كيفية تصدير كميات كبيرة من البيانات باستخدام بحث واجهة سطر الأوامر.

قابلية التطبيق

مؤسسة Splunk

الوصف

دليل خطوة بخطوة

لتصدير كميات كبيرة من البيانات، يمكنك إستخدام بحث على غرار ما يلي من مطالبة واجهة سطر الأوامر (CLI) على رأس بحث:

```
splunk search "index=pan_log sourcetype=pan:* src_ip!=<Internal_IP_Scheme> dest_ip!=<Int
| fillnull value=null
| dump basefilename=<insert_your_chosenfilename> compress=5 fields=_time,app,app:subcate
dest_ip,dest_port,dest_translated_ip,dest_user,dest_zone,direction,duration,filename,htt
packets_out,sig,signature,sourcetype,src_ip,src_translated_ip,src_user,target_id,threat:
```

وفيما يلي توزيع البحث المذكور أعلاه:

يتم الآن البحث في الفهرس 'pan_log' عن pan:* sourcetypes واستبعاد نطاق IP، قادر على تعبئة القيم الخالية، وانسياب إلى أمر تفريغ، والذي ينتقل بعد ذلك إلى القيام بما يلي:

يقوم هذا الأمر بتشغيل استعلام بحث محدد ونتيجة بحث عند التصدير السريع إلى القرص المحلي على SPLUNK_HOME/var/run/splunk/dispatch/<sid>/dump". وهو يتعرف على حقل خاص في أحداث الإدخال، _dstpath، والتي إذا تم تعيينها سيتم إستخدامها كمسار ليتم إلحاقه ب DST لحساب مسار الوجهة النهائية.

والجانب السلبي الرئيسي الوحيد لهذه العملية هو أن النتائج تحتوي على مدة مدة البقاء (TTL) تبلغ دقيقتين، لذلك يجب عليك إنشاء ملف رمز حفظ لتتأكد من عدم حصد هذه النتائج قبل أن تتمكن من التقاط ملفات *.gz التي تم إنشاؤها بواسطة العملية. راجع الارتباط "ذي الصلة" أدناه.

ذات صلة:

كيفية إنشاء ملف بدون ملحق في Windows

إستجلاء

أثناء التحقيق في هذه المشكلة، تم العثور عليها، دون الحصول على مجموعة بيانات كاملة.

تم تحديد أن ذلك يرجع إلى البحث الذي يحصد هذه البيانات ويفرزها أسرع مما كان متوقعا. وجد أن هذا السلوك طبيعي بعد البحث. عمليات بحث فهرس الملخص وغيرها يمكن تشغيلها باستخدام إرتباط مكون البحث TTL لمدة دقيقتين. لهذا السبب، قم بإنشاء ملف رمز مميز للحفظ في الدليل <sid>. هذا مغطى لأجهزة Windows في الارتباط الموجود في قسم الوصف في هذه المقالة. باستخدام *nix يمكنك التنقل إلى $SPLUNK_HOME/VAR/run/splunk/dispatch/<sid> ثم إصدار الأمر 'touch save'

وبمجرد أن يتحقق ذلك، ستتمكن من تجاوز مشكلة جمع القطع [***لا تنس حذف ملفات الحفظ!**]

بعد ذلك، اضغط خلال المزيد من أستكشاف الأخطاء وإصلاحها للحصول على إطار زمني صالح للعمل من شأنه إنشاء مجموعة كاملة معرفة من البيانات. كان من الضروري في النهاية إجراء عمليات بحث لمدة 24 ساعة لإتمامها في عملية التصدير من يوم إلى يوم، وذلك بسبب العدد الهائل من الأحداث في مجموعة البيانات.

رارق

بمجرد تضييق نطاق مجموعة البيانات التي يلزم تشغيلها مقابل فترة زمنية تبلغ 24 ساعة، يمكن إنشاء مكبات كاملة تبلغ مدتها 24 ساعة من عمليات تسجيل PAN. وقد تمكن مركز آخر لمعالجة الحالات الدامغ من إستخدام هذه الطريقة نفسها مؤخرا للعودة تاريخيا والحصول على بيانات محددة.

روابط ذات صلة

وثائق Splunk: دليل أوامر التفريغ: تفريغ مرجع البحث

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).