Collecte de données de diagnostic à partir du connecteur Linux AMP for Endpoints

Contenu

Introduction

Ce document décrit les étapes à suivre pour générer un fichier de diagnostic à partir du connecteur Linux AMP For Endpoints. Si vous rencontrez un problème technique avec le connecteur Linux, un ingénieur du support technique Cisco peut vouloir analyser les messages de journal disponibles dans un fichier de diagnostic.

Générer un fichier de diagnostic

Avec cette commande, vous pouvez générer un fichier de diagnostic directement à partir de l'interface de ligne de commande (CLI) de Linux :

```
/opt/cisco/amp/bin/ampsupport
```

Cela crée un fichier .7z sur votre bureau. Vous pouvez fournir ce fichier au centre d'assistance technique Cisco (TAC) pour une analyse plus approfondie.

Mode Debug

Le mode de débogage du connecteur fournit une description plus détaillée de la journalisation. Il permet d'obtenir plus d'informations sur un problème lié au connecteur. Cette section décrit comment activer le mode de débogage dans un connecteur.

> **Avertissement :** Le mode de débogage ne doit être activé que si Cisco demande ces données. Si vous activez le mode de débogage plus longtemps, il peut remplir l'espace disque très rapidement et empêcher le fichier de diagnostic du support de collecter le **journal**

du connecteur en raison d'une taille de fichier excessive.

