Analyser l'ensemble de diagnostics AMP macOS pour CPU élevé

Contenu

Introduction

Ce document décrit les étapes à suivre pour analyser un ensemble de diagnostics à partir d'Advanced Malware Protection (AMP) for Endpoints Public Cloud sur des périphériques macOS afin de dépanner une utilisation élevée du CPU.

Contribué par Uriel Torres et édité par Yeraldin Sanchez, Ingénieurs du TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation de base dans la console AMP
- Navigation du terminal MAC

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Console AMP for Endpoints 5.4.200512
- macOS Catalina version 10.15.4
- Connecteur AMP 1.12.3.738

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Le connecteur AMP analyse tous les fichiers actifs (ceux qui se déplacent, se copient et/ou se modifient) sur une machine, sauf indication explicite contraire, ce qui entraîne inévitablement des problèmes de performances si trop de processus et d'opérations sont exécutés pendant l'exécution du connecteur, ce qui entraîne une utilisation élevée du CPU, des ralentissements et dans certains cas des logiciels qui ne s'exécutent pas ou ne s'exécutent pas lentement. En outre, AMP Connector peut bloquer des fichiers en fonction de leur réputation dans le cloud, ce qui peut parfois être erroné (faux positif). La solution à ces deux problèmes consiste à exclure ces chemins et ces processus.

Le flux des problèmes de performances de dépannage est illustré dans l'image.

Dépannage

Cette section fournit les informations que vous pouvez utiliser pour dépanner votre configuration.

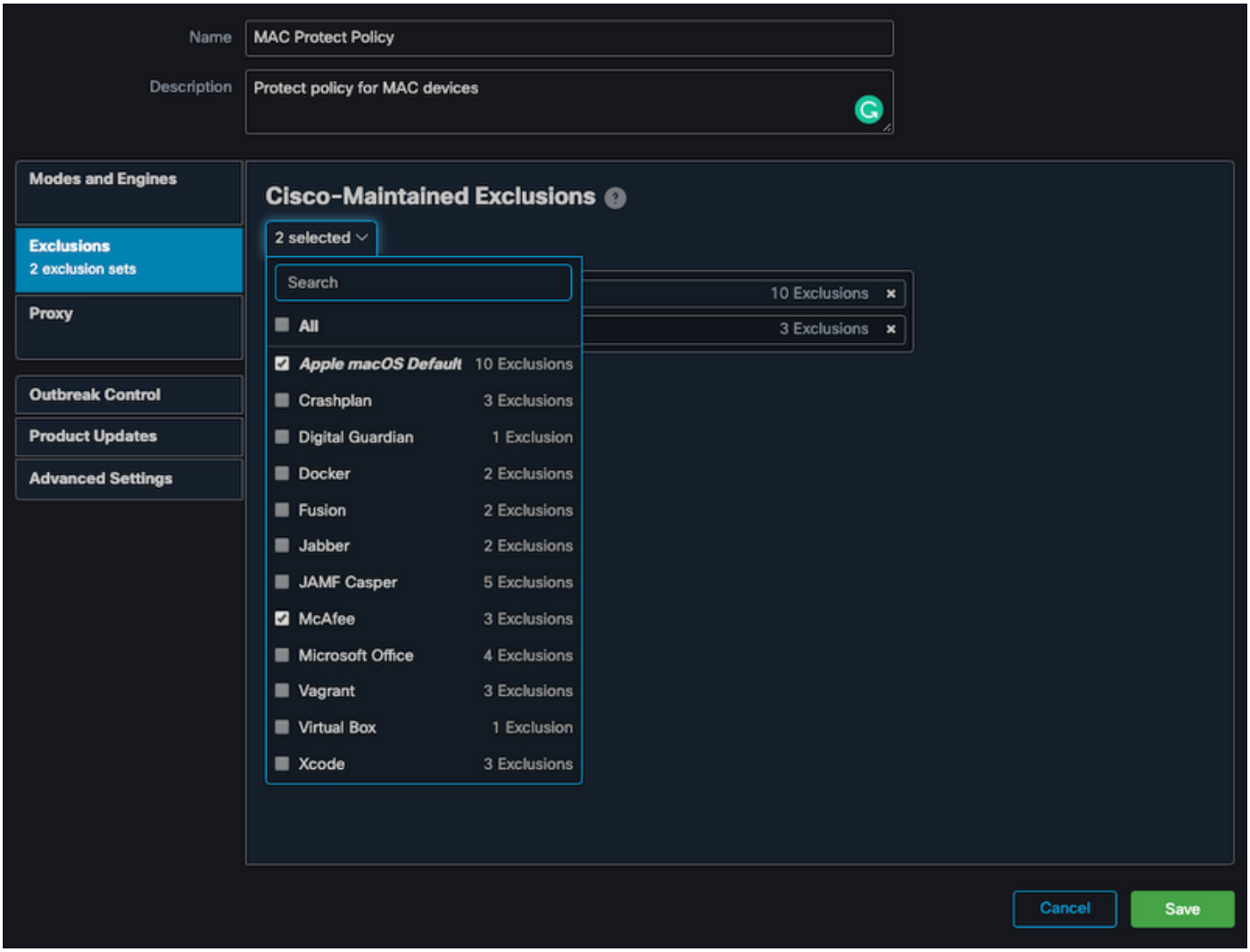
Vérifier si un autre antivirus est installé sur l'ordinateur

