Positive Technologies Network Attack Discovery версия 12.2

Руководство по установке на один сервер

Дата редакции документа: 19.03.2025

Содержание

1. Об этом документе

Руководство содержит инструкции по установке Positive Technologies Network Attack Discovery (далее также — PT NAD) на один физический сервер или виртуальную машину, а также по обновлению продукта в такой конфигурации.

Руководство адресовано специалистам, выполняющим установку и обновление PT NAD в организации.

Руководство предполагает наличие у читателя базовых знаний о сетевых технологиях, Unix-подобных операционных системах и синтаксисе YAML.

Комплект документации PT NAD включает в себя следующие документы:

- Этот документ.
- Руководство по проектированию — содержит информацию, необходимую для планирования развертывания продукта в сети организации в соответствии с топологией, имеющимися аппаратными ресурсами и задачами по выявлению угроз информационной безопасности.
- Руководство по установке на несколько серверов — содержит инструкции по установке PT NAD на два или три физических сервера, а также по обновлению продукта в таких конфигурациях.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.
- Справочное руководство по REST API — содержит информацию о доступных функциях сервиса REST API в PT NAD.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о PT NAD (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия

Пример	Описание
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о PT NAD

Вы можете найти дополнительную информацию о PT NAD на портале технической поддержки.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 14).

2. О PT NAD

PT NAD — система глубокого анализа трафика для выявления аномальной сетевой активности и сложных целенаправленных атак на периметре и внутри сети организации.

Под атакой понимаются сетевое взаимодействие или группа взаимодействий, которые по специальным правилам определяются как целенаправленная угроза информационной безопасности.

PT NAD выполняет следующие функции:

- **Захват и хранение сетевого трафика.** Захват трафика с пропускной способностью 100 Мбит/с — 10 Гбит/с, его индексация и хранение[1] в виде исходной копии в формате PCAP.
- **Разбор захваченного трафика.** Анализ сообщений сетевых протоколов (в частности, IPv4, IPv6, ICMP, TCP, UDP, HTTP, DNS, NTP, FTP, TFTP) для поиска и расследования инцидентов ИБ.
- **Извлечение и хранение файлов.** Извлечение и хранение[1] объектов, передаваемых по протоколам прикладного уровня.
- **Визуализация данных.** Отображение статистики сетевых взаимодействий в виде отчетов и графиков, а также наглядной карты сетевых взаимодействий.

PT NAD предоставляет следующие возможности:

- **Обнаружение угроз ИБ.** Использование эвристических и несигнатурных методов, а также поведенческого анализа для выявления сетевых аномалий, скрытого присутствия, активности вредоносного ПО.
- **Самозащита от сканирований, флуда и DDoS-атак.** Использование встроенного несигнатурного метода обнаружения нелегитимных сканирований, флуда и DDoS-атак для защиты PT NAD от переполнения базы данных и для повышения стабильности захвата трафика.
- **Поддержка открытого HTTP API.** Возможность разработки сторонних приложений для работы с проанализированным трафиком.
- **Отправка информации об угрозах ИБ в системы SIEM.** Передача сведений об обнаруженных угрозах ИБ в системы SIEM, в том числе в MaxPatrol 10, для инвентаризации активов и проверки результативности атак. Интеграция с MaxPatrol 10 осуществляется с помощью его API и специального агента, с другими системами SIEM — по протоколу системного журнала (syslog) или с помощью механизма webhook.

1 Хранение исходной копии трафика и файлов не предусмотрено в версии PT NAD Sensor (см. раздел 4).

- **Интеграция с внешней аналитической системой.** Передача извлеченных из сетевого трафика файлов на проверку в Positive Technologies MultiScanner (PT MultiScanner) для выполнения антивирусного сканирования и репутационного анализа или в Positive Technologies Sandbox (PT Sandbox) для выполнения антивирусного сканирования, экспертной оценки и поведенческого анализа.
- **Передача экспертизы в продукт.** Использование разработанной в Positive Technologies базы знаний об атаках, нацеленных на удаленную эксплуатацию уязвимостей, и о безопасности IP-адресов, доменных имен, ссылок и файлов.
- **Ретроспективный анализ.** Повторный анализ захваченного трафика с использованием обновленной базы знаний для обнаружения новейших угроз ИБ в сетевой инфраструктуре организации. PT NAD не только регулярно запускает ретроспективный анализ, но и повторно разбирает скопированный трафик для поиска инцидентов ИБ.
- **Импорт трафика для анализа.** Возможность анализировать трафик, полученный в виде PCAP-файлов из сторонних систем или программ.
- **Уведомления.** Оповещение операторов о результатах ретроспективного анализа и о поступлении или непоступлении в информационную инфраструктуру организации определенного трафика. Уведомления могут быть получены на электронную почту или с помощью системного журнала, а также могут отображаться в интерфейсе PT NAD.
- **Обнаружение DGA-доменов.** Поиск DGA-доменов при анализе доменных имен отправителя и получателя, а также при разрешении имен с помощью DNS. Поиск работает в реальном времени для захваченного трафика, а также выполняется в трафике, импортированном в формате PCAP.

3. Иерархия экземпляров PT NAD

Если в организации используется несколько экземпляров PT NAD, то их можно объединить в иерархию, где один экземпляр будет родительским, а другие — дочерними. Это позволит использовать родительскую систему в качестве единого интерфейса для работы с данными (активностями, сессиями, атаками, узлами), полученными из дочерних систем. Такой подход обеспечивает масштабирование PT NAD и может быть полезен для крупных территориально распределенных организаций.

Родительская система в иерархии называется центральной консолью (PT NAD Central Console). Эта система не захватывает сетевой трафик самостоятельно, а получает данные из подключенных к ней дочерних систем.

В центральной консоли отсутствуют возможности, связанные с захватом, разбором, анализом трафика, а также с хранением его исходной копии. Например, в центральной консоли нет правил для атак и правил для активностей, справочников и репутационных списков, поэтому в ее интерфейсе отсутствуют одноименные разделы.

Дочерняя система представляет собой самостоятельный PT NAD, который работает в обычном режиме и подключен к центральной консоли.

Для объединения PT NAD в иерархию вам нужно:

- Установить центральную консоль на отдельный сервер (или виртуальную машину) в подготовленной операционной системе (см. раздел 7) или вместе с операционной системой.
- Присвоить метку (см. раздел 8.2) каждой дочерней системе в иерархии.
- Зарегистрировать все экземпляры PT NAD в сервисе единого входа PT MC. Подробная инструкция приведена в разделе «Настройка аутентификации через PT MC» в Руководстве администратора.
- Обеспечить сетевое взаимодействие систем в иерархии (см. раздел «Сетевое взаимодействие в PT NAD» в Руководстве по проектированию).

4. PT NAD Sensor

Для интеграции с MaxPatrol 10 используется или полная, или упрощенная версия PT NAD. Последняя называется PT NAD Sensor. По сравнению с полной версией PT NAD Sensor позволяет снизить требования к аппаратным ресурсам за счет отключения или ограничения функций, не имеющих значения для работы в MaxPatrol 10:

— захваченный трафик не сохраняется на диск (нет хранилища файлов PCAP);

— полученные в ходе обработки трафика метаданные трафика хранятся не больше одного дня;

— скорость захвата трафика ограничена 1 Гбит/с.

5. Что нового в версии 12.2

Ниже приводится список новых возможностей и улучшений, которые появились в PT NAD версии 12.2.

Выбор языка мастера установки

При установке PT NAD 12.2 или при обновлении до этой версии можно выбрать язык мастера установки.

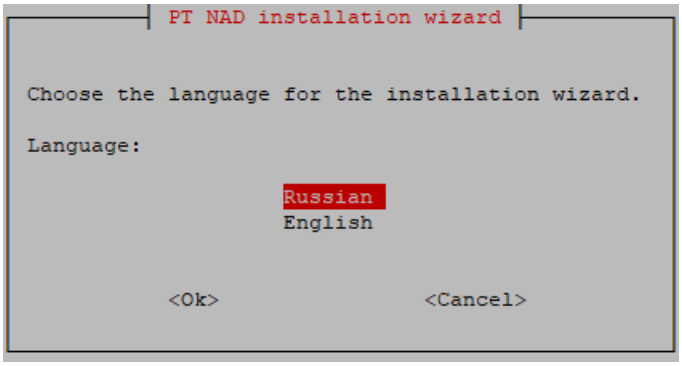

Рисунок 1. Выбор языка мастера установки

Раньше интерфейс мастера установки был на английском языке. Теперь при выборе варианта **Russian** все следующие окна мастера будут на русском.

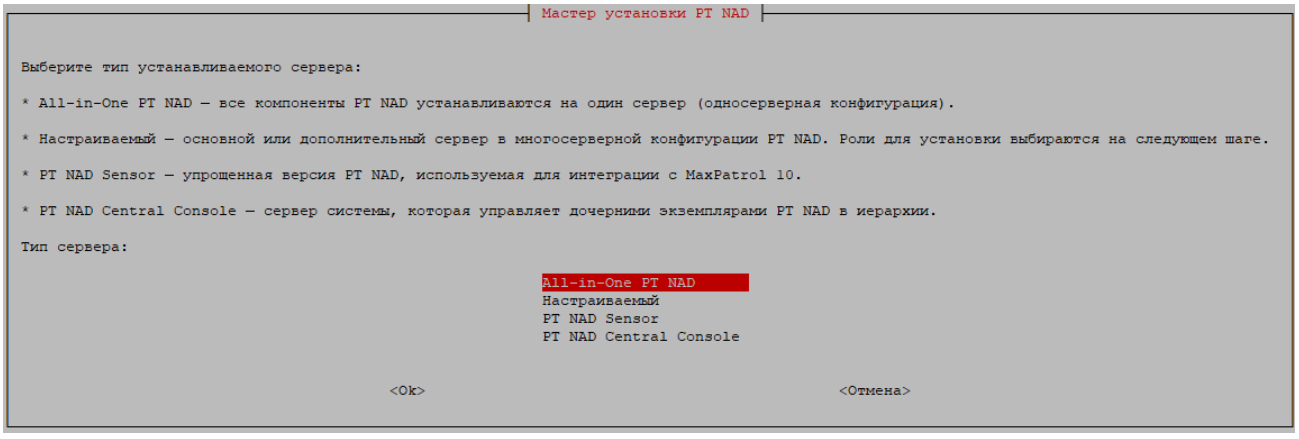

Рисунок 2. Окно выбора варианта установки на русском языке

Особенности перехода на новую версию

Обновление возможно только с версии 12.0 или выше. Для перехода с более низких версий необходимо сначала обновить продукт до версии 12.0.

6. Подготовка к установке или обновлению PT NAD

Перед началом установки или обновления вам нужно выполнить предварительные действия на сервере, где вы будете устанавливать или обновлять продукт: распаковать архив с дистрибутивом PT NAD и проверить доступ к серверу обслуживания.

В этом разделе

6.1. Установочный комплект PT NAD

Компакт-диск с дистрибутивом PT NAD упакован в картонную коробку.

Перед установкой PT NAD необходимо провести проверку комплектности путем сравнения содержимого коробки со сведениями, указанными в документе «Формуляр. 83128364.NAD 30 01».

Маркировка сертифицированного комплекта дополнительно содержит идентификатор, состоящий из прописных букв и групп цифр, разделенных точками, и имеющий формат РОСС RU.01.XXXXX.XXXXXX:

- первая группа знаков (РОСС RU.01) содержит прописные буквы и цифры, которые указывают на систему сертификации ФСТЭК России;
- вторая группа знаков содержит число от 00001 до 99999, которое указывает на номер сертификата соответствия средства защиты информации;
- третья группа знаков содержит число от 000001 до 999999, которое указывает на заводской или серийный номер образца сертифицированного средства защиты информации.

Идентификатор наклеен на коробку оптического диска с дистрибутивом изделия.

Установочный комплект PT NAD представляет собой архивные файлы с названиями `ptnad-installer.<Номер версии и сборки PT NAD>.tar.gz` и `ptnad-depends.<Номер версии и сборки PT NAD>.tar.gz`, например `ptnad-installer.12.2.1399.47.tar.gz` и `ptnad-depends.12.2.1399.47.tar.gz`. Файлы предназначены для создания отдельного экземпляра PT NAD.

