Часто задаваемые вопросы по Системе Обнаружения нарушений безопасности Cisco (Версии 3.1 и раньше)

Содержание

Введение

Этот документ содержит часто задаваемые вопросы (часто задаваемые вопросы) о Cisco Secure Intrusion Detection System (IDS), раньше известный как NetRanger, версии 3.1 и ранее.

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Вопрос. . Где я могу найти дополнительные сведения о Cisco Secure IDS?

О. См. полный набор документации по продукту для получения дополнительной информации о Cisco Secure IDS.

Вопрос. . Как я обновляю подписи для своей всей Системы IDS (сенсор IDS + IDS Management Software)?

О. Необходимо обновить Датчик и подписи Manager Platform отдельно. Обратите внимание на то, что Программное обеспечение для управления не в состоянии *изучить* подписи из Датчика, поэтому это должно быть обновленный также. Загрузите последний файл обновления подписи для каждого приложения от Загрузок Cisco Secure (только зарегистрированные клиенты). Файлы предварительных сведений, доступные в том же местоположении, содержат инструкции для процедуры обновления.

Вопрос. . Где я могу найти полный список подписей?

О. Список Подписей IDS доступен через Энциклопедию Cisco Secure (только

зарегистрированные клиенты).

Вопрос. . Каков пароль по умолчанию для пользователей на UNIX ID и автономном датчике?

O. На автономном датчике UNIX ID и IDS Management Software, пароль по умолчанию является "атакой" для пользовательского **netrangr** и **root**. При выдаче **su** команды для становления пользователем маршрута, пароль по умолчанию является "атакой". На блейде Модуля системы обнаружения проникновения (IDSM) пароль по умолчанию является "атакой" для **ciscoids** имени пользователя.

Вопрос. . Как я заставляю блейд Модуля системы обнаружения проникновения (IDSM) формировать дамп своих конфигураций?

O. Вам нужен локальный сервер FTP, таким образом, можно загрузить конфигурации.

1. Введите эту команду от режима диагностики на блейде.
   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. **Тип y** для продолжения, когда спросили "Продолжить генерировать Системный Отчёт?".
3. Введите пароль для FTP своего указанного пользователя, когда вам предложат. Когда процесс завершен, вы получаете сообщение, которое сообщает, отказал ли процесс или если передавался файл.

Вопрос. . Когда я устанавливаю/деинсталлирую IDS, где расположены файлы журнала?

O. Журналы установки/обновления могут быть найдены в этих местоположениях:

- Журналы установки управляющего узла находятся в/var/adm/nrInstall.log.
- Журналы обновления Пакета обновления датчика находятся в/usr/nr/sp-update/.
- Журналы обновления подписи находятся в/usr/nr/sig-update/.

Вопрос. . Какие подписи доступны на PIX для IDS?

O. IDS доступен только для PIX 6.0 и позже. Подписи содержатся в сообщениях системного журнала 400000 - 400051, называемых сообщениями с подписью Cisco Secure IDS. См. документацию Сообщений журнала системы PIX для получения дополнительной информации о каждой подписи.

Вопрос. . Когда обновления подписи освобождены, я могу быть уведомлен?

O. Зарегистрируйтесь в системе для активных уведомлений об обновлении Cisco IDS для получения уведомлений по электронной почте для новостей о продукте, отнесенных к Cisco Secure IDS.

Вопрос. . Какие приложения я должен использовать для управления моим сенсором IDS, и каково различие между ними?

O. До версии 3.1 параметры управления должны использовать Cisco Secure Policy Manager (CSPM) или UNIX Director. Основное различие между этими двумя - то, что CSPM выполняется как независимое приложение на Windows Server, в то время как UNIX Director выполняется поверх HP OpenView на Сервере Solaris UNIX. С IDS 3.1 Датчиками можно также управлять через IDS Event Viewer (IEV), установленный на ПК или IDS Device Manager использования, который является частью Датчика версии 3.1. Менеджеру устройств включает по умолчанию с помощью Протокола SSL после того, как вы установите Датчик.

Вопрос. . Где я могу получить программное обеспечение Software Development Kit (SDK)?

