Содержание

Введение

Этот документ описывает, как обновить образ и подпись для программного обеспечения Cisco Intrusion Detection Sensor (IDS) от версии 4.1 до системы предотвращения вторжений Cisco (IPS) (IPS) 5.0 и позже.

Примечание: От версии программного обеспечения 5.x и позже, Cisco IPS заменяет Cisco IDS, который применим до версии 4.1.

Примечание: Датчик не может загрузить обновления ПО от Cisco.com. Необходимо загрузить обновления ПО от Cisco.com до сервера FTP, и затем настроить датчик для загрузки их от сервера FTP.

См. Установку раздела Образа системы SSM AIP Обновления, Понижения и Установки Образов системы для процедуры.

См. Процедуру восстановления пароля для Датчика Cisco IDS и Моделей служб IDS (IDSM-1, IDSM-2), чтобы узнать больше, как восстановить Cisco Secure IDS (раньше NetRanger) устройство и модули для версий 3.x и 4. x .

Примечание: Трафик пользователя не становится влияемым во время обновления во **встроенном и значении Open сбоя** на ASA - SSM AIP.

Примечание: См. программное обеспечение Cisco IPS Обновления от 5.1 до 6.x раздел Настройки Датчик системы предотвращения вторжений Cisco (IPS) Использование Интерфейса командной строки 6.0 для получения дополнительной информации о процедуре для обновления IPS 5.1 к версии 6. x .

Примечание: Датчик не поддерживает прокси-серверы для автоматических обновлений.

Параметры прокси для Глобальной функции Корреляции только.

Предварительные условия

Требования

Минимальная версия необходимого программного обеспечения, в которой вы нуждаетесь для обновления к 5.0 4.1 (1).

Используемые компоненты

Сведения в этом документе основываются на Cisco аппаратные средства IDS серии 4200, которые работают под управлением ПО версии 4.1 (чтобы быть обновленными к версии 5.0).

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Обновление от Cisco 4.1 до 5.0 доступно как загрузка от Cisco.com. См. Получение программного обеспечения Cisco IPS для процедуры вы используете для доступа к Загрузкам программного обеспечения IPS на Cisco.com.

Можно использовать любой из методов, перечисленных здесь для выполнения обновления:

- После загрузки 5.0 файлов обновления обратитесь к Readme для процедуры о том, как установить 5.0 файлов обновления с командой **обновления**. Посмотрите Использование Раздел команд Обновления этого документа для получения дополнительной информации.
- При настройке Автоматического обновления для Датчика скопируйте 5.0 файлов обновления к каталогу на сервере, который Датчик опрашивает для обновлений. Посмотрите Использование Раздел команд автообновления этого документа для получения дополнительной информации.
- Если вы устанавливаете обновление на своем Датчике, и Датчик неприменим после того, как это перезагружает, необходимо повторно захватить образ Датчик. **Обновление датчика более ранней версии Cisco IDS, чем 4.1, также требует использования команды recover или компакт-диска восстановления или обновления**. Посмотрите Повторно захватывание образ раздела Датчика этого документа для получения дополнительной

информации.

Обновите датчик

В данных разделах объясняются способы использования команды upgrade для обновления ПО на датчике:

Обзор

Можно обновить Датчик с этими файлами, все из которых имеют расширение .pkg:

- Обновления подписи, например, IPS-sig-S150-minreq-5.0-1.pkg
- Обновления устройства для подписи, например, IPS-engine-E2-req-6.0-1.pkg
- Основные обновления, например, IPS-K9-maj-6.0-1-pkg
- Незначительные обновления, например, IPS-K9-min-5.1-1.pkg
- Обновления пакета обновления, например, IPS-K9-sp-5.0-2.pkg
- Обновления раздела восстановления, например, IPS-K9-r-1.1-a-5.0-1.pkg
- Версии исправления, например, IPS-K9-patch-6.0-1p1-E1.pkg
- Обновления раздела восстановления, например, IPS-K9-r-1.1-a-6.0-1.pkg

Обновление Датчика изменяет версию программного обеспечения Датчика.

Команда обновления и опции

Используйте **команду auto-upgrade-option enabled** в сервисном подрежиме хоста для настройки автоматических обновлений.

