تحليل حزمة تشخيص AMP لوحدة المعالجة المركزية (CPU) العالية

المحتويات

المقدمة

يصف هذا المستند الخطوات اللازمة لتحليل حزمة تشخيصية من الحماية المتقدمة من البرامج الضارة (AMP) لنقاط النهاية العامة على أجهزة Windows لاستكشاف أخطاء إستخدام وحدة المعالجة المركزية (CPU) المرتفع وإصلاحها.

ساهم به لويس فيلازكيز وحرر من قبل ياردين سانشيز، مهندس TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- الوصول إلى وحدة تحكم AMP

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- AMP لوحدة تحكم نقاط النهاية 5.4.20200204

- أجهزة نظام تشغيل Windows

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

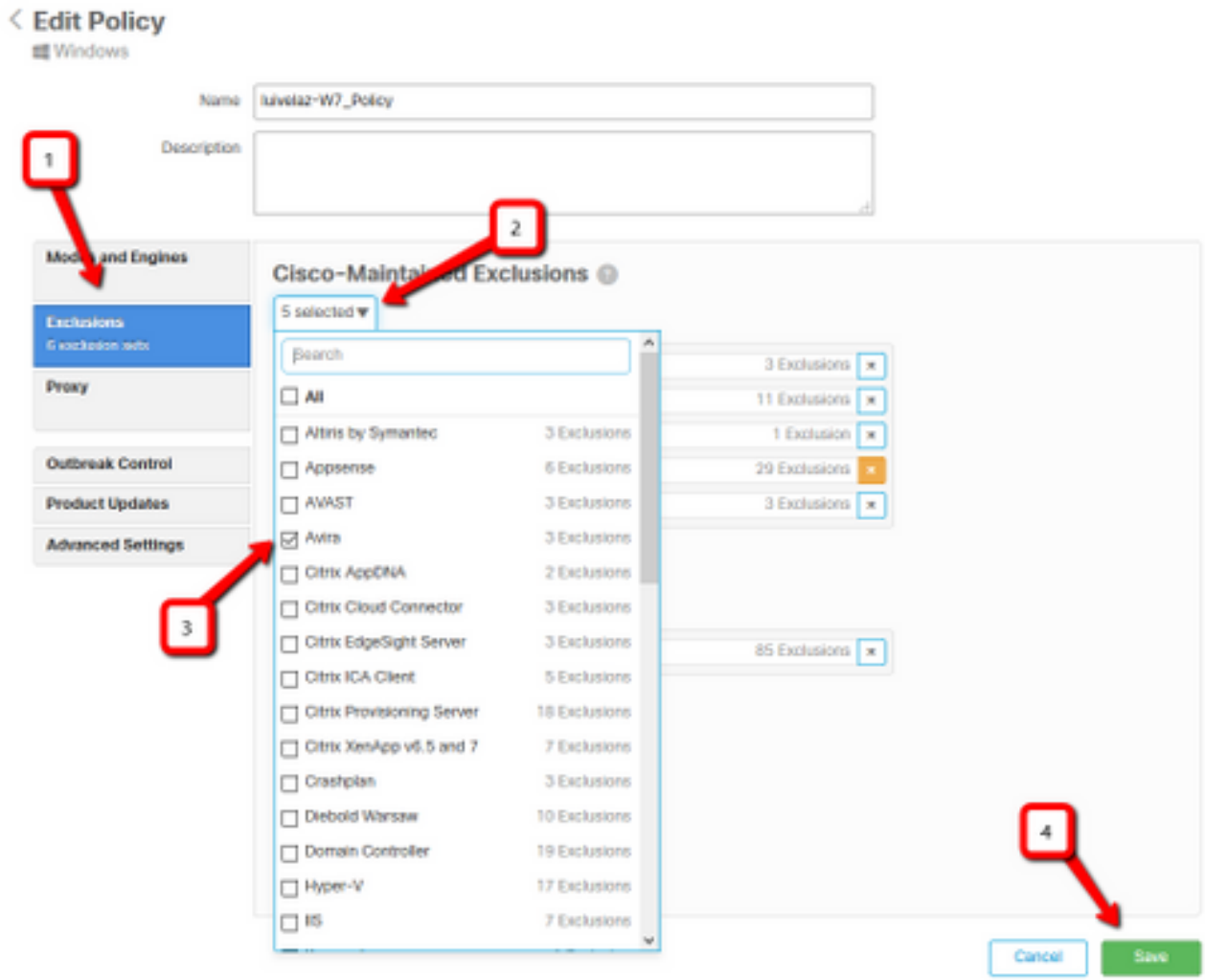
استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

التحقق من تثبيت برنامج مكافحة فيروسات آخر على الجهاز

في حالة تثبيت فيروس (AV) آخر، تأكد من إستبعاد العملية الرئيسية لل AV في تكوين النهج

> **تلميح**: أستخدم الاستثناءات التي يتم صيانتها من Cisco إذا تم تضمين البرنامج المستخدم في القائمة، تذكر أنه يمكن إضافة هذه الاستثناءات إلى الإصدارات الجديدة من تطبيق ما.
>
> لترى القوائم المتاحة في قسم استبعادات Cisco، انتقل إلى **الإدارة > السياسات > تحرير>الاستبعادات>الاستبعادات التي** تحتفظ بها **Cisco.**
> حدد ما ستحتاج إليه نقطة النهاية وقم للبرنامج المثبت حاليا على الجهاز، ثم احفظ النهج كما هو موضح في الصورة.



