دليل ضبط أداء موصل Mac Connector لنقطة النهاية الآمنة

المحتويات

المقدمة

لماذا نحتاج إلى الضبط؟

في كل مرة يتم إنشاء ملف أو نقله أو نسخه أو تنفيذه على نقطة نهاية Mac يتم إرسال حدث لذلك الملف من نظام التشغيل إلى موصل Mac لنقطة النهاية الآمنة. يؤدي الحدث إلى تحليل الملف بواسطة الموصل. تتضمن عملية التحليل بشكل عام تجزئة الملف المعني وتشغيله من خلال محركات تحليل مختلفة على كل من الكمبيوتر والسحابة. ومن المهم أن ندرك أن هذا الفعل من التمزيق يستهلك دورات وحدة المعالجة المركزية.

كلما زاد عدد عمليات الملف وتنفيذها على نقطة نهاية معينة، زاد عدد دورات وحدة المعالجة المركزية وموارد الإدخال/الإخراج التي سيتطلبها الموصل للتجزئة. هناك العديد من الميزات التي تمت إضافتها إلى الموصل لتقليل التكاليف الإضافية. على سبيل المثال، إذا تم تحليل ملف يتم إنشاؤه أو نقله أو نسخه مسبقا، سيستخدم الموصل نتيجة مخزنة مؤقتا. ومع ذلك، في حالة بعض الأحداث مثل تطبيق إجراءات الأمن التي تحتل فيها الأولوية، يتم دائما تحليل جميع الأحداث بشكل كامل بواسطة الموصل. وهذا يعني أن التطبيقات العمليات التي تنشر عمليات إعدام متكررة متعددة للأطفال - لا سيما على مدى فترة زمنية قصيرة - يمكن أن تسبب مشاكل في الأداء. إن العثور على التطبيقات التي تقوم بتنفيذ العمليات التابعة بشكل متكرر بمعدل أعلى مرة في الثانية واستبعادها يمكن أن يقلل استخدام وحدة المعالجة المركزية (CPU) لديك بشكل كبير ويزيد من عمر البطارية في أجهزة الكمبيوتر المحمولة.

بشكل عام، يكون لعمليات الملفات مثل الإنشاء والتحركات تأثير أقل من عمليات التنفيذ، لكن عمليات كتابة الملفات الزائدة وإنشاء الملفات المؤقت قد يؤدي إلى حدوث مشاكل مشابهة. يمكن أن يتسبب التطبيق الذي يكتب إلى ملف السجل بشكل متكرر، أو التطبيق الذي يقوم بإنشاء ملفات مؤقتة متعددة، في أن تستهلك نقطة النهاية الآمنة الكثير من دورات وحدة المعالجة المركزية مع التحليل غير الضروري، كما يمكن أن يحدث الكثير من التشويش للخلفية لنقطة النهاية الآمنة. إن التمييز بين الأجزاء الصاخبة من التطبيقات الشرعية يعد خطوة مهمة للغاية في الحفاظ على نقطة نهاية إنتاجية وآمنة.

الغرض من هذا المستند هو المساعدة في التمييز بين عمليات الملف (الإنشاء والنقل والنسخ) والتنفيذ الذي سيكون له تأثير سلبي على أداء الجهاز وتبديد دورات وحدة المعالجة المركزية. سيتيح لك تحديد مسارات الملفات والدلائل هذه إمكانية إنشاء مجموعات الاستبعاد المناسبة لمؤسستك والحفاظ بها.

يمكنك إضافة قوائم إستبعاد مت إنشاؤها مسبقا إلى السياسات الخاصة بك والتي يتم الاحتفاظ بها بواسطة Cisco لضمان أفضل توافق بين موصل نقطة النهاية الآمنة والبرامج الأخرى. توفر هذه القوائم على صفحة البرامج أو أمان الأو أو الفيروسات أو مكافحة الاستثناءات في وحدة التحكم إستثناءات مت صيانتها من Cisco.