Контрольная сумма архивного файла должна совпадать со значением, которое указано в документе «Формуляр.83128364.NAD 30 01», поставляемом вместе с дистрибутивом. Контрольная сумма рассчитывается при помощи специализированной программы gostsum в составе операционной системы Astra Linux.

6.2. Проверка доступа к серверу обслуживания PT NAD

При проверке лицензии PT NAD может обращаться к серверу обслуживания, доступному на поддомене update сайта Positive Technologies. Если в вашей организации используется ПО, ограничивающее сетевой доступ, вам необходимо убедиться, что с основного сервера PT NAD разрешен доступ по HTTPS к этому поддомену.

- Чтобы проверить доступ к серверу обслуживания PT NAD,

  выполните команду:

  ```
  wget -Sq -O /dev/null https://update.ptsecurity.com/test
  ```

  Результат выполнения команды будет начинаться со строки `HTTP/1.1 200 OK`.

Если результат выполнения команды отличается от указанного выше, вам нужно обеспечить доступ, а затем проверить его повторно.

6.3. Распаковка архивов с дистрибутивом PT NAD

Перед установкой или обновлением PT NAD вам нужно распаковать архивы с дистрибутивом PT NAD 12.2 на сервере, где вы будете устанавливать или обновлять компоненты PT NAD.

- Чтобы распаковать архивы с дистрибутивом PT NAD:

  1. Скопируйте архивы с дистрибутивом PT NAD в любой каталог.

     Примечание. Архивы имеют названия `ptnad-installer.<Номер версии и сборки PT NAD>.tar.gz` и `ptnad-depends.<Номер версии и сборки PT NAD>.tar.gz`, например `ptnad-installer.12.2.1399.tar.gz` и `ptnad-depends.12.2.1399.tar.gz`.

  2. Перейдите в каталог со скопированными архивами.

     Например:

     ```
     cd /home/user/ptnad-installer
     ```

  3. Распакуйте архивы:

     ```
     tar pxf ptnad-installer.<Номер версии и сборки PT NAD>.tar.gz
     tar pxf ptnad-depends.<Номер версии и сборки PT NAD>.tar.gz
     ```

     Например:

     ```
     tar pxf ptnad-installer.12.2.1399.tar.gz
     tar pxf ptnad-depends.12.2.1399.tar.gz
     ```

     Примечание. Рекомендуется сохранить каталог с распакованным архивом после установки (обновления), так как он может понадобиться для удаления PT NAD.

Теперь вы можете перейти к установке (см. раздел 7) или обновлению продукта.

7. Установка PT NAD

Перед выполнением инструкции нужно подготовить сервер к установке:

- Проверить на соответствие аппаратным и программным требованиям (см. раздел «Аппаратные и программные требования» в Руководстве по проектированию).
- Распаковать архив с дистрибутивом продукта (см. раздел 6.3).
- Установить пакет linux-headers, соответствующий версии ядра Linux:
  `sudo apt install linux-headers-$(uname -r)`

► Чтобы установить PT NAD:

1. Перейдите в каталог с распакованным дистрибутивом (см. раздел 6.3).

   Например:
   `cd /home/user/ptnad-installer`
2. Запустите мастер установки:
   `sudo ./install.sh`

   Начнется распаковка и подготовка файлов. По завершении подготовки откроется окно выбора языка мастера.
3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Подтвердите ознакомление с лицензионным соглашением, выбрав **Ok** и нажав клавишу Enter.
5. Примите условия лицензионного соглашения, выбрав **Да** и нажав клавишу Enter.
6. Выберите **All-in-One PT NAD** (для установки полноценной версии), **PT NAD Sensor** (для установки упрощенной версии, используемой в MaxPatrol 10) или **PT NAD Central Console** (для установки центральной консоли, используемой для управления экземплярами PT NAD в иерархии) и нажмите клавишу Enter.

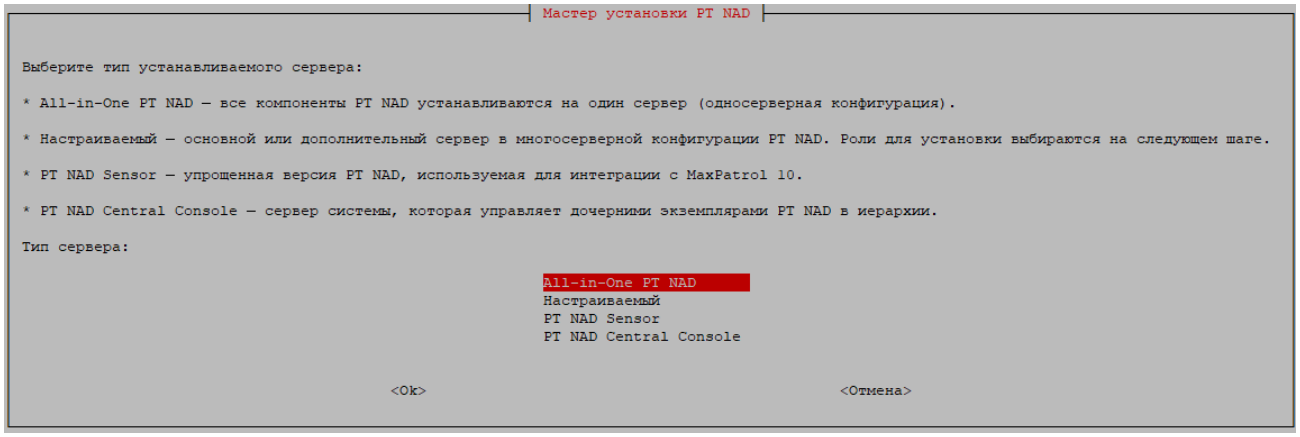

Рисунок 3. Выбор варианта установки

7. На следующих этапах нажимайте клавишу Enter, сохраняя параметры по умолчанию.

   Мастер установки начнет выполнение подготовительных шагов, после чего запустит установку компонентов PT NAD.

   После установки модуля ptdpi мастер сообщит об отсутствии или наличии на сервере сетевой карты NVIDIA Mellanox и предложит установить ее драйверы.

   Примечание. Этап проверки сетевой карты NVIDIA Mellanox отсутствует при установке PT NAD Central Console.

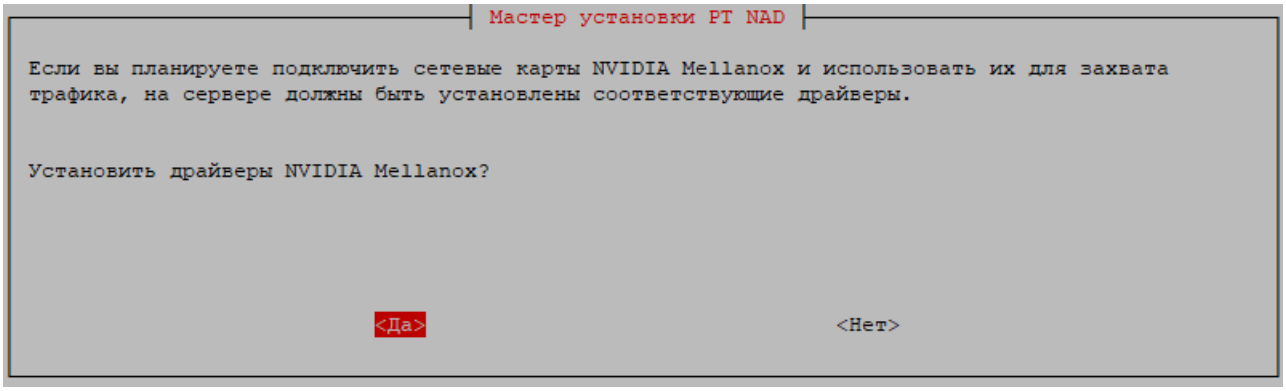

Рисунок 4. Проверка сетевой карты NVIDIA Mellanox

8. Если для захвата трафика планируется использовать интерфейсы сетевой карты NVIDIA Mellanox, выберите **Да** и нажмите клавишу Enter.

   Мастер продолжит установку PT NAD.

   По завершении установки появится сообщение `<Время генерации сообщения> install.sh INFO: PT NAD components are installed successfully`.

Теперь вам нужно перейти к настройке продукта (см. раздел 8).

См. также

Удаление PT NAD (см. раздел 13)

8. Настройка PT NAD с помощью мастера

Настройка PT NAD с помощью мастера делится на следующие этапы:

1. Запуск мастера настройки (см. раздел 8.1).
2. Присвоение метки дочерней системе в иерархии (см. раздел 8.2). Этот этап необходим, только если вы планируете использовать экземпляр PT NAD в качестве дочерней системы.
3. Выбор интерфейса управления и настройка его IP-адреса (см. раздел 8.3).
4. Настройка кластера Elasticsearch (см. раздел 8.4).
5. Настройка хранения метаданных трафика (см. раздел 8.6).
6. Настройка базовых параметров модуля ptdpi подсистемы захвата (см. раздел 8.7).
7. Проверка и подтверждение измененных параметров (см. раздел 8.8).

В этом разделе

8.1. Запуск мастера настройки PT NAD

- Чтобы запустить мастер настройки PT NAD,

  выполните команду:

  ```
  sudo nad-configure
  ```

  Появится приветственный экран мастера настройки PT NAD.

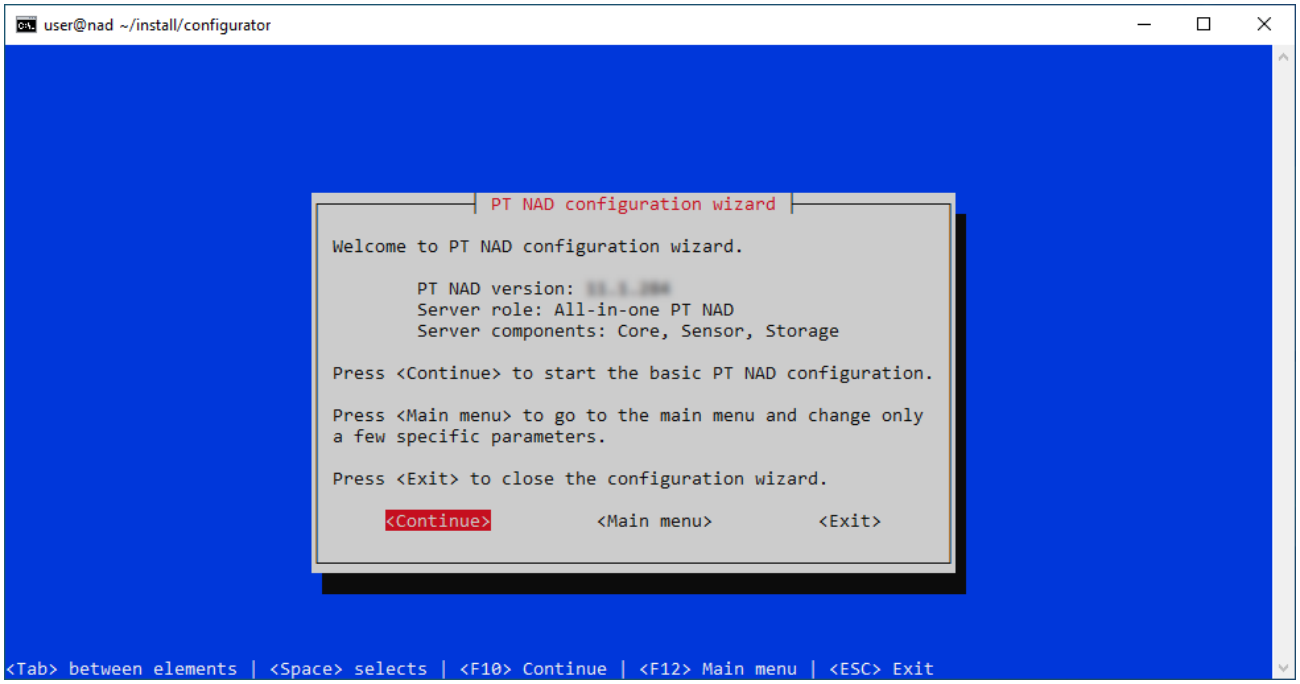

Рисунок 5. Приветственный экран мастера настройки PT NAD

На приветственном экране в поле **PT NAD version** отображается номер версии установленного экземпляра PT NAD.

