

Contenu

[Introduction](#)

[Produisez-vous dépannent le fichier](#)

[Supplémentaire dépannez les données](#)

Introduction

Un fichier de dépannage contient une collection de messages de log, de données de configuration, et de sorties de commande. Il est utilisé afin de déterminer le statut d'un système de Sourcefire. Si un ingénieur d'assistance technique de Cisco vous invite à envoyer un fichier de dépannage de votre plate-forme de X-gamme de BlueCoat (également connue sous le nom de capteur de traverse), suivez les instructions sur ce document. Ce document fournit également une liste des informations supplémentaires qui pourraient être nécessaires pour analyser une question.

Produisez-vous dépannent le fichier

1. Connectez-vous dans votre X-gamme de BlueCoat l'appliance en tant qu'utilisateur d'`admin`.
2. Trouvez le groupe VAP pour le logiciel de Sourcefire.

```
show application vap-group
```

La sortie suivante est un exemple de la commande ci-dessus. Dans cet exemple, le groupe de vap est `sf53`.

```
show application vap-group
```

3. Ensuite, nous devons augmenter le privilège de sorte que nous puissions le distant-shell dans le groupe VAP lui-même :

```
unix su
```

4. Puis, ouvrez une session de distant-shell :

```
rsh <VAP_group>_1
```

Exemple :

```
rsh sf53_1
```

5. Maintenant, chargez l'application spécifique de Sourcefire :

```
source /opt/sf/profile
```

6. En conclusion, générez un dépannage :

```
sf_troubleshoot.pl -t <case_number>
```

Supplémentaire dépannez les données

1. Copies de tout les `/var/log/messages *` les fichiers sur le module de processeur de contrôle (CPM) sont nécessaires pour l'analyse de log et le but de dépannage. Un capteur de Sourcefire se connecte tous les messages de Syslog sur le fichier de `/var/log/messages` d'un CPM, plutôt que sur un module de Processeur d'application (APM) où le logiciel de Sourcefire fonctionne.

Remarque: Veuillez noter * avec `/var/log/messages *`. L'utilisez * pour inclure tout les fichier de `messages` de CPM.

2. Une configuration en cours de plate-forme de X-gamme de BlueCoat nous permet pour comprendre comment un capteur est installé et configuré sur XOS. Les commandes copy suivantes une configuration en cours dans un fichier texte :

```
copy running-config /tmp/running_config.txt
```

3. Les sorties de commande suivantes sont importantes pour déterminer l'état du module et du châssis :

```
show module statusshow chassis
```

4. Si une erreur ou un symptôme est évident sur l'interface utilisateur d'utilisateur web, un tir d'écran de l'interface web est également utile d'identifier un problème.