# AMP pour le guide d'optimisation des performances de connecteur de MAC de points finaux

## Contenu



## Introduction

Édité par : Alex Yakimenko, Software Engineer

### Pourquoi devons-nous accorder ?

Chaque fois un fichier est créé, déplacé, copié, ou exécuté sur un point final de MAC un événement pour ce fichier est envoyé du système d'exploitation au connecteur de MAC d'AMP. L'événement a comme conséquence ce fichier analysé par le connecteur. Le processus d'analyse implique généralement de hacher le fichier en question et l'exécution il par différentes engines d'analyse sur l'ordinateur et dans le nuage. Il est important d'identifier que cet acte du hachage consomme des cycles CPU.

Plus d'exécutions de fichier et exécute qui se produisent sur un point final donné, plus de cycles CPU et des ressources E/S le connecteur exigera pour le hachage. Il y a plusieurs caractéristiques qui ont été ajoutées au connecteur pour réduire le temps système. Par exemple, si un fichier étant créé, déplacé, ou copié a été précédemment analysé, le connecteur utilisera un résultat caché. Cependant, dans le cas de certains événements comme exécute où la Sécurité est primordiale, tous les événements toujours sont entièrement analysés par le connecteur. Ceci signifie que les applications ou les processus qui propagent de plusieurs exécutions répétitives des processus fils - particulièrement sur une courte période - peuvent entraîner des problèmes de performance. Trouvant et excluant les applications qui exécutent répétitivement des processus fils un débit plus grand qui une fois par seconde peut de manière significative réduire votre vie de batterie d'utilisation du CPU et d'augmentation sur des ordinateurs portables.

Les exécutions de fichier comme crée et les mouvements ont généralement moins d'incidence qu'exécute, mais le fichier excessif écrit et la création de fichier temporaire peut avoir comme conséquence les problèmes semblables. Une application qui écrit à un fichier journal fréquemment, ou une qui génèrent de plusieurs fichiers temporaires peut faire consommer l'AMP beaucoup de cycles CPU avec l'analyse inutile et peut créer beaucoup de bruit pour le backend d'AMP. La distinction des parties bruyantes d'applications légitimes est une étape très importante en mettant à jour un point final productif et sûr.

Le but de ce document est d'aider à distinguer les exécutions de fichier (créez, déplacez-vous, et

copie) et exécute qui exerceront un effet négatif sur les cycles CPU de la représentation et des déchets du démon. Identifier ces fichier et chemins du répertoire te permettra pour créer et mettre à jour l'exclusion appropriée place pour votre organisation.

Vous pouvez ajouter les listes pré-créées d'exclusion à vos stratégies qui sont sont mises à jour par Cisco pour fournir une meilleure compatibilité entre l'AMP pour des points finaux connecteur et antivirus, Sécurité, ou tout autre logiciel. Ces listes sont disponibles à la page d'exclusions dans la console en tant qu'exclusions Cisco-mises à jour.

## Types d'accord

Il y a trois genres d'options de accord d'exclusion disponibles :

1. **Préinstallez l'accord – ceci peut être fait avant d'installer le connecteur de MAC d'AMP. Il vous donnera que les plus propres les regardent quels application et chemins sont les plus occupés sur votre ordinateur. Cependant, c'est un processus très bruyant et exige de l'utilisateur de faire un bit équitable d'analyse et d'agrégation sur leurs propres moyens.**
2. **Accord d'**outil d'assistance – ceci peut être fait après que le connecteur de MAC soit installé et puisse être exécuté sur n'importe quel point final sans binaires supplémentaires. Il exécute un aspect limité de retour et est grand pour identifier des applications ennuyeuses.
3. **Accord de Procmon** – ce processus exige également du connecteur d'être installé, mais exige également l'utilisation de la binaire de Procmon, notre outil de accord fait sur commande. C'est essentiellement une version plus sophistiquée de la caractéristique de accord d'outil d'assistance. Cette méthode exige la plus grande quantité de configuration ; cependant, il fournit les meilleurs résultats.

# 1. Préinstallez l'accord

Préinstallez l'accord est la forme la plus fondamentale de l'accord et est fait principalement par la ligne de commande en session de travail.