تحديد ما إذا كانت وحدة المعالجة المركزية عالية تحدث عند إستخدام تطبيق معين

حدد ما إذا كانت المشكلة تحدث أثناء تنفيذ أحد التطبيقات أو بعضها إذا كنت قادرا على تكرار المشكلة التي تساعد في عملية تحديد الاستباعادات المحتملة.

تجميع الحزمة التشخيصية للتحليل

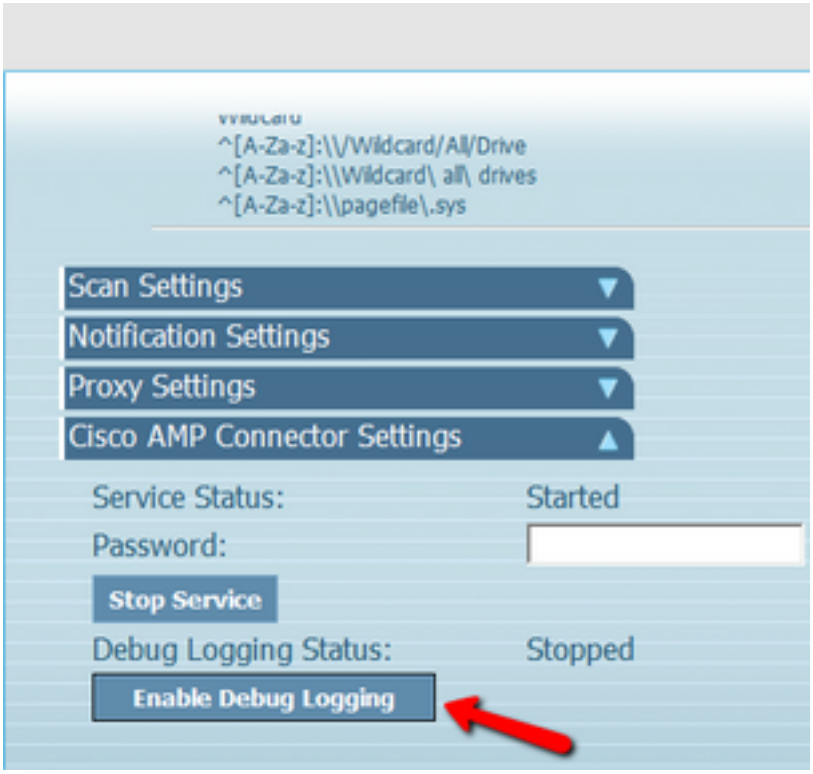
تمكين مستوى سجل التصحيح

لتجميع حزمة تشخيص مفيدة، يجب تمكين مستوى سجل تصحيح الأخطاء.

مستوى تصحيح الأخطاء في نقطة النهاية

إن يستطيع أنت نسخ الإصدار وأن يتلقى منفذ إلى النهاية، أدناه وه الإجراء الأفضل أن على قبض الحزمة التشخيصية:

1. واجهة المستخدم الرسومية المفتوحة AMP
2. انتقل إلى **الإعدادات**
3. قم بالتمرير إلى أسفل واجهة المستخدم الرسومية AMP وافتح **إعدادات موصل Cisco AMP**
4. انقر على **تمكين تسجيل تصحيح الأخطاء**
5. يجب تغيير **حالة تسجيل التصحيح** إلى **البدء.** يمكن هذا الإجراء مستوى تصحيح الأخطاء حتى نبض النهج التالي، بشكل افتراضي 15 دقيقة