Эти опции применяются:

- **default — возвращает значение по умолчанию.**
- **directory — каталог, в котором находятся файлы обновления на сервере файлов.**
- **file-copy-protocol — протокол копирования файлов, используемый для загрузки файлов с сервера файлов. Допустимыми значениями являются ftp или scp.Примечание:** При использовании SCP необходимо использовать **команду ssh host-key** для добавления сервера к SSH известный список хостов, таким образом, Датчик может связаться с ним через SSH. См. Добавление Хостов Известного Списка Хостов для процедуры.
- **ip-address — IP-адрес сервера файлов.**
- **password — пароль пользователя для аутентификации на сервера файлов.**
- **schedule-option — графики выполнения автоматических обновлений.** Календарное планирование запускает обновления в специфических временах в определенные дни. Периодическое планирование запускает обновления в определенных периодических интервалах.**calendar-schedule — настраивает дни недели и время в течение дня для автоматических обновлений.days-of-week — дни недели, в течение которых выполняются автоматические обновления.** Можно выбрать множественные дни. С воскресенья по субботу допустимые значения.**no — удаляет параметр записи или**

выбора.times-of-day — время в течение дня, когда начинается выполнение автоматических обновлений. Можно выбрать многократно. Допустимое значение является hh:mm [: ss].**periodic-schedule — настраивает время выполнения первого автоматического обновления и промежуток между автоматическими обновлениями.interval — количество часов, которое проходит между автоматическими обновлениями.** Допустимые значения от 0 до 8760.**start-time — время в течение дня, когда начинается первое автоматическое обновление.** Допустимое значение является hh:mm [: ss].

- **user-name — имя пользователя для аутентификации на сервере файлов.**

Для процедуры IDM для обновления датчика обратитесь к Обновлению Датчика.

Используйте команду обновления

Если у вас нет **сообщества только для чтения** и параметров **сообщества с правом записи чтения** настроенными прежде, чем обновить к IPS 6.0, вы получаете ошибки SNMP. При использовании **SNMP set** и/или **получаете** функции, необходимо настроить **сообщество только для чтения** и параметры **сообщества с правом записи чтения** перед обновлением к IPS 6.0. В IPS 5.x, **сообщество только для чтения** было установлено в общественность по умолчанию, и **сообщество с правом записи чтения** было установлено в частный по умолчанию. В IPS 6.0 эти две опции не имеют значений по умолчанию. Если вы не использовали SNMP**, получает** и **устанавливает** с IPS 5.x, например, enable-set-get был установлен в False, то нет никакой проблемы обновить к IPS 6.0. Если вы использовали SNMP**, получает** и **устанавливает** с IPS 5.x, например, enable-set-get был установлен в True, необходимо настроить **сообщество только для чтения** и параметры **сообщества с правом записи чтения** к определенным значениям или сбоям обновления IPS 6.0.

Отображается следующее сообщение об ошибке:

Примечание: IPS 6.0 запрещает критически важные события по умолчанию. Это - отличие от IPS 5. x . Для изменения по умолчанию создайте переопределение действия при событии для запрещать пакета встроенное действие и настройте его, чтобы быть отключенными. Если администратор не знает о сообществе с правом записи чтения тогда, они должны попытаться отключить SNMP полностью, прежде чем попытка обновить будет предпринята для удаления этого сообщения об ошибках.

Выполните эти шаги для обновления Датчика:

1. Загрузите главный файл (IPS-K9-maj-5.0-1-S149.rpm.pkg) обновления к FTP, SCP, HTTP или серверу HTTPS, который доступен от вашего Датчика.См. Получение программного обеспечения Cisco IPS для процедуры о том, как определить местоположение программного обеспечения на Cisco.com.**Примечание:** Необходимо войти к Cisco.com с помощью учетной записи с криптографическими привилегиями для загрузки файла. Не изменяйте имя файла. Необходимо сохранить название исходного файла для Датчика для принятия обновления.**Примечание:** Не изменяйте имя файла. Необходимо сохранить исходное имя файла для датчика для принятия обновления.
2. Войдите к CLI с помощью учетной записи с администраторскими привилегиями.
3. Переход в режим конфигурирования:`sensor#configure terminal`
4. Обновите датчик:`sensor(config)#upgrade scp://<username>@<server IP>//upgrade/<file name>`**Пример:Примечание:** Эта команда находится на двух линиях из-за пространственных причин.`sensor(config)#upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-`

maj-5.0-1-S149.rpm.pkg**Примечание:** См. Поддерживаемый FTP и Серверы HTTP/HTTPS для списка поддерживаемого FTP и серверы HTTP/HTTPS. См. Добавление Хостов SSH Известный Список Хостов для получения дополнительной информации о том, как добавить сервер SCP к SSH известный список хостов.