Теперь вы можете выбрать вариант **Continue** для перехода к пошаговой настройке основных параметров PT NAD.

Для перехода к главному меню и настройке только нужных вам параметров продукта необходимо выбрать вариант **Main menu**.

Для выхода из мастера настройки нужно выбрать вариант **Exit**.

8.2. Присвоение метки дочерней системе в иерархии

Метка — это уникальный идентификатор дочерней системы, без которого ее невозможно подключить к иерархии (см. раздел 3). Если вы планируете использовать установленный экземпляр PT NAD в качестве дочерней системы, то вам нужно присвоить ему метку. Иначе пропустите этот шаг мастера, выбрав вариант **Next**.

Кроме того, если вы планируете настроить облачное хранение метаданных трафика, то вам следует пропустить этот шаг мастера. Облачное хранение недоступно в экземплярах PT NAD, объединенных в иерархию.

Примечание. Описанная в этом разделе настройка недоступна в PT NAD Central Console.

Перед выполнением инструкции нужно запустить мастер настройки (см. раздел 8.1) и выбрать вариант **Continue**.

- Чтобы присвоить метку дочерней системе в иерархии:

  1. Введите метку.

     Примечание. Метка должна быть уникальной и состоять из латинских букв, цифр и символов «.», «-», «_». Максимальная длина — 10 символов.

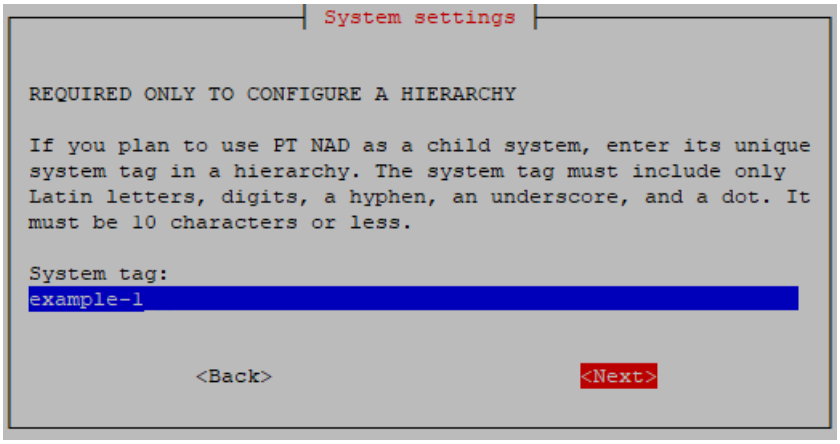

Рисунок 6. Присвоение метки дочерней системе в иерархии

  2. Выберите вариант **Next** для перехода к следующему шагу мастера.

Кроме того, вы можете изменять метку, присвоенную системе, выбрав в главном меню мастера вариант **System settings**.

Это может понадобиться, например, если два или более экземпляра PT NAD имеют одинаковые метки. В этом случае к иерархии можно подключить только один из них. Для подключения всех экземпляров их метки должны быть уникальными.

Если система подключена к иерархии, то после изменения ее метки необходимо повторно сформировать список дочерних систем. Это нужно для того, чтобы в интерфейсе центральной консоли новые данные, полученные от системы, отображались с новой меткой. А также, чтобы метка обновилась для данных об узлах и активностях, полученных до ее изменения. При этом для старых данных о сессиях и атаках метка не изменится.

8.3. Выбор интерфейса управления и настройка его IP-адреса

Интерфейс управления — это сетевой интерфейс с IP-адресом, по которому администраторы могут подключаться к PT NAD для его настройки (в частности, по SSH). По этому адресу также доступен веб-интерфейс продукта.

Настройка выполняется на шаге **Set up a management network interface** мастера.

- Чтобы выбрать интерфейс управления и настроить его IP-адрес:

  1. Выберите сетевой интерфейс, который должен использоваться в качестве интерфейса управления.

     Примечание. По умолчанию мастер выбирает первый интерфейс, у которого есть IP-адрес. Этот интерфейс помечается как MGMT.

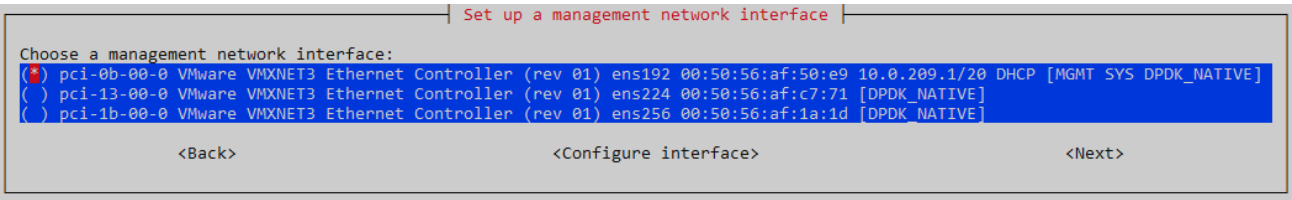

Рисунок 7. Выбор интерфейса управления

  2. Если IP-адрес выбранного интерфейса не задан или его нужно поменять, настройте статический (см. раздел 8.3.1) или динамический (см. раздел 8.3.2) IP-адрес, иначе выберите вариант **Next** для перехода к настройке кластера Elasticsearch (см. раздел 8.4).

     Внимание! Настройка IP-адреса с помощью мастера возможна, только если выбранный интерфейс не был настроен в процессе установки операционной системы или позднее не был сконфигурирован вручную.

     Примечание. Рекомендуется использовать статический IP-адрес: он не будет меняться при перезагрузке сервера.

В этом разделе

8.3.1. Настройка статического IP-адреса

- Чтобы настроить статический IP-адрес:

  1. На шаге мастера **Set up a management network interface** выберите вариант **Configure interface**.

     Откроется меню **Interface configuration method**.

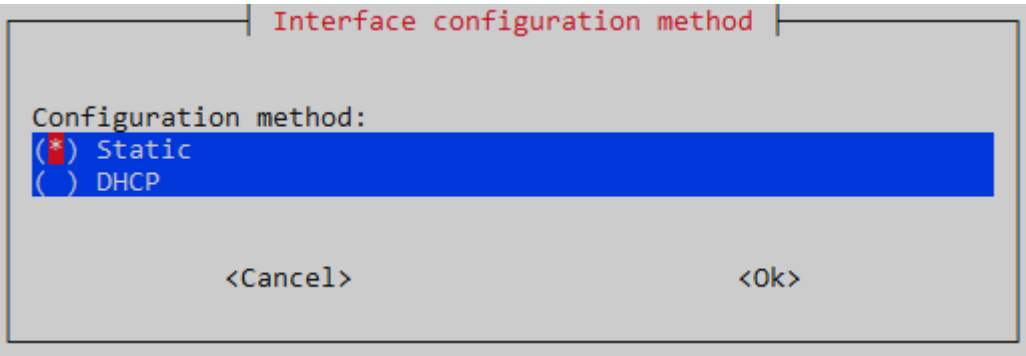

Рисунок 8. Выбор способа настройки IP-адреса

2. Выберите вариант **Static**, после чего **Ok**.

   Откроется форма **Interface configuration parameters**.

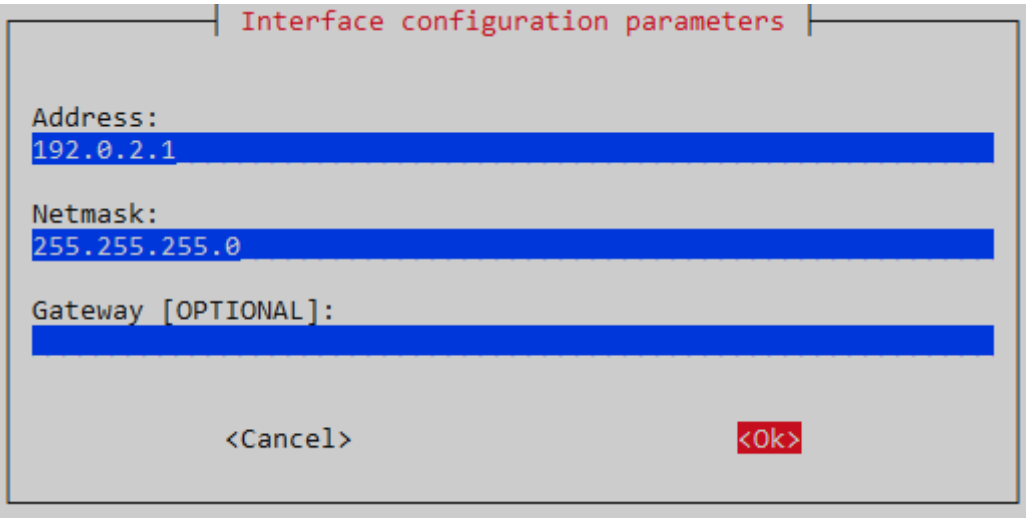

Рисунок 9. Настройка статического IP-адреса

3. В поле **Address** введите IP-адрес узла PT NAD.
4. В поле **Netmask** введите маску подсети.
5. При необходимости в поле **Gateway** введите IP-адрес шлюза.
6. Выберите вариант **Ok**.

   Появится сообщение `The interface <Название интерфейса> is configured successfully with static address`.

7. Нажмите клавишу Enter для перехода к настройке кластера Elasticsearch (см. раздел 8.4).

При необходимости вы можете настроить динамический IP-адрес (см. раздел 8.3.2).

8.3.2. Настройка динамического IP-адреса

- Чтобы настроить динамический IP-адрес:

1. На шаге мастера **Set up a management network interface** выберите вариант **Configure interface**.

   Откроется меню **Interface configuration method**.

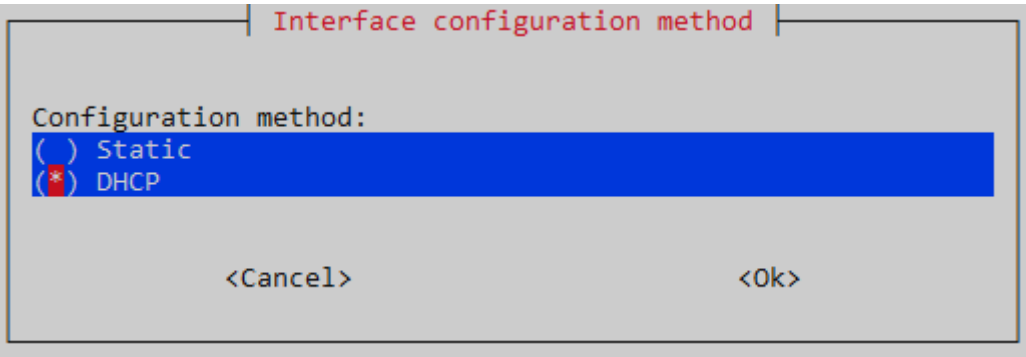

Рисунок 10. Выбор варианта автоматической настройки IP-адреса

2. Выберите вариант **DHCP**, после чего **Ok**.

   Появится сообщение `The interface <Название интерфейса> is configured successfully with DHCP`.

3. Нажмите клавишу Enter.

   Откроется меню **Set up a management network interface**.

См. также

Настройка статического IP-адреса (см. раздел 8.3.1)

8.4. Настройка кластера Elasticsearch

Мастер рассчитывает оптимальную конфигурацию кластера Elasticsearch исходя из доступных аппаратных ресурсов и требований модуля Elasticsearch к процессору и оперативной памяти. Подробная информация об аппаратных требованиях модуля приведена в разделе «Требования Elasticsearch к процессору и оперативной памяти» Руководства по проектированию.

На шаге **Elasticsearch cluster settings** вам нужно ознакомиться с предложенной мастером конфигурацией (см. рисунок ниже). Конфигурация определяет, сколько узлов должно быть в кластере, какие у них должны быть роли и какой объем аппаратных ресурсов необходимо выделить на работу узлов с той или иной ролью.