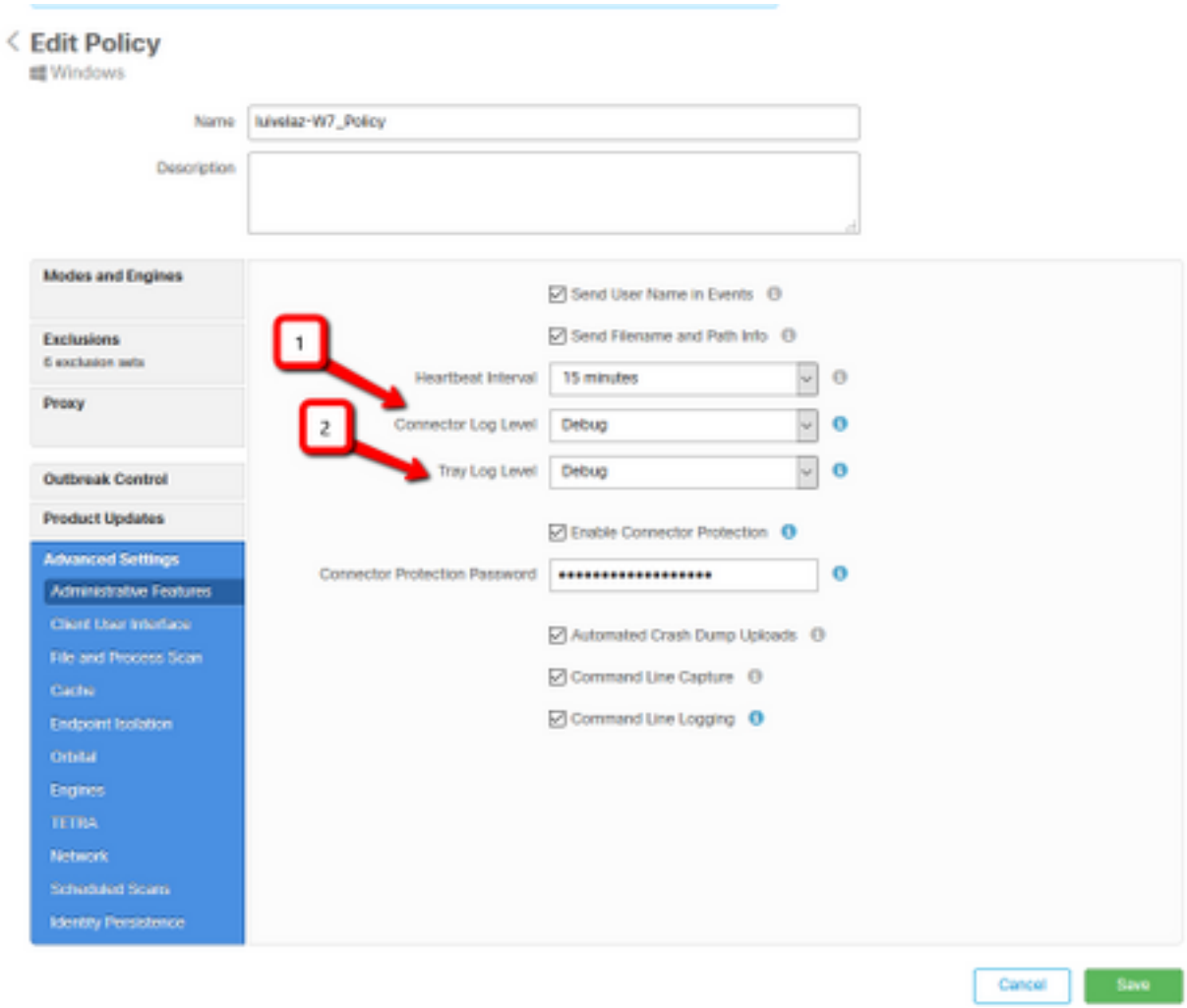


مستوى تصحيح الأخطاء في السياسة

إذا لم يكن لديك حق الوصول إلى نقطة النهاية أو أنه ال يمكن نسخ المشكلة بشكل

متناسق، فيجب تمكين مستوى سجل تصحيح الأخطاء في النهج.

لتمكين مستوى سجل التصحيح بواسطة السياسة، انتقل إلى الإدارة > السياسات > تحرير > إعدادات متقدمة > موصل **مستوى السجل** والإدارة سياسات > تحرير > إعدادات متقدمة > مستوى سجل درج، ثم حدد تصحيح الأخطاء واحفظ السياسة، كما هو موضح في الصورة.



تحذير: في حالة تمكين وضع تصحيح الأخطاء من النهج، تتلقى جميع نقاط النهاية هذا التغيير.

ملاحظة: قم بمزامنة نهج نقطة النهاية لضمان تطبيق مستوى تصحيح الأخطاء أو انتظار الفاصل الزمني لنبضات الفتحة، بشكل افتراضي هو 15 دقيقة.

إنتاج الإصدار وتجميع حزمة تشخيصية

عند تكوين مستوى تصحيح الأخطاء، انتظر حتى تحدث حالة وحدة المعالجة المركزية العالية على النظام أو قم بإعادة إنتاج الشروط المحددة مسبقا يدويا ثم قم بتجميع الحزمة التشخيصية.