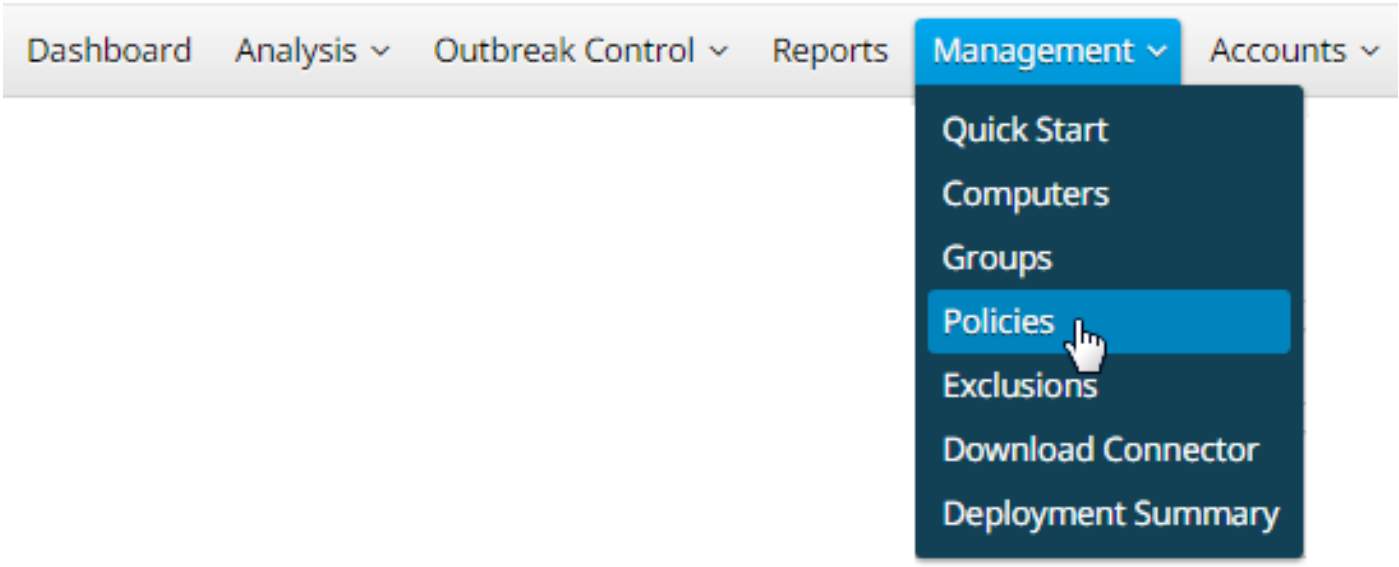
Utiliser la console AMP

Activer le mode débogage

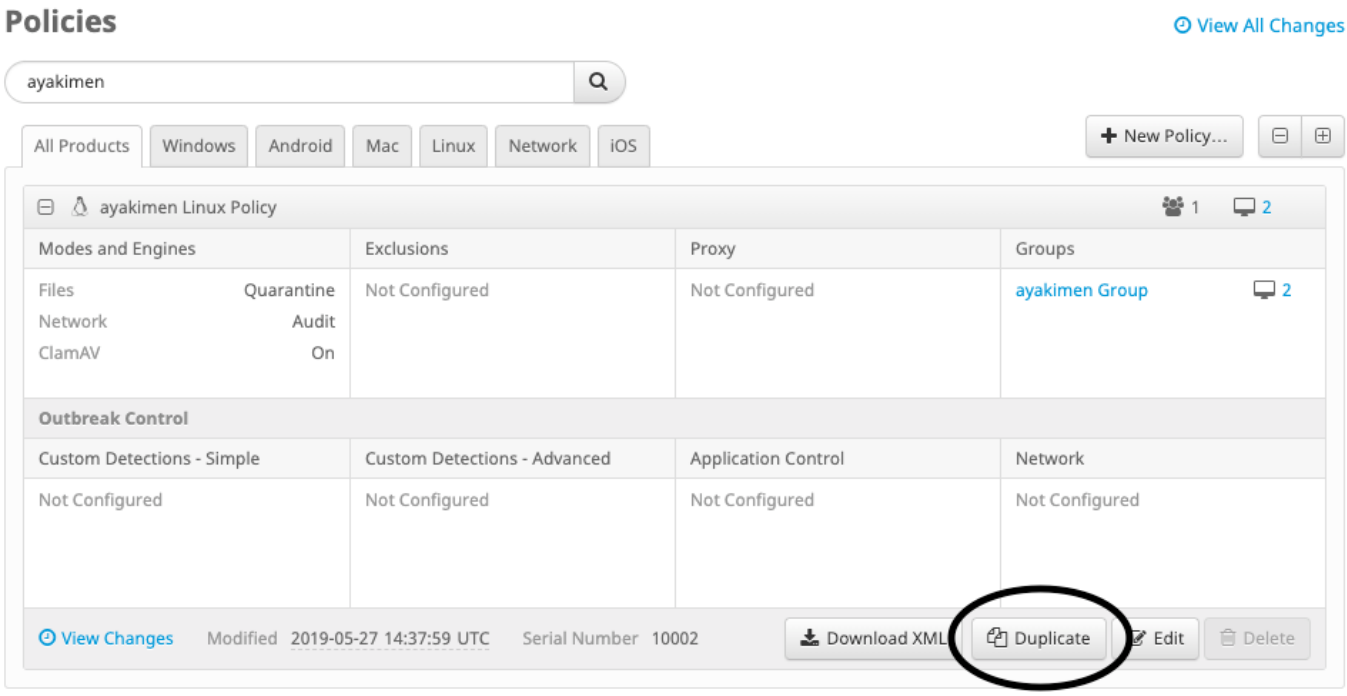
Vous pouvez activer le mode de débogage dans la stratégie actuelle avec les étapes 5 à 7 ou créer une nouvelle stratégie en mode de débogage avec toutes les étapes suivantes :

Étape 1. Connectez-vous à la console AMP.

