تم الإبلاغ عن تأخير الفهرسة بين وقت حدث سجل WinEvent ووقت فهرس Splunk

قابلية التطبيق

مؤسسة Splunk

الوصف

كيفية التعرف عليه

أولا تأكيد الدلتا بين وقت الحدث (_time) وفهرس Splunk IndexTime (_indexTime)، قم بتعديل ما يلي اعتمادا على نوع الفهرس والنوع المصدر الذي يتأثر. في هذا المثال، يتم الاستعلام عن تسجيل حدث قناة الأمان:

```
index=<splunk_index> sourcetype="WinEventLog:Security" host=<splunk_forwarder>
| fields _time, _indextime, host
| eval delay=(_indextime - _time)/60
| timechart avg(delay) by host
```

إستجلاء

أشياء مهمة للتحقق منها:

- متى ظهر تأخير الفهرسة لأول مرة؟
- ما هي التغييرات، إن وجدت، التي أدخلت على نشر القوات في الوقت الذي ظهر فيه التأخير للمرة الأولى؟
- هل يزداد زمن الوصول بمرور الوقت (خطي)، أو يتغير؟

تأكيد الحد الأقصى للحدث والمتوسط لكل ثانية (EPS):

```
index=_internal source=*metrics.log* security per_source_thruput host=<splunk_forwarder>
| timechart max(eps) max(max_age)
```

إذا كان زمن الوصول يتفاوت مع مرور الوقت، فقد تشير قيمة EPS العالية إلى وجود أختناقات في سعة معالجة البيانات.

قرار

إصلاح سريع

يطبق هذا الخيار فقط إذا كنت تريد الحصول على الأحداث الحالية والا تهتم بالبيانات التاريخية المفقودة. يجب تنفيذ ما يلي واحدا تلو الآخر على كل مصدر مشكلة:

1. تعيين `current_only = 1` in `$SPLUNK_HOME\etc\system\local\inputs.conf`:

```
[WinEventLog://Security]
current_only = 1
```

2. أوقف الراكب
3. إعادة تسمية ملف نقطة التفتيش القديمة:

```
ren "C:\Program Files\SplunkUniversalForwarder\var\lib\splunk\modinput\WinEventLog\Securit
```

4. بدء تشغيل الموجه
5. تأكد من إنشاء ملف نقطة تفتيش أمان جديد
6. تأكد من أن سجلات التفتيش والأمان لا تزيد عن بضع مئات من الأحداث
7. قم بإعادة تسمية الملف `$SPLUNK_HOME\etc\system\local\inputs.conf` لإرجاع الإعداد `current_only=1` إلى الإعداد الافتراضي.
8. إعادة تشغيل Splunk
9. البحث للتأكد من تزايد البيانات

لماذا إعادة تمهيد UF بشكل منتظم لن يساعد على الأرجح

إن إعادة تشغيل وحدة الاستقبال والبث بسطاة ترغمها على إعادة قراءة نقاط التفتيش

وتفريغ مخازن الذاكرة المؤقتة لفترة وجيزة. بما أن معدل إنشاء الحدث يتجاوز حد المعالجة/الدفع، فإن مقدم العرض سيبدأ في تجميع التأخير مرة أخرى خلال دقائق من إعادة التشغيل.

حلول طويلة الأجل

ويتطلب الحل السريع التدخل اليدوي على كل وحدة من وحدات حفظ السالم المتأثرة، وهو أمر غير ممكن بشكل عام في عملية نشر كبيرة (وبعض المسؤولين ليس لديهم إمكانية الوصول إلى سطر الأوامر في وحدات UF) المطبقة. وفوق كل هذا، من المرجح جدا أن يتخلف UF مرة أخرى. قد يتمثل الخيار الأفضل لك في توفير حل طويل الأجل. وحيث أن كل بيئة مختلفة، فال يوجد إعداد بسيط يمكن تطبيقه على كل سيناريو. ومع ذلك، يجب أن تكون التعارضات في قاعدة المعارف هذه مفيدة بالنسبة للعديد من حاالت االستخدام. تتطلب كافة التعارضات التكوين الوارده في هذه المقالة إعادة تشغيل Splunk على UF لكي تصبح نافذة المفعول، اذا تأكد من أن التطبيق المخصص على Deployment Server قد قام بإعادة تشغيل Splunkd المحدد.