من أجل تجميع الحزمة، انتقل إلى **C:\Program Files\Cisco\AMP\X.X.x** (حيث X.X.X هو أحدث إصدار AMP مثبت على النظام) وقم بتشغيل التطبيق **ipsupportTool.exe** تووم هذه العملية بإنشاء ملف **.7z** على سطح المكتب باسم **CiscoAMP_Support_Tool_%date%.7z**

ملاحظة: يستطيع الموصل الإصدار 6.2.3 والإصدارات الأحدث طلب الحزمة عن بعد، والتصفح إلى **الإدارة > أجهزة الكمبيوتر**، وتوسيع سجل نقطة النهاية واستخدام خيار التشخيص.

ملاحظة: يمكن أيضا تشغيل الحزمة التشخيصية من موجه أمر CMD باستخدام الأمر: **"C:\Program Files\Cisco\AMP\X.X.x\ipsupporttool.exe"**، أو **C:\Program Files\Cisco\AMP\X.X.x\ipsupporttool.exe" -o "X:\Folder\I\Can\Get\To"**، حيث يكون **X.X.X** هو أحدث إصدار من AMP مثبت، ويمكن إستخدام الأمر الثاني لتحديد مجلد الإخراج للملف .7z.

إجراء التحليل

هناك طريقتان لتحليل ملف تشخيصي:

- diag_analyzer.exe
- amphandlecount.ps1

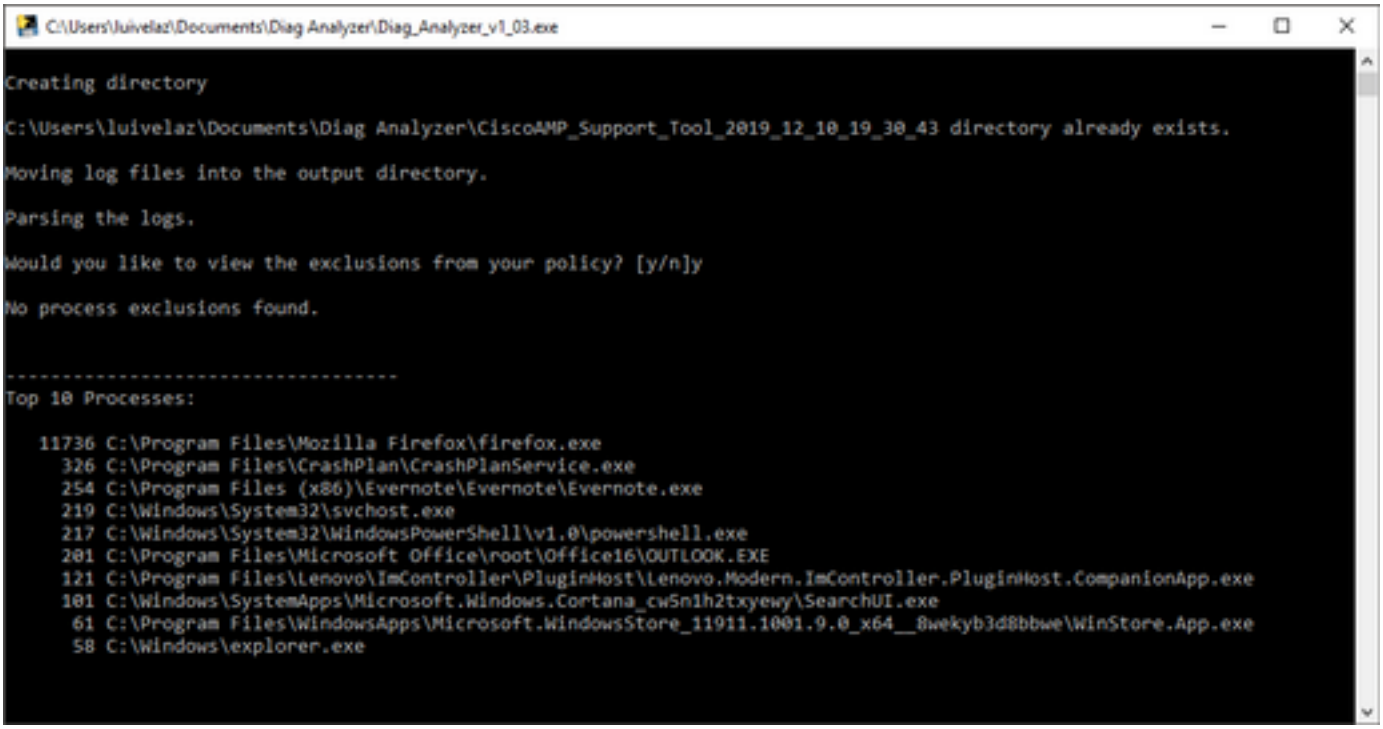
diag_analyzer.exe

الخطوة 1. تنزيل التطبيق من هنا.