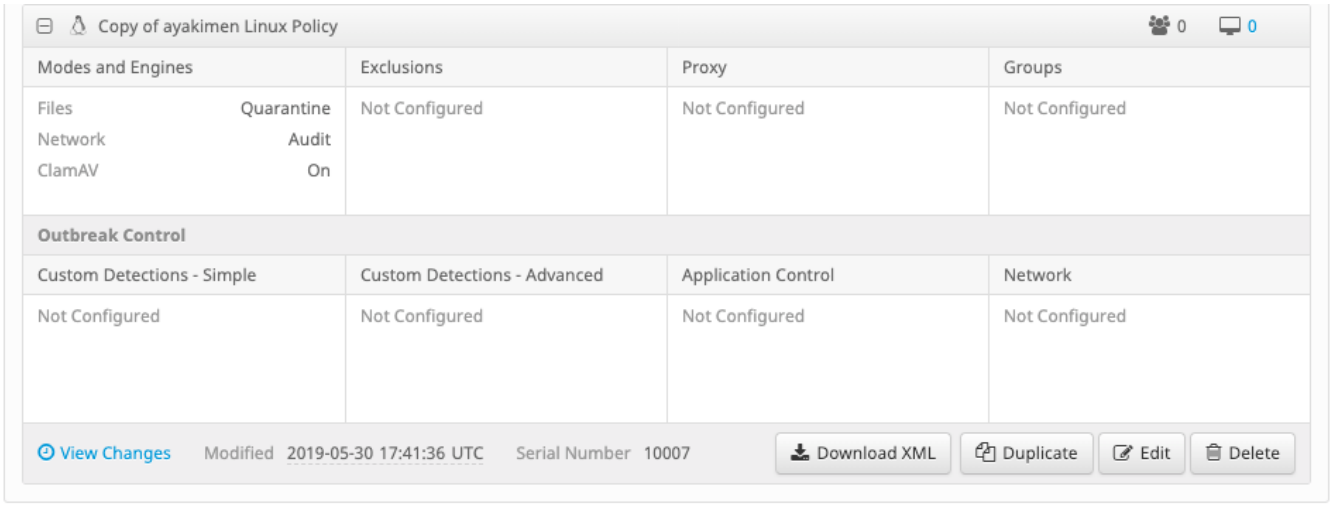
Étape 2. Sélectionnez **Gestion > Stratégies**.



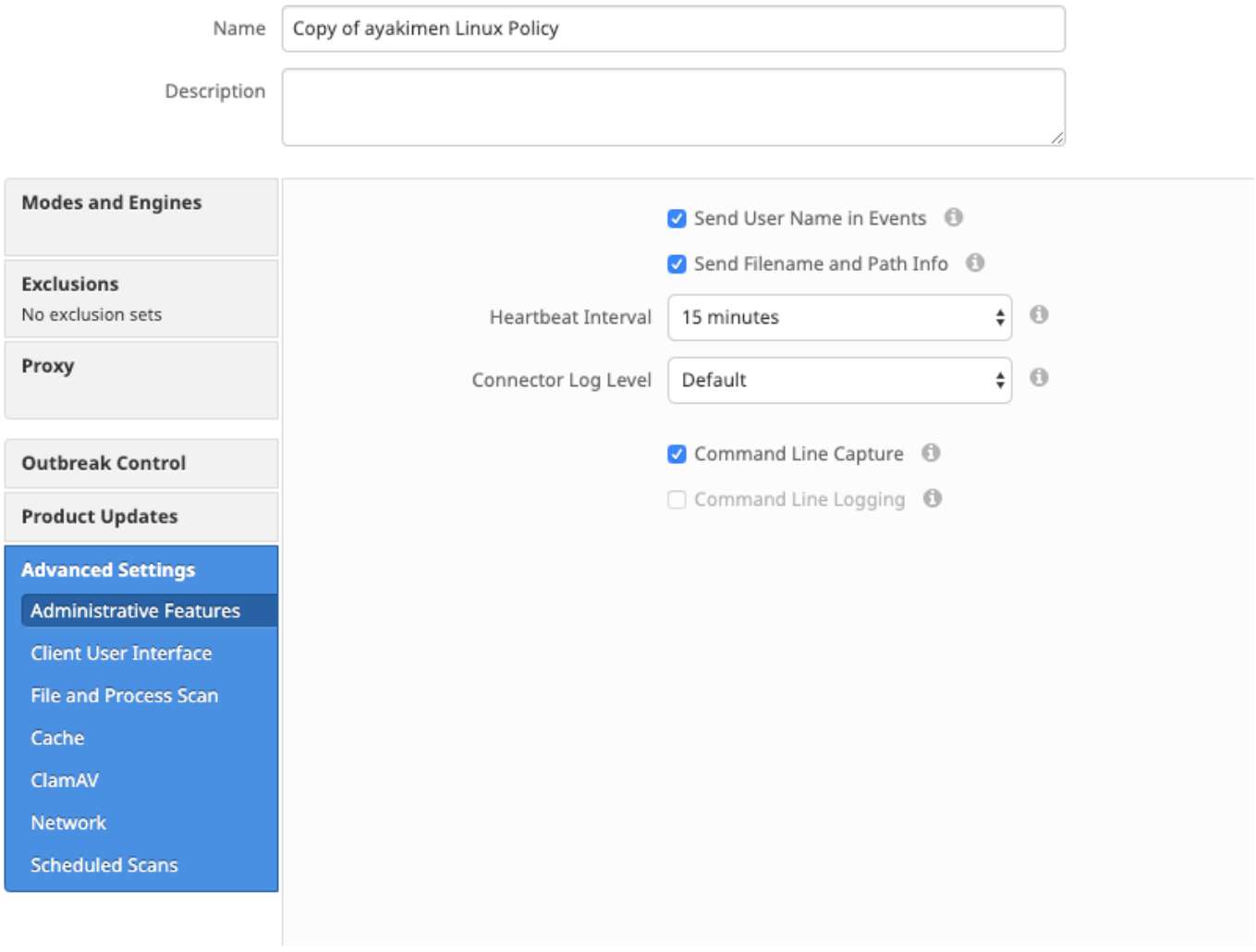
Étape 3. Recherchez la stratégie appliquée au périphérique ou à l'ordinateur final et cliquez sur Stratégie, ce qui agrandira la fenêtre Stratégie. **Cliquez sur Dupliquer**.



