Guide de réglage des performances du connecteur Mac des points de terminaison sécurisés

Contenu

Introduction

Pourquoi devons-nous nous ajuster ?

Chaque fois qu'un fichier est créé, déplacé, copié ou exécuté sur un point d'extrémité Mac, un événement pour ce fichier est envoyé du système d'exploitation au connecteur Mac de point d'extrémité sécurisé. L'événement entraîne l'analyse de ce fichier par le connecteur. Le processus d'analyse consiste généralement à hacher le fichier en question et à l'exécuter via différents moteurs d'analyse, à la fois sur l'ordinateur et dans le cloud. Il est important de reconnaître que cet acte de hachage consomme des cycles CPU.

Plus le nombre d'opérations et d'exécutions de fichiers survenant sur un point de terminaison donné est important, plus le processeur et les ressources d'E/S nécessaires au connecteur pour le hachage sont nombreuses. Plusieurs fonctions ont été ajoutées au connecteur pour réduire la surcharge. Par exemple, si un fichier en cours de création, de déplacement ou de copie a déjà été analysé, le connecteur utilise un résultat mis en cache. Cependant, dans le cas de certains événements tels que les exécutions où la sécurité est primordiale, tous les événements sont toujours entièrement analysés par le connecteur. Cela signifie que les applications ou les processus qui propagent plusieurs exécutions répétitives de processus enfants, en particulier sur une courte période, peuvent causer des problèmes de performances. Rechercher et exclure les applications qui exécutent des processus enfants de manière répétitive à un rythme supérieur à celui d'une fois par seconde peut réduire considérablement l'utilisation du processeur et augmenter l'autonomie de la batterie sur les ordinateurs portables.

Les opérations de fichiers telles que les créations et les déplacements ont généralement moins d'impact que les exécutions, mais les écritures excessives et la création temporaire de fichiers peuvent entraîner des problèmes similaires. Une application qui écrit fréquemment dans un fichier journal, ou qui génère plusieurs fichiers temporaires, peut entraîner une consommation excessive de cycles CPU avec analyse inutile du point de terminaison sécurisé et peut créer beaucoup de bruit pour le serveur principal du point de terminaison sécurisé. Distinguer les parties bruyantes des applications légitimes est une étape très importante pour maintenir un terminal productif et sûr.

L'objectif de ce document est d'aider à distinguer les opérations de fichiers (création, déplacement

et copie) et les exécutions qui auront un effet négatif sur les performances du démon et les cycles CPU de gaspillage. L'identification de ces chemins de fichiers et de répertoire vous permettra de créer et de gérer les jeux d'exclusion appropriés pour votre organisation.

Vous pouvez ajouter des listes d'exclusion précréées à vos politiques qui sont mises à jour par Cisco afin d'assurer une meilleure compatibilité entre le connecteur Secure Endpoint et l'antivirus, la sécurité ou d'autres logiciels. Ces listes sont disponibles sur la page Exclusions de la console sous la forme Exclusions gérées par Cisco.

Types de réglage

Il existe trois types d'options de réglage des exclusions :

1. **Réglage préalable à l'installation - ceci peut être fait avant l'installation du connecteur Mac Secure Endpoint. Il vous donnera le regard le plus net sur l'application et les chemins les plus fréquentés de votre machine. Cependant, il s'agit d'un processus très bruyant qui nécessite que l'utilisateur fasse un bon bout d'analyse et d'agrégation par lui-même.**
2. **Réglage de l'outil de support** : cette opération peut être effectuée après l'installation du connecteur Mac et peut être effectuée sur n'importe quel terminal sans binaires supplémentaires. Il effectue un retour en arrière limité et est idéal pour identifier les applications problématiques.
3. **Réglage procmon** - ce processus nécessite également l'installation du connecteur, mais nécessite également l'utilisation du binaire Procmon, notre outil de réglage personnalisé. Il s'agit essentiellement d'une version plus sophistiquée de la fonction de réglage de l'outil de support. Cette méthode nécessite la plus grande quantité de configuration ; cependant, il donne les meilleurs résultats.

1. Réglage avant installation

Le réglage pré-installation est la forme de réglage la plus basique et se fait principalement par la ligne de commande dans une session Terminal.

