Probleemoplossing voor Sourcefire-software genereren op BlauwCoat X-Series platform

Inhoud

Inleiding

Een problematische bestand bevat een verzameling logberichten, configuratiegegevens en opdrachtoutput. Het wordt gebruikt om de status van een Sourcefire-systeem te bepalen. Als een Cisco Support Engineer u vraagt om een probleemoplossingsbestand te verzenden vanuit uw BlauwCoat X-Series platform (ook bekend als CrossSensor), volgt u de instructies op dit document. Dit document bevat ook een lijst van de aanvullende gegevens die nodig kunnen zijn om een probleem te analyseren.

Probleemoplossing genereren

1. Meld u aan bij uw BlueCoat X-Series apparaat als beheerder-gebruiker.

2. Vind de VAP-groep voor Sourcefire-software.

```
show application vap-group
```

De volgende uitvoer is een voorbeeld van de bovenstaande opdracht. In dit voorbeeld is de vap groep 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. Vervolgens moeten we de voorrechten verhogen zodat we op afstand de VAP-groep zelf in kunnen zetten:

```
unix su
```

4. Open vervolgens een sessie op afstand:

```
rsh
```

Bijvoorbeeld:

```
rsh sf53_1
```

5. Start nu de Sourcefire-specifieke toepassing:

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

6. Ten slotte een probleemoplossing genereren:

```
sf_troubleshoot.pl -t
```

Aanvullende gegevens voor probleemoplossing

1. Kopieën van alle /var/log/boodschappen*-bestanden op de controlemodule (CPM) zijn nodig voor loganalyse en probleemoplossing. Een Sourcefire-sensor registreert alle syslogberichten in het /var/log/boodschappenbestand van een CPM in plaats van op een Application Processor Module (APM) waar de Sourcefire-software draait.

> Opmerking: Let op het * met de /var/log/berichten*. Gebruik het * om alle berichten van CPM te omvatten.

2. Met een actieve configuratie van BlueCoat X-Series Platform kunnen we begrijpen hoe een sensor op XOS is geïnstalleerd en ingesteld. De volgende opdracht kopieert een actieve configuratie in een tekstbestand:

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

3. De volgende opdrachtuitgangen zijn belangrijk om de status van de module en het chassis te bepalen:

```
show module status
```

```
show chassis
```

4. Als een fout of symptoom op de web user interface zichtbaar is, is een screenshot van de web interface ook handig om een probleem te identificeren.