جرب هذا أوال (limit.conf)

فتح maxKBps

قبل تعديل الخيارات أدناه، انظر إلى `limit.conf/[thruput]maxKBps`. يكون اإلعداد االفتراضي 256 وهو UF على 22 بايت/ثانية، مما يحد من إجمالي نقل الشبكة في اليوم بما يقارب 22 غيغابايت. ينتج الخادم المشغول الذي يقوم بإنشاء سجالت المانيفست أكثر من 256 بايت/ثانية، مما يجعل من المستحيل على الموجه مالحقته.

إذا، أول شيء: ثبتت هذا قيمة إلى 0 (غير محدود) في `limit.conf` أن يزيل غطاء الشبكة عرض النطاق:

```
[thruput]
maxKBps = 0
```

بما أن معظم العمالء العالميين يتصلون بالمنزل إلى خادم نشر، فإن أفضل ممارسة هي تعيين هذا التكوين عبر تطبيق نشر بحيث يتلقاه جميع العمالء في وقت واحد (أو في بيئة اختبار إن أمكن، ثم في مرحلة اإلنتاج). وثمة خيار آخر، في حالة عدم توفر بيئة اختبار، وهو النشر إلى فئة خادم "اختبار" لمجموعة صغيرة من وحدات UF والشاشة قبل التطبيق في كل مكان. وينطبق الأمر نفسه على كافة التعارضات المقدمة في هذه المقالة.

خيارات إضافية

إذا لم يحل فتح باب الدفاع المسألة كاملة، فتأمل اول في ما يلي:

خاص بالمدخلات.conf/[WinEventLog://Security]

الخيار#1 - تغيير حجم الدفعة

بشكل افتراضي، يلتقط Splunk الأحداث في حزم صغيرة (10 أحداث) ويقوم بتحديث ملف نقطة التفتيش على القرص بشكل متكرر. في الأجهزة المضيفة المشغولة، يصبح إدخال/إخراج القرص الموجود على ملف نقطة التفتيش نقطة اختناق رئيسية. إعداد `batch_size = 500`، وإعداد `checkpointInterval = 600` (أخير مزامنة القرص إلى 600s)، إعداد `suppress_checkpoint = true` يزيد بشكل كبير من سعة معالجة EPS (الأحداث في الثانية) لـ `splunk-winevtlog.exe`.

```
batch_size = 500
suppress_checkpoint = true
checkpointInterval = 600
```

Option#2 - إستخدام RenderXML لتقليل عدد إستدعاءات API

بشكل افتراضي، تقوم Splunk بإصدار إستدعاء واجهة برمجة تطبيقات لكل حقل داخل الحدث. بدلا من ذلك، سيؤدي تمكين RenderXml إلى إصدار إستدعاء واجهة برمجة تطبيقات لكل حدث، مما يؤدي إلى تحسين الأداء: عرض أحداث سجل أحداث Windows في XML

```
renderXml = true
```

الخيار#3 - تصفية أي الحقول يتم كبحها لتقليل حمولة البيانات

هذا الخيار فعال للسرعة الخام، لكن تأكد من أنه يفي بمتطلبات التدقيق (إن أمكن).

تقوم هذه الإعدادات بتشتيت حقول رؤوس الصفحات خارج الحدث الأولي قبل الإرسال لتقليل حجم البايت واستدعاءات عرض واجهة برمجة التطبيقات (API). إذا كانت نماذج SIEM أو CIM أو لوحات معلومات التوافق الخاصة بها تعتمد على أساسيات كاملة (على سبيل المثال،

نجاح/فشل التدقيق) وأ TaskCategory وأ Opcode، فإن إسقاط هذه الحقول سيؤدي إلى كسر هذه عمليات الكشف.

```
suppress_sourcename = true
suppress_keywords = true
suppress_type = true
suppress_task = true
suppress_opcode = true
```

الخيار#4 - تمكين واجهة برمجة تطبيقات **FormatMessage()** في نقطة الإدخال

EVTformatMessage() هو واجهة برمجة تطبيقات افتراضية في معظم عمليات نشر Windows، والتي تحتوي على زيادة في مصروفات المعالجة عند مقارنتها مع واجهة برمجة التطبيقات (API) السابقة لـ FormatMessage(). قد يؤدي الرجوع إلى واجهة برمجة التطبيقات (API) القديمة إلى تخفيف تأخر الفهرسة.