Pour les mac plus récents d'OS X El Capitan, vous devez d'abord démarrer pour récupérer le mode (commande-r) lors du démarrage et désactiver la protection pour dtrace :

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

Pour vérifier quelles exécutions de fichiers sont les plus courantes, exécutez les opérations suivantes :

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

Ceci montre généralement les applications qui sont exécutées à plusieurs reprises. De nombreuses applications de mise en service exécutent des scripts ou exécutent des binaires à intervalles courts pour gérer les stratégies logicielles de l'entreprise. Toute application considérée comme exécutée à un rythme supérieur à une seconde, ou exécutée plusieurs fois en brèves rafales, devrait être considérée comme un bon candidat à l'exclusion.

Pour vérifier les opérations de fichiers les plus courantes, exécutez la commande suivante :

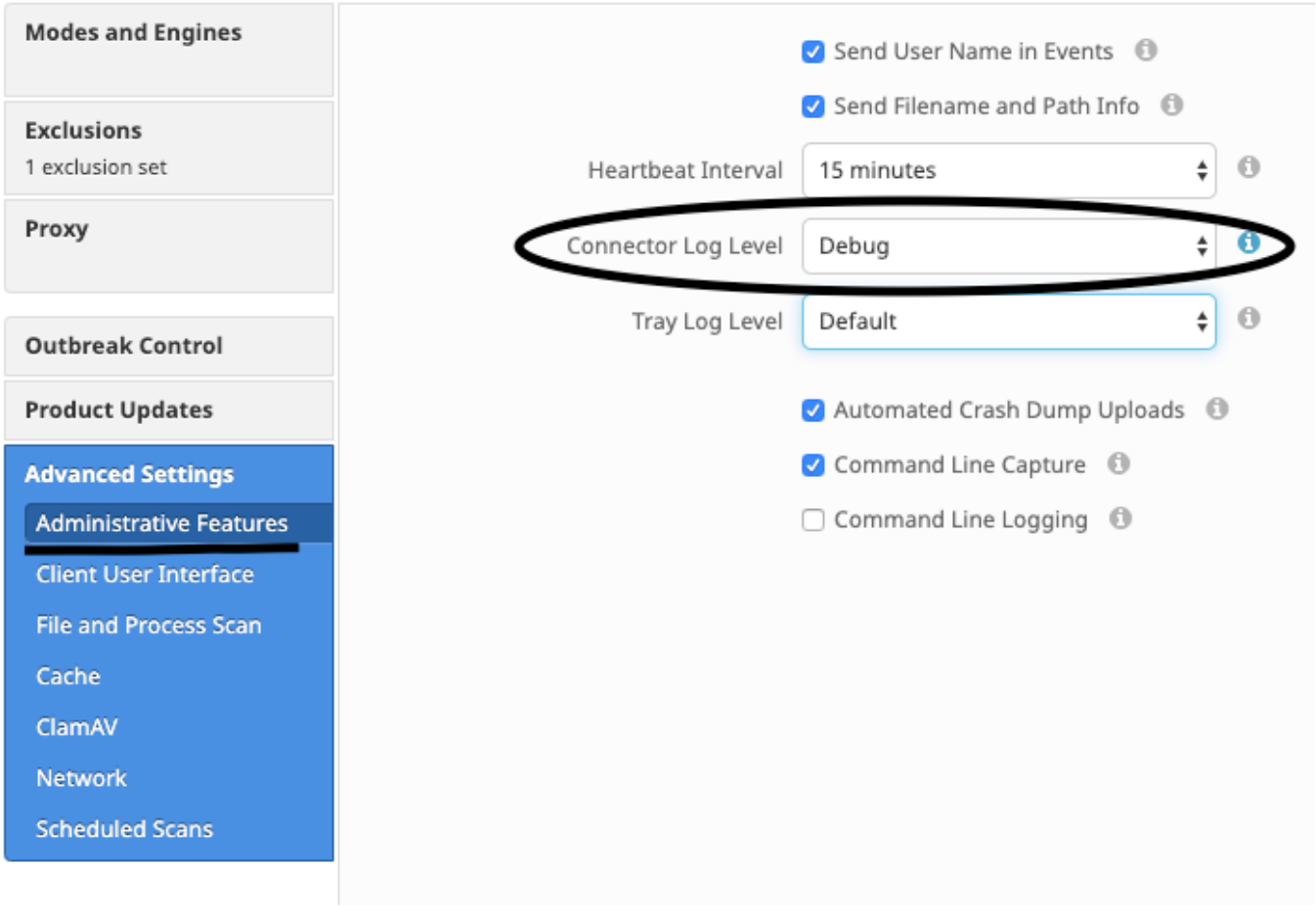
```
$ sudo iosnoop | perl -pe 'use POSIX strftime; print strftime "[%Y-%m-%d %H:%M:%S] ", localtime'
```

Vous verrez immédiatement à quels fichiers la plupart sont écrits. Souvent, il s'agit de fichiers journaux écrits par des applications en cours d'exécution, des logiciels de sauvegarde copiant des fichiers ou des applications de messagerie écrivant des fichiers temporaires. En outre, une bonne règle est que tout ce qui a une extension de fichier journal ou journal doit être considéré comme un candidat à l'exclusion approprié.

