Analyser l'offre groupée de diagnostic macOS Secure Endpoint pour CPU élevé

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Dépannage
  - Vérifiez si un autre antivirus est installé sur l'ordinateur
  - Identifier le CPU élevé lorsqu'une application spécifique est utilisée
  - Rassembler un bundle de diagnostic pour analyse
    - Niveau de débogage du point de terminaison
    - Niveau de débogage dans l'interface de ligne de commande Secure Endpoint (CLI)
    - Niveau de débogage dans la stratégie
  - Exclure Secure Endpoint d'autres solutions antivirus
  - Reproduire le problème et rassembler un lot de diagnostics
  - Analyse des performances élevées du processeur
- Informations connexes

Introduction

Ce document décrit les étapes à suivre pour analyser un bundle de diagnostic à partir du cloud public Secure Endpoint sur des périphériques macOS afin de dépanner une utilisation CPU élevée.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Navigation de base dans la console Secure Endpoint
- Navigation du terminal macOS

Composants utilisés

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

- Console de terminal sécurisé v5.4.20260915
- macOS : 27.0
- Connecteur de terminal sécurisé 1.27

The information in this document was created from the devices in a specific lab environment. 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 Secure Endpoint analyse tous les fichiers actifs (ceux qui se déplacent, se copient et/ou se modifient) sur une machine, sauf indication contraire explicite, ce qui entraîne inévitablement des problèmes de performances si trop de processus et d'opérations sont exécutés pendant que le connecteur est en cours d'exécution, ce qui entraîne une utilisation CPU élevée, des ralentissements ou des pannes. En outre, Secure Endpoint Connector peut bloquer les 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 de dépannage des problèmes de performances est illustré dans l'image.



Dépannage

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

Vérifiez si un autre antivirus est installé sur l'ordinateur

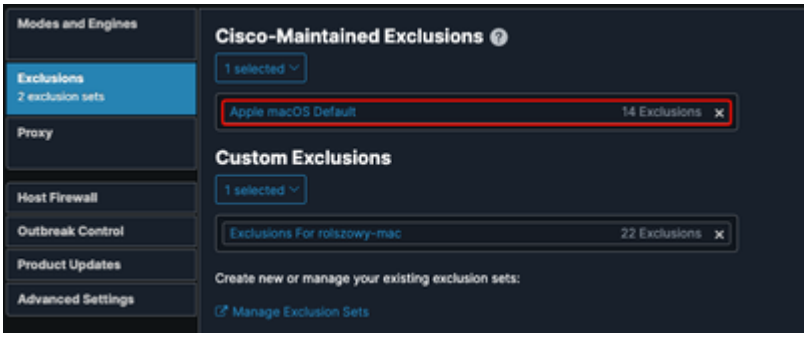
Conseil : Utilisez les exclusions maintenues par Cisco si le logiciel utilisé est inclus dans la

liste, n'oubliez pas 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 Secure Endpoint :

- Accédez à Gestion > Stratégies.
- Recherchez la stratégie et cliquez sur Edit.
- Dans la fenêtre Paramètres de la stratégie, cliquez sur Exclusions.

Sélectionnez celles dont votre terminal aurait besoin en fonction du logiciel actuellement installé sur la machine, puis enregistrez la stratégie, comme illustré dans l'image.



Identifier le CPU élevé lorsqu'une application spécifique est utilisée

Identifiez si le problème se produit pendant l'exécution d'une application ou de quelques-unes d'entre elles, si vous êtes en mesure de reproduire le problème, ce qui permet d'identifier les exclusions potentielles.

Rassembler un bundle de diagnostic pour analyse

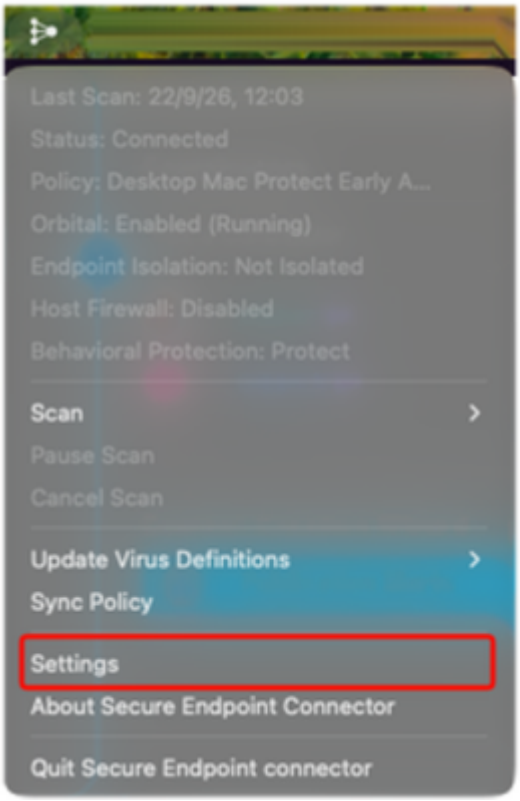
Afin de rassembler un ensemble de diagnostics utile, le niveau de journal de débogage doit être activé.

