排除不需要的出站電子郵件故障

目錄

[簡介](#)

[必要條件](#)

- [採用元件](#)

[疑難排解](#)

- [工作隊列檢查](#)
- [工作隊列中的電子郵件發件人或主題為已知](#)
- [傳遞隊列檢查](#)
- [主動監控和操作](#)

[相關資訊](#)

簡介

本指南可幫助您調查和解決您的ESA傳送意外或有害的出站電子郵件時發生的意外事件。它概述了識別源並停止行為的實際步驟和命令。

必要條件

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

疑難排解

如果您知道哪個帳戶傳送垃圾郵件，建議立即鎖定該帳戶。如果不知道該帳戶，則使用ESA進行調查，以確定責任帳戶，然後繼續將其鎖定。

工作隊列檢查

如果您發現工作隊列中的電子郵件數量較多，而傳入的電子郵件速率明顯超過傳出速率，則表明工作隊列存在問題。您可以使用workqueue命令檢視狀態和詳細資訊。

```
<#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
```

工作隊列中的電子郵件發件人或主題為已知

如果您知道影響工作隊列的電子郵件的發件人或主題，建議使用郵件過濾器。應用郵件過濾器使ESA能夠處理這些郵件，並在工作隊列中更早地對其執行操作，從而提高郵件刪除的效率。

您可以使用以下過濾器完成此操作：

<#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();
}
.
```

傳遞隊列檢查

tophosts命令顯示當前受影響的主機。在即時環境中，您可能會注意到收件人主機(如example.com)的傳遞隊列中有大量活動收件人，這表明存在影響。

<#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
```

如果受影響的主機是一個不熟悉的收件人域，並且在刪除所有電子郵件之前需要更多資訊，可以使用show recipients、show message和deleterecipients命令。showrecipientscommand提供詳細資訊，如郵件ID(MID)、郵件大小、嘗試傳遞的次數、信封發件人、信封收件人和郵件主題。

<#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

如果傳遞隊列中的疑似MID看起來合法，您可以在採取任何操作之前使用show message命令來顯示消息源。

<#root>

```
C370.lab>
```

showmessage

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

123456789

確認郵件為垃圾郵件後，可以使用deleterecipientscommand將其刪除。此命令提供三個從傳送隊列刪除電子郵件的選項：按信封發件人、收件人主機或傳送隊列中的所有電子郵件。

<#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

主動監控和操作

報頭重複規則

在一小時內，如果檢測到滿足以下任一條件的指定數量的消息，則「報頭重複」規則評估為true:

- 他們有著相同的話題。
- 它們來自同一個信封發件人。

規則語法為： header-repeats(<target>, <threshold> [, <direction>])

要使用此規則，請登入到CLI並部署相應的過濾器。例如，您可以建立一個過濾器來丟棄電子郵件或在達到定義的閾值後通知管理員。

<#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');
}
.
```

相關資訊

- 手動從傳遞隊列中刪除收件人
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。