> **Astuce** : Utilisez les exclusions maintenues par Cisco si le logiciel utilisé est inclus dans la liste, souvenez-vous que ces exclusions peuvent être ajoutées aux nouvelles versions d'une application.

Afin de voir les listes disponibles dans la section Exclusions gérées par Cisco sur la console AMP :

- Accédez à **Management > Policies**.
- Recherchez la stratégie et cliquez sur **Modifier**.
- Dans la fenêtre des paramètres, cliquez sur **Exclusions**.

Sélectionnez ceux dont votre point de terminaison aurait besoin en fonction du logiciel actuellement installé sur l'ordinateur, puis enregistrez la stratégie, comme illustré dans l'image.



Identifier le processeur élevé lorsqu'une application spécifique est utilisée

Déterminez si le problème se produit lors de l'exécution d'une application ou de quelques-unes d'entre elles si vous êtes en mesure de répliquer le problème aide dans le processus d'identification des exclusions potentielles.

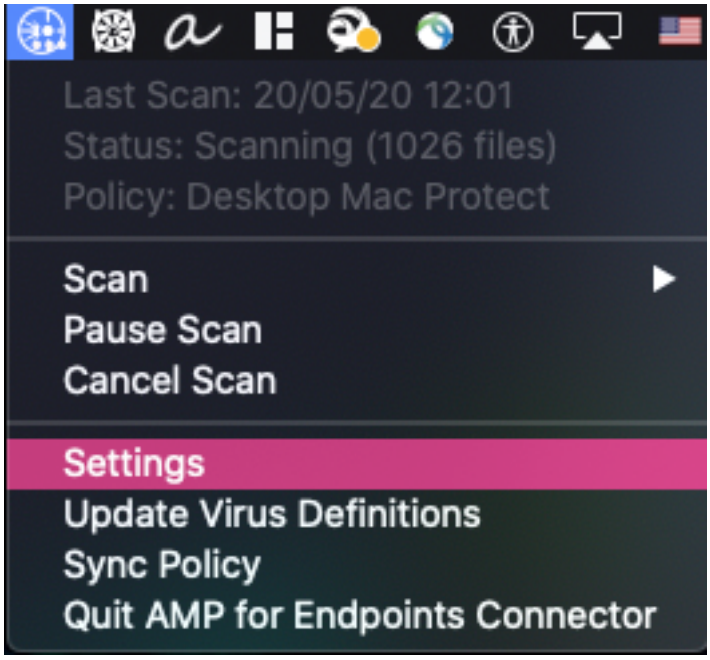
Obtenir un ensemble de diagnostics pour l'analyse

Afin de collecter un ensemble de diagnostics utile, le niveau du journal de débogage doit être activé.