2. Outil de support Réglage

Activation de la journalisation du débogage

Le démon du connecteur doit être mis en mode de journalisation de débogage avant de commencer le réglage du fichier de support. Cela se fait via la console Secure Endpoint, via les paramètres de stratégie du connecteur à *Management -> Policies*. Sélectionnez la stratégie, modifiez la stratégie et accédez à la section *Fonctions d'administration* sous la barre latérale *Paramètres avancés*. Modifiez le paramètre *Niveau du journal du connecteur* en **Débogage**.



Suivant, enregistrez votre stratégie. Une fois votre stratégie enregistrée, s'assurer qu'il a été synchroniséinventé à cconnecteur. Exécuter le cconnecteur dans ce mode pour au moins 15 à 20 minutes avant de continuer le reste du réglage.

NOTE: Lorsque votre réglage est terminé, ne oublier modifier *Niveau du journal du connecteur* retour à **Par défaut** pour que cconnecteur exécuter dans ses le plus efficace et le plus efficace mode effectif.

Exécution de l'outil de support

Cette méthode implique l'utilisation de l'outil de support, une application installée avec le connecteur Secure Endpoint Mac. Vous pouvez y accéder à partir du dossier Applications en double-cliquant sur /Applications->Cisco Secure Endpoint->Support Tool.app. Cela générera un package de support complet contenant des fichiers de diagnostic supplémentaires.

Un alternative, et plus rapide, est d'exécuter ligne de commande suivante expéditeur a Terminal session :

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

Cela se traduira par un fichier de support beaucoup plus petit contenant uniquement les fichiers de réglage pertinents.

Dans les deux cas, l'outil de support générera un fichier zip sur votre Bureau qui contient deux fichiers de support de réglage : fileops.txt et exécuts.txt. fileops.txt contient une liste des fichiers les plus fréquemment créés et modifiés sur votre machine. le fichier exécuts.txt contient la liste des fichiers les plus fréquemment exécutés. Les deux listes sont triées par nombre d'analyses, ce qui signifie que les chemins les plus fréquemment analysés apparaissent en haut de la liste.

Laissez le connecteur en mode Débogage pendant 15 à 20 minutes, puis exécutez l'outil de support. Une bonne règle de base est que tous les fichiers ou chemins qui ont en moyenne 1000 résultats ou plus pendant cette période sont de bons candidats à être exclus.

Création d'exclusions de chemin, de caractère générique, de nom de fichier et d'extension de fichier

Pour commencer avec les règles d'exclusion de chemin, recherchez les chemins d'accès de fichiers et de dossiers les plus fréquemment analysés à partir de fileops.txt, puis envisagez de créer des règles d'exclusion pour ces chemins. Une fois la stratégie téléchargée, surveillez l'utilisation du nouveau processeur. Cela peut prendre entre 5 et 10 minutes après la mise à jour de la stratégie avant que vous ne remarquiez la baisse de l'utilisation du CPU car il peut prendre du temps pour que le démon se rattrape. Si vous constatez toujours des problèmes, réexécutez l'outil pour voir quels nouveaux chemins vous observez.

- Une bonne règle est que tout ce qui a une extension de fichier journal ou journal doit être considéré comme un candidat à l'exclusion approprié.