أنواع التوليف

هناك ثلاثة أنواع من خيارات موالفة الاستبعاد المتوفرة:

1. **ضبط التثبيت المسبق - يمكن القيام بذلك قبل تثبيت موصل Mac لنقطة النهاية الآمنة. سوف تعطيك نظرة أكثر نظافة على أي التطبيقات والمسارات هي الأكثر انشغالا على جهازك. على أية حال، إنها عملية صاخبة جدا وتتطلب من المستخدم أن يقوم بالقليل العادل من التحليل والتجميع بنفسه.**
2. **ضبط أداة الدعم** - يمكن القيام بذلك بعد تثبيت موصل Mac ويمكن تنفيذه على أي نقطة نهاية بدون تثبيتات إضافية. حيث يؤدي نظرة محدودة إلى الوراء، كما أنه مثالي للتعرف على التطبيقات التي تتسبب في المشاكل.
3. **Procmon Tuning** - تتطلب هذه العملية أيضا تثبيت الموصل، ولكنها تتطلب أيضا إستخدام Procmon Binary، أداة التوليف المخصصة الخاصة بنا. وهو في الأساس إصدار أكثر تعقيدا من ميزة ضبط أداة الدعم. تتطلب هذه الطريقة أكبر قدر من التكوين، ومع ذلك، فهي توفر أفضل النتائج.

1. توليف التثبيت المسبق

ضبط التثبيت المسبق هو الشكل الأساسي للضبط ويتم ذلك بشكل أساسي من خلال سطر الأوامر في جلسة عمل الطرفية.

بالنسبة لنظام التشغيل Mac الأحدث من نظام التشغيل X El Capitan، ستحتاج إلى التمهيد أولا إلى وضع الاستعادة (الأمر-R) أثناء تمهيد الحماية وتعطيلها لتتبع المسار:

```
csrutil enable --without dtrace
```