O. Программное обеспечение SDK не доступно общественности.

Сенсор системы обнаружения атак

Вопрос. . Что является различием между Версиями датчика 3.x и 4. x?

O. Версия 4.0 предлагает несколько новых характеристик. Самая значимая новая характеристика является интерфейсом командной строки (CLI), подобным Cisco IOS®.

Вопрос. . Как я трудно кодирую Интерфейсную скорость на IDS?

O. Трудно установка скорости/дуплекса в 3.x и 4.0 кода не поддерживается и существует дефект против запроса новых функций (идентификатор ошибки Cisco CSCdy43054 (только зарегистрированные клиенты)). Функция доступна в 5.0 кодах, которые теперь доступны в Интерфейсах Настройки.

Вопрос. . Как я обновляю свое программное обеспечение Sensor от версии 3.0 до 3.1?

O. Клиенты могут загрузить файл обновления для версии 3.1 от Загрузок Cisco Secure (только зарегистрированные клиенты).

Вопрос. . Как я обновляю свое программное обеспечение Sensor от версии 2.5 до 3.0?

O. Клиенты могут загрузить файл обновления для версии 3.0 от Загрузок Cisco Secure (только зарегистрированные клиенты). Установите обновление ПО таким же образом, что пакет обновления и обновления подписи установлены в версии 2.5. Процедура описана подробно в Версии 3.0 Примечания Конфигурации сенсора Cisco IDS.

Вопрос. . Как я обновляю свое программное обеспечение Sensor от версии 2.2 до 3.0?

O. 3.0 файла обновления могут быть загружены от Загрузок Cisco Secure (только зарегистрированные клиенты), но этот файл не в состоянии к версиям обновления прежде 2.5. Необходимо использовать CD Обновления/Восстановления, доступный через Средство обновления продукта (только зарегистрированные клиенты) для обновления от версии

программного обеспечения 2.2 до 3.0. Номер изделия для этого CD является IDS-SW-U.

Примечание: У вас должен быть допустимый договор о технической поддержке для заказа CD Обновления/Восстановления.

Вопрос. . Я подключил клавиатуру и монитор к моему Датчику, но это не загружается должным образом. Какие действия следует предпринять?

О. Проверьте использование поддерживаемой клавиатуры и монитора. Некоторые бренды и модели не совместимы с Cisco Secure IDS и препятствуют тому, чтобы сенсор IDS загрузился должным образом. См. Ошибку загрузки Устройства Cisco Secure IDS для определенных подробных данных бренда.

Вопрос. . В разделе IDS Загрузок Cisco Secure я вижу два типа файлов обновления (пакет обновления и подпись). Каково различие между этими файлами?

О. Каждый из этих файлов содержит определенный набор обновлений ПО или добавлений, как обозначено соглашениями о записи имен, объясненными здесь.

- Обновление пакета обновления для Программного обеспечения аппаратного датчика системы обнаружения сетевых атак содержит улучшение программного обеспечения базового приложения сенсора IDS, а также исправлений ошибки. Например, файл, названный **IDSk9-sp-3.0-5-S17.bin**, включает обновления версии программного обеспечения 3.0 (5) плюс набор подписи номер 17.
- Файл обновления подписи содержит только обновления подписей (отпечатки пальца атаки). Например, файл, названный **IDSk9-sig-3.0-5-S18.bin**, содержит набор подписи номер 18 для 3.0 (5) программное обеспечение Sensor.

Клиенты могут загрузить эти файлы от Загрузок Cisco Secure (только зарегистрированные клиенты) узел.

Вопрос. . Как я могу сказать, настроен ли Датчик правильно для избегания маршрутизатора?

О. Войдите к Датчику как пользовательский **netrangr** и выполните эту команду:

nrgetbulk *<appID> <sensorHostID> <sensorOrgID> <priority> <token>*

Необходимо получить ответ, подобный" *<IP_address>*, Активному", который показывает, что IP-адрес избегающего устройства использовал блокировать атаки. Эти выходные данные показывают пример синтаксиса команды и ожидаемого ответа:

```
netrangr@sensor:/usr/nr
>nrgetbulk 10003 38 1000 1 NetDeviceStatus
10.48.66.68 Active
Success
```

Можно также зарегистрироваться (log in) на маршрутизаторе и выполнить команду who, чтобы увидеть, зарегистрировался ли Датчик.