ال توقم بتعيين هذا إذا كان **RenderXml = true**. تكون واجهة برمجة التطبيقات القديمة FormatMessage() أسرع فقط عند تحليل سجلات النصوص العادية متعددة الأسطر (RenderXml = false)، لأنها تتجاوز البحث عن سلسلة EvtFormatMessage() DLL القليلة. عند استخدام RenderXml = true، تتم قراءة Splunk بالفعل مباشرة من واجهة برمجة تطبيقات EVTX الحديثة (EvtRender) بتنسيق هيكل دون استدعاء DLLs الخاصة بتنسيق الرسائل.

```
use_old_eventlog_api = true
```

زيادة خطوط اتصال UF (server.conf)

بشكل افتراضي، يقوم الموجه بتشغيل واحد تحليل وانسياب هضم. بالنسبة للآلات متعددة النوى التي تأخذ حجم الحدث الكبير، يمكن زيادة مجموعة التدفقات للسماح بالمعالجة المتوازية. يؤدي هذا إلى التحكم في عدد مؤشرات الترابط الداخلية التي يستخدمها الموجه لقراءة البيانات من واجهات برمجة التطبيقات (API) المحلية في Windows وتجميعها ودفعها إلى الشبكة.

على وحدة UF تعد بصمة دورة زيادة أنابيب البلع من 1 إلى 2 خفيفة جدا مقارنة بمفهرس أو مجمع تحميل ثقيل، لأن وحدة UF تقوم بالقراءة خفيفة الوزن فقط والتجميع ومخرجات المعالج (لا يوجد تحويلات regex أو إسقاط ميداني أو الفهرسة إلى القرص).

إذا كان خادم Windows يحتوي على 4 مراكز على الأقل لوحدة المعالجة المركزية (CPU) وذاكرة

وصول عشوائي (RAM) سعة 8 جيجابايت، فإن إعداد طوطخ `ParallelIntegrationPipelines = 2` يكون فعالاً. ومع ذلك، قد يؤدي هذا إلى زيادة استخدام وحدة المعالجة المركزية بشكل كبير في الحالات التي يتم فيها اكتشاف UF الأخير في المستقبل. قد يزداد استخدام وحدة المعالجة المركزية بشكل كبير في الحالات التي يتم فيها اكتشاف UF الأخير في المستقبل. ومن المتوقع أن يتحسن الأداء بشكل عام، ولكن سينخفض مرة أخرى بمجرد عودة عملية الامتصاص إلى المستويات العادية.

```
[general]
parallelIngestionPipelines = 2
```

حجم قائمة انتظار Output.conf

إذا قمت بضبط دفعة الإدخال على 500، فاعتبر التأكد من أن قائمة انتظار إخراج TCP بها مخزن مؤقت كافٍ للذاكرة حتى لا تتوقف طبقة الشبكة بحظر عامل الإدخال:

```
[tcpout:myindexers]
maxQueueSize = 50MB
```

التحقق من إستثناءات Windows Defender / برنامج مكافحة الفيروسات

يمكن أن يتوقف وكلاء نقاط نهاية الأمان (مثل Defender و CrowdStrike و Carbon Black) بفحص `splunk-winevtlog.exe` بشكل عدواني وتأميني دليل `$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\`. تأكد من إستبعاد دليل `$SPLUNK_HOME` بأكمله و`splunk-winevtlog.exe` من فحص نظام الملفات في الوقت الفعلي.

صلة وحدة التحكم بالمجال / توجيه الشبكة:

إذا كانت وحدات UF المشكلة قيد التشغيل على وحدات التحكم بالمجال أو معالجة حركة مرور المصادقة، فتأكد من عدم وجود جدار حماية محلي أو تحديد معدل الشبكة، وتأكد من أن وحدات UF يمكنها الوصول إلى الطبقة المتلقية (HFs أو الفهارس).

روابط ذات صلة

- وثائق Splunk:
  - مراقبة بيانات Windows EventLog باستخدام Splunk Enterprise

    - التكوينات المتقدمة للموجه العام
    - ملفات المواصفات: server.conf، input.conf، output.conf
- مقالات قاعدة المعارف الرئيسية
    - أستكشاف أخطاء السجلات المتأخرة من UF أو HF وإصلاحها
    - UF لا يرسل سجلات الأمان إلى Splunk
- مقالة الفانوس العملاق: ضبط الأداء طبقة إعادة التوجيه

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).