الخطوة 2. في صفحة GitHub، هناك ملف README مع إرشادات إضافية حول الاستخدام.

الخطوة 3. انسخ الملف التشخيصي **CiscoAMP_Support_Tool_%date%.7z** في نفس المجلد الذي يوجد فيه Diag_Analyzer.exe.

الخطوة 4. تنفيذ التطبيق **diag_analyzer.exe.**



الخطوة 5. في المطالبة الجديدة، تأكد ما إذا كنت تريد الحصول على الاستبعادات من النهج باستخدام **Y** أو **N**.

الخطوة 6. تحتوي نتيجة البرنامج النصي على:

- أفضل 10 عمليات
- أهم 10 ملفات
- أهم 10 ملحقات
- أعلى 100 مسار
- كل الملفات

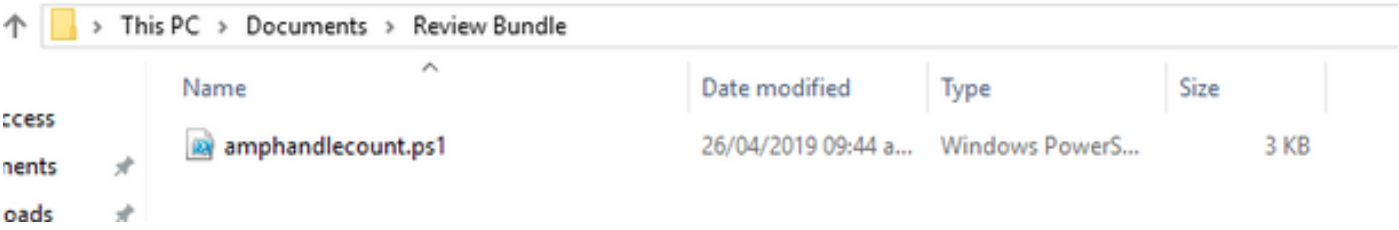
ملاحظة: يقوم Diag_Analyzer.exe بالتحقق من ملف تشخيص AMP المتوفر للملفات sfc.exe.log. ثم يقوم بإنشاء دليل جديد باسم ملف التشخيص وتخزين ملفات السجل خارج .7z، في الدليل الأصلي للتشخيص، بعد ذلك، يقوم بتحليل السجلات وتحديد أفضل 10 عمليات وملفات وملحقات ومسارات، وأخيرا يقوم بطباعة المعلومات على الشاشة وكذلك إلى ملف {Diagnostic}-summary.txt.

amphandlecount.ps1

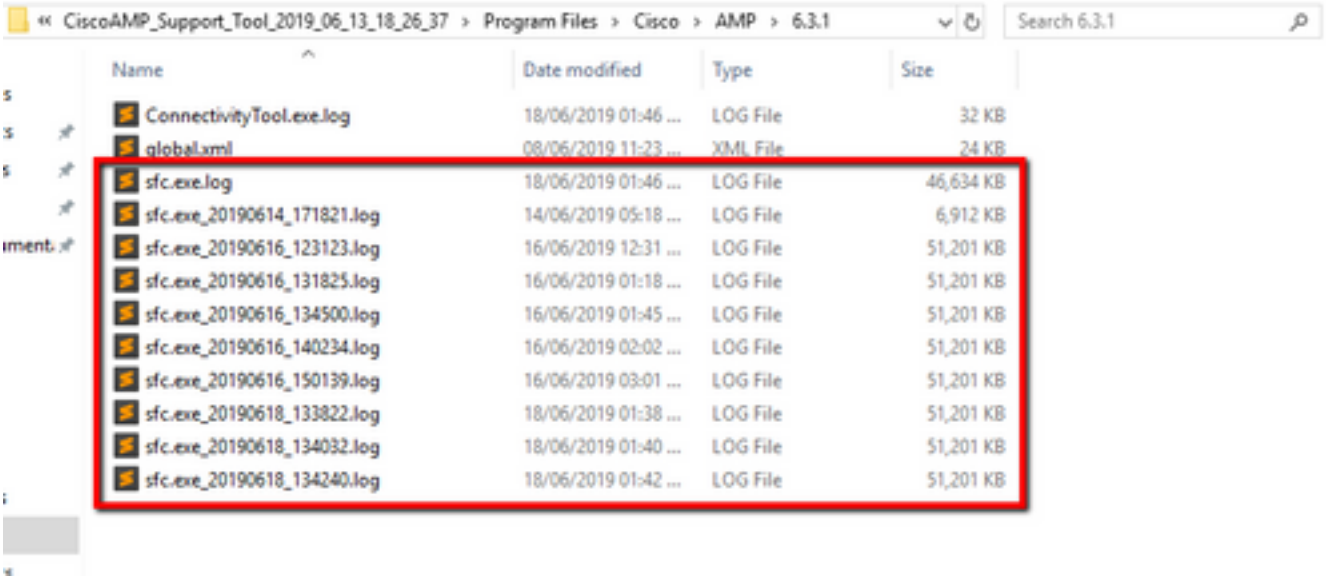
الخطوة 1. قم بتنزيل البرنامج النصي **amphandlecounts.txt** من أسفل مادة النشر المجتمعية هذه مراجعة الملفات المسموحة ضوئيا من AMP.

