

Collecte de données diagnostiques d'un connecteur de FireAMP qui fonctionne sur le Linux

Contenu

[Introduction](#)

[Générez le fichier diagnostique](#)

[Mode de debug](#)

[Console d'AMP d'utilisation](#)

[Mode de debug d'enable](#)

[Mode de debug de débranchement](#)

[Ligne de commande d'utilisation](#)

[Mode de debug d'enable](#)

[Mode de debug de débranchement](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes pour générer un fichier diagnostique d'un connecteur de FireAMP qui fonctionne sur le Linux. Si vous éprouvez un problème technique avec un connecteur de FireAMP qui fonctionne sur le Linux, un ingénieur de support technique de Cisco pourrait vouloir analyser les messages de log disponibles dans un fichier diagnostique.

Générez le fichier diagnostique

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

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

Ceci crée un fichier .7z sur votre appareil de bureau. Vous pouvez fournir ce fichier au centre d'assistance technique Cisco (TAC) pour l'analyse approfondie.

Mode de debug

Le mode de débogage d'un connecteur de FireAMP fournit la verbosité supplémentaire à se connecter. Il laisse plus de vue dans un problème avec le connecteur. Cette section décrit comment activer mettent au point le mode dans un connecteur de FireAMP.

Avertissement : Le mode de debug devrait être activé seulement si des demandes de Cisco de ces données. Si vous activez mettez au point le mode pendant un plus long temps, il peut remplir l'espace disque très rapidement et pourrait empêcher le fichier diagnostique de

support de recueillir le **log de connecteur** dû à la taille de fichier excessive.

