

ASA : dépannage du module AIP-SSM

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Dépannage](#)

[État Insensible](#)

[Impossible d'accéder au module AIP SSM via ASDM](#)

[Impossible de mettre à niveau/mettre à jour le SSM IPS](#)

[Erreur de mise à niveau : execUpgradeSoftware](#)

[Impossible de se connecter à IPS avec l'observateur d'événements IPS \(IEV\)](#)

[Impossible d'accéder à AIP-SSM](#)

[Erreur lors du branchement du module AIP-SSM sur l'ASA](#)

[AIP-SSM échoue après la mise à jour des signatures](#)

[Problèmes de latence avec le capteur IPS](#)

[Informations connexes](#)

Introduction

Ce document décrit comment effectuer le dépannage de l'état de non réponse de l'Advanced Inspection and Prevention Security Services Module (AIP SSM) dans le dispositif de sécurité adaptatif dédié de la gamme Cisco 5500 (ASA).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur le module AIP-SSM de la gamme Cisco 5500 ASA.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Dépannage

État Insensible

Problème :

Le module AIP-SSM passe à l'état non réactif, ne répond pas à l'accès HTTP ou ASDM, mais est accessible à partir de l'interface de ligne de commande, comme illustré :

```
<#root>
```

```
show module
```

Mod	Card Type	Model	Serial No.
0	ASA 5510 Adaptive Security Appliance	ASA5510	JMX0934K021
1	ASA 5500 Series Security Services Module-10	ASA-SSM-10	JAB093203S3

Mod	MAC Address Range	Hw Version	Fw Version	Sw Version
0	0013.c480.a11d to 0013.c480.a121	1.0	1.0(10)0	7.0(2)
1	0013.c480.b204 to 0013.c480.b204	1.0	1.0(10)0	5.0(2)S152.0

```
Mod Status
```

```
-----  
0 Up Sys  
1
```

```
Unresponsive
```

Solution :

Émettez la commande `hw-module module 1 reset` sur votre ASA. Cette commande effectue une réinitialisation matérielle du module AIP-SSM. Elle s'applique lorsque la carte est dans l'un des états suivants :

- vers le haut
- duvet
- insensible
- se remettre

Si vous redémarrez l'ASA dans un état de non réponse, votre SSM doit être ré-imaginé. Référez-vous à la section [Installation de l'image du système AIP-SSM](#) de [Mise à niveau, mise à niveau et installation des images du système](#) pour plus d'informations et les étapes sur la façon de ré-

imager l'AIP-SSM.

Remarque : reportez-vous à la section [Reloading, Shutting Down, Reset, and Recovering AIP-SSM](#) de la section [Configuring ASA-SSM](#) pour plus d'informations sur les différentes commandes disponibles pour dépanner l'AIP-SSM.

Ce problème est dû au bogue Cisco ayant l'ID [CSCts58648](#) (clients [enregistrés](#) uniquement) .

Impossible d'accéder au module AIP SSM via ASDM

Problème :

Ce message d'erreur s'affiche sur l'interface utilisateur graphique.

```
Error connecting to sensor. Error Loading Sensor error
```

Solution :

Vérifiez que l'interface de gestion IPS SSM est up/down, et vérifiez son adresse IP configurée, son masque de sous-réseau et sa passerelle par défaut. Il s'agit de l'interface permettant d'accéder au logiciel Cisco Adaptive Security Device Manager (ASDM) à partir de la machine locale. Essayez d'envoyer une requête ping à l'adresse IP de l'interface de gestion de IPS SSM à partir de l'ordinateur local auquel vous souhaitez accéder à l'ASDM. Si vous ne parvenez pas à envoyer une requête ping, vérifiez les listes de contrôle d'accès du capteur.

Problème :

Le message d'erreur `cannot communication with main app` s'affiche lorsque vous tentez de vous connecter au module AIP SSM.

Solution :

Rechargez le module ASA ou AIP SSM afin de résoudre cette erreur.

Impossible de mettre à niveau/mettre à jour le SSM IPS

Problème :

Le message d'erreur `Error: execUpgradeSoftware Connection failed` est affiché sur l'interface de ligne de commande.

Solution :

Vérifiez que l'interface de gestion IPS SSM est up/down et qu'il s'agit de l'interface par laquelle l'ASA-IPS tente de contacter afin de télécharger le logiciel. Il ne s'agit pas d'une connexion de fond de panier entre l'ASA et l'IPS-SSM ; c'est la connexion Ethernet sur le module AIP-SSM lui-même, qui doit être connectée à un port de commutateur et configurée avec une adresse IP, un

masque de sous-réseau et une passerelle par défaut. Si http ne fonctionne toujours pas, essayez d'utiliser l'option FTP ou SCP avec la commande [upgrade](#).