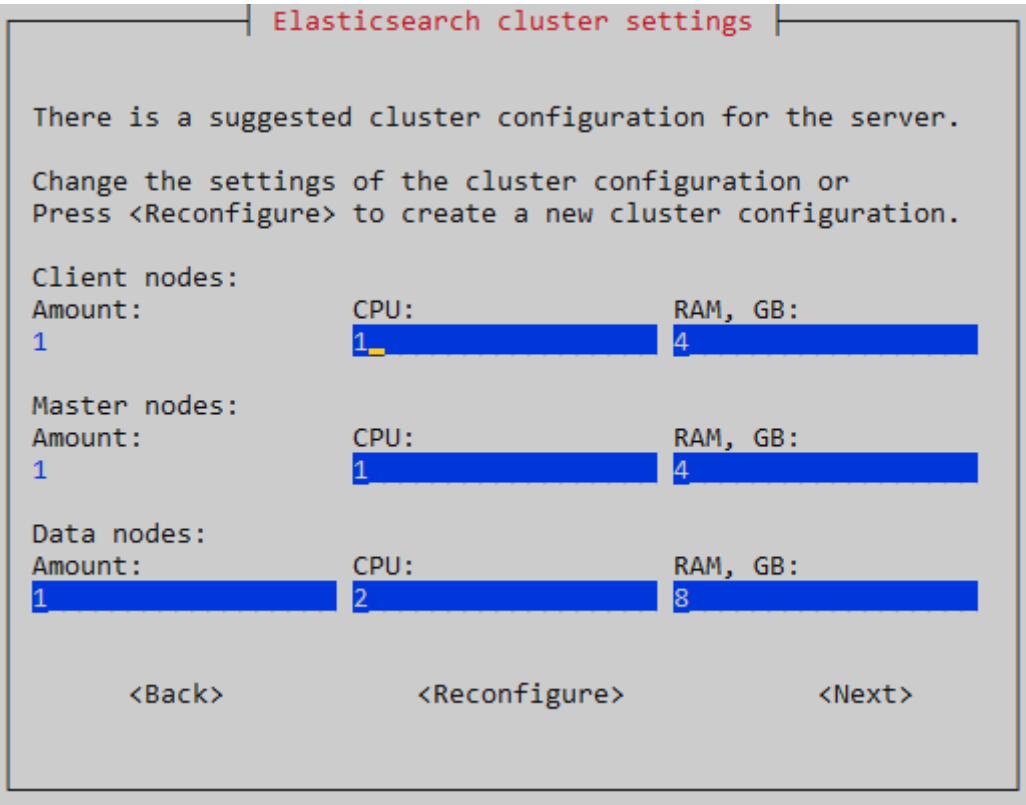

Рисунок 11. Выделение аппаратных ресурсов для работы хранилища метаданных Elasticsearch

Вы можете изменить объем ресурсов, выделенный для работы узлов, а также изменить количество узлов данных.

Если вам нужно превратить кластер, состоящий из одного узла, в кластер из нескольких узлов или наоборот, необходимо пересоздать кластер (см. раздел 8.5).

> **Примечание.** Кластер Elasticsearch для PT NAD Central Console состоит из одного узла, выполняющего роли главного узла (master node) и клиентского узла удаленного кластера (remote cluster client node). Если вы настраиваете продукт для этой версии, то на шаге **Elasticsearch cluster settings** вы можете изменить только количество ядер процессора и объем ОЗУ, выделенные для работы узла (шаги 1 и 2 инструкции).

► Чтобы настроить кластер Elasticsearch:

1. Если требуется, в полях **CPU** измените количество ядер процессора, выделенное для работы узлов соответствующей роли.

   Значение указывается для одного узла.

2. Если требуется, в полях **RAM, GB** измените объем ОЗУ в ГБ, выделенный для работы узлов соответствующей роли.

   Значение указывается для одного узла.

3. Если требуется, в поле **Amount** измените количество узлов данных.

Теперь вы можете выбрать вариант **Next** для перехода к настройке хранения метаданных трафика (см. раздел 8.6).

8.5. Пересоздание кластера Elasticsearch

Примечание. Описанная в этом разделе настройка недоступна в PT NAD Central Console.

По умолчанию на шаге **Elasticsearch cluster settings** мастер отображает конфигурацию кластера Elasticsearch, автоматически рассчитанную для установки на сервер исходя из его доступных аппаратных ресурсов. Вы можете пересоздать кластер, если автоматическая конфигурация не соответствует конфигурации, спроектированной в ходе подготовки к развертыванию PT NAD. Например, в автоматически рассчитанной конфигурации кластер состоит только из одного узла, который выполняет все роли, тогда как вам нужен кластер из нескольких узлов.

- Чтобы пересоздать кластер Elasticsearch:

  1. На шаге **Elasticsearch cluster settings** выберите вариант **Reconfigure**.

     Откроется меню **Elasticsearch cluster type**.

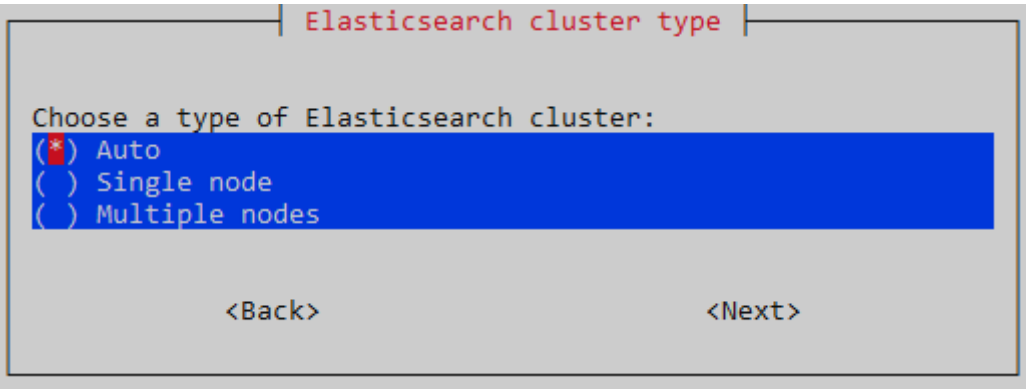

Рисунок 12. Выбор типа кластера Elasticsearch

  2. Выберите тип кластера Elasticsearch — **Single node**, если кластер должен состоять из одного узла, выполняющего все роли, или **Multiple nodes**, если узлов в кластере должно быть несколько.
  3. Выберите вариант **Next**.

Теперь вы можете вернуться к настройке кластера Elasticsearch (см. раздел 8.4). Чтобы пересоздать кластер с автоматическим определением его типа, нужно повторить инструкцию, выбрав вариант **Auto**.

8.6. Настройка хранения метаданных трафика

Примечание. Описанная в этом разделе настройка недоступна в PT NAD Central Console.

Хранение метаданных трафика хранилищем Elasticsearch настраивается на этапе **Elasticsearch storage settings** мастера.

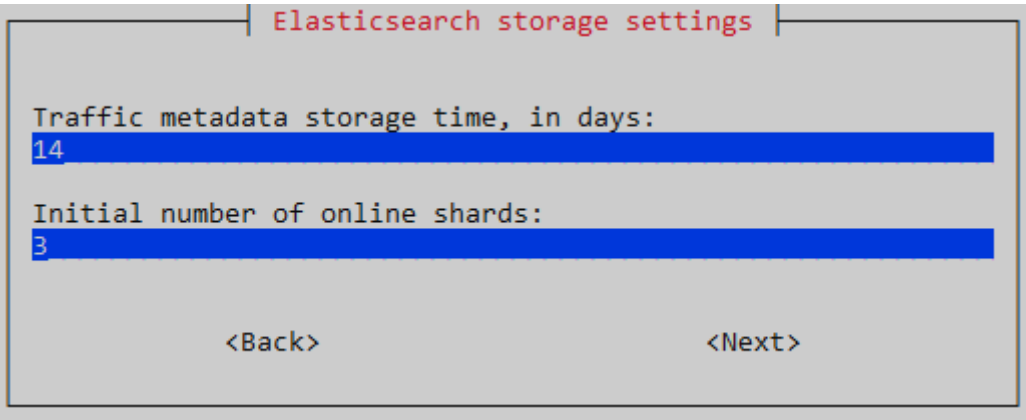

Рисунок 13. Настройка хранения метаданных трафика

- Чтобы настроить хранение метаданных трафика:

  1. В поле **Traffic metadata storage time, in days** введите максимальное время хранения метаданных трафика в днях.

     Время хранения зависит от объема твердотельных накопителей, выделенных для метаданных трафика, и расчетной скорости захвата трафика в организации. Формула для расчета значения приведена в разделе «Требования к свободному месту» Руководства по проектированию.

     Примечание. Метаданные удаляются автоматически по истечении времени их хранения. Если дисковое пространство заполняется на 90% или более, самые старые метаданные перемещаются на свободный узел Elasticsearch или удаляются раньше времени хранения. Крайне не рекомендуется это допускать: если к моменту удаления метаданные не успеют переместиться на свободный узел или займут более 95% свободного места на узле данных, то фрагменты индекса узла перейдут в режим чтения и запись новых метаданных на них будет остановлена.

  2. В поле **Initial number of online shards** введите изначальное количество фрагментов индекса.

     Подробная информация о расчете количества фрагментов индекса приведена в разделе «Требования Elasticsearch к процессору и оперативной памяти» Руководства по проектированию.

Теперь вы можете выбрать вариант **Next** для перехода к настройке базовых параметров модуля ptdpi подсистемы захвата (см. раздел 8.7).

8.7. Настройка базовых параметров модуля ptdpi подсистемы захвата

Примечание. Описанная в этом разделе настройка недоступна в PT NAD Central Console.

Настройка базовых параметров модуля ptdpi подсистемы захвата включает в себя:

- **Выбор интерфейсов захвата трафика.** Выбор сетевых интерфейсов, с которых нужно захватывать трафик.

  Вы не можете выбрать интерфейс, который уже используется операционной системой или выбран в качестве интерфейса управления (см. раздел 8.3).

- **Выбор механизма захвата трафика.** По умолчанию модуль ptdpi использует механизм захвата трафика DPDK. Если по какой-то причине модуль ptdpi не запускается с DPDK, вы можете использовать для захвата трафика механизм AF_PACKET.

- **Увеличение MTU.** Значение по умолчанию (1518 байт) соответствует MTU в стандарте Ethernet и используется в большинстве сетей. Однако некоторые сетевые карты могут обрабатывать фреймы большего размера — jumbo-фреймы, размер каждого из которых может достигать 9600 байт. Если вы задействовали для захвата трафика такую сетевую карту и часть сетевых сообщений в организации передается в jumbo-фреймах, вам нужно увеличить MTU. В противном случае PT NAD не сможет обрабатывать сообщения, переданные в jumbo-фреймах, и, как следствие, обнаруживать связанные с такими сообщениями события ИБ.

  Увеличение MTU также может потребоваться при использовании технологии ERSPAN для захвата трафика.

- **Выбор расчетной скорости захвата трафика.** От этого зависят параметры конфигурации модуля ptdpi. Чем выше скорость, тем более производительным должен быть сервер, на котором работает модуль ptdpi.

- **Настройка ERSPAN.** Ввод IP-адресов для приема трафика в случае использования ERSPAN.

Более детальная справочная информация приведена в разделах «Выбор точек захвата трафика», «Требования модуля ptdpi к процессору и сетевой карте», «Минимальные аппаратные требования», «Механизмы захвата трафика» и «Захват трафика с применением ERSPAN» в Руководстве по проектированию.

- Чтобы настроить базовые параметры модуля ptdpi:

  1. Выберите один или несколько сетевых интерфейсов, с которых модуль ptdpi должен захватывать трафик, после чего — вариант **Next**.

     Примечание. Интерфейс, используемый для захвата трафика, помечен как `PTDPI`, полностью совместимый с DPDK — `DPDK_NATIVE`, используемый операционной системой — `SYS`, интерфейс управления — `MGMT`.

