

ASA: Устранение неполадок AIP-SSM

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Устранение неисправностей](#)

[Безразличное Состояние](#)

[Неспособный обратиться к SSM AIP через ASDM](#)

[Неспособный Обновить/Обновить SSM IPS](#)

[Ошибка обновления: execUpgradeSoftware](#)

[Неспособный соединиться с IPS с Просмотром событий IPS \(IEV\)](#)

[Неспособный обратиться к SSM AIP](#)

[Ошибка, когда модуль SSM AIP включен в ASA](#)

[Сбои SSM AIP после обновления подписи](#)

[Задержка выходит с сенсором IPS](#)

[Дополнительные сведения](#)

Введение

В этом документе описано решение проблемы отсутствия отклика модуля усовершенствованных служб безопасности для контроля и предотвращения (SSM AIP) в устройстве адаптивной защиты Cisco ASA серии 5500.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на SSM AIP в ASA серии 5500 Cisco.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

Устранение неисправностей

Безразличное Состояние

Проблема:

SSM AIP входит в безразличное состояние, сбои для ответа на HTTP или ASDM обращаются, но доступно от CLI, как показано:

```
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
```

Решение:

Выполните команду **hw-module module 1 reset** на своем ASA. Эта команда выполняет перенастройку оборудования SSM AIP. Когда карта находится в любом из этих состояний, это применимо:

- _____ включен
- _____ отключен
- безразличный
- восстановиться

При перезагрузке ASA в состоянии `unresponsive` SSM должен быть повторно захвачен образ. См. [Установку](#) раздела [Образа системы SSM AIP Обновления, Понижения и Установки Образов системы](#) для получения дополнительной информации и шагов в то, как повторно захватить образ SSM AIP.

Примечание: См. [Повторную загрузку, Завершение, Сброс и Восстановление](#) раздела [SSM AIP SSM ASA Настройки](#) для получения дополнительной информации о различных командах, доступных для устранения проблем SSM AIP.

Эта проблема происходит из-за идентификатора ошибки Cisco [CSCts58648 \(только зарегистрированные клиенты\)](#).

Неспособный обратиться к SSM AIP через ASDM

Проблема:

Это сообщение об ошибках замечено на GUI.

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

Решение:

Проверьте, что интерфейсом управления SSM IPS является `up/down`, и проверьте его настроенный IP - адрес, маску подсети и шлюз по умолчанию. Это - интерфейс для доступа к Cisco Adaptive Security Device Manager (ASDM) программное обеспечение от локального компьютера. Попробуйте пропинговать IP-адрес интерфейса управления SSM IPS от локального компьютера, что вы хотите обратиться к ASDM. Если неспособный для прозванивания проверяют ACL на датчике.

Проблема:

В то время как вы пытаетесь соединиться с модулем SSM AIP, сообщение об ошибках `cannot communicate with main app` появляется.

Решение:

Повторно загрузите ASA или модуль SSM AIP для решения этой ошибки.

[Неспособный Обновить/Обновить SSM IPS](#)

Проблема:

Сообщение об ошибках `Error: execUpgradeSoftware Connection failed` замечено на CLI.

Решение:

Проверьте, что интерфейсом управления SSM IPS является `up/down` и что это - интерфейс, через который IPS ASA пытается связаться для загрузки программного обеспечения. Это не магистральное соединение между ASA и SSM IPS; это - Подключение по технологии Ethernet на самом модуле SSM AIP, который должен быть связан с портом коммутатора и настроен с IP-адресом, маской подсети и шлюзом по умолчанию. Если `http` все еще не работает, попробуйте использовать опцию FTP или SCP с командой [обновления](#).

[Ошибка обновления: execUpgradeSoftware](#)

Проблема:

Сообщение об ошибках `Error: execUpgradeSoftware The update requires 60340 KB in /usr/cids/idsRoot/var/updates, there are only 57253 KB available.` замечено во время обновления.

Решение 1:

Для устранения этой проблемы необходимо войти в CLI датчика с учетной записью сервиса. Если у вас нет учетной записи сервиса, можно создать одну с этими командами:

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

Как только вы входите в учетную запись сервиса, выполняете их `rm/usr/cids/idsRoot/var / *pmz` команды и выходите из учетной записи сервиса. Затем проверьте, что обновление завершает.

Решение 2:

Эта ошибка происходит из-за меньшего количества пространства, доступного на Модуле ips, так как файлы восстановления занимают больше места на Модуле. Выполните эти шаги, чтобы удалить файлы восстановления и решить эту ошибку:

```
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
```

[Неспособный соединиться с IPS с Просмотром событий IPS \(IEV\)](#)

Проблема:

Это сообщение об ошибках появляется:

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

Решение:

Этот вопрос может быть решен при регенерации сертификата *t/s* с этой командой:

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

[Неспособный обратиться к SSM AIP](#)

Проблема:

Когда вы пытаетесь обратиться к SSM, это сообщение об ошибках отображено.

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

Решение:

Выполните команду `hw-module module 1 recover` для решения этой проблемы. См. [Восстановление SSM AIP](#) для получения дополнительной информации об этой команде.

[Ошибка, когда модуль SSM AIP включен в ASA](#)

Проблема:

Когда вы пытаетесь вставить модуль SSM AIP в ASA, это сообщение об ошибках отображено.

```
module in slot 1 experienced a channel communication failure
```

Решение:

Повторно загрузите ASA для решения вопроса. Если проблема все еще существует, свяжитесь с TAC для дальнейшей справки.

[Сбои SSM AIP после обновления подписи](#)

Проблема:

Сбои SSM AIP после подписи обновлены. Обновление подписи заставляет SSM AIP исчерпывать память и становится безразличным, когда количество подписей включило, высоко.

Решение:

Перезагрузите определение подписи для решения вопроса. Если слишком много подписей включены, то попробуйте перезагрузить определение подписи. SSH к датчику и использованию эти команды:

```
configure terminal service signature-definition sig0 default signatures exit exit
```

[Задержка выходит с сенсором IPS](#)

Проблема:

Проблема задержки происходит с сенсором IPS.

Решение:

Когда `deny action inline` и `deny packet` включены для каждой подписи в VS0, проблема задержки происходит. При включении всех подписей это приводит к задержке, поскольку IPS осматривает каждый пакет, через который это проходит. Хорошо включить только определенную подпись, требуемую согласно потоку сетевого трафика для решения вопроса задержки.

[Дополнительные сведения](#)

- [Страница поддержки устройств адаптивной защиты Cisco](#)
- [Cisco Systems – техническая поддержка и документация](#)