الخطوة 2. لتشغيل البرنامج النصي في Windows، أعد تسميته إلى **amphandlecont.ps1**.

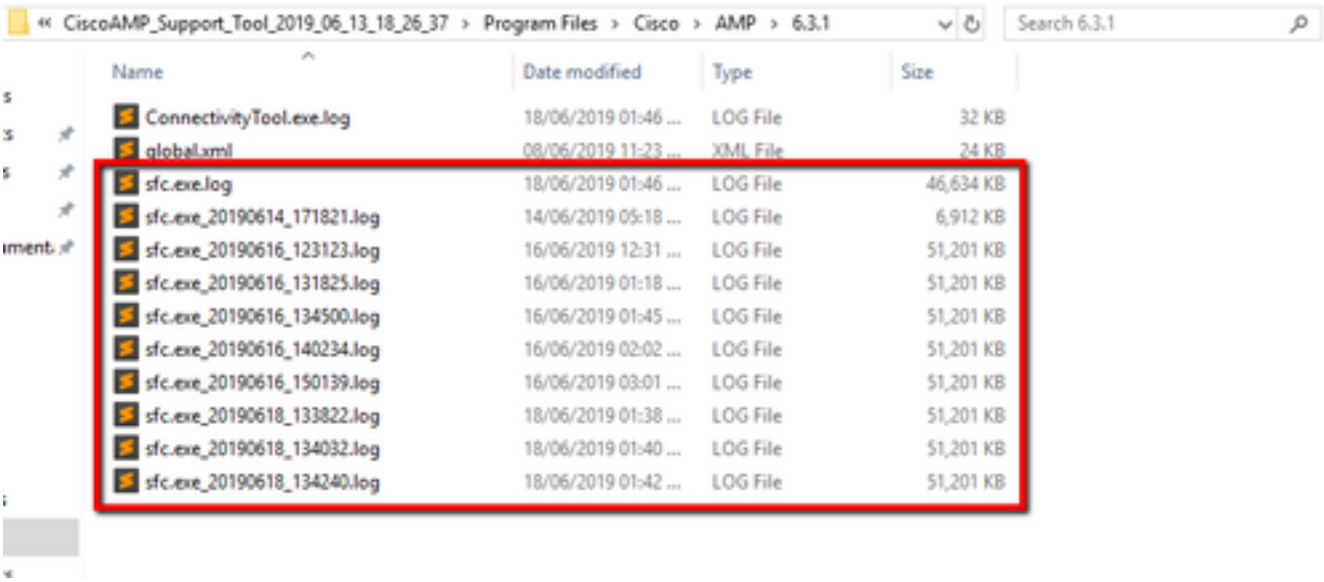
الخطوة 3. من أجل سهولة الاستخدام، انسخ ملف **amphandlecont.ps1** إلى مجلد خاص به.



الخطوة 4. قم بإلغاء ضغط ملف **CiscoAMP_Support_Tool_%date%.7z** وحدد ملفات **sfc.log** على المسار **Cisco AMP_Support_Tool_2019_06_13_18_26_37\Program Files\Cisco\AMP\X.X.X .**



الخطوة 5. انسخ ملفات **sfc.log** على المجلد **amphandlecount.ps1**.

