

ينورت كل إل دي ربل لئاسر عا طخأ فاشكتسأ ESA يلع اه حال صا واهي ف بوغرم لا ريغ ةرداصل لا اهقارتخا مت يتلا تاباسحلانم

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [تحقق قائمة انتظار العمل](#)
- [المرسل أو موضوع رسائل البريد الإلكتروني في قائمة انتظار العمل معروف](#)
- [التحقق من قائمة انتظار التسليم](#)
- [المراقبة والإجراءات الاستباقية](#)
- [معلومات ذات صلة](#)

المقدمة

يوضح هذا المستند كيفية استكشاف أخطاء قوائم الانتظار الموجودة على "جهاز أمان البريد الإلكتروني (ESA)" وإصلاحها وتصحيحها في حالة تعرض حساب مستخدم داخلي للخطر وإرسال رسائل بريد إلكتروني غير قابلة لإعادة التوجيه بشكل عام.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى AsyncOS 7.6 والإصدارات الأحدث لـ ESA.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

استكشاف الأخطاء وإصلاحها

من المستحسن إغلاق الحساب الذي يرسل البريد العشوائي إذا كان معروفاً، وإلا قم بإغلاق الحساب بمجرد اكتشافه من خلال التحقيق في ESA.

تحقق قائمة انتظار العمل

عندما تكون هناك أعداد كبيرة من رسائل البريد الإلكتروني في عداد قائمة انتظار العمل وتتجاوز نسبة رسائل البريد الإلكتروني التي تدخل النظام المعدل الذي تخرج منه النظام بكثير، فإن ذلك يشير إلى وجود تأثير على قائمة انتظار العمل. يمكنك استخدام أمر قائمة انتظار العمل لتنفيذ التحقق.

```
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
2	48	48654	12:48:04
0	31	48700	12:48:09

المرسل أو موضوع رسائل البريد الإلكتروني في قائمة انتظار العمل معروف

لإزالة رسائل البريد الإلكتروني التي تؤثر على قائمة انتظار العمل، يوصى باستخدام عامل تصفية الرسائل. سيتيح استخدام عامل تصفية الرسائل ل ESA إجراء رسائل البريد الإلكتروني هذه في بداية قائمة انتظار العمل بدلا من النهاية للمساعدة في إزالة رسائل البريد الإلكتروني في فترة زمنية أكثر فعالية.

يمكن استخدام عامل التصفية هذا لتحقيق ما يلي:

```
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
{
.
```

التحقق من قائمة انتظار التسليم

سيظهر الأمر **tophosts** البيانات المضيفة المتأثرة الحالية. في بيئة مباشرة، ستري المضيف المستلم (قائمة انتظار التسليم النشطة الحالية) متأثرا بعدد كبير من المستلمين النشطين. لهذا الإخراج، يكون المثال **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.<br>Recipient Host | Deliv. | Soft<br>Recip. | Hard<br>Out | Hard<br>Recip. | Bounced      | Bounced     | # |
|--------------------------------|--------|----------------|-------------|----------------|--------------|-------------|---|
| <b>impactedhost.queue</b>      |        | <b>321550</b>  | <b>50</b>   | <b>440</b>     | <b>75568</b> | <b>8984</b> | 1 |
| the.euq.queue                  |        | 0              | 0           | 0              | 0            | 0           | 2 |
| the.euq.release.queue          |        | 0              | 0           | 0              | 0            | 0           | 3 |

إذا كان المضيف المتأثر هو مجال مستلم غير مألوف يتطلب مزيد من المعلومات قبل إزالة جميع رسائل البريد الإلكتروني، يمكن استخدام الأوامر **show recipients**، **showMessage**، و **deleterecipients**. سيعرض الأمر **show recipients** معرف الرسالة (متوسط)، حجم الرسالة، محاولات التسليم، مرسل المغلفات، مستلم (مستلمين) المغلفات، وموضوع البريد الإلكتروني.

```
C370.lab> showrecipients
```

```
:Please select how you would like to show messages
.By recipient host .1
.By Envelope From address .2
.All .3
1 <[1]
```

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

في حالة ما إذا كان MID المشتبه فيه في قائمة انتظار التسليم يبدو شرعيا، يمكنك استخدام الأمر **show message** لعرض مصدر الرسالة قبل إتخاذ أي إجراء.

```
C370.lab> showmessage
```

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

بمجرد التأكد من أنها بريد عشوائي، لإزالة رسائل البريد الإلكتروني هذه، قم بالمتابعة واستخدام الأمر **deleterecipient**. يوفر الأمر ثلاثة خيارات لحذف البريد الإلكتروني من قائمة انتظار التسليم، أو بواسطة مرسل المغلف، أو بواسطة مضيف المستلم، أو كل رسائل البريد الإلكتروني في قائمة انتظار التسليم.

```
C370.lab> deleterecipients
```

```
:Please select how you would like to delete messages
 .By recipient host .1
 .By Envelope From address .2
 .All .3
 2 <[1]
```

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

## المراقبة والإجراءات الاستباقية

في الإصدار AsyncOS +9.0 على ESA، يتوفر شرط عامل تصفية رسالة جديد يسمى قاعدة تكرار الرأس.

### قاعدة تكرار الرأس

يتم تقييم قاعدة تكرار الرأس إلى TRUE في حالة وجود عدد محدد من الرسائل في نقطة معينة من الوقت:

- بنفس الموضوع يتم الكشف عنه في آخر ساعة.
  - من نفس مرسل المغلف تم الكشف عنه في الساعة الأخيرة.
  - ([<header-repeats(<target>, <threshold> [, <direction>
- يتوفر المزيد من المعلومات حول هذه الحالة في دليل التعليمات عبر الإنترنت الخاص بجهازك.

قم بتسجيل الدخول إلى واجهة سطر الأوامر (CLI) ونشر عامل التصفية لتشغيل هذا التحقق والإجراء المطلوب. عامل تصفية المثال لإفلات رسائل البريد الإلكتروني أو إعلام المسؤول بعد استيفاء الحد.

```
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
```

## معلومات ذات صلة

- [الأسئلة المتداولة حول ESA: كيف يمكنني مسح المستلمين يدويا من قائمة انتظار البريد الإلكتروني؟](#)
- [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاينقتل نم ةومجم مادختساب دن تسمل اذه Cisco تچرت  
ملاعلاء انء عي مچ يف نيم دخت سمل لمعد ىوتحم مي دقتل ةيرشبل او  
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تغلب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب ي صؤت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچنل دن تسمل