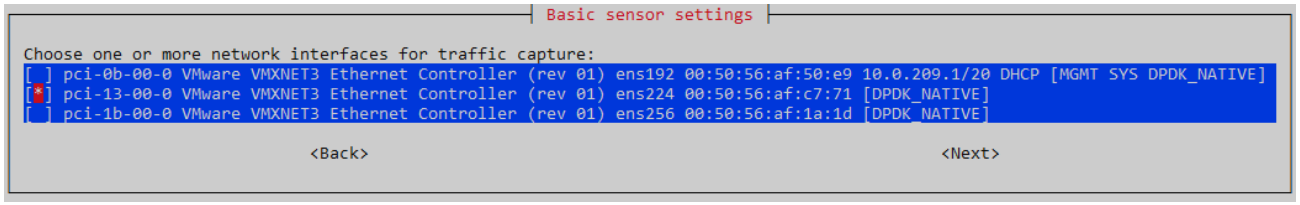

Рисунок 14. Выбор интерфейсов для захвата трафика

После перезапуска модуля ptdpi каждый выбранный сетевой интерфейс станет доступен этому модулю и недоступен операционной системе. Если для захвата трафика используются сетевые интерфейсы производства NVIDIA Mellanox, они остаются доступны операционной системе.

2. Выберите механизм захвата трафика, после чего — вариант **Next**.

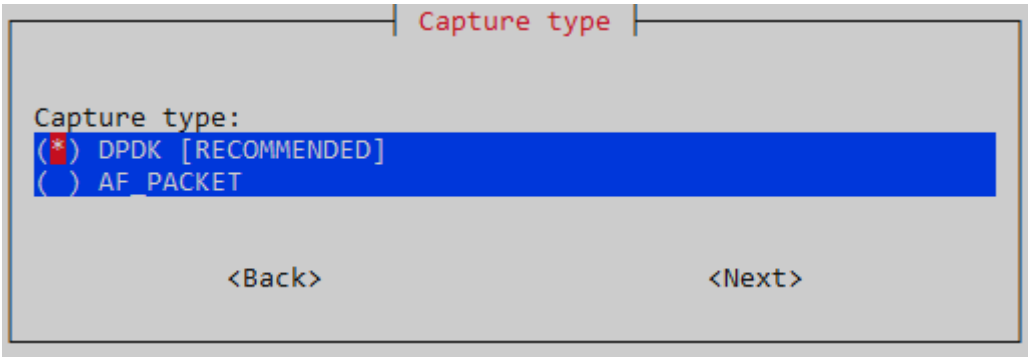

Рисунок 15. Выбор механизма захвата трафика

3. При необходимости в поле **Capture MTU** увеличьте максимальный размер фрейма (MTU).

   Внимание! Увеличение MTU приводит к росту потребления оперативной памяти. Для MTU 9000 операционная система зарезервирует по 10 ГБ оперативной памяти на каждый сетевой интерфейс, используемый для захвата трафика (для MTU по умолчанию — по 4 ГБ).

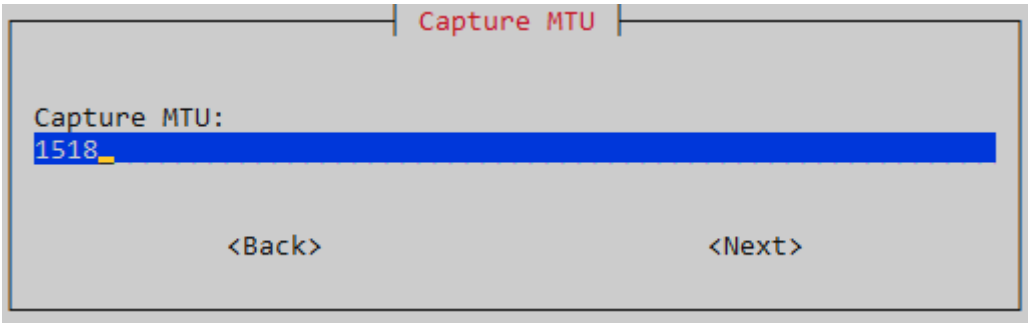

Рисунок 16. Увеличение MTU

4. Выберите вариант **Next**.

5. Выберите расчетную скорость захвата трафика в организации, после чего — вариант **Next**.

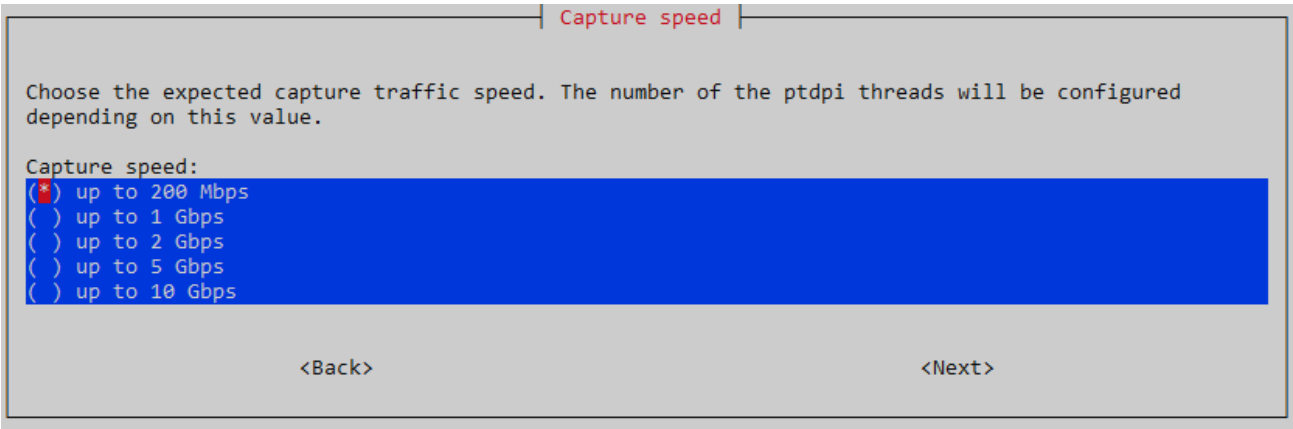

Рисунок 17. Выбор расчетной скорости захвата трафика

В соответствии с выбранной скоростью мастер настройки рассчитает и настроит количество потоков выполнения модуля ptdpi.

6. Если захват трафика осуществляется при помощи технологии ERSPAN, введите IP-адреса для сетевых интерфейсов, на которых PT NAD должен принимать трафик, после чего выберите вариант **Next**.

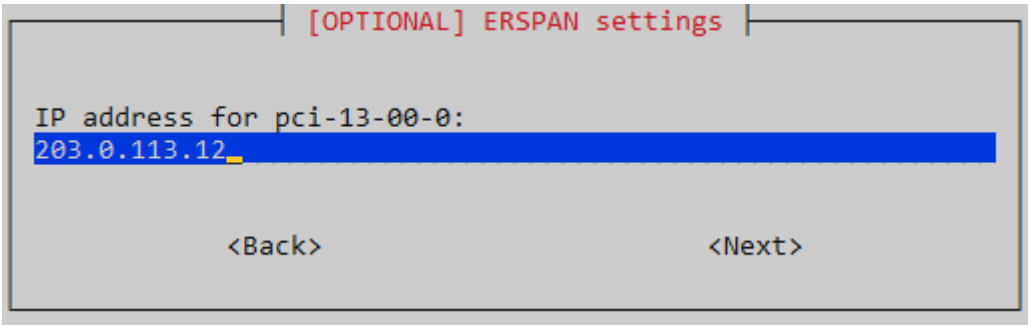

Рисунок 18. Ввод IP-адреса для настройки ERSPAN

Модуль ptdpi будет отвечать на ARP-запросы для указанных IP-адресов на соответствующих интерфейсах. На разные интерфейсы можно указывать разные или одинаковые IP-адреса или не задавать их вовсе (по умолчанию).

Если ERSPAN не используется, поля нужно оставить пустыми.

Теперь вы можете перейти к проверке и подтверждению измененных параметров (см. раздел 8.8).

8.8. Проверка и применение измененных параметров

На этапе **Confirmation of the settings** мастера нужно проверить корректность измененных параметров на сервере и применить их.

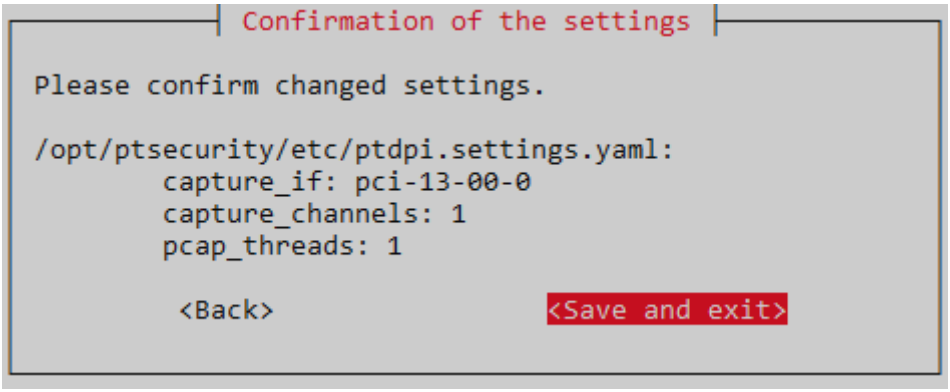

Рисунок 19. Проверка измененных параметров

- Чтобы применить измененные параметры,

  выберите вариант **Save and exit**.

  Мастер начнет применение новых параметров. Если это затрагивает изменение конфигурации загрузчика операционной системы, то по завершении настройки мастер предложит перезагрузить сервер. Если таких изменений не было, мастер перезапустит только службы, необходимые для работы PT NAD.

  Когда мастер завершит работу, появится сообщение `[INFO] PT NAD configuration is finished`.

8.9. Клавиши для управления мастером настройки

Для управления мастером настройки используются следующие клавиши:

— для переключения между элементами мастера — Tab;

— выбора вариантов и пунктов меню — Enter;

— выбора элементов списка — пробел;

— возврата к предыдущему экрану — Esc;

— перехода к следующему экрану с подтверждением изменений — F10.

9. Обновление PT NAD до версии 12.2

Внимание! Обновление возможно только с версии 12.0 или выше. Для перехода с более низких версий на версию 12.2 вам нужно предварительно обновить продукт до версии 12.0 по инструкции с учетом поддерживаемых операционных систем.

Перед выполнением инструкции нужно подготовить сервер к обновлению:

- Проверить на соответствие аппаратным и программным требованиям (см. раздел «Аппаратные и программные требования» в Руководстве по проектированию).
- Распаковать архив с дистрибутивом продукта (см. раздел 6.3).
- Установить пакет linux-headers, соответствующий версии ядра Linux:
  `sudo apt install linux-headers-$(uname -r)`

В версиях PT NAD ниже 12.1 использовался Elasticsearch 5.6. Начиная с версии 12.1 при новой установке продукта устанавливается Elasticsearch 8.13, а при обновлении дается выбор: продолжать использовать Elasticsearch 5.6 с сохранением уже записанных метаданных трафика или перейти на версию Elasticsearch 8.13, но с удалением этих данных. Новая версия Elasticsearch дает ряд преимуществ, в частности — обеспечивает более высокую скорость работы с метаданными трафика.

> **Внимание!** Объединять в иерархию можно только экземпляры продукта, на которых установлена версия Elasticsearch 8.13. Если вы планируете использовать PT NAD в качестве дочерней системы, то вам нужно обновить его с переходом на новую версию Elasticsearch.

В этом разделе

9.1. Обновление PT NAD без перехода на новую версию Elasticsearch

► Чтобы обновить PT NAD без перехода на новую версию Elasticsearch:

1. Перейдите в каталог с распакованным дистрибутивом (см. раздел 6.3).

   Например:
   `cd /home/user/ptnad-installer`
2. Запустите мастер установки:
   `sudo ./install.sh`

   Начнется распаковка и подготовка файлов. По завершении подготовки откроется окно выбора языка мастера.
3. Выберите язык мастера установки и нажмите клавишу Enter.