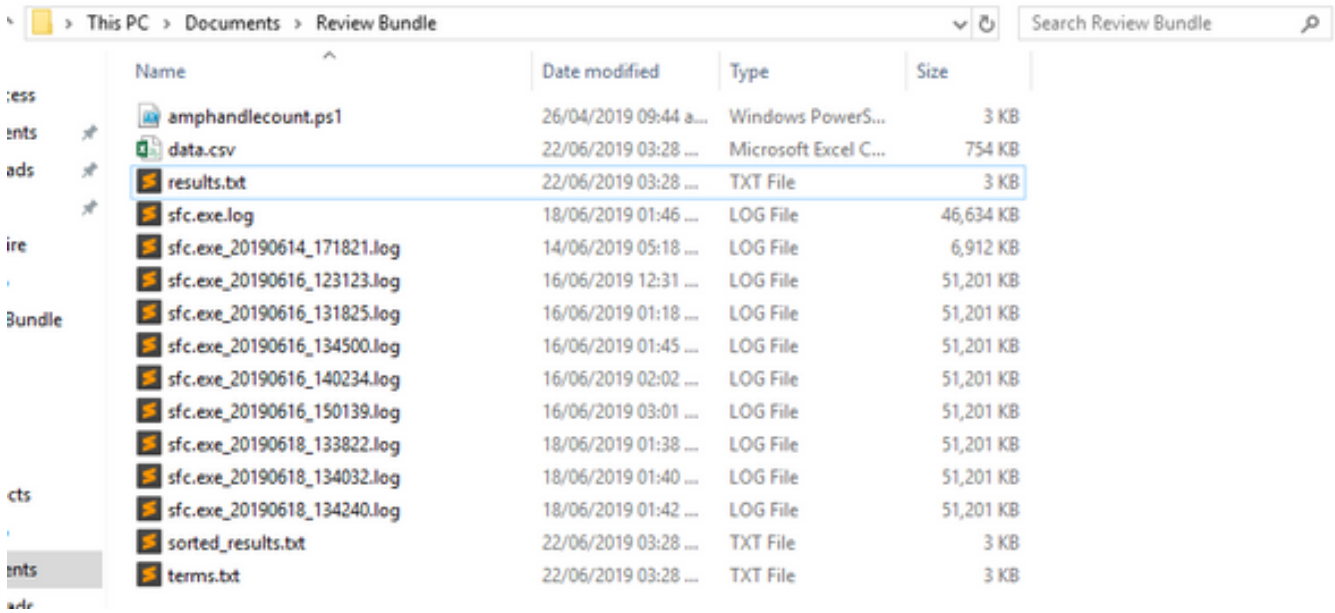


الخطوة 6. قم بتشغيل **amphandlecont.ps1** مع PowerShell، ثم يتم فتح نافذة، واعتمادا على نهج التنفيذ على نقطة النهاية، يمكن طلب إذن للتشغيل.

> **تلميح**: لتغيير نهج التنفيذ، افتح Windows PowerShell واستخدم الأوامر التالية:
> تعيين النهج للسماح بالوصول إلى التنفيذ غير المقيد - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy غير مقيد**
> تعيين النهج لتقييد الوصول إلى التنفيذ - **Set-ExecutionPolicy -Scope CurrentUser -ExecutionPolicy Restricted**

الخطوة 7. اسمح بانتهاء PowerShell (قد يستغرق الأمر بعض الوقت، اعتمادا على عدد sfc.log الموجود في المجلد) بعد انتهاء PowerShell، يتم إنشاء أربعة ملفات على المجلد:

- **data.csv**
- **results.txt**
- **sorted_results.txt**
- **terms.txt**



الخطوة 8. تحتوي الملفات الأربعة الجديدة على نتيجة التحليل:

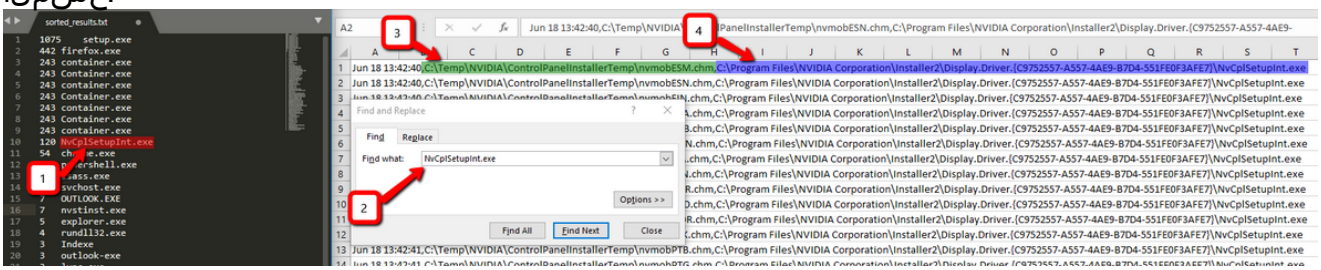
- **data.csv:** يحتوي على المسار الكامل للملفات المرموزة ضوئيا والعملية الرئيسية التي أنشأت/عدلت/نقلت الملف
- **Results.txt:** يحتوي على قائمة العمليات التي تم مسحها ضوئيا بواسطة AMP
- **sorted_results.txt:** يحتوي على قائمة العمليات التي تم مسحها ضوئيا بواسطة AMP بأكثر عملية مرموزة ضوئيا
- **Terms.txt:** يحتوي على اسم العمليات التي تم فحصها بواسطة AMP

الخطوة 9. قم بتصفية اسم العملية باستخدام عدد كبير من **العناصر المرفوزة_results.txt** في **data.csv** يمكنك تعريف العملية الأصلية بالمسار الكامل الخاص بها، ثم قم بالمتابعة لإضافة إستثناء للنهج في قائمة مخصصة إذا كانت موثوق بها.

