مثال تكوين مدير الحدث المضمن ASA

المحتويات

المقدمة

يصف هذا المستند مدير الحدث المضمن (EEM)، وهو أداة لاستكشاف الأخطاء وإصلاحها تمت إضافتها في الإصدار 9.2(1) من جهاز الأمان القابل للتكيف (ASA). الوظيفة مماثلة لوظيفة IM المستندة إلى Cisco IOS. هو طريقة فعالة أن يركض CLI أمر يؤسس على ASA حادث (syslogs) ويحفظ الإنتاج. يغطي هذا المستند مقدمة للميزة بالإضافة إلى مثال لتطبيقات IM.

المتطلبات الأساسية

المتطلبات

يتطلب إستخدام EEM تكوين ASA في وضع سياق واحد.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى الإصدار 9.2(1) من ASA أو إصدار أحدث.

المبادئ التوجيهية والقيود

يتضمن هذا القسم الإرشادات والقيود لهذه الميزة.

إرشادات وضع السياق

يتم دعم IM حاليا على جدران حماية ASA التي تعمل في وضع سياق واحد فقط. جدران الحماية التي تم تكوينها في وضع سياق متعدد غير مدعومة حاليا.

إرشادات وضع جدار الحماية

يتم دعم EEM حاليا في أوضاع جدار الحماية الموجهة والشفافة على حد سواء.

إرشادات إضافية

- وبينما تتعطل الوحدة فإن حالة نظام المحاسبة ASA غير معروفة بشكل عام. قد لا تكون بعض الأوامر آمنة للتشغيل بينما يكون ASA في هذه الحالة.
- لا يمكن أن يحتوي اسم التطبيق الصغير لإدارة الأحداث على مسافات.
- لا يمكنك تعديل معلمات الحدث None و Crashinfo.
- قد يتأثر الأداء لأن رسائل syslog يتم إرسالها إلى IM لمعالجتها.
- الإخراج الافتراضي هو **إخراج none** لكل تطبيق لإدارة الأحداث. لتغيير الإخراج الافتراضي، يجب عليك إدخال قيمة إخراج مختلفة.
- قد يكون لديك خيار إخراج واحد فقط معرف لكل برنامج إدارة أحداث.

التكوين

يقوم الأمر **event manager applet** بإنشاء/تحرير برنامج إدارة أحداث، وهي عملية تقوم بربط الأحداث بالإجراءات والإخراج. يقتصر *<name>*على 32 حرفا ولا يمكن أن تحتوي على مسافات. يدخل هذا الوضع الوضع الفرعي لبرنامج إدارة الأحداث.

```
ASA(config)# [no] event manager applet
```

يمكن إضافة وصف **إلى** برنامج. وذلك لأغراض إعلامية فقط. *<text>* محدد ب 256 حرفا.

```
ASA(config-applet)# [no] description
```

تكوين الحدث

قد تتم إضافة أحداث مختلفة إلى برنامج صغير يقوم بتشغيل البرنامج الصغير لاستدعاء الإجراءات التي تم تكوينها عليه. يتم تعريفها باستخدام الكلمة الأساسية **الحدث**. قد يتم تكوين أحداث متعددة لكل برنامج.

أحداث Syslog

نوع الحدث الأول الذي يتم دعمه هو **syslog**. يستخدم ASA معرفات syslog لتحديد syslog التي تشغل تطبيقا. ويتم إكمال هذا الإجراء من خلال الكلمة الأساسية id، والتي قد تكون syslog واحدة أو مدى. تشير الكلمة الأساسية **occurs** الاختيارية إلى عدد المرات التي يجب أن يحدث فيها syslog للتطبيق الذي سيتم استدعاؤه (الافتراضي هو 1). تشير الكلمة الأساسية **الفترة** الاختيارية إلى مقدار الوقت، بالثواني، الذي يجب أن يقع فيه الحدث. إنه يحد من تكرار إستدعاء التطبيق إلى مرة واحدة على الأكثر الفترة التي تم تكوينها. **يقع 5** مع **فترة** 30، يعني أن ال syslog ينبغي وقعت 5 مرات في غضون 30 ثاني قبل أن الحدث يكون أطلقت. إذا حدث 11 syslog مرة في 30 ثانية، يتم تشغيل التطبيق الصغير مرة واحدة فقط. تعني القيمة 0 **للفترة** أنه لم يتم تعريف أي فترة.

يمكن تكوين العديد من syslogs، ولكن لا يمكن أن تتداخل النطاقات.

```
ASA(config-applet)# [no] event syslog id
```

```
ASA(config-applet)# no event syslog id
```

تحتوي **قيمة** *n*<**occurs**>على نطاق مسموح به من 1 إلى 4294967295. تحتوي قيمة **الفترة** <seconds> على نطاق مسموح به من 0 إلى 604800. تعني القيمة 0 (صفر) عدم تكوين أي فترة.