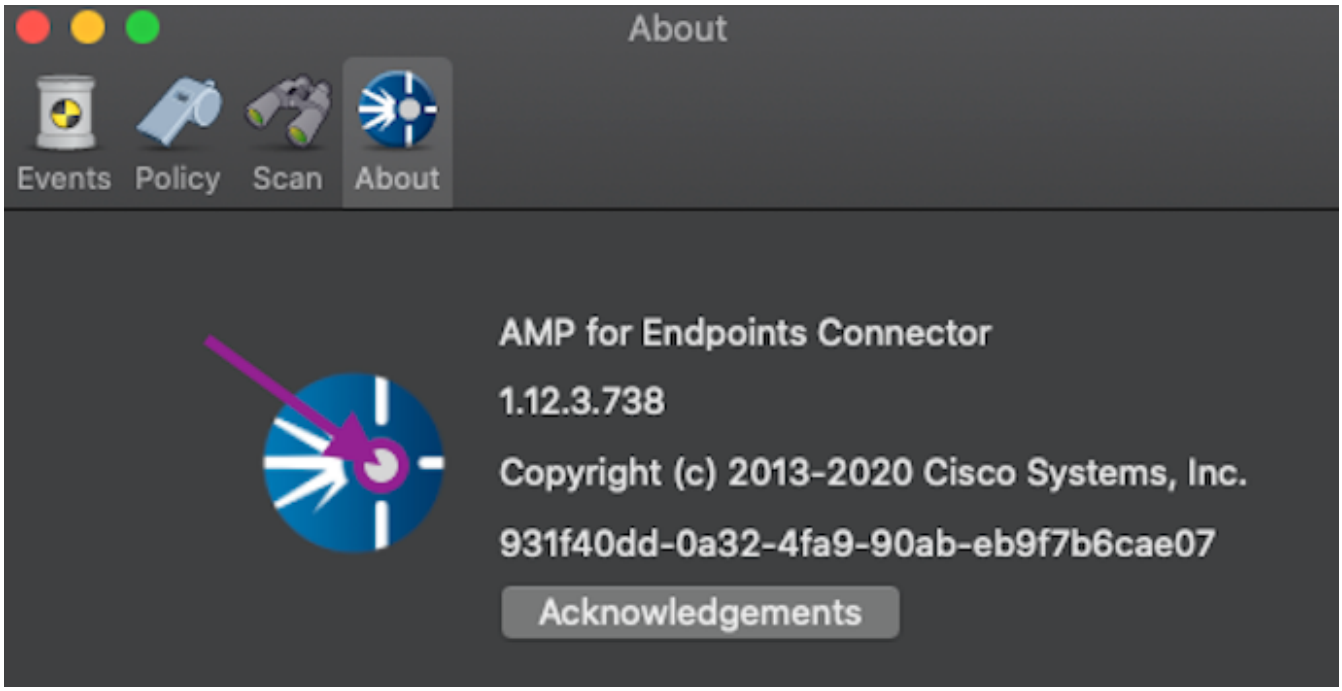
Niveau de débogage dans le point de terminaison

Si vous pouvez répliquer le problème et avoir accès au point de terminaison, voici la meilleure procédure pour capturer l'ensemble de diagnostics.

- Dans la barre de menus MAC, cliquez sur l'icône AMP.
- Accédez à la section **Paramètres**, comme illustré dans l'image.



- Dans les fenêtres de paramètres, accédez à **À propos**.
- Afin d'activer le mode de débogage, cliquez à l'intérieur du logo AMP, comme indiqué dans l'image.



Une fenêtre contextuelle indique que le connecteur AMP est en mode de débogage

Cette procédure active le niveau du journal de débogage jusqu'au prochain intervalle de pulsation de stratégie.

Niveau de débogage dans l'interface de ligne de commande (CLI) AMP

- Ouvrir un terminal
- Accédez à **/opt/cisco/amp/bin/**
- Exécuter ampcli :
  `./ampcli`