Вопрос. . Я получаю сообщение об ошибках, которое указывает на "value not

set" (значение не установлено), когда я выполняю команду nrconns. Как устранить эту проблему?

O. Это сообщение об ошибках указывает на потенциальные проблемы c/usr/nr/etc/routes и/или/usr/nr/etc/hosts файлами на вашем Датчике. Эти.../маршруты файлов определяют связи почтовой станции между Датчиком и Управляющим узлом. Эти.../файлы hosts определяют названия и IP-адреса Датчиков и Управляющих узлов.

Можно также войти как **пользователь root**, выполнить **команду sysconfig-sensor** и ввести Сведения об инфраструктуре подключения IDS снова.

Вопрос. . Как я использую FTP для копирования файлов журнала с Датчика для хранения их где-то в другом месте?

O. См. Копирование Файлов журнала IP, которые будут Просматриваться для получения дополнительной информации об этой процедуре.

Вопрос. . Что произошло с демоном configd в версиях программного обеспечения 2.5 и 3.1 Датчика?

O. Configd является демоном, который обрабатывает все команды на обоих UNIX Director, а также Датчиках в 2.2.x основание кода. В 2.5 и 3.0 основаниях кода эта функциональность была поглощена в других демонов, и демон configd больше не существует.

Вопрос. . Когда я обновляю подписи на Датчике, я получаю : `NetRanger . . .` Что я должен сделать об этом?

O. Отредактируйте/usr/nr/etc/daemons файл на Датчике, чтобы гарантировать, что nr.packetd находится в списке демона. Затем остановите и запустите сервисы.

Вопрос. . На IDS 4210, который является контрольным интерфейсом и который является интерфейсом анализатора?

O. Контрольный интерфейс на вершине является **iprb1:** и интерфейс анализатора на нижней части является **iprb0:**.

Вопрос. . Когда я выполняю `ifconfig-a` команда на моем Датчике, почему я только вижу один интерфейс?

O. Команда ifconfig должна показать только контрольный интерфейс. Другой интерфейс (интерфейс анализатора) все еще используется Датчиком, но пользователи, как предполагается, не в состоянии видеть его. Если необходимо видеть этот интерфейс, войти как root и выполнить **ifconfig-a** команда для определения имен интерфейсов. Выполните *<interface>* **ifconfig вертикальная** команда для проверки статуса определенного интерфейса.

Вопрос. . Как я могу жестко закодировать интерфейсную скорость на Датчике?

O. Жесткое кодирование интерфейсной скорости на Датчике не должно быть необходимым и не поддерживается технической поддержкой Cisco. Если коммутатор установлен для

автосогласования, интерфейс выполняет согласование о скорости с коммутатором, к которому это подключено. Трафик с сети на Датчик однонаправлен (другими словами, Датчик получает). Поэтому это обычно соответствует, если коммутатор показывает, что о 100 полудуплексе выполнили согласование (предположение - то, что порт коммутатора составляет 100 M).

UNIX Director

Вопрос. . Я могу использовать новые 3.0 Датчика с 2.2.x версия director?

O. Да, но необходимо обновить Программное обеспечение Director к версии 2.2.3 или позже. Зарегистрированные заказчики могут загрузить эти файлы от Загрузок Cisco Secure (только зарегистрированные клиенты).

Вопрос. . Как я могу сказать, какую версию Демона директора я использую?

O. Выполните команду **cat/usr/nr/VERSION** и проверьте номер версии, который содержат выходные данные.

Примечание: Выходные данные **команды nrvers** на Управляющем узле говорят вам версию демонов, которые работают на Управляющем узле, но это не говорит вам версию самого Программного обеспечения Director.

Вопрос. . Как я заставляю Управляющий узел формировать дамп его конфигурации?

O. Войдите как пользовательский **netrangr** и выполните сценарий/usr/nr/bin/director/nrCollectInfo для передачи сведений о конфигурации к файлу, названному/usr/nr/var/tmp/Report_For_Director.html.