وللتأكد من أي عمليات إعداد للملفات هي الأكثر شيوعا، يمكن تنفيذ ما يلي:

```
$ sudo newproc.d | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

سيظهر ذلك بشكل عام التطبيقات التي يتم تشغيلها مرارا وتكرارا. سيقوم العديد من التطبيقات بتزويد تشغيل البرامج النصية أو تنفيذ الثنائيات في فترات زمنية قصيرة للحفاظ على سياسات برامج الشركة. أي طلبات يتم تنفيذها بمعدل أكبر من مرة في الثانية، أو يتم تنفيذها عدة مرات في فترات قصيرة، يجب أن تعتبر مرشحة جيدة للاستبعاد.

للتحقق من عمليات الملفات الأكثر شيوعا، قم بتشغيل الأمر التالي:

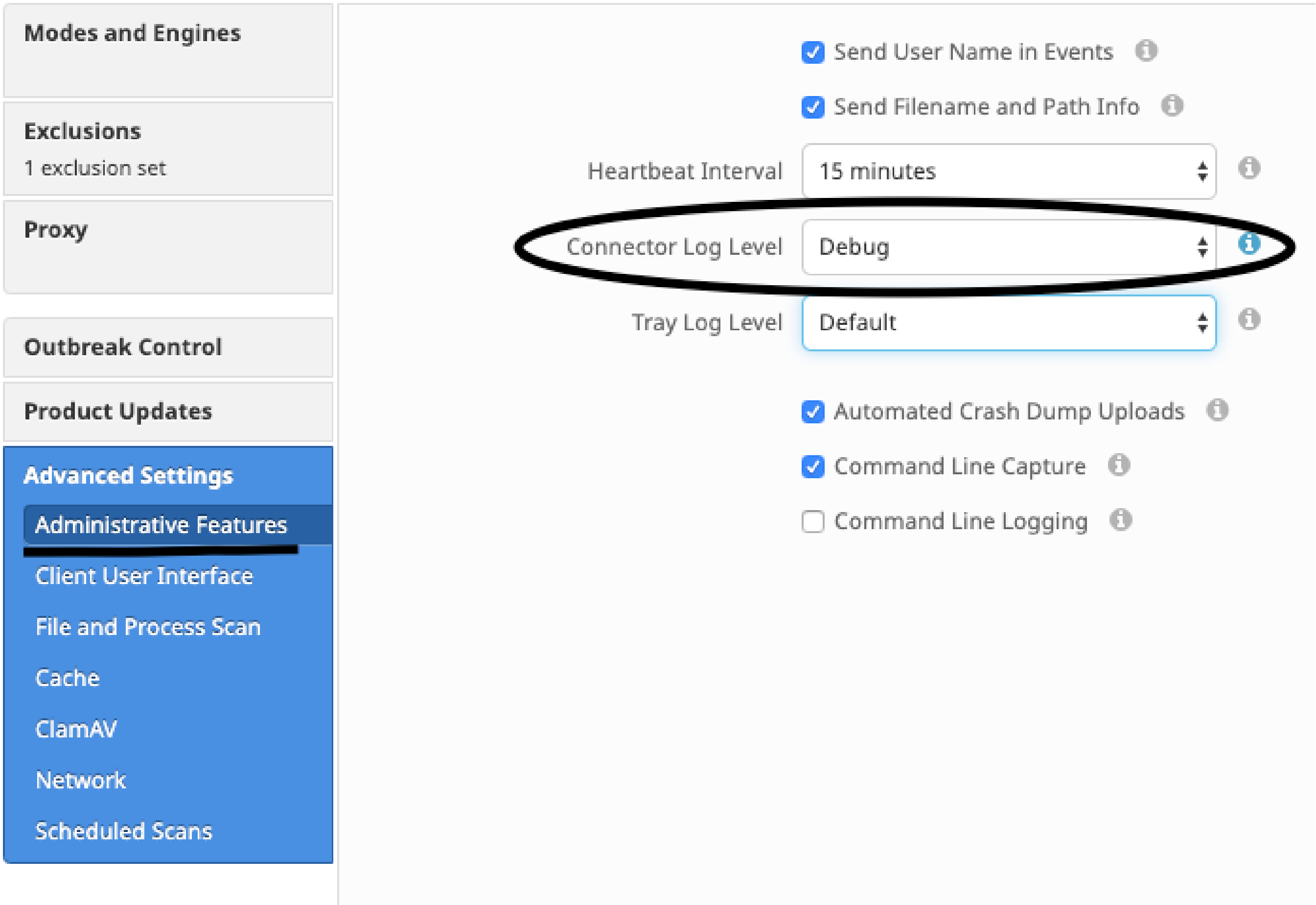
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

هذه تكون ما غالبا الأشخاص. سترى على الملفات التي يتم كتابتها إلى معظم المرف الإحتياطي للبرامج أو التشغيل دقيق التطبيقات بواسطة كتاباتها تتم تدوين ملفات للملفات أو تطبيقات بريد إلكترونية توقع بكتابة ملفات مؤقتة. بالإضافة إلى ذلك، هناك قاعدة صحيحة للتجربة وهي أن أي شيء يحتوي على ملحق ملف سجل أو ملف دفتر يومية يجب إعتباره مرشح إستبعاد مناسب.

2. أداة الدعم توليف

تمكين تسجيل تصحيح الأخطاء

يجب وضع الخوارزمية الخاصة بالموصل في وضع تسجيل التصحيح قبل بدء ضبط ملف الدعم. ويتم تحقيق ذلك عبر [وحدة تحكم نقطة النهاية الآمنة]، من خلال إعدادات نهج الموصل في *الإدارة -> السياسات*. حدد النهج، وقم بتحرير النهج، وانتقل إلى قسم *الميزات الإدارية* ضمن الشريط الجانبي *للإعدادات المتقدمة*. قم بتغيير إعداد *مستوى سجل الموصل* إلى **تصحيح الأخطاء**.



التالي، حفظ النهج. بمجرد حفظ النهج، تأكد من أنه تمت مزامنتهنتن إلى cموصل. تشغيل Cموصل في هذا الوضع ل على الأقل 15-20 دقيقة قبل متابعة بقية الضبط.

ملاحظة: عند اكتمال الضبط، لا تنسى تغيير *مستوى سجل الموصلات* رجوع إلى **افتراضي** علشان ال cموصل تدارين في إنه الأكثر كفاءة الوضع الفعال.

تشغيل أداة الدعم

تتضمن هذه الطريقة إستخدام "أداة الدعم"، وهي تطبيق تم تثبيته مع موصل Mac لنقطة النهاية الآمنة. يمكن الوصول إليه من مجلد "التطبيقات" بالنقر المزدوج فوق /Applications->Cisco Secure Endpoint->أداة الدعم.app. سيؤدي ذلك إلى إنشاء حزمة دعم كاملة تحتوي على ملفات تشخيص إضافية.

AN بديل، وبسرعة أكبر، الطريقة هي تشغيل سطر الأوامر التالي من ج جاز طرفي الجلسة:

```
sudo/Library/Application Support/Cisco/AMP for Endpoints/SupportTool-x
```

سيؤدي ذلك إلى إنشاء ملف دعم أصغر يحتوي فقط على ملفات التطبيق ذات الصلة.

فبأي طريقة تختارها لتشغيله، ستقوم "أداة الدعم" بإنشاء ملف zip على سطح المكتب الخاص بك يحتوي على ملفين دعم التطبيق: fileops.txt و exec.txt. يحتوي fileops.txt على قائمة بالملفات الأكثر تكرارا التي تم إنشاؤها وتعديلها على الجهاز. سوف يحتوي exs.txt على قائمة بالملفات التي تم تنفيذها بشكل متكرر. يتم فرز كل القائمتين حسب عدد المسح الضوئي، مما يعني أن المسارات التي تم مسحها ضوئيا بشكل متكرر تظهر في أعلى القائمة.

أترك الموصل قيد التشغيل في وضع تصحيح الأخطاء لمدة 15-20 دقيقة، ثم قم بتشغيل أداة الدعم. القاعدة الأفضل للتجربة هي أن أي ملفات أو مسارات بمعدل 1000 زيارة أو أكثر خلال ذلك الوقت هي مرشحين جيدين ليتم إستبعادها.

إنشاء إستثناءات المسار وحرف البدل واسم الملف وامتداد الملف

هناك طريقة واحدة للبدء باستخدام قواعد إستثناء المسار وهي العثور على مسارات الملفات والمجلد التي تم مسحها ضوئيا بشكل متكرر من fileops.txt ثم النظر في إنشاء قواعد إستبعاد لتلك المسارات. بمجرد تنزيل النهج، قم بمراقبة إستخدام وحدة المعالجة المركزية (CPU) الجديدة. قد يستغرق الأمر من 5 إلى 10 دقائق بعد تحديث النهج قبل أن تلاحظ انخفاض إستخدام وحدة المعالجة المركزية حتى يستغرق وقتا أطول. إذا كنت لا تزال ترى مشاكل، قم بتشغيل الأداة مرة أخرى لترى أي مسارات جديدة تراقبها.

- هناك قاعدة صحيحة للتجربة وهي أن أي شيء يحتوي على ملف سجل أو ملف دفتر يومية يجب اعتباره مرشح إستبعاد مناسب.

إنشاء إستبعادات العملية

NOTE: Process Exclusions on Mac can only be implemented for Mach-O files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts) or .app (Application Bundles).
للحصول على أفضل الممارسات المتعلقة باستبعادات العملية، راجع:إستثناءات العملية في Linux و MacOS: نقاط النهاية الآمنة

من ضبط جيد وهو تعريف العمليات أو الاستخدام عدد كبير من عمليات التنفيذ من exs.txt، والبحث عن المسار إلى الملف التنفيذي، وإنشاء إستثناء لهذا المسار. ومع ذلك، هناك بعض العمليات التي يجب عدم تضمينها، وهذا يشمل:

- برامج المرافق العامة - ال يوصى باستبعاد برامج المرافق العامة (مثل: USR/BIN/GREP) دون مراعاة ما يلي. يمكن للمستخدم تحديد أي تطبيق يسمى العملية، (على سبيل المثال: البحث عن العملية الأصلية التي تقوم بتنفيذ GREP) واستبعاد العملية الأصلية. يجب القيام بذلك إذا، وفقط إذا، كان الاستثناء الأصلي ينطبق على العملية. إذا كان يمكن توجيل العملية الأصلية بشكل آمن إلى إستثناء للعملية. يمكن تحديد المستخدم الذي يقوم بتنفيذ العملية. (على سبيل المثال: إذا تم إستدعاء عملية على مستوى عال من قبل المستخدم "root"، يمكن إستبعاد العملية، ولكن فقط بالنسبة للمستخدم "root" المحدد، وهذا سيسمح لنقطة النهاية الآمنة بمراقبة عمليات تنفيذ عملية معينة من قبل أي مستخدم ليس "root").**الملاحظة:إستثناءات العملية جديدة في إصدارات الموصل 1.11.0 والإصدارات الأحدث. ولهذا السبب، يمكن إستخدام برامج المرافق العامة كاستثناء مسار في إصدارات الموصل 1.10.2 والإصدارات الأقدم. غير أن هذه الممارسة ال يوصى بها إال عندما يكون من الضروري تماما إجراء تقييم للأداء.**