Niveau de débogage du point de terminaison

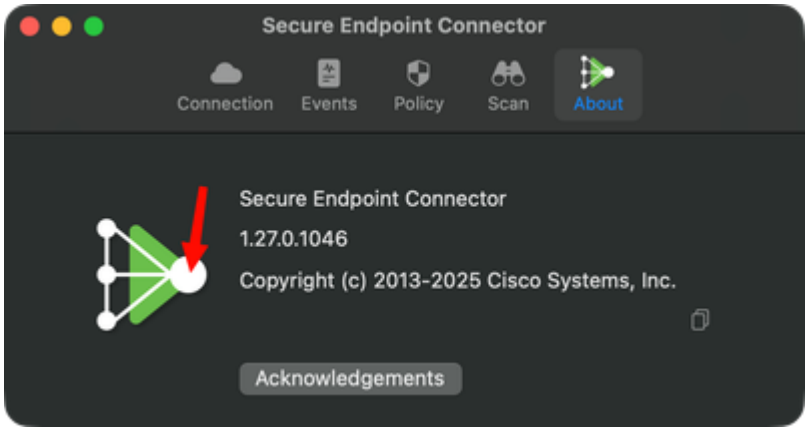
Si vous pouvez répliquer le problème et accéder au point d'extrémité, il s'agit de la meilleure procédure pour capturer l'ensemble de diagnostics.

- Dans la barre de menus de macOS, sélectionnez l'icône Secure Endpoint.

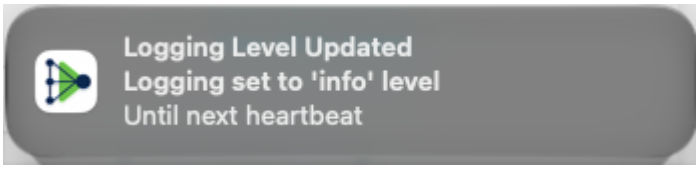
- Sélectionnez Paramètres :



- Sélectionnez About.
- Pour activer le mode de débogage, cliquez dans le logo Secure Endpoint :



Une notification indique que le connecteur Secure Endpoint Connector est en mode débogage.



Cette procédure active le niveau de journal de débogage jusqu'à l'intervalle de pulsation de stratégie suivant.

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

- Ouvrir un terminal
- Exécuter ampcli

```
/opt/cisco/amp/ampcli
```

- Sur l’interface de ligne de commande Secure Endpoint, activez le mode débogage

```
ampcli>debuglevel 1
```

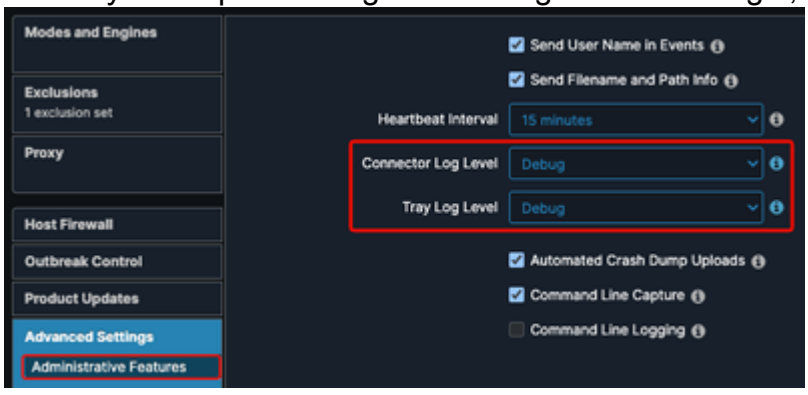
Ce processus active le niveau de journal de débogage jusqu'à l'intervalle de pulsation de stratégie suivant.

