تحديد المصير النهائي لرسالة ESA

المحتويات

المقدمة

يوضح هذا المستند كيفية تحديد مصير رسالة باستخدام سجلات البريد التي تم إستردادها من أوامر مختلفة على جهاز أمان البريد الإلكتروني (ESA) من Cisco.

المتطلبات الأساسية

تستند المعلومات الواردة في هذا المستند إلى:

- إسا
- جميع إصدارات AsyncOS

تعقب الرسائل

إذا قمت بتشغيل AsyncOS للإصدار 6.0 من البريد الإلكتروني أو إصدار أحدث، فإن الطريقة الأكثر فعالية لتحديد ما حدث لرسالة معينة هي إستخدام صفحة تعقب الرسائل من علامة التبويب "جهاز العرض". وهذا يتيح لك البحث باستخدام مجموعة متنوعة من الخيارات في واجهة ويب سهلة الاستخدام.

إذا قمت بتشغيل إصدار أقدم أو احتجت إلى تجميع جميع خطوط السجل لأغراض أستكشاف الأخطاء وإصلاحها، فاستخدم أوامر **GREP** أو **FINDEVENT** كما هو مفصل في الأقسام التالية.

أمر Findevent

إذا كان لديك AsyncOS للبريد الإلكتروني الإصدار 5.1.2 أو إصدار أحدث، فإن أمر **CLI Findevent** يجعل من السهل البحث عن رسالة معينة. يتيح لك **Findevent** البحث حسب المظروف من، مستلم المظروف، أو موضوع الرسالة. وهذا من الممكن أن يتم بصرف النظر عن الحالة أيضا. وبمجرد العثور على رسالتك، يمكنك إرجاع كل سطر سجل مرتبط بتلك الرسالة. إذا قمت بتشغيل **Findevent** بدون وسيطات، فإنه يقوم بتشغيل معالج لإرشادك خلال العملية. كما هو الحال دائما، يمكنك إستخدام الأمر **help** لتعلم النموذج القصير:

```
help findevent >
```

```
findevent [-i] [-f from | -s subject | -t to] log_name
findevent -m mid log_name
```

يجري النموذج الأول عملية بحث عن مظروف معين من، موضوع، أو مظروف إلى داخل اسم log_name المسمى ويسرد معرفات الرسائل (MIDs) التي تطابق. يمكن إستخدام علامة -i لعمليات البحث غير الحساسة لحالة الأحرف.

يعرض النموذج الثاني كافة سطور السجل ل MID المحدد.

إذا كان لديك إصدار أقدم، يمكن إستخدام أمر grep **CLI** من أجل إنجاز نفس الشيء. ومع ذلك، يتطلب إستخدام الأمر **grep** معرفة أكثر تفصيلا لكيفية تسجيل أحداث رسائل ESA.

أمر GREP

التحدي الأول عند البحث في سجلات البريد هو العثور على رسالتك. يمكنك القيام بذلك إذا قمت بالبحث عن المرسل أو المستلم أو الموضوع. بمجرد العثور على رسالتك، من المهم فهم كيفية تنظيم سجلات البريد. يتم إعطاء مختصرات لأحداث سجل بريد أمان المحتوى. أهم الأحداث هي ICID و Mid و RID و DCID.

معرف اتصال الحقن (ICID): عندما يقوم مضيف بعيد بإنشاء اتصال بالجهاز، يتم تعيين ICID لهذا الاتصال. يمكن أن ينتج عن واحد ICID العديد من MIDs.

ملاحظة: يحدد **ICID 0** الرسالة التي تم حقنها من نفسها. في الواقع، يشير الرقم 0 بعد ICID أو DCID إلى جلسات عمل مفتوحة إلى أو من عنوان التكرار المحلي للجهاز.

متوسط: بمجرد إنشاء اتصال، **يقوم** كل **بريد** بروتوكول نقل البريد البسيط الناجح (SMTP) **من:** الأمر بإنشاء منتصف جديد. ويمكن لمنتصف واحد ان يولد الكثير من الريفيين.