Pour un plus nouveau MAC d'EL Capitan d'OS X vous devrez démarrer d'abord pour récupérer le mode (commande-r) tout en amorçant et désactivez la protection pour le dtrace :

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

Pour examiner qui classent des exécutions soyez la plupart de répandu exécutent ce qui suit :

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

Ceci affichera généralement quelles applications sont exécutées maintes et maintes fois. Beaucoup d'applications de ravitaillement exécuteront des scripts ou exécuteront des binaires dans des intervalles courts pour mettre à jour des stratégies de logiciel de société. Tout être exécuté vu par applications un débit plus grand qu'une fois qu'une seconde, ou de plusieurs temps exécutés dans les courtes rafales, est considérée un bon candidat pour l'exclusion.

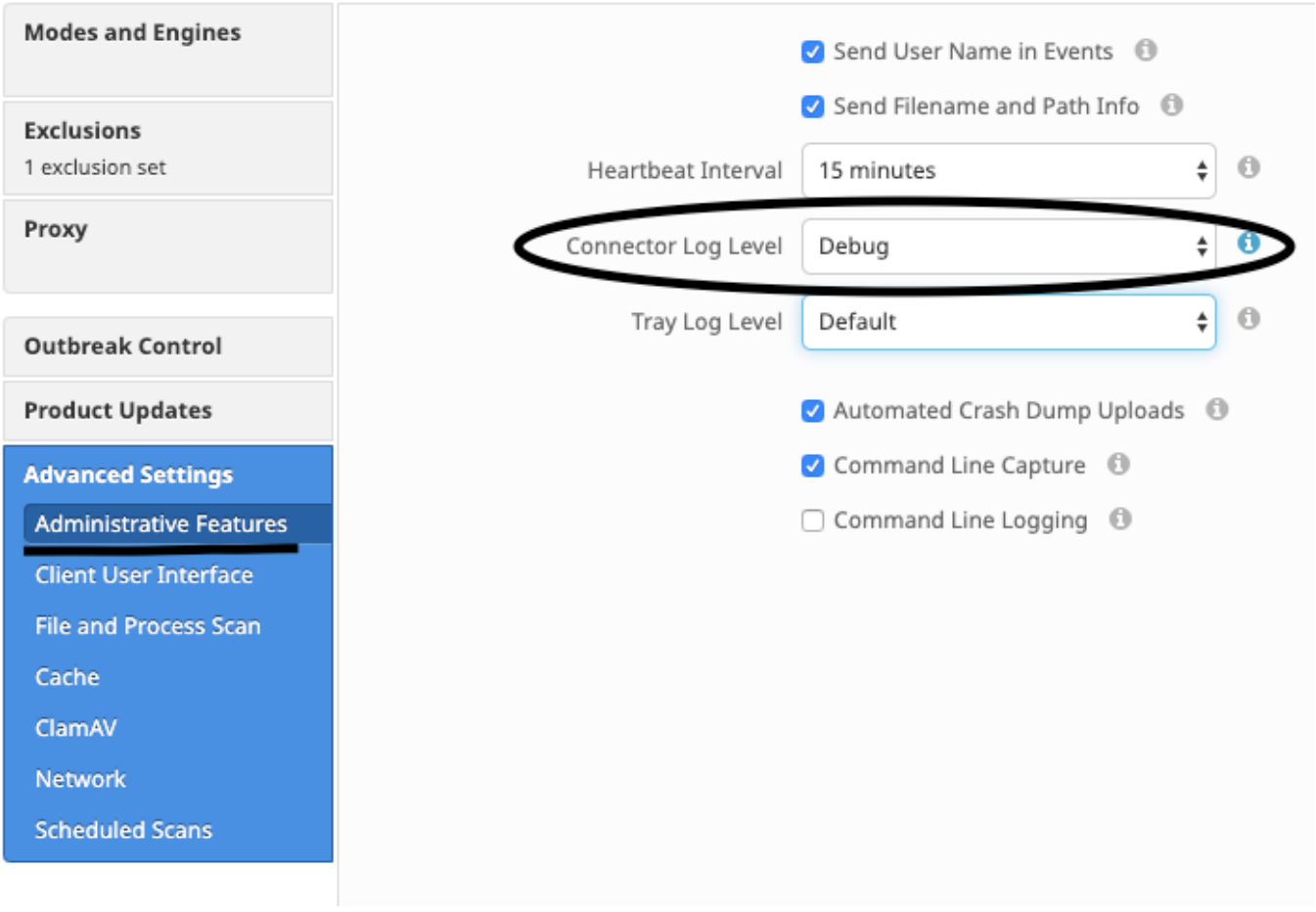
Pour examiner qui classent des exécutions soyez la plupart de répandu, exécutent la commande suivante :

```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```
Vous verrez immédiatement quels fichiers sont écrits aux la plupart. Souvent ce sera des fichiers journal étant écrits par aux applications en cours d'exécution, au logiciel de sauvegarde copiant des fichiers, ou aux applications de messagerie électronique écrivant les fichiers temporaires. En plus de ceci, une bonne règle empirique est que quelque chose avec une extension de fichier de log ou de journal devrait être considéré un candidat approprié d'exclusion.

# 2. Accord d'outil d'assistance

## Activation du debug logging

Le démon du connecteur doit être mis dans le mode de debug logging avant que commençant l'accord de fichier de support. Ceci est fait par l'intermédiaire de l'AMP pour la console de points finaux, par les paramètres de la stratégie du connecteur à la *Gestion - > des stratégies*. Sélectionnez la stratégie, éditez la stratégie, et allez aux *caractéristiques la* section *administrative* sous la barre latérale de *paramètres avancés*. Changez la configuration de *niveau de log de connecteur* **pour déboguer**.




Prochain, sauvegardez votre stratégie. Une fois que votre stratégie a été enregistrée, assurez qu'elle a été synchronisée au connecteur. Exécutez le connecteur en ce mode pendant au moins 15-20 minutes avant de continuer le reste de l'accord.

REMARQUE: Quand votre accord est complet, n'oubliez pas de changer la configuration de *niveau de log de connecteur* de nouveau au **par défaut** de sorte que le connecteur fonctionne en son mode adressage effectif plus efficace et.

## Outil d'assistance courant

Cette méthode implique d'à l'aide de l'outil d'assistance, une application installée du connecteur de MAC d'AMP. Il peut être accédé à du dossier Applications en double-cliquer sur le >Cisco AMP->Support Tool.app de /Applications-. Ceci génèrera un module de support complet contenant les fichiers diagnostiques supplémentaires.

Une alternative, et un plus rapide, méthode est d'exécuter la ligne de commande suivante d'une session de travail :

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

Ceci aura comme conséquence un fichier beaucoup plus petit de support contenant seulement les fichiers de accord appropriés.