Niveau de débogage dans la stratégie

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

Pour activer le niveau de journal de débogage par la stratégie :

- Sélectionnez Management > Policies.
- Recherchez la stratégie et cliquez sur Edit.
- Sélectionnez Advanced Settings > Administrative Features.
- Configurez le niveau de consignation du connecteur et le niveau de consignation de la barre d'état système pour déboguer et enregistrer la stratégie, comme illustré dans l'image



⚠ Mise en garde : Si le mode de débogage est activé à partir de la stratégie, tous les terminaux reçoivent cette configuration.

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

Exclure Secure Endpoint d'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 Secure Endpoint Connector pour macOS. Les répertoires à exclure sont les suivants :

- /Applications/Cisco Secure Endpoint/Secure Endpoint Service.app

Reproduire le problème et rassembler un lot de diagnostics

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

Pour collecter le groupe de débogage :

- Ouvrir un terminal
- Utilisez la commande

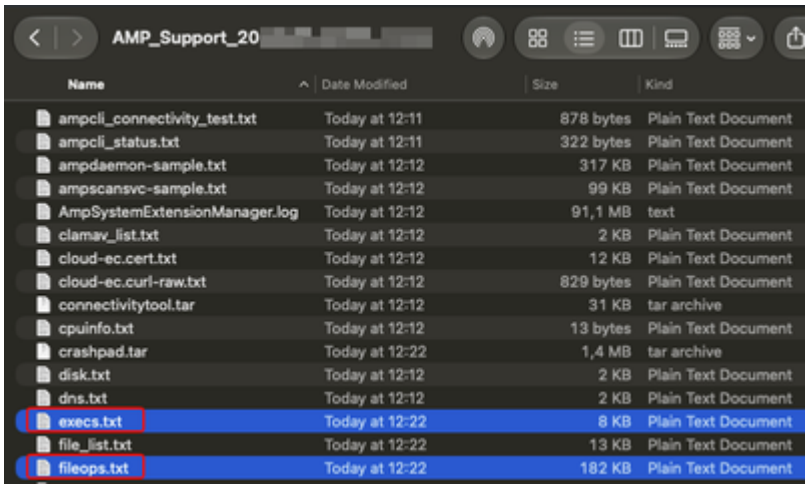
```
sudo /Applications/Cisco\ Secure\ Endpoint/Secure\ Endpoint\ Service.app/Contents/MacOS/SupportTool
```

Le bundle de débogage est enregistré dans le dossier ~/Desktop sous l'extension .zip.

Analyse des performances élevées du processeur

Le bundle de diagnostic de débogage est stocké dans le Bureau, pour démarrer l'analyse :

- Décompressez le bundle de diagnostic
- Il y a 2 dossiers à examiner
    - Exécutions de fichiers : execs.txt
    - Opérations de fichiers : fileops.txt



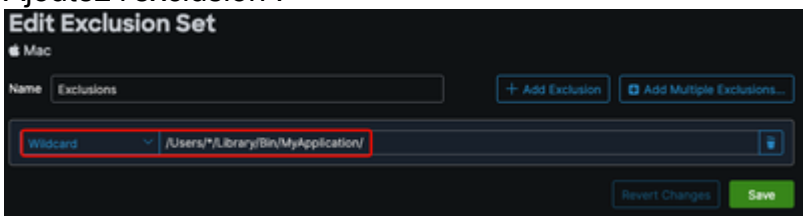
- Le fichier fileops.txt constitue le principal outil de dépannage en matière de performances. Elle répertorie toutes les opérations actuellement actives sur votre point d'extrémité pendant que le connecteur s'exécute. Elle est lue comme suit :
  <Nombre d'analyses effectuées sur le chemin lorsque le lot est collecté> / <Chemin analysé>



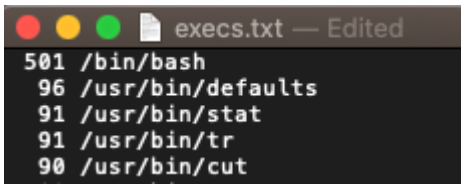
Par exemple, si vous avez une application homebrew, fileops.txt affiche les opérations suivantes actives :

```
639 /Users/user/Library/Bin/MyApplication/support/
460 /Users/user/Library/Bin/MyApplication/logs/
219 /Users/user/Library/Bin/MyApplication/Collection/Node/Server/
```

- Une fois le processus identifié, créez une exclusion : sélectionnez Gestion > Exclusions.
- Sélectionnez le jeu d'exclusions, puis Modifier.
- Ajoutez l'exclusion :



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



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

Informations connexes

- Configuration et identification des exclusions de terminaux sécurisés
- Documentation et assistance techniques

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.