5. Введите пароль, когда предложено:`sensor(config)#` **`upgrade scp://tester@10.1.1.1//upgrade/IPS-K9-maj-5.0-1-S149.rpm.pkg`**
6. **Чтобы выполнить обновление, введите yes.Примечание:** Основные обновления, незначительные обновления и пакеты обновления могли бы вызвать перезапуск процессов IPS или даже вынудить перезагрузку Датчика завершить установку. Так, существует прерывание сервиса в течение по крайней мере двух минут. Однако обновления подписи не требуют перезагрузки после того, как будет сделано обновление. См. Обновления подписи Загрузки (только зарегистрированные клиенты) для последних обновлений.
7. Проверьте свою новую Версию датчика:`sensor#` **`show version`**`Application Partition:Cisco Intrusion Prevention System,` **`Version 5.0(1)S149.0`**`OS Version 2.4.26-IDS-smp-bigphysPlatform: ASA-SSM-20Serial Number: 021No license presentSensor up-time is 5 days.Using 490110976 out of 1984704512 bytes of available memory (24% usage)system is using 17.3M out of 29.0M bytes of available disk space (59% usage)application-data is using 37.7M out of 166.6M bytes of available disk space (24 usage)boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)MainApp 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600 RunningAnalysisEngine 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600 RunningCLI 2005_Mar_04_14.23 (Release) 2005-03-04T14:35:11-0600Upgrade History: IDS-K9-maj-5.0-1- 14:16:00 UTC Thu Mar 04 2004`**`Recovery Partition Version 1.1 - 5.0(1)S149`**`sensor#`**Примечание:** Для IPS 5.x, вы получаете сообщение, которое сообщает, что обновление имеет неизвестный тип. Можно проигнорировать это сообщение.**Примечание:** Операционная система повторно захвачена образ и все файлы, которые были размещены в датчик через учетную запись сервиса, удалены.

См. Обновление Датчика для получения дополнительной информации о процедуре IDM для обновления датчика.

Автоматические обновления Настройки

Автоматические обновления

Можно настроить датчик для поиска новых файлов обновления в каталоге обновления автоматически. Например, несколько датчиков могут указать к тому же удаленному каталогу сервера FTP с другими списками обновления, такой как каждые 24 часа, или в понедельник, в среду, и в пятницу в 23:00.

Вы задаете эту информацию для планирования автоматических обновлений:

- IP-адрес сервера
- Путь каталога на файловом сервере, где датчик проверяет для файлов обновления
- Протокол архивного экземпляра (SCP или FTP)
- Имя пользователя и пароль
- Список обновления

Необходимо загрузить обновление программного обеспечения от Cisco.com и скопировать его к каталогу обновления, прежде чем датчик сможет опросить для автоматических обновлений.

Примечание: При использовании автоматического обновления с IPS AIM и другими устройствами IPS или модулями удостоверьтесь, что вы помещаете и 6.0 (1) файл обновления, IPS-K9-6.0-1-E1.pkg, и файл обновления IPS AIM, IPS-AIM-K9-6.0-4-E1.pkg, на сервере автоматического обновления так, чтобы IPS AIM мог правильно обнаружить, какой файл должен быть автоматически загружен и установлен. Если вы только помещаете 6.0 (1) файл обновления, IPS-K9-6.0-1-E1.pkg, на сервере автоматического обновления, загрузках IPS AIM и попытках установить его, который является неправильным файлом для IPS AIM.

См. Обновление Датчика Автоматически для получения дополнительной информации о процедуре IDM для автоматического обновления датчика.

Используйте Команду автообновления

См. раздел данного документа Команда Upgrade и параметры, чтобы получить сведения о командах auto-update.

