تكوين سجلات تصحيح الأخطاء على خدمة Proxy Watch / Proxy Ingest

المحتويات

المقدمة

معلومات أساسية

تمكين تصحيح أخطاء محلل الوكيل

تعطيل تصحيح أخطاء محلل الوكيل

المقدمة

يوضح هذا المستند كيفية تبديل سجلات تصحيح الأخطاء لخدمة Proxy Watch / Proxy Ingest في مجمع تدفق تحليلات الشبكة الآمنة (SNA).

معلومات أساسية

من الضروري في بعض الأحيان تمكين سجلات تصحيح الأخطاء من محلل الوكيل لميزة إدخال وكيل مجمع تدفق SNA.

تدعم ميزة Ingest للوكيل أصلية إلى مجمع تدفق SNA وتدعم إستخدام سجل الوكيل من Cisco Web Security Appliance (WSA) و McAfee و Bluecoat و Squid.

لتكوين هذه الخدمة، راجع دليل "الوكيل المفوض" المناسب لإصدار تحليلات الشبكة الآمنة.

يمكن العثور على مستندات التكوين في صفحة دعم المنتج:
https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html

تمكين تصحيح أخطاء محلل الوكيل

يمكنك الوصول إلى وحدة تحكم مجمع التدفق كمستخدم جذر أو افتح "طبقة جذر" من قائمة "تكوين النظام" التي يمكن الوصول إليها بواسطة النظام بمجرد تسجيل الدخول.

قم بإنشاء ملف التكوين الفارغ باستخدام touch /lancope/var/sw-flow-proxyparser/config/a.xml الأمر.

```
<#root>

741fc:~#

touch /lancope/var/sw-flow-proxyparser/config/a.xml

741fc:~#
```

ملاحظة: يمكن أن يكون لملف التكوين أي اسم. يتم تحميل ملفات التكوين بالترتيب الأبجدي، لذلك فإن الإعداد المعرف في b.xml يستبدل نفس الإعدادات المحملة من a.xml.

قم بتحرير ملف a.xml باستخدام الأمر vi /lancope/var/sw-flow-proxyparser/config/a.xml وأدخل مثال التكوين.

تلميح: اضغط على المفاتيح 'i' للدخول إلى وضع الإدراج في الرقم السادس. اضغط على المفاتيح 'Esc' للخروج من وضع الإدراج في VI. اكتب ":wq" لحفظ وإنهاء في VI. اكتب ":q!" لإنهاء وتجاهل التغييرات في vi.

```
<command-line>
<param>--loglevel</param>
<param>com.lancope.sws.syslogprocess.handlers=DEBUG</param>
</command-line>
```

بمجرد حفظ ملف التكوين، قم بإعادة تكوين خدمة محلل الوكيل باستخدام الأمر systemCTL restart sw-flow-proxyParser

```
<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#
```

راقب السجل مباشرة للوكيل سجل أخطاء تحليل باستخدام الأمر tail -f /lancope/var/sw-flow-proxyparser/logs/syslogprocessor.log.

تتم إضافة مزيد من المعلومات الوصفية إلى ملف sysLogProcessor.log الذي يمكن أن يشير إلى مصدر الخطأ في بيانات رسائل الوكيل المستلمة.

إذا لم تظهر رسائل تصحيح الأخطاء، فاستخدم هذه التكوين البديل المطلوب للإصدارات الأقدم.

```
<command-line>
<param>--loglevels</param>
<param>com.lancope.sws.syslogprocess.handlers=DEBUG</param>
</command-line>
```

تعطيل تصحيح أخطاء محلل الوكيل

قم بتشغيل الأمر rm -i /lancope/var/sw-flow-proxyparser/config/a.xml وأدخل y عند المطالبة لحذف ملف التكوين.

```
<#root>

741fc:~#

rm -i /lancope/var/sw-flow-proxyparser/config/a.xml

rm: remove regular file '/lancope/var/sw-flow-proxyparser/config/a.xml'?

y

741fc:~#
```

قم بإعادة تشغيل خدمة محلل الوكيل باستخدام الأمر system restart sw-flow-proxyParser.

```
<#root>

741fc:~#

systemctl restart sw-flow-proxyparser.service

741fc:~#
```

تمت إزالة تكوين تصحيح الأخطاء.

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).