مثال على أحداث Syslog

في هذا المثال، يتخذ IM إجراء عندما يكتشف حالة كتلة ذاكرة منخفضة. في حالة استنفاد كتل 1550 بايت المتوفرة، فإنها تجمع **بيانات تفريغ تجمع كتل العرض 1550** وتحفظ إلى القرص. تقوم بذلك، على الأكثر، مرة كل 10 دقائق.

```
event manager applet depletedblock
"description "Take a snapshot of block output when it is depleted
event syslog id 321007 period 600
"action 1 cli command "show blocks pool 1550 dump
output file rotate 10
```

أحداث دورية

ويمكن أيضا تهيئة IM للقيام بعمل بشكل دوري. عند تكوين حدث مستند إلى مؤقت، أستخدم الكلمة الأساسية **timer**

في تكوين الأحداث. هناك 3 خيارات تستند إلى المؤقت:

- مطلق - المؤقت الأول هو مؤقت **مطلق** يشغل التطبيق الصغير مرة واحدة في اليوم في الوقت المحدد ويعيد تشغيله تلقائيا.

```
ASA(config-applet)# [no] event timer absolute time
```

```
ASA(config-applet)# no event timer absolute
```

- العد العكسي - المؤقت الثاني هو مؤقت **العد العكسي** الذي يشغل التطبيق الصغير مرة واحدة ولا يتم إعادة تشغيله ما لم تتم إزالته وإعادة إضافته.

```
ASA(config-applet)# [no] event timer countdown time
```

```
ASA(config-applet)# no event timer countdown
```

- المراقبة - تعد وحدة التوقيت الثالثة وحدة توقيت **مراقبة** تقوم بتشغيل التطبيق مرة واحدة في كل فترة يتم تكوينها ثم تقوم بإعادة التشغيل تلقائيا.

```
ASA(config-applet)# [no] event timer watchdog time
```

```
ASA(config-applet)# no event timer watchdog
```

مثال على الأحداث الدورية

على سبيل المثال، يقوم تكوين هذا الحدث بتجميع 192.168.1.100 كل دقيقة واحدة. يمكن إستخدام هذا الأمر لضمان الحفاظ على نفق VPN وتشغيله حتى أثناء فترات حركة المرور في وضع الخمول. إنه يستخدم موقت **المراقبة** لينفذ كل 60 ثانية.

```
event manager applet period-event
"description "Run a command once per minute"
event timer watchdog time 60
"action 0 cli command "ping 192.168.1.100"
output none
```

يقوم هذا التطبيق بتسجيل معلومات تخصيص كتلة الذاكرة كل ساعة ويكتب الإخراج إلى مجموعة دوارة من ملفات السجل، نظرا لأنه يحتفظ بعدد يوم من السجلات. يستخدم جهاز توقيت **المراقبة** لينفذ الحكم كل ساعة.

```
event manager applet blockcheck
"description "Log block usage"
event timer watchdog time 3600
output rotate 24
"action 1 cli command "show blocks old"
```

تقوم هذه التطبيقات بتعطيل الواجهة المحددة (Gig 0/0) بين منتصف الليل و 3 صباحا. وتستخدم المؤقت **المطلق** للتنفيذ مرة واحدة في اليوم.

```
event manager applet disableintf
"description "Disable the interface at midnight
```

```
event timer absolute time 0:00:00
output none
"action 1 cli command "interface GigabitEthernet 0/0
"action 2 cli command "shutdown
"action 3 cli command "write memory
!
event manager applet enableintf
"description "Enable the interface at 3am
event timer absolute time 3:00:00
output none
"action 1 cli command "interface GigabitEthernet 0/0
"action 2 cli command "no shutdown
"action 3 cli command "write memory
```

حدث يدوي

كما يمكن إستخدام تطبيقات IM هذه يدويا. للقيام بذلك، يجب أن يقوم التطبيق الصغير بتكوين **الحدث none**. لتشغيل برنامج صغير يدويا، أدخل الأمر **event manager run** متبوعا باسم البرنامج الصغير. إذا تم تكوين التطبيق الصغير لأي آلية مشغل حدث باستثناء 'none'، فإن محاولة تشغيله يدويا تؤدي إلى حدوث خطأ. باستخدام أحد الأمثلة السابقة، 'Depletedblock'، ترى:

```
ASA# event manager run depletedblock
'ERROR: Applet not configured with 'event none
```

مثال على حدث يدوي

يمكن إستخدام الأحداث اليدوية بطريقة مشابهة للماكرو. على سبيل المثال، يمكن إستخدام حدث يدوي لتنفيذ بعض الأوامر بالترتيب. في هذا المثال، يقوم بحفظ التكوين، واختبار جهاز مضيف، ومسح كل الخيارات.

```
event manager applet clean-up
event none
"action 0 cli command "write mem
"action 1 cli command "ping 192.168.1.100
"action 2 cli command "clear shun
output none
```

حدث عطل

يقوم الحدث **crashinfo** بتشغيل برنامج صغير عند حدوث عطل في ASA. بغض النظر عن قيمة الأمر **output**، يتم توجيه أوامر **الإجراء** إلى ملف crashinfo. يتم إنشاء الإخراج قبل إنشاء جزء **show tech** من crashinfo.