4. Подтвердите ознакомление с лицензионным соглашением, выбрав **Ok** и нажав клавишу Enter.
5. Примите условия лицензионного соглашения, выбрав **Да** и нажав клавишу Enter.

   Мастер установки запустит обновление конфигурации и компонентов PT NAD.

   После обновления модуля ptdpi мастер сообщит об отсутствии или наличии на сервере сетевой карты NVIDIA Mellanox и предложит установить ее драйверы.

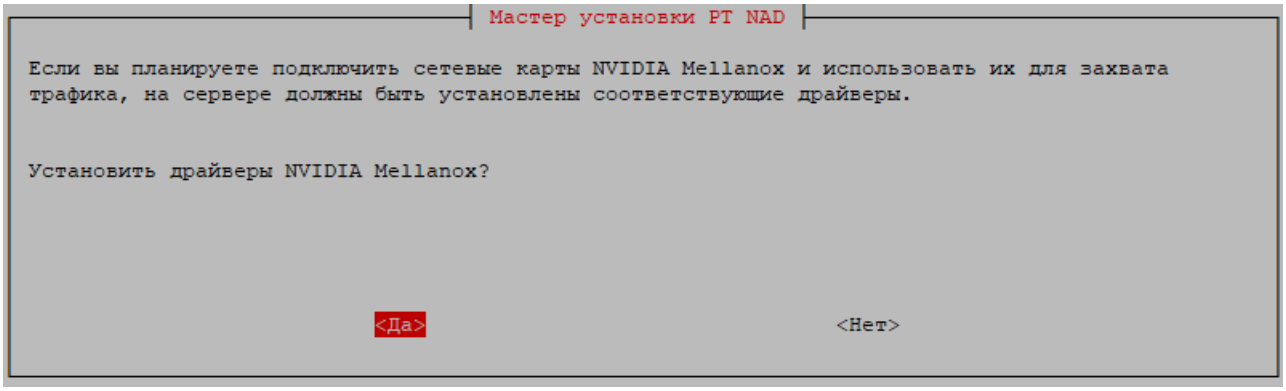

Рисунок 20. Проверка сетевой карты NVIDIA Mellanox

6. Если для захвата трафика планируется использовать интерфейсы сетевой карты NVIDIA Mellanox, выберите **Да** и нажмите клавишу Enter.

   Мастер продолжит обновление PT NAD. Если в конфигурационном файле `/opt/ptsecurity/etc/ptdpi.settings.yaml` в параметре `workers` не прописаны обязательные типы модулей ptdpi-worker, мастер установки предложит их добавить.

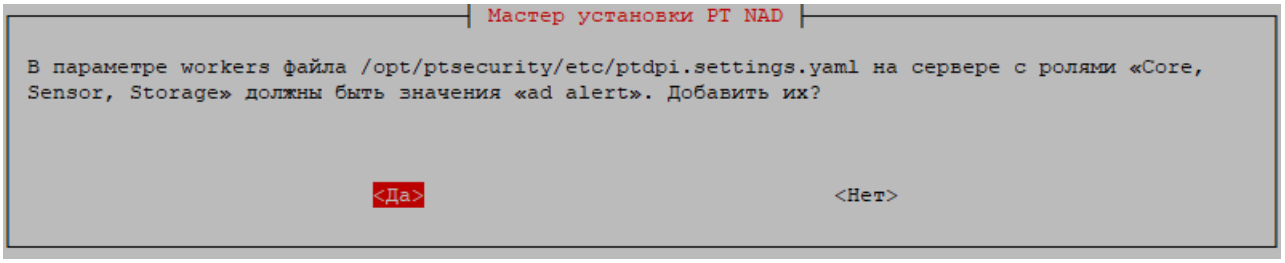

Рисунок 21. Исправление параметра `workers`

При возникновении этого вопроса нужно выбрать **Да** и нажать клавишу Enter.

По завершении обновления появится сообщение `<Время генерации сообщения> install.sh INFO: PT NAD components are updated successfully`.

9.2. Обновление PT NAD с переходом на новую версию Elasticsearch

- Чтобы обновить PT NAD с переходом на новую версию Elasticsearch:

1. Перейдите в каталог с распакованным дистрибутивом (см. раздел 6.3).

   Например:

   ```
   cd /home/user/ptnad-installer
   ```

2. Запустите мастер установки с ключом `--es-version 8`:

   ```
   sudo ./install.sh --es-version 8
   ```

   Начнется распаковка и подготовка файлов. По завершении подготовки откроется окно выбора языка мастера.

3. Выберите язык мастера установки и нажмите клавишу Enter.
4. Подтвердите ознакомление с лицензионным соглашением, выбрав **Ok** и нажав клавишу Enter.
5. Примите условия лицензионного соглашения, выбрав **Да** и нажав клавишу Enter.

   Мастер предложит заменить версию Elasticsearch на новую.

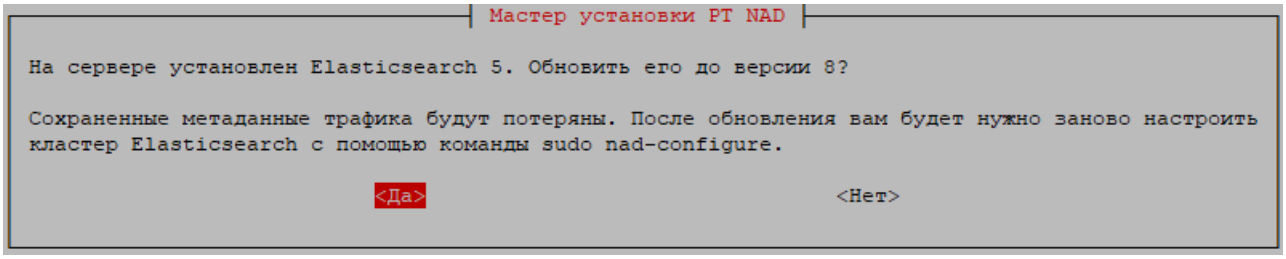

Рисунок 22. Предупреждение о переходе на новую версию Elasticsearch

6. Нажмите клавишу Enter.

   Внимание! База метаданных трафика будет очищена.

   Мастер установки запустит обновление конфигурации и компонентов PT NAD.

   После обновления модуля ptdpi мастер сообщит об отсутствии или наличии на сервере сетевой карты NVIDIA Mellanox и предложит установить ее драйверы.

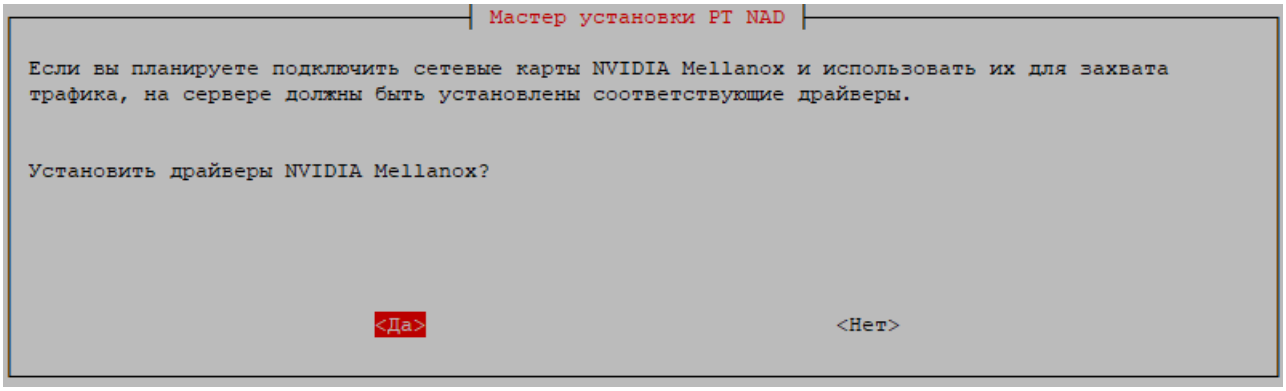

Рисунок 23. Проверка сетевой карты NVIDIA Mellanox

7. Если для захвата трафика планируется использовать интерфейсы сетевой карты NVIDIA Mellanox, выберите **Да** и нажмите клавишу Enter.

   Мастер продолжит обновление PT NAD. Если в конфигурационном файле `/opt/ptsecurity/etc/ptdpi.settings.yaml` в параметре `workers` не прописаны обязательные типы модулей ptdpi-worker, мастер установки предложит их добавить.

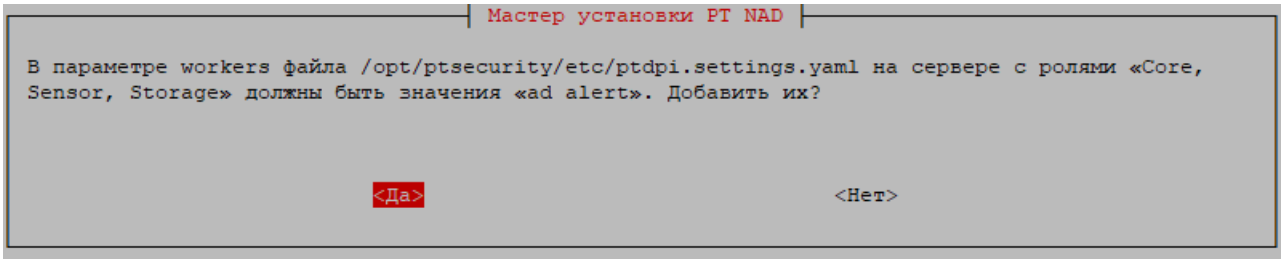

Рисунок 24. Исправление параметра `workers`

   При возникновении этого вопроса нужно выбрать **Да** и нажать клавишу Enter.

   По завершении обновления появится сообщение `<Время генерации сообщения> install.sh INFO: PT NAD components are updated successfully`.

8. Запустите мастер настройки:

   ```
   sudo nad-configure
   ```

   Появится приветственный экран мастера настройки PT NAD.

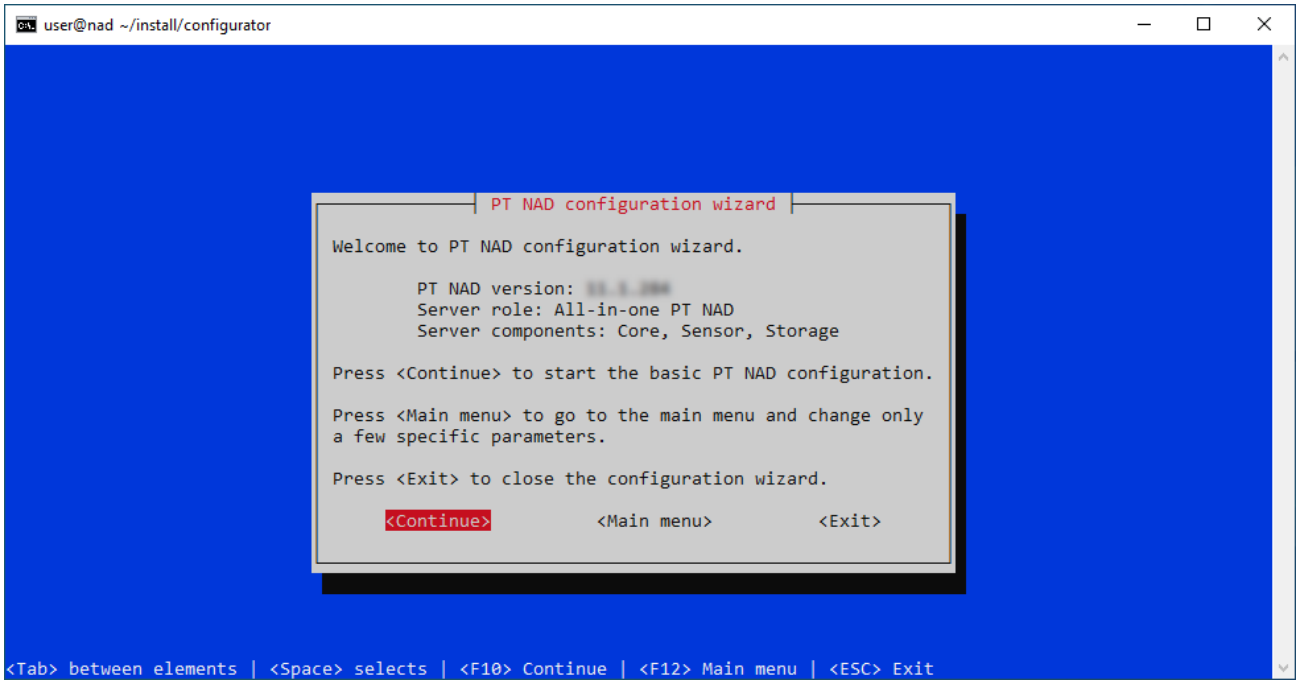

Рисунок 25. Приветственный экран мастера настройки PT NAD

9. Выберите вариант **Main menu** для перехода в главное меню мастера.
10. Выберите вариант **Elasticsearch settings**.
11. Выберите вариант **Elasticsearch cluster settings**.
12. Настройте кластер Elasticsearch (см. раздел 8.4).
13. Нажмите клавишу Esc для возврата в главное меню.
14. Выберите вариант **Save and exit** и подтвердите применение измененных параметров.

