en-tête

La règle Répéter l'en-tête est évaluée comme vraie lorsque, au cours d'une période d'une heure, un nombre spécifié de messages répondant à l'un des critères suivants sont détectés :

- Ils ont le même sujet.
- Ils proviennent du même expéditeur d'enveloppe.

La syntaxe de la règle est la suivante : header-repeats(<target>, <threshold> [, <direction>])

Pour utiliser cette règle, connectez-vous à l'interface de ligne de commande et déployez le filtre approprié. Par exemple, vous pouvez créer un filtre pour supprimer les e-mails ou avertir un administrateur lorsque le seuil défini est atteint.

<#root>

```
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@example.com');
}
.
```

Informations connexes

- Supprimer manuellement les destinataires de la file d'attente de remise
- Assistance et documentation techniques - Cisco Systems

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.