

# 排除故障在ESA的不需要的出站电子邮件从受损帐户

## 目录

[简介](#)

[使用的组件](#)

[排除故障](#)

[Workqueue检查](#)

[电子邮件的发送方或主题在workqueue的被认识](#)

[交付队列检查](#)

[积极监控和操作](#)

[相关信息](#)

## 简介

本文描述如何排除故障和更正在电子邮件安全工具(ESA)的队列在事件内部用户用户帐号减弱了和被派出的unsolicited电子邮件全局。

## 使用的组件

本文档中的信息根据ESA的AsyncOS 7.6向前。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始(默认)配置。如果您使用的是真实网络,请确保您已经了解所有命令的潜在影响。

## 排除故障

锁定在发送垃圾邮件的该帐户下,如果知道是可行的,否则锁定在帐户下通过在ESA的调查曾经发现。

## Workqueue检查

当有在workqueue的很大数量的电子邮件抵抗,并且时输入系统的速率电子邮件超出退出系统的速率,这是预示的有在workqueue的一影响。您能使用workqueue命令执行检查。

```
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
```

## 电子邮件的发送方或主题在workqueue的被认识

要删除电子邮件影响的workqueue,推荐使用消息过滤器。消息过滤器的使用情况将提供ESA对操作这些电子邮件在workqueue初而不是与删除电子邮件的结尾协助在更有效的间隔。

以下过滤器可以用于达到此:

```
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(); } .
```

## 交付队列检查

tophosts命令将显示当前被影响的主机。在一个实际环境您看到接收主机(当前活动交付队列)有很大数量的活动收件人将影响。对于此输出，示例是**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. Active Conn.
Deliv. Soft Hard # Recipient Host Recip. Out Recip. Bounced Bounced 1 impactedhost.queue 321550
50 440 75568 8984 2 the.euq.queue 0 0 0 0 0 3 the.euq.release.queue 0 0 0 0 0
```

如果被影响的主机是更多信息在所有电子邮件前删除要求的一个不熟悉的接收域，可以使用命令**showrecipients**、**showmessage**和**deleterecipients**。**showrecipients**命令将显示消息ID (MID)，消息大小、交付尝试、信封发送方、信封收件人和电子邮件的主题。

```
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
```

在交付队列的怀疑的MID可能看起来合法情况下您能使用**showmessage**命令在采取前显示消息来源所有行动。

```
C370.lab> showmessage Enter the MID to show. [ ]>
```

一旦确认，垃圾邮件，删除这些电子邮件，继续和使用**deleterecipient**命令。命令为电子邮件删除将提供3个选项交付队列。由信封发送方，由接收主机或所有电子邮件在交付请排队。

```
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. [ ]>
```

## 积极监控和操作

在版本9.0+在ESA的AsyncOS，一个新的消息过滤器情况呼叫的Header Repeats规则是可用的。

### 报头重复规则

报头重复规则评估对真，如果在给的此刻，消息指定的编号：

- 使用相同主题在最后一个小时内检测。
- 从同样信封发送方在最后一个小时内检测。
- 报头重复(<target>， <threshold> [， <direction>])

关于此情况的更多信息是可用的在您的设备的在线帮助指南。

登录CLI并且部署过滤器运行希望的此检查和操作。

丢弃电子邮件或通知admin的示例过滤器在阈值以后满足。

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'); } .
```

## 相关信息

- [ESA FAQ : 手工从电子邮件队列的清楚收件人 ?](#)
- [技术支持和文档 - Cisco Systems](#)