IPS 5.x والإصدارات الأحدث: طرق مختلفة لمراقبة الأحداث

المحتويات

المقدمة

يزود هذا وثيقة مختلف طريقة أن يراقب ال ips حادث.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى IPS 5.x والإصدارات الأحدث.

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

طرق مراقبة أحداث IPS

حاليا، هناك أربعة خيارات لمراقبة أجهزة الاستشعار:

1. يتوفر IME (IPS Manager Express) من تنزيل البرامج في Cisco.com. يمكن لهذا التطبيق الاشتراك بأمان في مستشعر IPS باستخدام SDEE واسترداد الأحداث/السجلات التي تم إنشاؤها نتيجة لأي مشاكل أو توقيعات

تم تشغيلها بسبب التطابق.يتم إستدعاء IDM (IPS Device Manager) عند الوصول إلى المستشعر مباشرة من خلال HTTPS.عرض مخزن الأحداث مباشرة على جهاز الاستشعار باستخدام أدوات مراقبة IDM أو مراقبة حدث IME. لا يعد كل من IDM و IME حلولا صالحة إذا كنت بحاجة إلى تخزين الأحداث على المدى البعيد نظرا لأن مخزن الأحداث المحلي الخاص بالمستشعر عبارة عن مخزن مؤقت دائري بسرعة 30 ميجابت ويبدأ في تجاوز نفسه بمجرد الوصول إلى حد 30 ميجابت. هذا الحد غير قابل للتكوين.

2. أستخدم جهاز CS-MARS من أجل سحب الأحداث وربطها بشكل روتيني من المستشعر. يستخدم CS-MARS بروتوكول SDEE لإنشاء اتصال آمن بالمستشعر لاسترداد الأحداث واسترداد الأحداث الجديدة كل بضع ثوان.اتصل بفريق الحساب/بائع/SE للحصول على مزيد من المعلومات إذا كنت مهتما بتقديم عرض توضيحي لجهاز CS-MARS.بالنسبة لأجهزة Cisco IPS 5.x و x.6، تقوم MARS بسحب السجلات باستخدام SDEE عبر SSL. لذلك، يجب أن يكون لدى MARS وصول HTTPS إلى المستشعر. لتجهيز المستشعر، يجب أن تسمح لحركة مرور HTTPS من محطة الإدارة IDM/IME، وتأكد من تعريف عنوان IP الخاص ب MARS على أنه مضيف مسموح به على المستشعر.

```
sensor#conf t
sensor(config)#service host
sensor(config-hos)#network-settings
sensor(config-hos-net)#access-list x.x.x.x/subnet_mask
sensor(config-hos-net)#exit
sensor(config-hos)#exit
:[Apply Changes?[yes
#(sensor(config
```

3. راقب الأحداث مع مكتب الشؤون الداخلية. إن "عارض أحداث IDS" هو تطبيق قائم على تطبيق جافا يمكنك من عرض وإدارة التنبيهات لما يصل إلى خمسة أجهزة إستشعار. باستخدام عارض أحداث IDS يمكنك الاتصال بالتحذيرات وعرضها في الوقت الحقيقي أو في ملفات السجل المستوردة. يمكنك تكوين عوامل التصفية وطرق العرض لمساعدتك في إدارة التنبيهات. يمكنك أيضا إستيراد بيانات الحدث وتصديرها لمزيد من التحليل. ومثل MARS، يقوم IEV بإنشاء اتصال آمن بالمستشعر ويستعيد الأحداث كل بضع ثوان. يخزن مدير البنية الداخلية هذه الأحداث في قاعدة بيانات على الخادم المثبت عليه خدمة البنية التحتية. كما يتم تضمين قاعدة البيانات مع نظام الإدخال والإخراج الأساسي (IEV) ويتم تثبيتها مع التطبيق. طقطقت IEV in order to جلبت.**ملاحظة:** يتم العثور على وثائق IEV من خلال قائمة التعليمات بعد تثبيتها. يحتوي المستند التمهيدي على معلومات التثبيت.
4. قم بتكوين التواقيع على المستشعر لديك ليكون لديك إجراء من **طلب-snmp-trap** وتكوين المستشعر لإرسال التصادفات إلى خادم SNMP. يمكنك بعد ذلك إستخدام هذا الخادم لترحيل الرسائل على أنها syslogs إلى جهاز آخر.SNMP هو بروتوكول طبقة تطبيق يسهل تبادل معلومات الإدارة بين أجهزة الشبكة. ويتيح SNMP لمسؤولي الشبكات إدارة أداء الشبكة واكتشاف مشاكل الشبكات وحلها، والتخطيط لزيادة حجم الشبكة.بروتوكول SNMP هو بروتوكول بسيط للطلب/الاستجابة. يصدر نظام إدارة الشبكة طلبا، وترجع الأجهزة المدارة استجابات. وينفذ هذا السلوك باستخدام عملية من عمليات البروتوكولات الأربع التالية:إحضارGetNextمجموعةالاعتراضيمكنك تكوين المستشعر للمراقبة بواسطة SNMP. يحدد SNMP طريقة قياسية لمحطات إدارة الشبكة لمراقبة صحة وحالة العديد من أنواع الأجهزة، والتي تتضمن المحولات والموجهات وأجهزة الاستشعار.

معلومات ذات صلة

- أجهزة إستشعار Cisco IPS 4200 Series
- نظام Cisco لمنع الاقتحام
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك اكتشاف إقتحام CiscoSecure)
- الدعم التقني والمستندات - Cisco Systems

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).