تحذير: عندما ينهار ASA، تكون حالة الصندوق غير معروفة بشكل عام. قد لا تكون بعض أوامر CLI آمنة للتشغيل عندما تكون الوحدة في هذه الحالة.

```
ASA(config-applet)# [no] event crashinfo
```

إجراء التكوين

عند تشغيل التطبيق الصغير، يتم تنفيذ الإجراءات على التطبيق الصغير. كل **إجراء** له ترتيب يتم إستخدامه لتحديد ترتيب العمليات. يمكن تكوين إجراءات متعددة لكل تطبيق، ولكن يمكن إستخدام كل ترتيب مرة واحدة فقط. الأوامر هي أوامر CLI نموذجية، مثل **show blocks**. يوصى بشدة بعلامات الاقتباس، ولكنها غير مطلوبة.

```
ASA(config-applet)# [no] action
```

```
ASA(config-applet)# no action
```

قيمة معرف الإجراء *<n>* لها نطاق من 0 إلى 4294967295. يجب اقتباس قيمة <command>، وإلا يحدث خطأ إذا كان الأمر يتكون من أكثر من كلمة. يتم تنفيذ الأمر في وضع التكوين كمستخدم ذي مستوى الامتياز 15 (الأعلى). قد لا يقبل الأمر أي إدخال، حيث سيتم تعطيل الإدخال إذا كان الأمر يحتوي على خيار **noconfirm**. يجب إستخدام ذلك نظرا لعدم معالجة الأوامر بشكل تفاعلي.

تكوين الإخراج

يمكن توجيه مخرجات العمليات إلى موقع محدد من خلال أمر **المخرجات**. يمكن تمكين قيمة إخراج واحدة فقط في أي وقت. القيمة الافتراضية هي **إخراج none**. يتجاهل هذا القيمة أي مخرجات من أوامر العملية.

```
ASA(config-applet)# [no] output none
```
يرسل الأمر **output console** إخراج أوامر الإجراء إلى وحدة التحكم.

```
ASA(config-applet)# [no] output console
```
يوجه أمر **مخرجات ملف** مخرجات أوامر العملية إلى الملفات. هناك أربعة خيارات يمكن إستخدامها. يكتب الخيار **الجديد** مخرجات البرنامج التفاعلي إلى ملف جديد لكل عملية إستدعاء. *اسم الملف* لديه تنسيق **im-<*applet*>-<*timestamp*>.log**. حيث *<applet>* هو اسم التطبيق و*<timestamp>* هو طابع زمني مؤرخ بتنسيق *YYYYMMDD-hhmss*.

```
ASA(config-applet)# [no] output file new
```
يتم إستخدام خيار **التدوير** لإنشاء مجموعة من الملفات التي يتم تدويرها مثل آلية تدوير سجل لينوكس. تنسيق اسم الملف هو **im-<*applet*>-<*x*>.log**. حيث *<applet>* هو اسم التطبيق الصغير، *<x>* هو رقم الملف. يشار إلى الملف الأحدث برقم 0 (صفر)، ويشار إلى الملف الأقدم بأعلى رقم (<*n*>-1). عندما تتم كتابة ملف جديد، فإن الملف الأقدم يتم حذفه ويتم إعادة ترقيم كل الملفات التالية قبل كتابة الملف العاشر.

```
ASA(config-applet)# [no] output file rotate
```

قيمة التدوير *<n>*لها نطاق من 2 إلى 100.