يعتبر العثور على العملية الأصلية مهما لاستثناءات العملية. بمجرد العثور على العملية الأصلية و/أو مستخدم العملية، يمكن للمستخدم إنشاء الاستثناء لمستخدم معين وتطبيق إستثناء العملية على العمليات الفرعية، مما يؤدي بدوره إلى إستبعاد العمليات الصاخبة التي يمكن توجيلها إلى استبعادات عملية.

تعريف العملية الأصلية

1. من exec.txt، حدد عملية كبيرة الحجم (على سبيل المثال: /bin/rm).
2. افتح ampdaemon.log من حزمة الدعم، وقم بإلغاء zip syslog.tar، ثم اتبع المسار /Library/Logs/Cisco/ampdaemon.log (يتوفر فقط في حزمة الدعم، وليس من حزمة دعم تم إنشاؤها باستخدام الخيارات الافتراضية).
3. ابحث في الأمر ampdaemon.log عن العملية المراد إستبعادها. العثور على سطر السجل الذي يظهر تنفيذ العملية (على سبيل المثال: أغسطس 19:09:47:29 devs-mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962]: Daemon Rx: VNODE:Execute X:6210 p:3296 pp:3200 u:502 [/bin/rm]).
4. تعريف العملية الأصلية باستخدام أحد الأساليب التالية: حدد مسار العملية الأصلية الذي قد يتبع مسار العملية المراد إستبعادها

(على سبيل المثال: [/bin/rm] [*مسار العملية الأصلية*]).إذا لم يتضمن السجل مسار العملية الأصل، قم بتعريف معرف العملية الأصل من PP: قسم من سطر السجل (على سبيل المثال: PP:3200).

5. باستخدام إما المسار الأصل وأ معرف العملية الأصل، قم بتكرار الخطوات 4 و 3 لتحديد أصل العملية الأصلية الحالية. تابع هذه العملية حتى ال يمكن تحديد أي أصل، أو معرف العملية الأصل = 1 (على سبيل المثال: pp:1).
6. بمجرد معرفة شجرة العملية، ابحث عن مسار البرنامج الذي يغطي معظم العمليات أو كلها التي يجب إستبعاداه وتعرف على التطبيق بشكل فريد. وهذا يقلل إلى أدنى حد من فرصة إستبعاد العمليات التي يقوم بها تطبيق آخر عن غير قصد.

تعريف مستخدم العملية

1. اتبع الخطوات من 1 إلى 3 لتعريف العملية الأصل من أعلى.
2. تعريف مستخدم عملية باستخدام إحدى الطرق التالية: ابحث عن معرف المستخدم للعملية المحددة من U: في سطر السجل (ex: U:502).من نافذة المحطة الطرفية قم بتشغيل الأمر التالي: `dscl . list /Users UniqueID | GREP #`، حيث # وهو معرف المستخدم.يجب أن ترى إنتاج مماثل لـ: `username 502`، حيث `username` وهو المستعمل من العملية المحددة.
3. يمكن إضافة اسم المستخدم هذا إلى إستثناء العملية ضمن فئة "المستخدم" لتقليل نطاق الاستبعاد، وهو أمر مهم لبعض إستثناءات العملية. **ملاحظة: إذا كان مستخدم العملية هو المستخدم المحلي للجهاز، ويجب تطبيق هذا الاستبعاد على أجهزة متعددة ذات مستخدمين محليين مختلفين، فيجب ترك فئة المستخدم فارغة للسماح بتطبيق إستثناء العملية على جميع المستخدمين.**

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).