

ASA:AIP-SSM 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[문제 해결](#)

[무응답 상태](#)

[ASDM을 통해 AIP SSM에 액세스할 수 없음](#)

[IPS SSM을 업그레이드/업데이트할 수 없음](#)

[업그레이드 오류:exec업그레이드 소프트웨어](#)

[IPS 이벤트 뷰어\(IEV\)를 사용하여 IPS에 연결할 수 없습니다.](#)

[AIP-SSM에 액세스할 수 없습니다.](#)

[AIP-SSM 모듈이 ASA에 연결된 경우 오류 발생](#)

[시그니처 업데이트 후 AIP-SSM 실패](#)

[IPS 센서의 레이턴시 문제](#)

[관련 정보](#)

소개

이 문서에서는 Cisco 5500 Series ASA(Adaptive Security Appliance)에서 AIP-SSM(Advanced Inspection and Prevention Security Services Module)의 무응답 상태를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco 5500 Series ASA의 AIP-SSM을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙을 참고하십시오.](#)

문제 해결

무응답 상태

문제/장애:

AIP-SSM은 무응답 상태로 전환되고, HTTP 또는 ASDM 액세스에 응답하지 않지만, CLI에서 액세스할 수 있습니다.

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

해결책:

ASA에서 **hw-module module 1 reset** 명령을 실행합니다. 이 명령은 AIP-SSM의 하드웨어 재설정을 수행합니다. 카드가 다음 상태 중 하나에 있을 때 적용됩니다.

- 위로
- 아래로
- 응답 없음
- 복구

ASA를 상태로 재부팅할 경우 SSM을 다시 이미지화해야 합니다. AIP-SSM을 재이미지화하는 방법에 대한 자세한 내용 및 단계는 [시스템 이미지 업그레이드](#), 다운그레이드 및 설치의 [AIP-SSM 시스템 이미지](#) 설치 섹션을 참조하십시오.

참고: AIP-SSM 문제 해결에 사용할 수 있는 다양한 명령에 대한 자세한 내용은 ASA-SSM [구성](#)의 [Reloading, Shutting Down, Reset, and Recovering AIP-SSM](#) 섹션을 참조하십시오.

이 문제는 Cisco 버그 ID CSCts58648([등록된](#) 고객만 해당) 때문입니다.

[ASDM을 통해 AIP SSM에 액세스할 수 없음](#)

문제/장애:

이 오류 메시지는 GUI에 표시됩니다.

Error connecting to sensor. Error Loading Sensor error

해결책:

IPS SSM 관리 인터페이스가 중지되었는지 확인하고 구성된 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 확인합니다. 로컬 시스템에서 Cisco ASDM(Adaptive Security Device Manager) 소프트웨어에 액세스하기 위한 인터페이스입니다. ASDM에 액세스하려는 로컬 시스템에서 IPS SSM의 관리 인터페이스 IP 주소를 ping해 보십시오. ping할 수 없는 경우 센서에서 ACL을 확인합니다.

문제/장애:

AIP SSM 모듈에 연결하려고 시도하는 동안 는 오류 메시지와 .

해결책:

이 오류를 해결하려면 ASA 또는 AIP SSM 모듈을 다시 로드합니다.

IPS SSM을 업그레이드/업데이트할 수 없음

문제/장애:

오류:execUpgradeSoftware Connection 오류 메시지가 CLI에 표시됩니다.

해결책:

IPS SSM 관리 인터페이스 /중단되어 있고 ASA-IPS가 소프트웨어를 다운로드하기 위해 연결을 시도하는 인터페이스인지 확인합니다. 이는 ASA와 IPS-SSM 간의 백플레인 연결이 아닙니다. AIP-SSM 모듈 자체의 이더넷 연결이며, 스위치 포트에 연결하고 IP 주소, 서브넷 마스크 및 기본 게이트웨이로 구성해야 합니다. http가 계속 작동하지 않으면 FTP 또는 SCP 옵션을 upgrade 명령과 함께 사용하려고 합니다.

업그레이드 오류:exec업그레이드 소프트웨어

문제/장애:

오류:execUpgradeSoftware /usr/cids/idsRoot/var/updates 60340KB 57253KB. 업그레이드하는 동안 오류 메시지가 표시됩니다.

솔루션 1:

이 문제를 해결하려면 서비스 계정으로 센서의 CLI에 로그인해야 합니다. 서비스 어카운트가 없는 경우 다음 명령으로 생성할 수 있습니다.

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

서비스 계정에 로그인하면 다음 `rm /usr/cids/idsRoot/var/*pmz` 명령을 실행하고 서비스 계정에서 로그아웃합니다. 그런 다음 업그레이드가 완료되었는지 확인합니다.

솔루션 2:

이 오류는 복구 파일이 모듈에서 더 많은 공간을 차지하기 때문에 IPS 모듈에서 사용 가능한 공간이 부족하기 때문에 발생합니다. 복구 파일을 제거하고 이 오류를 해결하려면 다음 단계를 완료하십시오.

```
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
```

[IPS 이벤트 뷰어\(IEV\)를 사용하여 IPS에 연결할 수 없습니다.](#)

문제/장애:

다음과 같은 오류 메시지가 나타납니다.

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

해결책:

이 명령을 사용하여 tls 인증서를 재생성하는 경우 이 문제를 해결할 수 있습니다.

```
sensor(config)#tls generate-key
```

[AIP-SSM에 액세스할 수 없습니다.](#)

문제/장애:

SSM에 액세스하려고 하면 이 오류 메시지가 표시됩니다.

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

해결책:

이 문제를 해결하려면 `hw-module module 1 recover` 명령을 실행합니다. 이 명령에 [대한 자세한 내용은 AIP-SSM 복구](#)를 참조하십시오.

[AIP-SSM 모듈이 ASA에 연결된 경우 오류 발생](#)

문제/장애:

ASA에 AIP SSM 모듈을 삽입하려고 하면 이 오류 메시지가 표시됩니다.

module in slot 1 experienced a channel communication failure

해결책:

문제를 해결하려면 ASA를 다시 로드합니다.문제가 계속되면 TAC에 지원을 요청하십시오.

시그니처 업데이트 후 AIP-SSM 실패

문제/장애:

서명이 업데이트된 후 AIP-SSM이 실패합니다.서명 업데이트로 인해 AIP-SSM의 메모리가 부족해 지고 활성화된 서명 수가 많으면 응답이 없게 됩니다.

해결책:

문제를 해결하기 위해 서명 정의를 재설정합니다.너무 많은 서명이 활성화된 경우 서명 정의를 재 설정해 보십시오.센서에 SSH를 연결하고 다음 명령을 사용합니다.

```
configure terminal
```

```
service signature-definition sig0
```

```
default signatures
```

```
exit
```

```
exit
```

IPS 센서의 레이턴시 문제

문제/장애:

IPS 센서에서 레이턴시 문제가 발생합니다.

해결책:

레이턴시 문제는 VS0의 각 시그니처에 대해 및 이 활성화된 경우 발생합니다. 모든 시그니처를 활성화하면 IPS가 해당 패킷을 통과하는 모든 단일 패킷을 검사하므로 레이턴시가 발생합니다.레이턴시 문제를 해결하려면 네트워크 트래픽 흐름에 따라 필요한 특정 서명만 활성화하는 것이 좋습니다.

관련 정보

- [Cisco Adaptive Security Appliance 지원 페이지](#)
- [기술 지원 및 문서 - Cisco Systems](#)