L'un ou l'autre de manière que vous choisissez de l'exécuter, outil d'assistance génèrera un fichier zip sur votre appareil de bureau qui contient deux fichiers de accord de support : fileops.txt et execs.txt. fileops.txt contient une liste le plus souvent des fichiers créés et modifiés sur votre ordinateur. execs.txt contiendra la liste le plus souvent des fichiers exécutés. Les deux listes sont triées par le compte de balayage, signifiant que le plus souvent les chemins balayés apparaissent en haut de la liste.

Laissez l'exécution de connecteur en mode de débogage pendant une période 15-20 minute, et puis exécutez l'outil d'assistance. Une bonne règle empirique est que tous les fichiers ou chemins qui font la moyenne de 1000 hit ou plus pendant ce temps sont de bons candidats à exclure.

#### Création du chemin, du masque, du nom du fichier, et des exclusions d'extension de fichier

Une manière d'obtenir commencé par des règles d'exclusion de chemin trouve le plus souvent les chemins balayés de fichier et dossier de fileops.txt et puis d'envisager de créer des règles d'exclusion pour ces chemins. Une fois que la stratégie a été téléchargée, surveillez la nouvelle utilisation du CPU. Il pourrait prendre 5 à 10 minutes après que la stratégie est mise à jour avant que vous notiez la baisse d'utilisation du CPU comme cela pourrait prendre du temps pour que le démon rattrape. Si vous voyez toujours des questions, exécutez l'outil de nouveau pour voir quels nouveaux chemins vous observez.

- Une bonne règle empirique est que quelque chose avec une extension de fichier de log ou de journal devrait être considéré un candidat approprié d'exclusion.

#### Création des exclusions de processus

**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).
Pour des pratiques recommandées concernant des exclusions de processus voyez : AMP pour des points finaux : Exclusions de processus dans le MaOS et le Linux

Un bon modèle de accord est premier identifiant les processus avec un grand volume de exécute d'execs.txt, trouve le chemin à l'exécutable, et crée une exclusion pour ce chemin. Cependant, il y a quelques processus qui ne devraient pas être inclus, ceci inclut :

- Programmes utilitaires généraux - il n'est pas recommandé pour exclure des programmes utilitaires généraux (ex : usr/coffre/grep) sans expliquer le suivant. L'utilisateur peut déterminer ce que l'application appelle le processus, (ex : trouvez le processus père qui exécute le grep) et excluez le processus père. Ceci devrait être fait si et seulement si, le processus père peut être sans risque transformé en exclusion de processus. Si l'exclusion de parent s'applique aux enfants, alors les appels à tous les enfants du processus père seront également exclus.L'utilisateur qui exécute le processus peut être déterminé. (ex : si un processus s'appelle à un grand volume par l'utilisateur « racine », on peut exclure le processus, mais seulement pour l'utilisateur spécifié 'racine », ceci laissera l'AMP pour surveiller exécute d'un processus donné par n'importe quel utilisateur qui n'est pas « racine »).**REMARQUE: Les exclusions de processus sont nouvelles dans des versions 1.11.0 et plus récentes de connecteur. Pour cette raison, les programmes utilitaires généraux peuvent être soient utilisés comme exclusion de chemin dans des versions 1.10.2 de connecteur et plus vieux.**