Вопрос. . У меня есть много ошибок (потенциально больше чем 1,000) на моем показе HP OpenView. Я удаляю их, но они продолжают возвращаться. В чем причина?

O. Если IDS Director лавинно рассылается ошибками и не может отобразить их всех, это начинает буферизовать к файлу. Остановите демоны IDS и выйдите из любых карт OpenView, которые вы имеете открытый для избавлений от файла. Удалите файл**/usr/nr/var/nrDirmap.buffer.default**, затем перезапустите демоны IDS и вашу карту OpenView.

Вопрос. . У меня есть проблемы при получении сигналов тревоги на карту HP OpenView. Я продолжаю получать ошибки в/usr/nr/var/errors.nrdirmap. Какие действия следует предпринять?

O. В Версиях IDS до 2.2.2, самая легкая вещь сделать состоит в том, чтобы вытереть Базу данных OpenView. Сроки службы базы данных в/var/opt/OV/share/databases/openview. Выполните эти шаги для удаления Базы данных OpenView.

1. Закройте все открытые карты OpenView с **командой ovstop**, затем остановите сервисы

IDS с **командой nrstop**.
2. Войдите как **пользователь root** и выполните**/usr/nr/bin/director/nrDeleteOVwDb**.
3. Удалите всю "ошибку.*" файлы в/usr/nr/var каталоге (например, errors.configd).
4. Перезапустите сервисы с **командой nrstart**, затем перезапустите OpenView с **командой ovstart**. **Примечание:** В Версии Director 2.2.2 можно удалить только часть IDS Базы данных OpenView вместо всей базы данных. Эта процедура описана в Руководстве по конфигурации IDS Director.

Вопрос. . Я не могу получить сигналы тревоги на своей карте OpenView./usr/nr/var/errors.postofficed файл на Управляющем узле содержит сообщения, что nrdirmap SAID не разрешают работать на этой машине. Как это исправить?

О. Выполните эту команду.

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

Гарантируйте, что пользовательский **netrangr** владеет файлами, затем перезапустите сервисы IDS.

Вопрос. . Когда я выполняю утилиту конфигурации nrConfigure и дважды нажимаю на Director, я получаю это сообщение: "Неспособный найти тип датчика для *<director_name>*. Проверьте, что работают Почта и packetd". Какие действия следует предпринять?

О. Проблема происходит, потому что nrConfigure видит процесс packetd в файле демонов Управляющего узла (который это не должно). Когда nrConfigure делает запрос Управляющего узла для своей версии, как будто это был Датчик, Управляющий узел не может ответить Версией датчика.

Выполните эти шаги для решения этого вопроса.

1. Отредактируйте/usr/nr/etc/daemons файл и удалите записи для nr.packetd, nr.sensord, и nr.managed, так как эти процессы должны только работать на Датчике.
2. Остановите сервисы с **командой nrstop**, затем перезапустите сервисы с **командой nrstart**.
3. Гарантируйте, что был закрыт nrConfigure.
4. Запустите OpenView с **команды ovw**.
5. Выберите **Security> Advanced> nrConfigure DB> Delete** для удаления поврежденной базы данных nrConfigure.
6. Введите **да**, когда спросили продолжиться.
7. Выделите свой Управляющий узел и все ваши Датчики в главном окне OpenView.
8. Выберите **Security> Advanced>, DB nrConfigure> Создает** для создания новой базы данных nrConfigure с версиями текущей конфигурации от машин.

Вопрос. . Как я мешаю приложению nrdirmap включаться по умолчанию на картах OpenView?

O. Пользователи, которые выполняют Приложение ids на UNIX Director, могут также запустить другие приложения на OpenView. Это не рекомендуется, но в некоторых случаях этого нельзя избежать. Проблема состоит в том, что nrdirmap включен по умолчанию для каждой карты OpenView, которая не выбираема, когда другие приложения работают на OpenView.

Выполните эти шаги на UNIX Director для изменения по умолчанию так, чтобы можно было выбрать, который картам включили nrdirmap на них.