- Sur le mode de débogage AMP CLI enable :
  `ampcli>debuglevel 1`

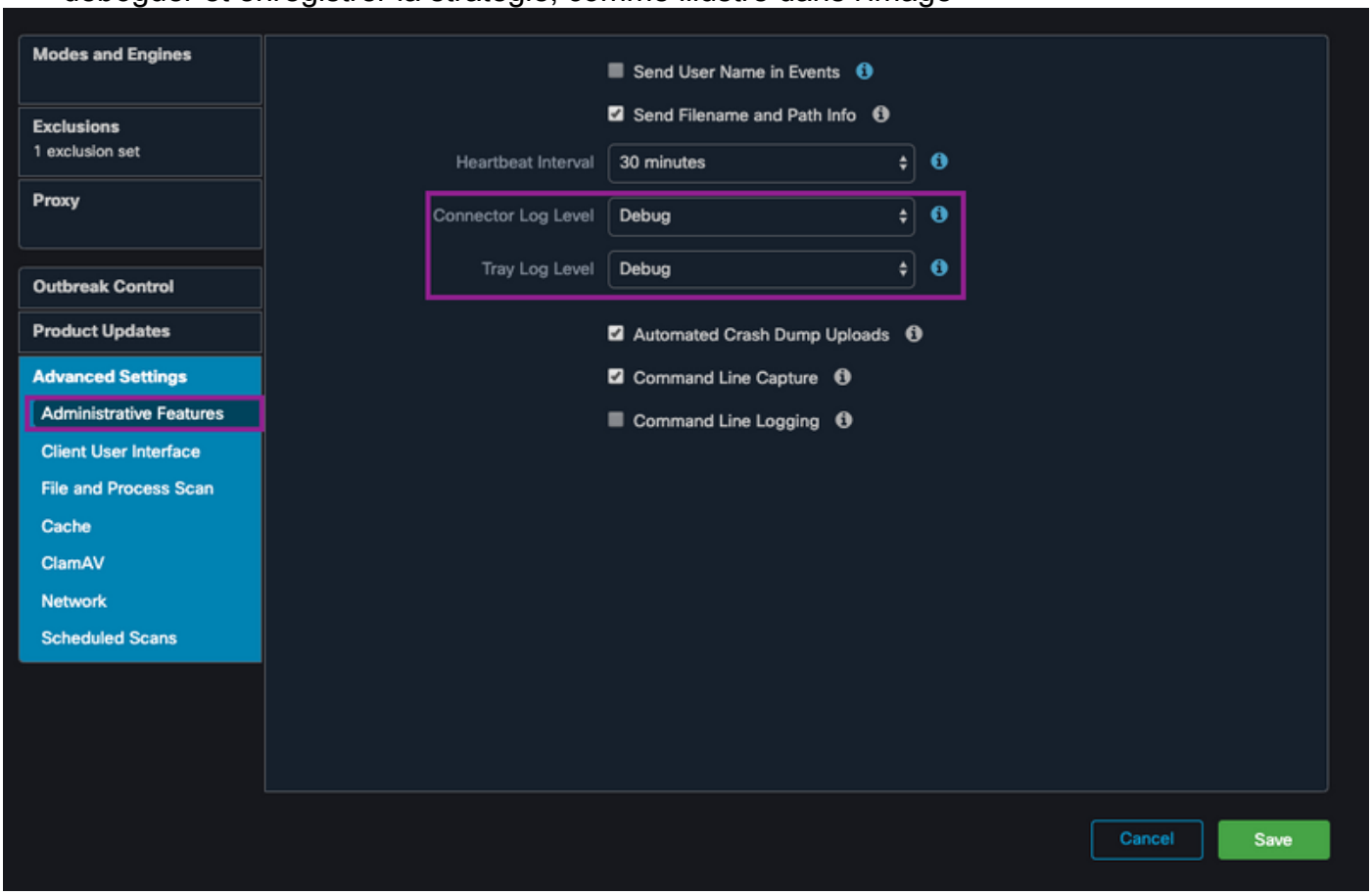
Ce processus active le niveau du journal de débogage jusqu'au prochain intervalle de pulsation de stratégie.

Niveau de débogage dans la stratégie

Si vous n'avez pas accès au point de terminaison ou si le problème ne peut pas être reproduit de manière cohérente, le niveau du journal de débogage doit être activé dans la stratégie.

Afin d'activer le niveau du journal de débogage par la stratégie :

- Accédez à **Management > Policies**
- Rechercher la stratégie et cliquer sur **Modifier**
- Accédez à **Advanced Settings > Administrative Features**
- Configurez le **niveau du journal du connecteur** et le **niveau du journal du plateau** pour déboguer et enregistrer la stratégie, comme illustré dans l'image



Attention : Si le mode de débogage est activé à partir de la stratégie, tous les points de terminaison reçoivent cette configuration.

Note: Synchronisez la stratégie du point de terminaison pour garantir le mode de débogage.