Création d'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 connaître les meilleures pratiques concernant les exclusions de processus, consultez :Point de terminaison sécurisé : Exclusions de processus dans macOS et Linux

Un bon modèle de réglage consiste d'abord à identifier les processus avec un volume élevé d'exécutables à partir du fichier exécuts.txt, à trouver le chemin d'accès à l'exécutable et à créer une exclusion pour ce chemin. Cependant, certains processus ne doivent pas être inclus, notamment :

- Programmes d'utilité générale - Il n'est pas recommandé d'exclure les programmes d'utilité générale (ex : usr/bin/grep) sans tenir compte des éléments suivants. L'utilisateur peut déterminer quelle application appelle le processus (par exemple : rechercher le processus parent qui exécute grep) et exclure le processus parent. Cela doit être fait si et seulement si le processus parent peut être transformé en une exclusion de processus. Si l'exclusion parente s'applique aux enfants, les appels à n'importe quel enfant du processus parent seront également exclus.L'utilisateur qui exécute le processus peut être déterminé. (ex : si un processus est appelé à un volume élevé par l'utilisateur « root », on peut exclure le processus, mais seulement pour l'utilisateur spécifié « root », cela permettra à Secure Endpoint de surveiller les exécutions d'un processus donné par tout utilisateur qui n'est pas « root »).**REMARQUE : Les exclusions de processus sont nouvelles dans les versions 1.11.0 et ultérieures du connecteur. Pour cette raison, les programmes d'utilitaires généraux peuvent être utilisés comme une exclusion de chemin dans les versions 1.10.2 et ultérieures du connecteur. Cependant, cette pratique n'est recommandée que lorsqu'un compromis de performance est absolument nécessaire.**

La recherche du processus parent est importante pour les exclusions de processus. Une fois le processus parent et/ou l'utilisateur du processus trouvé, l'utilisateur peut créer l'exclusion pour un utilisateur spécifique et appliquer l'exclusion de processus aux processus enfants, ce qui à son tour exclut les

processus bruyants qui ne peuvent pas eux-mêmes être transformés en exclusions de processus.

Identification du processus parent

1. À partir du fichier exécuts.txt, identifiez le processus de volume élevé (par exemple : /bin/rm).
2. Ouvrez ampdaemon.log à partir du package de support, dézip syslog.tar, puis suivez le chemin /Library/Logs/Cisco/ampdaemon.log (uniquement disponible dans le package afullsupport, et non à partir d'un package de support généré avec les options par défaut).
3. Recherchez ampdaemon.log pour exclure le processus. Recherchez la ligne de journal qui indique l'exécution du processus (ex : 19 août 09:47:29 devs-Mac.local [2537] [fileop] :[info]-[kext_processor.c@938] :[210962] : Démon Rx : VNODE : EXECUTE X:6210 P:3296 PP:3200 U:502 [/bin/rm]).
4. Identifiez le processus parent à l'aide de l'une des méthodes suivantes : Identifier le chemin du processus parent qui peut suivre le chemin du processus à exclure (ex : [/bin/rm] [*Chemin du processus parent*]).Si le journal n'inclut pas le chemin d'accès du processus parent, identifiez l'ID du processus parent dans la section `PP :` de la ligne du journal (par exemple : PP : 3200).
5. À l'aide du chemin parent ou de l'ID de processus parent, répétez les étapes 3 et 4 pour déterminer le parent du processus parent actuel. Poursuivez ce processus jusqu'à ce qu'aucun parent ne puisse être déterminé ou que l'ID de processus parent = 1 (ex : PP : 1).
6. Une fois l'arborescence des processus connue, recherchez le chemin du programme qui couvre la plupart ou la totalité des opérations qui doivent être exclues et identifie de manière unique l'application. Cela réduit au minimum le risque d'exclure involontairement les opérations effectuées par une autre application.

Identifier l'utilisateur du processus

1. Suivez les étapes 1 à 3 de l'identification du processus parent ci-dessus.
2. Identifiez l'utilisateur d'un processus à l'aide de l'une des méthodes suivantes : Rechercher l'ID utilisateur du processus donné à partir de `U :` dans la ligne de journal (ex : U : 502).Dans la fenêtre Terminal, exécutez la commande suivante : `dscl . liste /Users UniqueID | grep #`, où # est l'ID utilisateur.La sortie doit être similaire à : `Username 502`, où `Username` est l'utilisateur du processus donné.
3. Ce nom d'utilisateur peut être ajouté à une exclusion de processus sous la catégorie Utilisateur afin de réduire la portée de l'exclusion, qui est importante pour certaines exclusions de processus. **REMARQUE : si l'utilisateur d'un processus est l'utilisateur local de l'ordinateur et que cette exclusion doit s'appliquer à plusieurs ordinateurs ayant des utilisateurs locaux différents, la catégorie Utilisateur doit rester vide pour permettre à l'exclusion de processus de s'appliquer à tous les utilisateurs.**