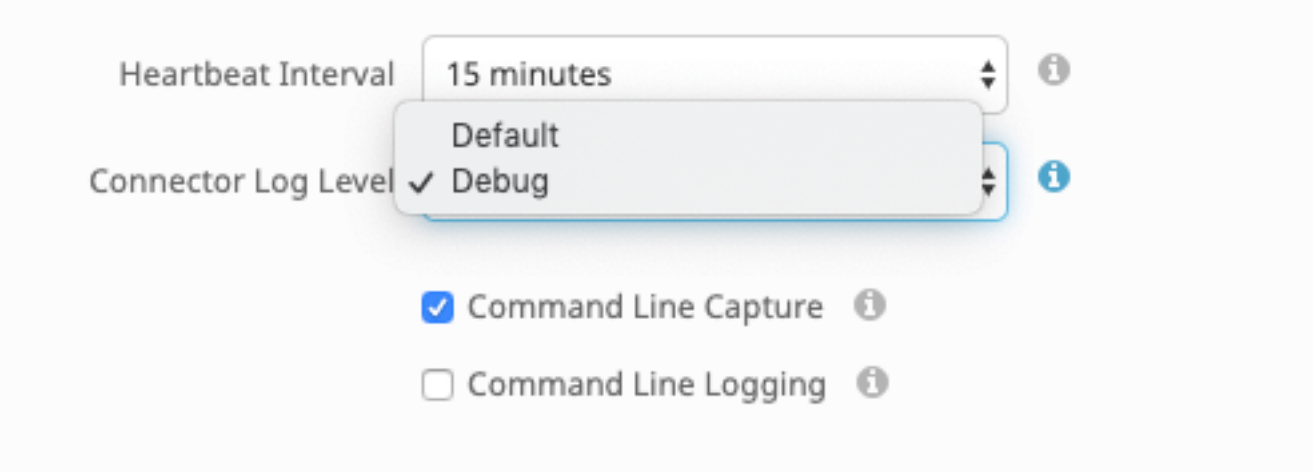
Étape 4. Après avoir **cliqué sur Duplicate**, la console AMP se met à jour avec la stratégie copiée.



Étape 5. **Cliquez sur Modifier**, **cliquez sur Paramètres avancés**, puis sélectionnez **cliquez sur** Fonctionnalités **administratives** dans la barre latérale.



Étape 6. **Pour le niveau du journal du connecteur**, sélectionnezDéboguer dans les listes déroulantes.



Étape 7. Cliquez sur Enregistrer pour enregistrer les modifications.