يتم إستخدام الخيار **overwrite** لكتابة إخراج أمر الإجراء دائما إلى ملف واحد يتم قصه كل مرة.

```
ASA(config-applet)# [no] output file overwrite
```

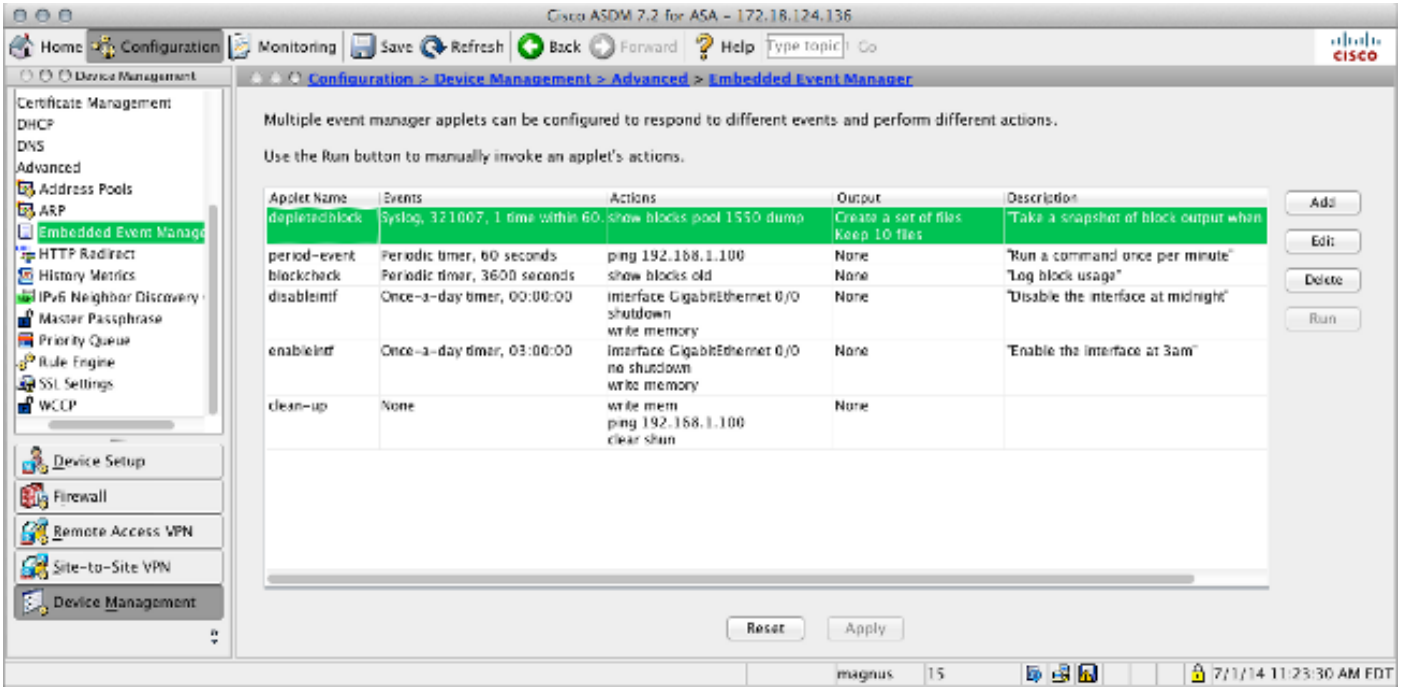
يتم إستخدام خيار **الإلحاق** لكتابة مخرجات أمر العملية دائما على ملف واحد، لكن يتم إلحاق ذلك الملف في كل مرة.

```
ASA(config-applet)# [no] output file append
```

الوسيطة *<filename>* هي اسم ملف محلي (إلى ASA). يمكن أن يستخدم أمر الكتابة فوقه أيضا **tftp** ،**ftp**: وsmb**:** الملفات المستهدفة.

تكوين ASDM

كما يمكن تكوين IM من داخل ASDM. أختر **التكوين > إدارة الأجهزة > خيارات متقدمة > إدارة الأحداث المضمنة**. في هذا القسم من ASDM، يمكنك تكوين تطبيقات IM الخاصة بك باستخدام نفس المعلمات التي تمت مناقشتها سابقا. بعد تكوين برنامج صغير، انقر فوق **تطبيق** لدفع التكوين إلى ASA.



التحقق من الصحة

أوامر وضع EXEC

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

يتم إستخدام جميع هذه الأوامر في وضع EXEC.

يعرض هذا الأمر التكوين الجاري تشغيله لنظام مدير الحدث.

ASA# **show running-config event manager**

يقوم هذا الأمر بتنفيذ برنامج لإدارة الأحداث تم تكوينه باستخدام Event None. إذا قمت بتشغيل برنامج لم يتم تكوينه باستخدام Event None، يتم الإبلاغ عن خطأ.

ASA# **event manager run**

ASA# event manager applet period-event, hits 1, last 2014/07/01
10:51:52
last file none
event watchdog 60 secs, left 54 secs, hits 1, last 2014/07/01 10:51:52
CLI)show) . action 0 cli command "ping 192.168.1.100", hits 1, last 2014/07/01 10:51:52
. im counter

.show " " .show( ) ASA# show counters protocol eem

.debug :. IM in order to

ASA# [no] debug event manager

. . ASA# show debug event manager

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).