    Мастер применит новые параметры и перезапустит службы, необходимые для работы PT NAD.

    Когда мастер завершит работу, появится сообщение `[INFO] PT NAD configuration is finished`.

10. Интеграция с Zabbix

Zabbix — это программное обеспечение для мониторинга параметров, работоспособности и целостности компонентов PT NAD. Zabbix обеспечивает прозрачную отчетность и визуализацию состояния компонентов и использует гибкий механизм оповещений, что позволяет быть в курсе событий в работе PT NAD и быстро реагировать на возникающие проблемы.

PT NAD поддерживает интеграцию с Zabbix версий 3—5.4.

> **Примечание.** Подробная информация о системе Zabbix, инструкции по ее установке и настройке приведены на официальном сайте.

Интеграция Zabbix в PT NAD делится на следующие этапы:

1. Установка и настройка Zabbix.
2. Установка и настройка агента Zabbix на узлах с компонентами PT NAD (если вам нужно отслеживать работу операционной системы на этих узлах).
3. Запуск сервера Zabbix.
4. Загрузка шаблона продукта в Zabbix (см. раздел 10.1).
5. Настройка мониторинга узлов продукта в Zabbix (см. раздел 10.2).
6. Настройка передачи статистики на сервер Zabbix (см. раздел 10.3).

В этом разделе

10.1. Загрузка шаблона PT NAD в Zabbix

Мониторинг в Zabbix включает ряд проверок, которым подвергаются компоненты PT NAD. Результаты мониторинга представлены в виде, определяемом специальными шаблонами. Шаблон — это набор объектов (триггеры, графики, вложенные шаблоны и их группы), который может применяться к нескольким узлам в сети.

- Чтобы загрузить шаблон PT NAD в Zabbix:

  1. Скачайте шаблон PT NAD.

     Шаблон хранится на узле с установленным модулем ptdpistat в файле `/opt/ptsecurity/dpistat/templates/zabbix/zbx_template_ptnad.xml`.

  2. Войдите в веб-интерфейс Zabbix.
  3. В главном меню в разделе **Configuration** выберите пункт **Templates**.

Откроется страница **Templates**.

4. В правом верхнем углу страницы нажмите кнопку **Import**.

   Откроется форма загрузки шаблона в Zabbix.

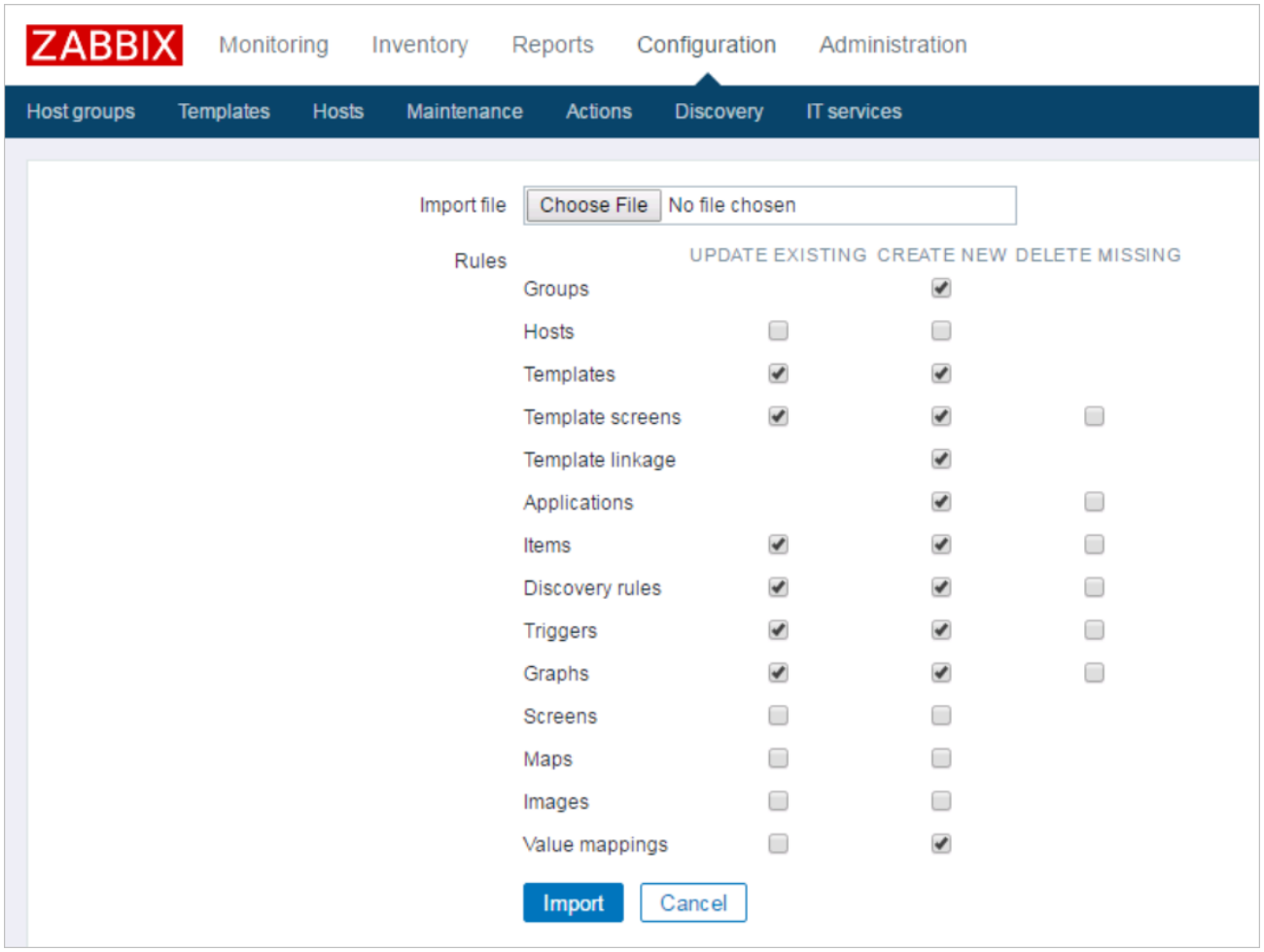

Рисунок 26. Загрузка шаблона в Zabbix

5. В поле **Import file** выберите файл шаблона, скачанный на шаге 1.
6. Нажмите кнопку **Import**, оставив остальные параметры без изменений.

Шаблон PT NAD загружен в Zabbix.

Теперь вам нужно привязать загруженный шаблон к каждому узлу PT NAD для мониторинга в Zabbix (см. раздел 10.2).

10.2. Настройка мониторинга узла PT NAD в Zabbix

Вам нужно настроить в Zabbix каждый из наблюдаемых узлов с компонентами PT NAD: привязать к нему шаблон PT NAD и добавить в группу.

► Чтобы настроить мониторинг узла PT NAD в Zabbix:

1. В главном меню в разделе **Configuration** выберите пункт **Hosts**.

   Откроется страница **Hosts** со списком узлов, состояние которых отслеживается в Zabbix.

2. Нажмите кнопку **Create host**.

   Откроется вкладка **Host** с параметрами мониторинга узла.

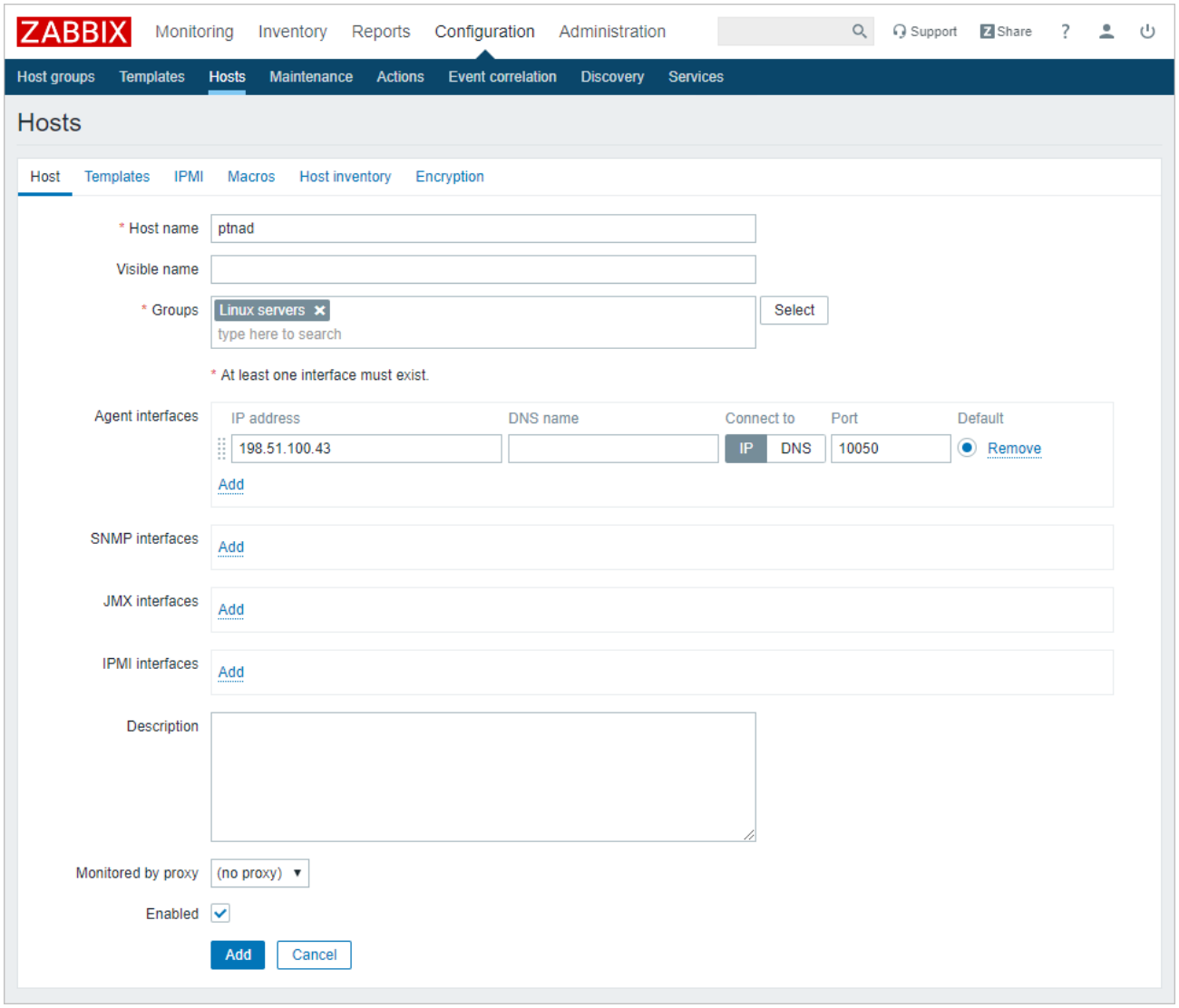

Рисунок 27. Настройка мониторинга узла в Zabbix

3. В поле **Host name** введите название узла (hostname) с установленным PT NAD.
4. В поле **Groups** начните вводить **Linux servers** и в раскрывающемся списке выберите название этой группы.