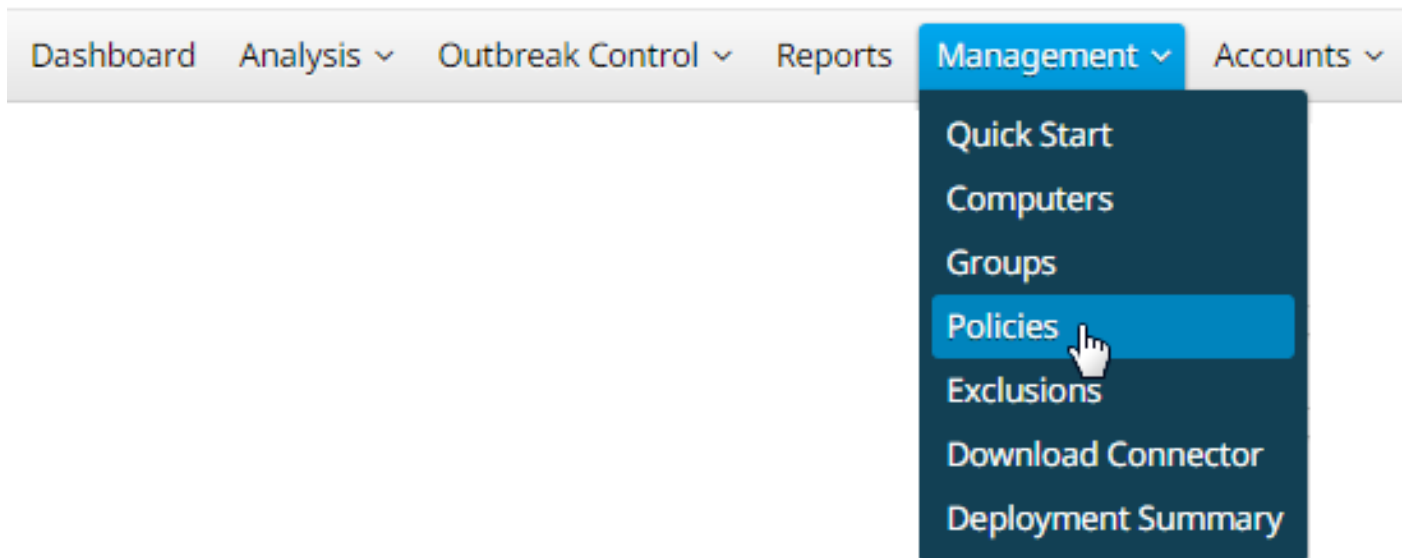
Console d'AMP d'utilisation

Mode de debug d'enable

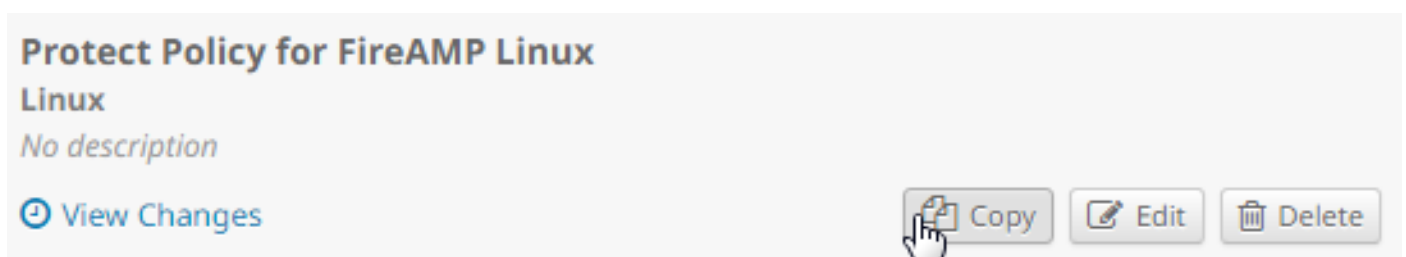
Vous pouvez activer le mode de débogage dans la stratégie en cours avec les étapes 5 - 7 ou créer une nouvelle stratégie mettez au point dedans le mode avec toutes ces étapes :

Étape 1. Connectez-vous dans la console de FireAMP.

Étape 2. **Gestion > stratégies** choisies.



Étape 3. Localisez la stratégie qui est appliquée au périphérique ou à l'ordinateur d'extrémité et cliquez sur la **copie**.



Étape 4. Après que vous cliquez sur la **copie**, les mises à jour de console de FireAMP avec la stratégie copiée.



Étape 5. Cliquez sur Edit et puis cliquez sur les **caractéristiques administratives**.

< Edit Policy: Copy of Protect Policy for FireAMP Linux

Policy for Linux

Name	<input type="text" value="Copy of Protect Policy for FireAMP Linux"/>
Description	<input type="text"/>

CUSTOM DETECTIONS

Simple	<input type="text" value="Quick SCD"/>
Advanced	<input type="text" value="None"/>

APPLICATION CONTROL

Blocking	<input type="text" value="None"/>
Whitelisting	<input type="text" value="Custom Whitelist"/>

NETWORK

IP Blacklists & Whitelists	<input type="button" value="Edit"/>
----------------------------	-------------------------------------

Exclusions

General | File | Network

Administrative Features

Send Filename and Path Info	<input checked="" type="checkbox"/>
Heartbeat Interval	<input type="text" value="30 minutes"/>
Connector Log Level	<input type="text" value="Default"/>
Command Line Capture	<input checked="" type="checkbox"/>
Command Line Logging	<input type="checkbox"/>

Étape 6. Pour le **niveau de log de connecteur**, sélectionnez le **debug des** listes déroulantes.

Administrative Features

Send Filename and Path Info

Heartbeat Interval 30 minutes ▼

Connector Log Level Default ▼

Command Line Capture

Command Line Logging

Étape 7. **Stratégie de mise à jour de clic** afin de sauvegarder les modifications.

Étape 8. Après que vous mettiez à jour la stratégie, vous devez changer votre groupe pour inclure le périphérique d'extrémité où vous voulez se produire mettez au point les informations.

Mode de debug de débranchement

Pour désactiver mettez au point le mode, passent par les mêmes étapes que vous vous êtes terminé pour activer le mode de débogage, mais changeant le **niveau de log de connecteur pour se transférer**.

Ligne de commande d'utilisation

Mode de debug d'enable

Si vous éprouvez n'importe quels problèmes de connectivité au portail, et vous voulez activer mettez au point le mode, exécutez ces commandes sur le CLI :

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

Voici le résultat :

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

Mode de debug de débranchement

Pour désactiver mettez au point le mode, utilisent ces commandes :

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

[Informations connexes](#)

- [Collecte de données diagnostiques d'une exécution de connecteur de FireAMP sur Windows](#)

- [Collecte de données diagnostiques d'une exécution de connecteur de FireAMP sur Mac OS](#)
- [Support et documentation techniques - Cisco Systems](#)