Étape 8. Après avoir enregistré la nouvelle stratégie, vous devez créer/modifier un groupe pour inclure *la nouvelle stratégie*, et *le périphérique final* où vous voulez générer des informations de débogage.

Désactiver le mode de débogage

Pour désactiver le mode de débogage, procédez comme vous l'avez fait pour activer le mode de débogage, mais définissez le **niveau du journal du connecteur** sur **Par défaut**.

Utiliser la ligne de commande

Activer le mode débogage

Si vous rencontrez des problèmes de connectivité à la console et que vous souhaitez activer le mode de débogage, exécutez ces commandes sur l'interface de ligne de commande :

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 1
```

Voici le résultat :

```
ampcli>debuglevel 1
Daemon now logging at 'info' level until next policy update
```

Désactiver le mode de débogage

Pour désactiver le mode de débogage, utilisez les commandes suivantes :

```
/opt/cisco/amp/bin/ampcli
ampcli>debuglevel 0 Daemon now logging at 'notice' level until next policy update
```

Outil de support Réglage pendant le 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 AMP, via les paramètres

de stratégie du connecteur *à* l'*emplacement Management -> Policies*. Modifiez la stratégie et accédez à *la* section Fonctionnalités *administratives* sous *l'*onglet Paramètres *avancés*. Modifiez *le* paramètre *de* niveau *du journal* du connecteur **en Debug**.

Ensuite, enregistrez votre stratégie. Une fois votre stratégie enregistrée, assurez-vous qu'elle a été synchronisée avec le connecteur. Exécutez le connecteur dans ce mode pendant au moins 15 à 20 minutes avant de continuer le réglage.

NB : Une fois le réglage terminé, n'oubliez pas de modifier *le* réglage *du* niveau *du journal* du connecteur pour qu'il fonctionne dans son mode le plus efficace et le plus efficace.

Exécution de l'outil de support

Cette méthode implique l'utilisation de l'outil de support, une application installée avec le connecteur MAC AMP. Vous pouvez y accéder à partir du dossier Applications en double-cliquant sur /Applications->Cisco AMP->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 suivanteexpéditeur a Terminal session :

```
sudo /opt/cisco/amp/bin/ampsupport -x
```

```
sudo /opt/cisco/amp/bin/ampsupport
```

La première option se traduit par un fichier de support beaucoup plus petit contenant uniquement les fichiers de réglage appropriés. La deuxième option fournit un package de support complet qui contient plus d'informations, telles que les journaux, qui peuvent être nécessaires pour régler les exclusions de processus (disponibles dans Connector versions 1.11.0 et ultérieures).

Dans les deux cas, l'outil de support générera un fichier zip sur votre ~home 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. Ces fichiers seront utiles pour les exclusions Path/Wildcard. Le fichier exécuts.txt contiendra la liste des fichiers les plus fréquemment exécutés, qui seront utiles pour les exclusions de processus. 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.

Réglage des exclusions

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 d'accès, 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 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 Linux can only be implemented for ELF files. Users cannot implement Process Exclusions for file formats such as .sh (Shell Scripts).
Pour connaître les meilleures pratiques concernant les exclusions de processus, consultez : AMP pour terminaux : 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 AMP de surveiller les exécutions d'un processus donné par tout utilisateur qui n'est pas « root »).**REMARQUE : Les exclusions de processus sont nouvelles dans Connector versions 1.11.0 et ultérieures. Pour cette raison, les programmes utilitaires généraux peuvent être utilisés comme une exclusion de chemin dans Connector Versions 1.10.2 et versions ultérieures. 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. 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 : 0).Dans la fenêtre Terminal, exécutez la commande suivante : `getent passwd # | couper -d : -f1`, où `#` est l'ID utilisateur.Vous devriez voir une sortie similaire à : `Nom d'utilisateur`, où Nom d'utilisateur est l'utilisateur du processus donné.
3. Ceci Le 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.**

Informations connexes

- Collection de données de diagnostic à partir d'un connecteur FireAMP exécuté sous Windows
- Collection de données de diagnostic à partir d'un connecteur FireAMP exécuté sur Mac OS
- **Support et documentation techniques - Cisco Systems**