معرف المستلم (RID): يحصل كل مستلم (إلى: CC: أو BCC على RID. لا تنشئ RIDs سوى معرفات تحكم في البيانات (DCIDs) متعددة إذا كان هناك ثقب ناعم (خطأ اتصال) وتمت إعادة محاولة التسليم.

معرف اتصال التسليم (DCID): يتلقى كل مستلم يذهب إلى نفس مجال الوجهة نفس DCID حتى حدود النظام المتلقي. لذلك إذا ذهبت مستلمي الرسائل كلها إلى نفس المجال، ثم هناك DCID واحد لكل RIDs. ولكن إذا تم ذلك بدلا من ذلك، فإن كل RID يذهب إلى مجال منفصل، ثم هناك إرتباط واحد إلى واحد.

ملاحظة: يحدد **DCID 0** رسالة لم يتم إرسالها مطلقا. في الواقع، يشير الرقم 0 بعد ICID أو DCID إلى جلسات عمل مفتوحة إلى أو من عنوان التكرار المحلي للجهاز.

بشكل عام، عندما تجد رسالتك، تجد أنها متوسطة. ثم تقوم بالتجريف للوسط وتحديد ICID و RID. باستخدام ICID، يمكنك تحديد "علامة سمعة SenderBase (SBRS)" للمرسل. باستخدام RID ثم DCID، يمكنك تحديد ما حدث عندما حاولت ESA التسليم.

ملاحظة: بمجرد أن يكون لديك MID و ICID و DCID، يمكنك إسترداد جميع الصفوف الخاصة بتلك الرسالة في GREP واحد، إذا كان أصل الرسالة ليس أقدم من أقدم سجل بريد.

```
example.com> grep -e " MID 11123" -e " ICID 11092" -e " DCID 23349" mail_logs
```

مثال

1. البحث عن موضوع الرسالة:

```
example.com> grep
:Currently configured logs
mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll" .16
.Enter the number of the log you wish to grep
16 <[]
.Enter the regular expression to grep
test <[]
<[Do you want this search to be case insensitive? [Y
<[Do you want to tail the logs? [N
<[Do you want to paginate the output? [N
Mon Jan 23 10:25:03 2006 Info: SMTP listener testpairlist starting
Tue Jan 24 12:10:15 2006 Info: Message aborted MID 8 Dropped by filter
'testdrop'
'Tue Jan 31 23:55:38 2006 Info: MID 32 Subject 'testmsgquarantine
'Wed Feb 1 00:23:59 2006 Info: MID 62 Subject 'testmsgquarantine
'Wed Feb 1 00:27:48 2006 Info: MID 64 Subject 'testmsg2
'Wed Feb 1 22:30:37 2006 Info: MID 80 Subject 'test zip
'Wed Feb 1 22:37:51 2006 Info: MID 83 Subject 'FW: test zip
'Wed Feb 1 22:41:50 2006 Info: MID 84 Subject 'FW: test zip
'Fri Feb 3 15:17:47 2006 Info: MID 94 Subject 'test
'Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test
```

وقد أدى ذلك إلى إنشاء العديد من التطابقات التي تحتوي على **إختبار** في الموضوع. تم إرسال الرسالة في الساعة 3:42 مساء تقريبا، لذا يمكنك إستخدام MID للبحث التالي.

اليكم بعض النقاط المهمة التي يجب ملاحظتها عن الاسئلة:

هل تريد أن يكون هذا البحث غير حساس لحالة الأحرف؟ [Y]>
إذا قمت بالإجابة عن **نعم** على هذا السؤال، فإنه يجد الإدخالات بغض النظر عن الحالة.

هل تريد تذييل السجلات؟ [N]>
إذا قمت بالإجابة على **نعم** على هذا السؤال، فستجد الإدخالات الجديدة عند إنشائها فقط. لا يقوم بالبحث في كل ملفات السجلات. أخترت **ما من** in order to بحثت all of the log.