Выполните эти шаги для планирования автоматических обновлений:

1. Войдите к CLI с учетной записью, которая имеет администраторские привилегии.
2. Настройте Датчик для автоматического поиска новых обновлений в каталоге обновления.`sensor#`**`configure terminal`**`sensor(config)#`**`service host`**`sensor(config-hos)#`**`auto-upgrade-option enabled`**
3. Задайте планирование:Для календарного планирования, которое запускает обновления в специфических временах в определенные дни:`sensor(config-hos-ena)#`**`schedule-option calendar-schedule`**`sensor(config-hos-ena-cal#`**`days-of-week sunday`**`sensor(config-hos-ena-cal#`**`times-of-day 12:00:00`**Для периодического планирования, которое запускает обновления в определенных периодических интервалах:`sensor(config-hos-ena)#`**`schedule-option periodic-schedule`**`sensor(config-hos-ena-per)#`**`interval 24`**`sensor(config-hos-ena-per)#`**`start-time 13:00:00`**
4. Задайте IP-адрес файлового сервера:`sensor(config-hos-ena-per)#`**`exit`**`sensor(config-hos-ena)#`**`ip-address 10.1.1.1`**
5. Задайте каталог, где файлы обновления расположены на файловом сервере:`sensor(config-hos-ena)#`**`directory /tftpboot/update/5.0_dummy_updates`**
6. Задайте имя пользователя для аутентификации на файловом сервере:`sensor(config-hos-ena)#`**`user-name tester`**
7. Задайте пароль пользователя:`sensor(config-hos-ena)#`**`password`**`Enter password[]: ******Re-enter password: ******`
8. Задайте протокол файловых серверов:`sensor(config-hos-ena)#`**`file-copy-protocol ftp`**Примечание: При использовании SCP необходимо использовать **команду ssh host-key** для добавления сервера к SSH известный список хостов, таким образом, Датчик может связаться с ним через SSH. См. Добавление Хостов Известного Списка Хостов для процедуры.
9. !--- Проверьте настройки:`sensor(config-hos-ena)#`**`show settings`**` enabled ---------- ------------------------------ schedule-option ---------- ------------------------------ ------------- periodic-schedule ---------- --- ----- start-time: 13:00:00 interval: 24 hours ---------- ------------------------------ ---------- --- ip-address: 10.1.1.1 directory: /tftpboot/update/5.0_dummy_updates user-name: tester password: <hidden> file-copy-protocol: ftp default: scp ---------- ------------------------------sensor(config-hos-ena)#`
10. Выходной подрежим автообновления:`sensor(config-hos-ena)#`**`exit`**`sensor(config-hos)#`**`exit`**`Apply Changes:?`**`[yes]:`**

11. Нажмите **Enter**, чтобы применить изменения или ввести **не** для отмены от них.

Повторно захватите образ датчик

Можно повторно захватить образ Датчик этими способами:

- Для Устройств ids с дисководом для компакт-дисков используйте CD восстановления/обновления.См. Использование раздела CD Восстановления/Обновления Обновления, Понижения и Установки Образов системы для процедуры.
- **Для всех датчиков используйте команду recover.**См. Восстановление раздела Раздела установки приложения Обновления, Понижения и Установки Образов системы для процедуры.
- Для IDS-4215 IPS 4240 и IPS 4255, используют ROMMON для восстановления образа системы.См. Установку Образа системы IDS-4215 и Установку IPS 4240 и разделов образа системы IPS 4255 Обновления, Понижения и Установки Образов системы для процедур.
- Для CID NM используйте загрузчик.См. Установку раздела Образа системы CID NM Обновления, Понижения и Установки Образов системы для процедуры.
- Для IDSM-2 повторно захватите образ раздел установки приложения от разделения обслуживания.См. Установку раздела Образа системы IDSM-2 Обновления, Понижения и Установки Образов системы для процедуры.
- **Для AIP-SSM переустановите образ из ASA с помощью команды hw-module module 1 recover [configure | boot].**См. Установку раздела Образа системы SSM AIP Обновления, Понижения и Установки Образов системы для процедуры.

Дополнительные сведения

- Страница технической поддержки системы предотвращения вторжений Cisco (IPS)
- Обновление, понижая и устанавливая образы системы для IPS 6.0
- Cisco Catalyst система обнаружения проникновения серии 6500 (IDSM-2) страница поддержки модулей
- Процедура восстановления пароля для датчика Cisco IDS и моделей служб IDS 1, IDSM-2)
- Устранение проблем автообновлений подписи
- Cisco Systems – техническая поддержка и документация