Exclure AMP des autres solutions antivirus

Selon le guide de l'utilisateur, les produits antivirus doivent exclure les répertoires suivants et tous

les fichiers, répertoires et fichiers exécutables qu'ils contiennent pour être compatibles avec le connecteur AMP pour MAC, les répertoires à exclure sont les suivants :

- **/Prise en charge des bibliothèques/applications/Cisco/AMP pour le connecteur des terminaux**
- **/opt/cisco/amp**

Reproduire le problème et rassembler une offre de diagnostic

Lorsque le niveau de débogage est configuré, attendez que l'état du CPU élevé se produise sur le système ou reproduisez manuellement les conditions précédemment identifiées, puis rassemblez le bundle de diagnostic.

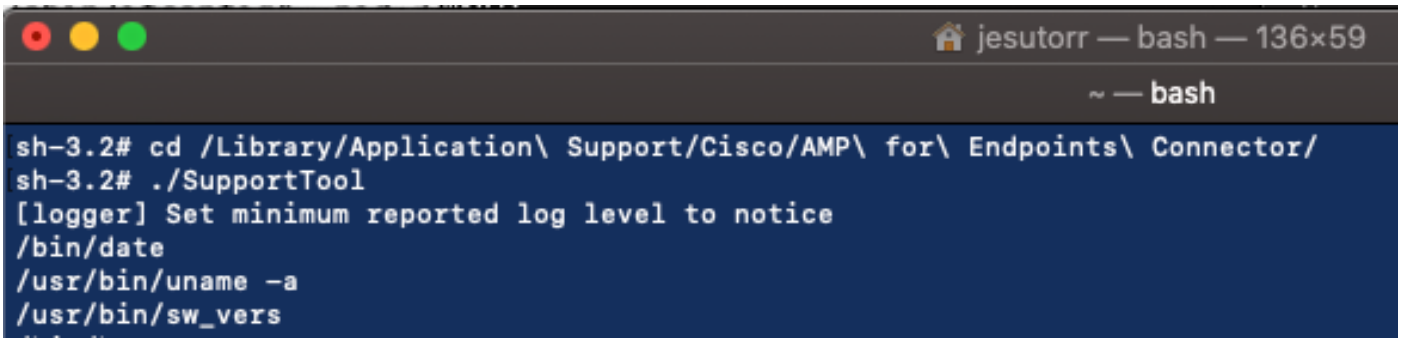
Afin de collecter le bundle de débogage :

- Ouvrez un terminal.
- Accédez au niveau de superutilisateur, puis accédez à **/Library/Application Support/Cisco/AMP for Endpoints Connector** :

```
cd /Library/Application\ Support/Cisco/AMP\ for\ Endpoints\ Connector/
```

- Pour exécuter l'outil de support, utilisez la commande suivante :

```
./SupportTool
```