هل تريد ترقيم المخرجات؟ [N]>
إذا أجبت **بنعم** على هذا السؤال، فإنه يعرض المدخلات صفحة واحدة في كل مرة. ويكون هذا الإجراء مفيدا إذا كنت بحاجة إلى إجراء بحث عام وتوقعت إسترداد العديد من الإدخالات. يؤدي هذا إلى إيقاف الإدخالات من التمرير خارج الشاشة.

2. البحث عن المتوسط:

```
mail.example.com> grep
:Currently configured logs
mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll" .16
.Enter the number of the log you wish to grep
16 <[]
.Enter the regular expression to grep
MID 96 <[]
<[Do you want this search to be case insensitive? [Y
<[Do you want to tail the logs? [N
<[Do you want to paginate the output? [N
Fri Feb 3 15:41:43 2006 Info: Start MID 96 ICID 10394
```

```
<Fri Feb 3 15:41:43 2006 Info: MID 96 ICID 10394 From: <bob@example.net
:Fri Feb 3 15:41:58 2006 Info: MID 96 ICID 10394 RID 0 To
<nasir@example.com>
Fri Feb 3 15:42:06 2006 Info: MID 96 Message-ID
<4o8836$30@mail.example.com>
'Fri Feb 3 15:42:06 2006 Info: MID 96 Subject 'test
Fri Feb 3 15:42:06 2006 Info: MID 96 ready 23 bytes from
<bob@example.net>
Fri Feb 3 15:42:06 2006 Info: MID 96 matched all recipients for
per-recipient policy DEFAULT in the outbound table
Fri Feb 3 15:42:06 2006 Info: MID 96 antivirus negative
Fri Feb 3 15:42:06 2006 Info: MID 96 queued for delivery
[Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0
[Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0
Fri Feb 3 15:42:06 2006 Info: MID 96 RID [0] Response '2.6.0
'4o8836$30@mail.example.com> Queued mail for delivery>
Fri Feb 3 15:42:06 2006 Info: Message finished MID 96 done
```

لاحظ أن إدخالات MID توفر المزيد من المعلومات حول كيفية معالجة الرسالة. تشير إدخالات المنتصف أيضا إلى ICID و DCID. إذا أردت معرفة المزيد حول الاتصال الوارد، **GREP** ل ICID. إذا كنت تريد معرفة المزيد حول ما حدث عند محاولة ESA التسليم، **GREP** لمعرف فئة المورد (DCID).

3. لتحديد مكان تسليم الرسالة، ابحث عن معرف فئة المورد (DCID).

```
mail.example.com> grep
:Currently configured logs
mail_logs" Type: "IronPort Text Mail Logs" Retrieval: FTP Poll" .16
.Enter the number of the log you wish to grep
16 <[]
.Enter the regular expression to grep
DCID 14 <[]
<[Do you want this search to be case insensitive? [Y
<[Do you want to tail the logs? [N
<[Do you want to paginate the output? [N
Fri Feb 3 15:42:06 2006 Info: New SMTP DCID 14 interface 192.168.0.199
address 10.1.1.112 port 25
[Fri Feb 3 15:42:06 2006 Info: Delivery start DCID 14 MID 96 to RID [0
[Fri Feb 3 15:42:06 2006 Info: Message done DCID 14 MID 96 to RID [0
Fri Feb 3 15:42:11 2006 Info: DCID 14 close
```

لاحظ أنه تم تسليم الرسالة من الواجهة **192.168.0.199** إلى المضيف بعنوان **10.1.1.112** IP عبر المنفذ 25.

إذا لم تتم محاولة التسليم، ولكن تم **وضع** الرسالة **في قائمة الانتظار للتسليم**، فإنها تشير إلى أن النظام قد يواجه صعوبة في إتصالاته مع الخادم الوجهة. يمكنك إستخدام **hoststatus** من واجهة سطر الأوامر (CLI) لمعرفة ما إذا كانت حالة مضيف المستلم **معطلة** والتحقق من تطابق عناوين IP المطلوبة مع مسارات SMTP للمجال الوجهة أو سجلات MX العامة، حسب الاقتضاء.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).