Connecteur de FireAMP pour la collecte des informations de diagnostic de MAC

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Composants utilisés](#)
[Informations générales](#)
[Générez un fichier diagnostique avec l'outil d'assistance](#)
[Lancez l'outil d'assistance du GUI](#)
[Lancez l'outil d'assistance du CLI](#)
[Dépannage](#)
[Mode de debug d'enable](#)
[Mode de debug de débronchement](#)

Introduction

Ce document décrit le processus qui est utilisé afin de générer un fichier diagnostique par l'intermédiaire de l'application d'outil d'assistance qui est disponible sur le connecteur de Cisco FireAMP pour des ordinateurs de Macintosh (MAC) et de la façon dépanner des problèmes de performance.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connecteur de Cisco FireAMP pour le MAC
- MacOSX

[Composants utilisés](#)

Les informations dans ce document sont basées sur le connecteur de Cisco FireAMP pour le MAC.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Le connecteur de Cisco FireAMP pour le MAC installe une application appelée l'*outil d'assistance*, qui est utilisé afin de générer les informations de diagnostic au sujet du connecteur de FireAMP qui est installé sur votre MAC. Les données diagnostiques incluent des informations sur votre MAC comme :

- Utilisation de ressource (disque, CPU, et mémoire)
- logs de FireAMP-particularité
- Les informations de configuration de FireAMP

Générez un fichier diagnostique avec l'outil d'assistance

Cette section décrit comment lancer l'application d'outil d'assistance du GUI ou du CLI afin de générer un fichier diagnostique.

Lancez l'outil d'assistance du GUI

Terminez-vous ces étapes afin de lancer le connecteur de FireAMP pour l'outil d'assistance de MAC du GUI :

1. Naviguez vers le répertoire de FireAMP dans votre dossier Applications et localisez le lanceur d'outil d'assistance :

2. Double-cliquer le lanceur d'outil d'assistance, et vous êtes incité pour les qualifications administratives :

3. Après que vous entriez dans vos qualifications, l'icône d'outil d'assistance devrait apparaître dans votre lieu :

   Note: L'application d'outil d'assistance fonctionne à l'arrière-plan et prend un certain temps de se terminer (approximativement 20-30 minutes).
4. Quand l'application d'outil d'assistance se termine, un fichier est généré et placé sur votre appareil de bureau :

Voici un exemple de la sortie non compressée :

5. Afin d'analyser les données, fournissez ce fichier à l'équipe de support technique de Cisco.

Lancez l'outil d'assistance du CLI

Le lanceur d'outil d'assistance se trouve dans ce répertoire :

```
/Library/Application Support/Sourcefire/FireAMP Mac/
```

Afin de lancer l'application d'outil d'assistance, sélectionnez cette commande dans le CLI :

> **Note**: Vous devez exécuter cette commande comme racine, ainsi assurez-vous que vous commutez pour enraciner ou préfacer la commande avec le **sudo**.

```
root@mac# cd /Library/Application\ Support/Sourcefire/FireAMP\ Mac
root@mac# ./SupportTool
```

> **Note: Cette commande fonctionne bavard. Une fois qu'il est complet, un fichier diagnostique est généré et placé sur votre appareil de bureau.**

Dépannage

Cette section décrit comment activer et le débronchement mettent au point le mode sur le connecteur de FireAMP afin de dépanner des problèmes de performance.

Mode de debug d'enable

> **Avertissement** : Le mode de debug devrait être activé seulement si un ingénieur de support technique de Cisco fait une demande de ces données. Si vous gardez pour mettre au point le mode activé pendant une longue période, il peut remplir l'espace disque très rapidement et pourrait empêcher les données de log de connecteur et de log de barre d'état d'être recueillie dans le fichier diagnostique de support dû à la taille de fichier excessive.

Le mode de debug est utile avec des tentatives de dépanner des problèmes de performance sur un connecteur de FireAMP. Terminez-vous ces étapes afin d'activer mettent au point le mode et collectent le data&colon diagnostique ;

1. Procédure de connexion à la console de nuage de FireAMP.
2. Naviguez vers la **Gestion > les stratégies**.
3. Localisez une stratégie qui est appliquée à un ordinateur et cliquez sur la **copie**. Les mises à

jour de console de FireAMP avec la stratégie copiée :

4. Cliquez sur Edit et changez le nom de la stratégie. Par exemple, vous pourriez utiliser la *stratégie de debug mac.*

5. Cliquez sur les **caractéristiques administratives** et sélectionnez le **debug de** chacun des deux le niveau de log de barre d'état et le niveau de log de connecteur relâchent vers le bas des menus :

6. Cliquez sur le bouton de **stratégie de mise à jour** afin de sauvegarder les modifications.

7. Naviguez vers la **Gestion > les groupes** et cliquez sur le **groupe +Create** près du côté en haut à droite de votre écran.

8. Écrivez un nom pour le groupe. Par exemple, vous pourriez utiliser le *groupe de debug mac*.

9. Changez la stratégie de MAC de FireAMP de la *stratégie par défaut de MAC au* copié, la nouvelle stratégie que vous avez juste créée, qui est **stratégie de debug mac** dans cet exemple.

10. Cliquez sur les **ordinateurs** et identifiez votre ordinateur dans la liste. Sélectionnez-le et le clic **ajoutent sélectionné**.

11. Le clic **créent le groupe**. Votre MAC devrait maintenant faire mettre au point un fonctionnel la stratégie. Vous pouvez sélectionner l'icône de FireAMP qui apparaît sur votre barre de menus et vous assurez que la nouvelle stratégie est appliquée :

Mode de debug de débronchement

Après que les données diagnostiques mettent au point dedans le mode est obtenu, vous doit retourner le connecteur de FireAMP de nouveau au mode normal. Terminez-vous ces étapes afin de désactiver mettent au point le mode :

1. Procédure de connexion à la console de nuage de FireAMP.

2. Naviguez vers la **Gestion > les groupes**.

3. Localisez le nouveau groupe, le *groupe de debug mac*, que vous avez créé mettez au point dedans le mode.

4. Cliquez sur **Edit**.

5. Cliquez sur les **ordinateurs** et localisez votre ordinateur dans la liste. Sélectionnez-le et le clic **retirent sélectionné**.

6. **Groupe de mise à jour de** clic.

7. Cliquez sur la **stratégie de sync** sur la barre de menus où l'icône de FireAMP se trouve.

8. Vérifiez que la stratégie est maintenant retournée à la valeur par défaut précédente. Vérifiez ceci sur la barre de menus. La stratégie devrait maintenant être revenue à la stratégie d'origine qui a été utilisée avant que vous l'ayez changée à la *stratégie de debug mac* :

   Le mode de debug est maintenant désactivé, et le connecteur de FireAMP devrait fonctionner normalement.