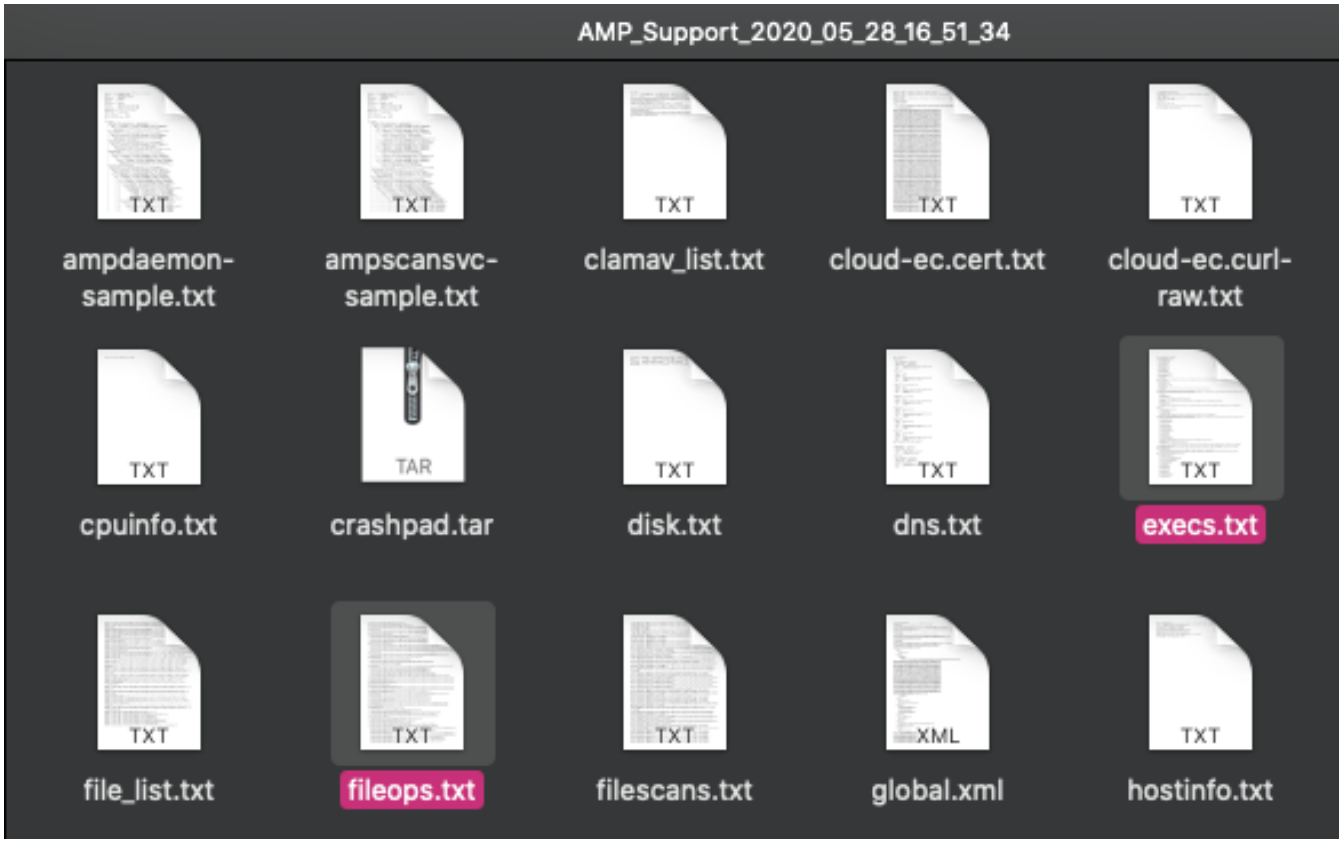


Le bundle de débogage est enregistré dans le dossier Desktop sous la forme d'une extension de fichier .zip.

Analyse des performances élevées du processeur

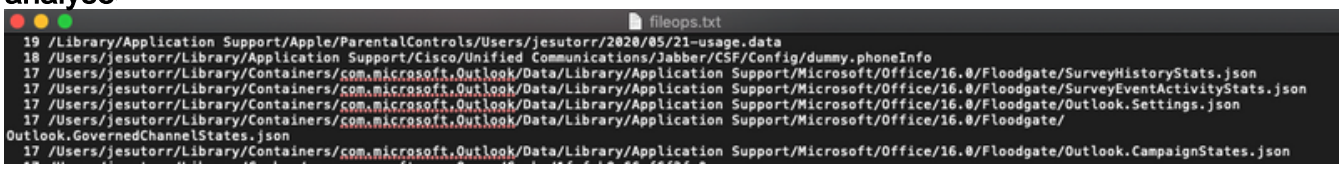
Le bundle de diagnostic de débogage est le stockage sur le Bureau, pour commencer l'analyse :

- Décompresser l'offre groupée de diagnostic
- Il y a 2 fichiers à consulter Opérations de fichiers : fileops.txtExécutions de fichiers : execs.txt



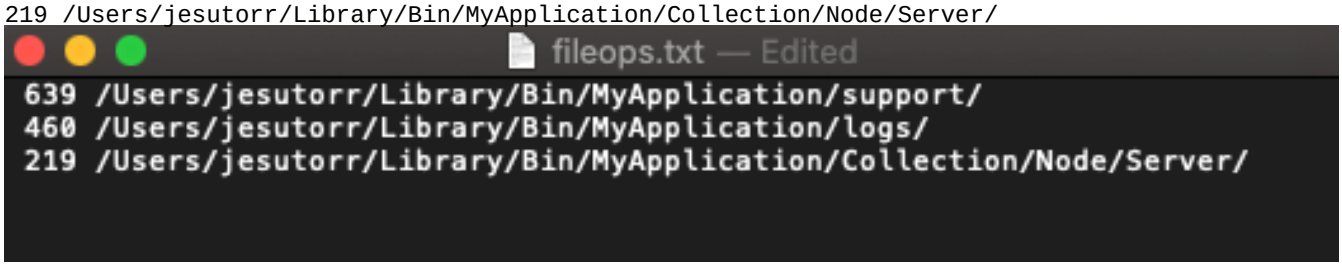
- Le fichier fileops.txt sert d'outil de performance principal pour le dépannage. Il répertorie toutes les opérations actives en cours sur votre point de terminaison pendant l'exécution du connecteur. Il est lu comme suit :

