Générer des données de dépannage pour le logiciel Sourcefire exécuté sur la plate-forme BlueCoat X

Contenu

Introduction

Un fichier de dépannage contient un ensemble de messages de journal, de données de configuration et de sorties de commande. Il sert à déterminer l'état d'un système Sourcefire. Si un ingénieur d'assistance Cisco vous demande d'envoyer un fichier de dépannage à partir de votre plate-forme BlueCoat X-Series (également appelée capteur de faisceaux), suivez les instructions de ce document. Ce document fournit également une liste des données supplémentaires qui pourraient être nécessaires pour analyser un problème.

Générer un fichier de dépannage

1. Connectez-vous à votre appareil BlueCoat X-Series en tant qu'utilisateur administrateur.

2. Recherchez le groupe VAP pour le logiciel Sourcefire.

`show application vap-group`
Le résultat suivant est un exemple de la commande ci-dessus. Dans cet exemple, le groupe vap est sf53.

```
VAP Group                    : sf53
App ID : SfSensor
Name : SF Sensor
Version : 5.3.0.1
Release : 55
Start on Boot : yes
App Monitor : on
App State (sf530_1) : Up
```

3. Ensuite, nous devons augmenter les privilèges afin de pouvoir installer Remote-Shell dans le groupe VAP lui-même :

```
unix su
```

4. Ensuite, ouvrez une session Remote Shell :

```
rsh
```

Exemple :

```
rsh sf53_1
```

5. Maintenant, chargez l'application spécifique Sourcefire :

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

6. Enfin, générez un dépannage :

```
sf_troubleshoot.pl -t
```

Données de dépannage supplémentaires

1. Des copies de tous les fichiers /var/log/messages* du module CPM (Control Processor Module) sont nécessaires à l'analyse des journaux et au dépannage. Un capteur Sourcefire enregistre tous les messages syslog dans le fichier /var/log/messages d'un CPM, plutôt que dans un module APM (Application Processor Module) où le logiciel Sourcefire s'exécute.

> Note: Veuillez noter le * avec le /var/log/messages*. Utilisez le * pour inclure tous les messages du CPM.

2. Une configuration en cours de BlueCoat X-Series Platform nous permet de comprendre comment un capteur est installé et configuré sur XOS. La commande suivante copie 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 status
```

```
show chassis
```

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