عمليات للبحث:

1. CNTRL + F على "data.csv" والبحث
2. مسار الملف الذي تم فحصه بواسطة AMP
3. مسار العملية الأصلية التي تنسخ/تنقل/تعدل الملف

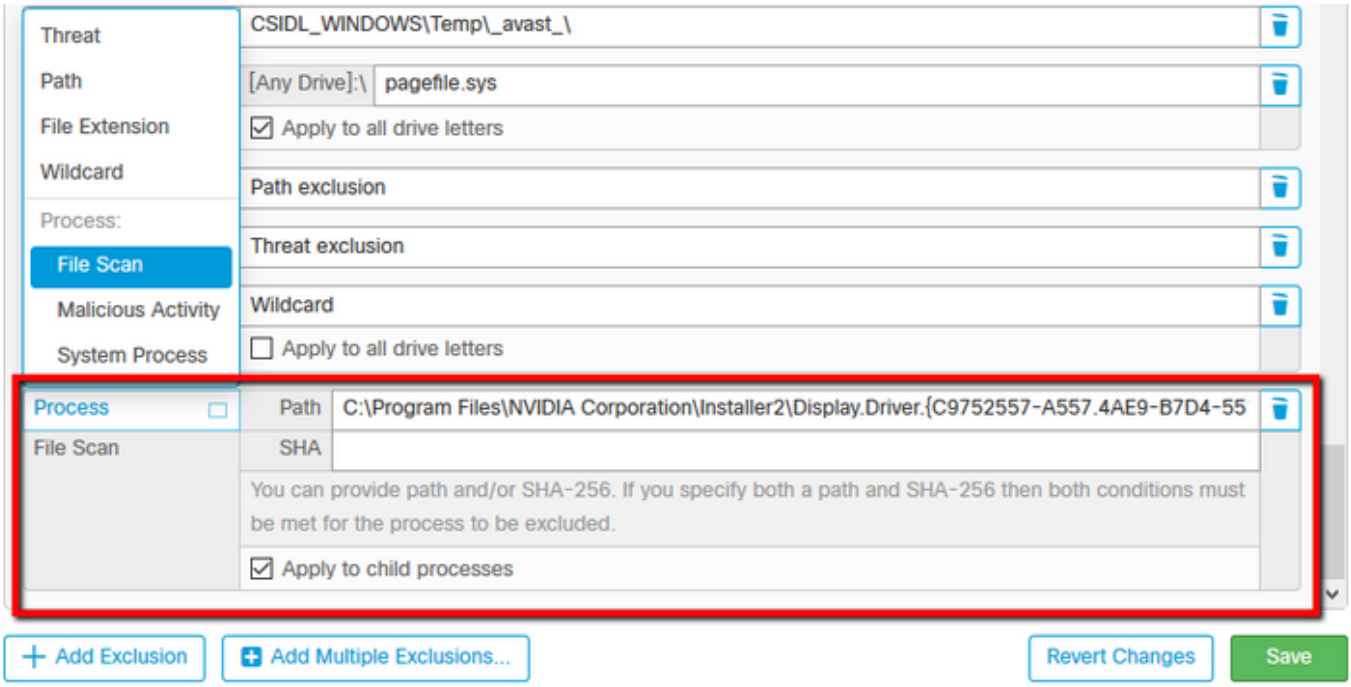
ملاحظة: ملاحظة: عادة ما يكون الاستثناء هو النوع "العملية: مسح الملف" مع "العمليات الفرعية تتضمن" للعملية الأصلية التي يتم الحصول عليها في عمليات
المسح:



ملاحظة: [هنا] يمكنك العثور على مزيد من المعلومات المتعلقة بأفضل الممارسات لإنشاء استبعادات.

استبعادات الضبط

بمجرد أن يتم تحديد العمليات أو المسارات، يمكنك إضافتهم إلى قائمة الاستبعاد المرتبطة بالسياسة المطبقة على نقطة النهاية، انتقل إلى **إدارة > إستثناءات > اسم الاستثناء > تحرير**، كما هو موضح في الصورة.



إرسال الحزمة للتحليل إلى TAC

يمكن أن يساعد ATS TAC في أستكشاف هذه السيناريوهات وإصلاحها، إذا كان الأمر كذلك، فيرجى أن تكون مستعدا لتقديم المعلومات التالية عند إنشاء الحالة:

- متى تبدأ هذه المشكلة؟
- هل هناك أي تغيير حديث؟
- هل تحدث المشكلة مع تطبيق معين؟إذا كان الجواب نعم، أي تطبيق؟
- هل يوجد برنامج مضاد للفيروسات آخر على النظام؟إذا كان الجواب نعم، أي مضادات للفيروسات؟
- تجمع حزمة تصحيح أخطاء أثناء نسخ المشكلة: خطوات تجميع حزمة 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).