Erreur de mise à niveau : execUpgradeSoftware

Problème :

Erreur : execUpgradeSoftware La mise à jour nécessite 60340 Ko dans /usr/cids/idsRoot/var/updates, il n'y a que 57253 Ko disponibles. Un message d'erreur s'affiche pendant la mise à niveau.

Solution 1 :

Afin de résoudre ce problème, vous devez vous connecter à l'interface de ligne de commande du capteur avec un compte de service. Si vous ne disposez pas d'un compte de service, vous pouvez en créer un à l'aide des commandes suivantes :

```
configure terminal
user (username) priv service password (pass)
exit
```

Une fois que vous vous connectez au compte de service, émettez ces commandes `rm /usr/cids/idsRoot/var/*pmz` et déconnectez-vous du compte de service. Vérifiez ensuite que la mise à niveau est terminée.

Solution 2 :

Cette erreur se produit en raison de l'espace disponible moins important sur le module IPS, car les fichiers de récupération occupent plus d'espace sur le module. Complétez ces étapes afin de supprimer les fichiers de récupération et de résoudre cette erreur :

```
<#root>
```

```
bash-2.05b#
```

```
cd /usr/cids/idsRoot/var/updates/
```

```
bash-2.05b#
```

```
ls -l
```

```
drwxr-xr-x  2 cids  cids      1024 Jul  1 22:35 backups
drwxr-xr-x  2 cids  cids      1024 Oct 19 15:26 download
drwxrwxr-x  2 cids  cids      1024 Oct 19 15:26 logs
-rw-r--r--  1 root  root        183 Sep  6 21:54 package
-rw-r--r--  1 cids  cids    27587840 Jul  9 2009 recovery.gz
drwxr-xr-x  2 cids  cids      1024 Jul  1 22:35 scripts
```

```
bash-2.05b#
```

```
rm recovery.gz
```

Impossible de se connecter à IPS avec l'observateur d'événements IPS (IEV)

Problème :

Ce message d'erreur apparaît :

```
Cannot send xml document to sensor.  
java.security.cert.CertificateExpiredException: NotAfter:
```

Solution :

Ce problème peut être résolu si vous régénérez le certificat tls avec cette commande :

```
<#root>  
sensor(config)#  
tls generate-key
```

Impossible d'accéder à AIP-SSM

Problème :

Lorsque vous essayez d'accéder à SSM, ce message d'erreur s'affiche.

```
Opening command session with slot 1.  
Card in slot 1 did not respond to session request
```

Solution :

Émettez la commande `hw-module module 1 recover` afin de résoudre ce problème. Référez-vous à [Récupération d'AIP-SSM](#) pour plus d'informations sur cette commande.

Erreur lors du branchement du module AIP-SSM sur l'ASA

Problème :

Lorsque vous essayez d'insérer le module AIP SSM dans l'ASA, ce message d'erreur s'affiche.

module in slot 1 experienced a channel communication failure

Solution :

Rechargez l'ASA afin de résoudre le problème. Si le problème persiste, contactez le TAC pour obtenir de l'aide.

AIP-SSM échoue après la mise à jour des signatures

Problème :

AIP-SSM échoue après la mise à jour de la signature. La mise à jour des signatures entraîne une saturation de la mémoire du module AIP-SSM et l'absence de réponse lorsque le nombre de signatures activées est élevé.

Solution :

Réinitialisez la définition de signature afin de résoudre le problème. Si trop de signatures sont activées, essayez de réinitialiser la définition de signature. Établissez une connexion SSH avec le capteur et utilisez les commandes suivantes :

```
<#root>
```

```
configure terminal
```

```
service signature-definition sig0
```

```
default signatures
```

```
exit
```

```
exit
```

Problèmes de latence avec le capteur IPS

Problème :

Un problème de latence se produit avec le capteur IPS.

Solution :

Le problème de latence se produit lorsque l'action `deny inline` et le paquet `deny` sont activés pour chaque signature dans VS0. Si vous activez toutes les signatures, cela entraîne une latence, car IPS inspecte chaque paquet par lequel il passe. Il est judicieux d'activer uniquement la signature spécifique requise selon le flux de trafic réseau afin de résoudre le problème de latence.

Informations connexes

- [Page d'assistance pour Serveur de sécurité adaptatif Cisco](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.