1. Войдите как пользовательский **netrangr**.
2. Введите **$OV_REGISTRATION/C CD**. (OV_REGISTRATION является частью ваших переменных окружений. Стандартный путь является/etc/opt/OV/share/registration/C.)
3. Введите **root su**.
4. Отредактируйте файл nrdirmap и измените линию "Команды" как показано в выходных данных ниже:
   ```
   Command -Shared -Initial "nrdirmap";
   !--- Changes to: Command -Shared -Initial "nrdirmap -d";
   ```
5. Сохраните файл nrdirmap.
6. Переработайте OpenView. Теперь, когда карта переведена в рабочее состояние с **командой ovw**, введя **ps - ef |, grep dirmap** должен привести к выходным данным, подобным показанному здесь. Обратите внимание `nrdirmap` с коммутатором `-d`. `>ps -ef | grep dirmap`
   ```
   netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmap
   netrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d
   ```

Новым картам, созданным в OpenView теперь, не включили nrdirmap по умолчанию. Если вы хотите создать карту с установленным nrdirmap, необходимо сделать это от GUI OpenView, как эта процедура объясняет.

1. От основного меню OpenView выберите **Map> New** и введите имя для новой карты.
2. В соответствии с настраиваемыми приложениями, необходимо видеть Netranger/Управляющий узел. Выберите **NetRanger/Director** и нажмите **Configure For эта Карта**.
3. Для опции, которая говорит "Nrdirmap, должен быть включен для этой карты?", выбирает **True**, если вы хотите включить nrdirmap.
4. Выберите **Verify** и нажмите **OK**.

Вопрос. . Я обновил к Версии Director 2.2.3, и теперь я не могу установить степени серьезности ошибки события к уровню выше, чем 5, даже при том, что я мог сделать так в более ранних версиях. В чем причина?

O. Уровни важности были изменены в версии 2.2.3 Управляющего узла для поддержки только диапазона 1 - 5.

IDS Cisco Secure Policy Manager (CSPM)

Вопрос. . Какую версию CSPM я должен использовать для управления моим сенсором IDS?

O. В настоящее время версия 2.3i CSPM является той, которая может управлять сенсором

IDS, тогда как CSPM 3.0 не может. При использовании CSPM для управления Датчиком и другими устройствами Cisco Secure (такими как PIX, маршрутизаторы), необходимо установить две других версии CSPM (2.3i и 3.x) на двух серверах отдельных окон. Можно использовать каждый из серверов для управления соответствующими устройствами: CSPM 2.3i для Датчиков и CSPM 3.x для PIX, маршрутизаторов, и т.д.

Вопрос. . Как я настраиваю CSPM, чтобы управлять моим сенсором IDS и удостовериться, что работает связь?

O. См. Настройку работает Датчик Cisco Secure IDS в CSPM для получения дополнительной информации о том, как настроить CSPM, чтобы управлять вашим сенсором IDS и гарантировать связь.

Вопрос. . Я могу настроить подписи для устройства с CSPM?

O. Настройка включает изменение, что она берет для подписи для увольнения (такие как количество хостов в развертке) и не означает устанавливать действия и уровни важности.

CSPM не может (ни в какой версии) подписи мелодии для устройства. Это может только установить действия и степени серьезности ошибки подписи. Другими словами, CSPM может установить, какие степени серьезности ошибки и какое действие привязать к подписи, но не может установить то, что запускает ту подпись. SigWizMenu на Датчике должен использоваться для настройки Датчиков. SigWizMenu и CSPM могут оба использоваться для настройки того же Датчика, так как они влияют на другие части конфигурации.

Примечание: При использовании версии 2.2.3 UNIX Director или позже утилита конфигурации nrConfigure в состоянии настроить все, что настраивает SigWizMenu. После обновления к 2.2.3 необходимо использовать nrConfigure вместо SigWizMenu для настройки подписей.

Дополнительные сведения

- Поддержка продуктов системы предотвращения вторжений Cisco (IPS)
- Документация по системе обнаружения несанкционированного доступа Cisco
- Уведомления о дефектах для Cisco Secure Intrusion Detection System
- Cisco Systems – техническая поддержка и документация