**Cependant, cette pratique est seulement recommandée quand un compromis de représentation est absolument nécessaire.**

Trouver le processus père est important pour des exclusions de processus. Une fois le processus père et/ou l'utilisateur du processus sont trouvés, l'utilisateur peuvent créer l'exclusion pour un utilisateur spécifique et s'appliquer l'exclusion de processus aux processus fils, qui à leur tour excluront les processus bruyants qui ne peuvent pas eux-mêmes être transformés en exclusions de processus.

**Identifiez le processus père**

1. D'execs.txt, identifiez le processus à fort débit (ex : /bin/rm).
2. Ouvrez ampdaemon.log de programme de soutien, défaites la fermeture éclair de syslog.tar, puis suivez le chemin /Library/Logs/Cisco/ampdaemon.log (seulement fourni en module d'afullsupport, pas par un programme de soutien généré avec les options par défaut).
3. Recherche ampdaemon.log du processus à exclure. Trouvez la ligne de log qui affiche l'exécution de processus (ex : 19 août 09:47:29 devs-Mac.local [2537] [fileop]:[info]-[kext_processor.c@938]:[210962] : Démon Rx : VNODE : EXÉCUTEZ X:6210 P:3296 PP:3200 U:502 [/BIN/RM]).
4. Identifiez le processus père utilisant une des méthodes suivantes : Identifiez le chemin du processus de parent qui peut suivre le chemin du processus à exclure (ex : [/bin/rm] [*chemin du processus de parent*]).Si le log n'inclut pas le chemin du processus de parent, identifiez l'ID de processus de parent de `pp :` section de la ligne de log (ex : PP:3200).
5. Utilisant le chemin de parent ou l'ID de processus de parent, répétez les étapes 3 et 4 pour déterminer le parent du processus père en cours. Continuez ce processus jusqu'à l'un ou l'autre d'aucun parent peut être déterminé, ou l'ID de processus de parent = 1 (ex : PP:1).
6. Une fois que l'arborescence de processus est connue, recherchez le chemin de programme qui couvre les la plupart ou toutes les exécutions qui devraient être exclues et identifient seulement l'application. Ceci réduit la possibilité d'involontairement à l'exclusion des exécutions exécutées par une autre application.

**Identifiez l'utilisateur du processus**

1. Suivez les étapes 1-3 d'identifier le processus père d'en haut.
2. Identifiez l'utilisateur d'un processus utilisant un la méthode suivante : Trouvez l'user-id du processus donné d'`U :` dans la ligne de log (ex : U:502).Du terminal window exécuté la commande suivante : `dscl. liste /Users UniqueID | grep #`, où `#` est l'user-id.Vous devriez voir la sortie semblable à : `Nom d'utilisateur 502`, où le `nom d'utilisateur` est l'utilisateur du processus donné.
3. Ce nom d'utilisateur peut être ajouté à une exclusion de processus sous la catégorie d'utilisateur pour réduire la portée de l'exclusion, qui pour certaines exclusions de processus, est importante. **REMARQUE: si l'utilisateur d'un processus est l'utilisateur local de l'ordinateur, et cette exclusion doit appliquer à de plusieurs ordinateurs avec différents utilisateurs locaux, la catégorie d'utilisateur doit être blanc de gauche pour permettre à l'exclusion de processus pour s'appliquer à tous les utilisateurs.**