  <Numéros analysés sur le chemin d'accès lors de la collecte de l'offre groupée> / **<Chemin analysé>**

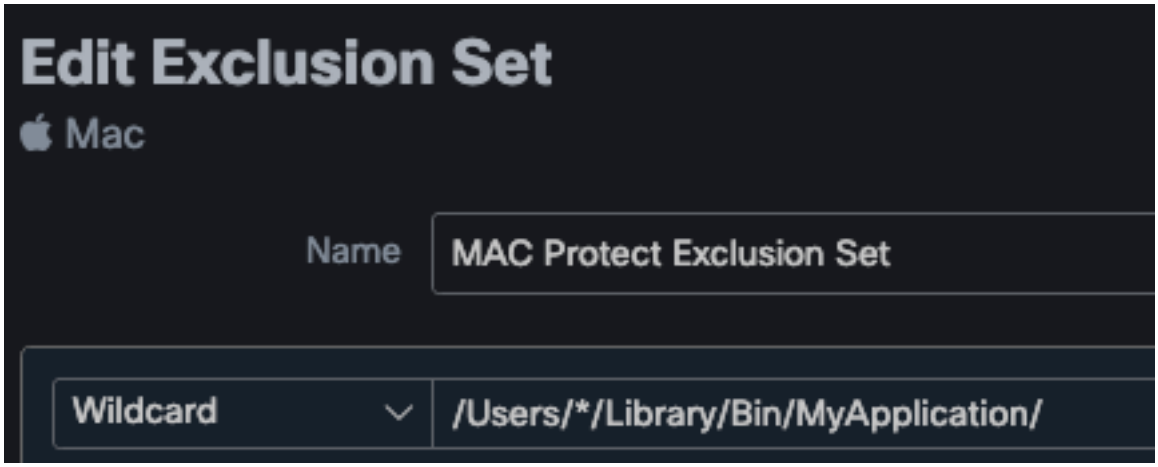


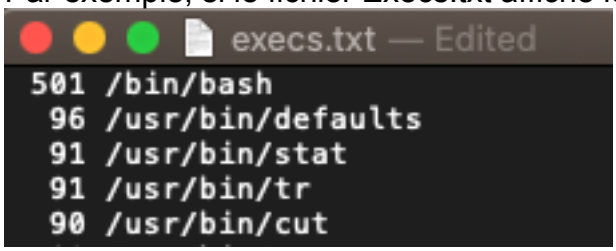
  Par exemple, si vous avez une application de sélection résidentielle, fileops.txt affiche les opérations actives suivantes :

```
639 /Users/jesutorr/Library/Bin/MyApplication/support/

460 /Users/jesutorr/Library/Bin/MyApplication/logs/

219 /Users/jesutorr/Library/Bin/MyApplication/Collection/Node/Server/
```



- Une fois le processus identifié, une exclusion peut être créée
- Afin de créer l'exclusion
- Sur la console AMP, accédez à **Management > Exclusions**
- Sélectionnez le jeu d'exclusions et cliquez sur **Modifier**
- L'exclusion peut être ajoutée comme l'illustre l'image



- Le fichier Execs.txt contient toutes les commandes utilisées par les processus qui s'exécutent pendant que le connecteur collecte les bundles. Les chemins répertoriés ici ne doivent pas être exclus de la stratégie AMP, car il s'agit de binaires (/bin) et de binaires système (/sbin) que tous les processus utilisent, cependant, sur Execs.text peut fournir le processus principal qui est en cours d'exécution.
  Par exemple, si le fichier Execs.txt affiche les journaux suivants.
  

  Puisque l'application home-brew utilise bash, vous pouvez confirmer que l'application est la cause du CPU élevé.

Informations connexes

- AMP pour terminaux : Exclusions de processus dans macOS et Linux
- Meilleures pratiques pour les exclusions d'AMP for Endpoints
- Support et documentation techniques - Cisco Systems