5. В группе параметров **Agent interfaces** в поле **IP address** введите IP-адрес узла с установленным PT NAD.

   Примечание. Если на сервере Zabbix настроено корректное соответствие IP-адресов и доменных имен, вы можете указать доменное имя узла с PT NAD вместо его IP-адреса и выбрать вариант **DNS**.

6. Выберите вкладку **Templates**.

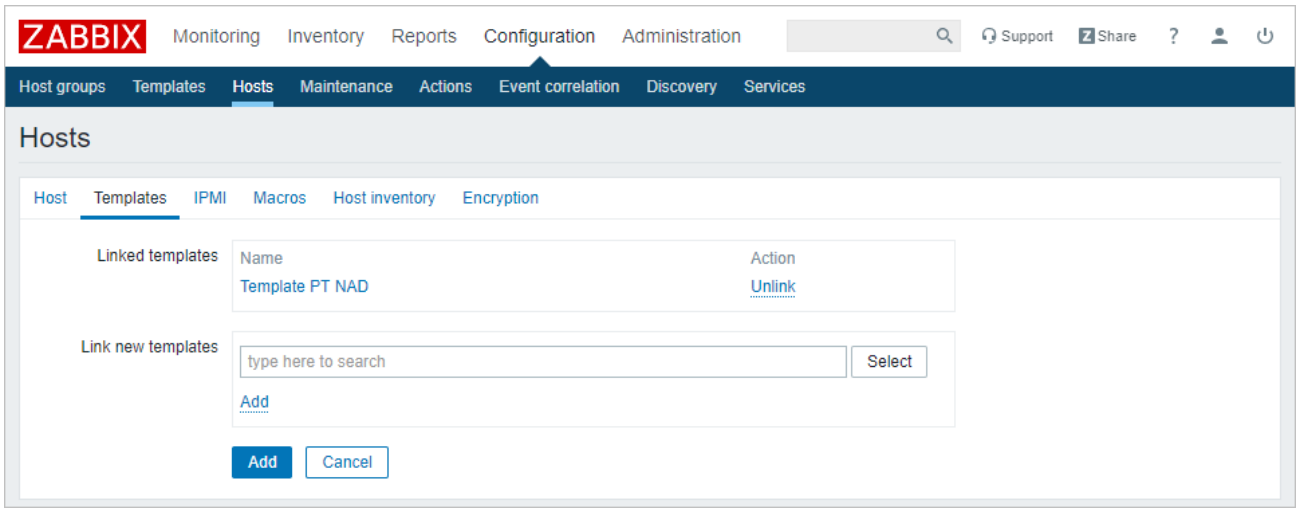

Рисунок 28. Привязка шаблона к узлу

7. В поле **Link new templates** введите `PT NAD` и в раскрывающемся списке выберите **Template PT NAD**.
8. По ссылке **Add** привяжите шаблон к узлу PT NAD.

   Шаблон **Template PT NAD** появится в списке **Linked templates**.

9. Нажмите кнопку **Add**.

   Откроется страница **Hosts** со списком узлов. В верхней части страницы появится уведомление Host added.

Мониторинг узла PT NAD в Zabbix настроен.

Теперь вы можете перейти к настройке передачи статистики в Zabbix.

10.3. Настройка передачи статистики в Zabbix

- Чтобы настроить передачу статистики в Zabbix:

1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

   ```
   sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
   ```

2. Раскомментируйте параметр `ptdpi.config.ZABBIX_SERVER` и в качестве его значения укажите адрес сервера Zabbix, на который нужно отправлять статистику.

Например:

```
ptdpi.config.ZABBIX_SERVER: 192.0.2.10
```

3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
4. Примените внесенные изменения:

   ```
   sudo /opt/ptsecurity/dpi/sync_configs.py
   ```

5. Перезапустите модуль ptdpistat:

   ```
   sudo systemctl restart ptdpistat.service
   ```

11. Интеграция с Graphite и Grafana

Graphite — это программное обеспечение для мониторинга параметров работоспособности и целостности компонентов компьютерных систем. Источником для мониторинга служат статистические данные за определенные промежутки времени. Graphite может принимать эти данные от PT NAD и записывать их на диск для дальнейшего построения графиков мониторинга в Grafana.

Grafana — веб-интерфейс для построения графиков мониторинга и анализа метрик. Grafana может получать данные для мониторинга из разных источников, в том числе из Graphite. В сценарии интеграции PT NAD с Graphite интерфейс Grafana используется вместо стандартного интерфейса Graphite.

Вы можете войти в интерфейс Grafana, нажав на индикатор состояния продукта и перейдя по ссылке **Мониторинг PT NAD** во всплывающем окне.

> **Примечание.** Чтобы у пользователя был доступ к интерфейсу Grafana, ему должна быть присвоена роль с привилегией на просмотр журнала аудита.

Рисунок 29. Мониторинг PT NAD в Grafana

12. Интеграция с внешней аналитической системой для проверки файлов

Вы можете настроить интеграцию PT NAD с внешней аналитической системой для проверки файлов, извлеченных из трафика. В качестве такой системы может выступать один из продуктов Positive Technologies: Positive Technologies MultiScanner (PT MultiScanner) или Positive Technologies Sandbox (PT Sandbox). При настроенной интеграции PT NAD отправляет извлеченные из трафика файлы на проверку во внешнюю аналитическую систему, которая возвращает результаты проверки в PT NAD. Информация об обнаруженных угрозах отображается в карточках сессий и атак, а также в таблицах сессий и атак в столбце с метками репутации.

Интеграция осуществляется по ICAP с помощью модуля ptdpi-worker@icap. Он является ICAP-клиентом, который отправляет извлеченные файлы ICAP-серверу внешней аналитической системы и получает от него результаты проверки файлов. Настройка интеграции выполняется в веб-интерфейсах PT NAD и внешней аналитической системы.

> **Примечание.** Если экземпляры PT NAD объединены в иерархию (см. раздел 3), то описанные в этом разделе возможности отсутствуют в интерфейсе центральной консоли.

В этом разделе

12.1. Настройка интеграции с внешней аналитической системой для проверки файлов

Перед настройкой интеграции вам или администратору внешней аналитической системы нужно установить и настроить ее ICAP-сервер. Вы можете найти подробную информацию об установке и настройке ICAP-сервера в документации к этой системе (PT Sandbox или PT MultiScanner).

Перед выполнением инструкции нужно указать адрес веб-интерфейса (см. раздел «Указание адреса веб-интерфейса PT NAD» в Руководстве администратора).

- Чтобы настроить интеграцию с внешней аналитической системой для проверки файлов:

  1. В главном меню выберите → **Центр управления**.
  2. Выберите вкладку **Интеграция с продуктами Positive Technologies**.

3. В блоке параметров **Интеграция с PT Sandbox или PT MultiScanner** по кнопке **Настроить** откройте окно **Настройка интеграции с PT Sandbox или PT MultiScanner**.
4. Включите интеграцию.
5. Выберите продукт, с которым вам нужна интеграция.
6. В поле **Адрес ICAP-сервера** укажите IP-адрес или доменное имя ICAP-сервера.
7. В поле **Порт ICAP-сервера** укажите порт для доступа к ICAP-серверу.
8. В параметре **Типы файлов для передачи на проверку** установите флажки напротив типов файлов (см. таблицу 2).

   Внешняя аналитическая система будет проверять только файлы, соответствующие выбранным типам.
9. Если требуется, по кнопке **Проверить соединение** запустите проверку соединения с ICAP-сервером.

   Отобразятся результаты проверки соединения.
10. Нажмите кнопку **Сохранить**.
11. Нажмите **Применить все** и подтвердите применение.

    Изменения будут применены через некоторое время.
12. Если вы поменяли адрес ICAP-сервера PT Sandbox уже после того, как интеграция с этой системой была настроена ранее, на узле с веб-интерфейсом обновите конфигурацию ссылок на внешние ресурсы:

    ```
    sudo /opt/ptsecurity/nad/bin/manage external_resources upsert
    ```

Таблица 2. Типы файлов

Типы файлов	MIME-типы	Расширения файлов
Исполняемые файлы	application/x-dosexec; application/x-executable; application/x-sharedlib	.com
Скрипты	—	.bat, .cmd
Java-файлы	application/java-archive; application/x-java-applet	—
Архивы	application/zip; application/gzip	—
Установщики программ Windows	application/x-msi	.msi
PDF-документы	application/pdf	—

Типы файлов	MIME-типы	Расширения файлов
Документы Microsoft Office	application/msword; application/msexcel; application/mspowerpoint; application/vnd.openxmlformats-officedocument	.doc, .docm, .docx, .dot, .dotm, .dotx, .xls, .xlsx, .xlsm, .xlsb, .xlt, .xltx, .xltm, .xlam, .ppt, .pptx, .pptm, .pps, .ppsx, .pot, .potx, .potm, .ppa, .ppam
Документы OpenOffice	—	.odt, .ods, .odp
Электронные письма	message/rfc822	.eml

12.2. Проверка интеграции с внешней аналитической системой для проверки файлов

Примечание. В многосерверной конфигурации инструкцию нужно выполнять на основном сервере.

- Чтобы проверить интеграцию с внешней аналитической системой для проверки файлов,

  выполните команду:

  ```
  sudo /opt/ptsecurity/icap-worker/bin/check-icap <Путь к файлу>
  ```

  Например:

  ```
  sudo /opt/ptsecurity/icap-worker/bin/check-icap /home/user/archive.tar.gz
  ```

  Если интеграция настроена правильно, PT NAD отправит указанный файл на проверку во внешнюю аналитическую систему. Результат проверки отобразится в выводе команды, например:

  ```
  {
    "type": "ms",
    "cat": "no_malware",
    "color": "0",
    "ref": "https://198.51.100.32/files/478064f5ea272e...4eaa86d501a",
    "sandbox": false
  }
  ```

13. Удаление PT NAD

В этом разделе приводится инструкция по удалению модулей PT NAD с помощью мастера удаления.

- Чтобы удалить PT NAD с помощью мастера:

  1. Перейдите в каталог с распакованным дистрибутивом (см. раздел 6.3).

     Например:

     ```
     cd /home/user/ptnad-installer
     ```

  2. Запустите мастер удаления:

     ```
     sudo ./uninstall.sh
     ```

     Откроется окно подтверждения удаления.

  3. Нажмите клавишу Enter.

     Мастер начнет процесс удаления PT NAD.

     По завершении удаления появится окно подтверждения перезагрузки сервера.

  4. Выберите **Да** и нажмите клавишу Enter.

     Появится сообщение `<Время генерации сообщения> uninstall.sh INFO: PT NAD has been successfully uninstalled`.

     Сервер перезагрузится.

     Примечание. Перезагрузить сервер можно позже вручную, выбрав **Нет** в окне подтверждения перезагрузки сервера.

14. О технической поддержке

Базовая техническая поддержка доступна для всех владельцев действующих лицензий на продукты Positive Technologies в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продуктов

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продуктов в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках технической поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продуктов.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продуктов в рамках выпуска обновленных версий продукта

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

Для получения технической поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг технической поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по технической поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по технической поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 3. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист технической поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

— предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение A. Настройка захвата трафика с использованием механизма AF_PACKET

По умолчанию модуль ptdpi подсистемы захвата использует механизм захвата трафика DPDK. Если по какой-то причине модуль ptdpi не может запуститься с DPDK, вы можете использовать для захвата трафика механизм AF_PACKET. Подробная информация о механизмах захвата трафика приведена в разделе «Механизмы захвата трафика» Руководства по проектированию.

Настройка захвата трафика с использованием механизма AF_PACKET делится на следующие этапы:

1. Обновление драйвера сетевой карты Intel (см. раздел A.1). Этот этап необходим, только если сетевой интерфейс для захвата трафика принадлежит сетевой карте Intel.
2. Смена механизма захвата трафика на AF_PACKET (см. раздел A.2).
3. Задание сетевого интерфейса для захвата трафика (см. раздел A.3).
4. Изменение количества потоков выполнения модуля ptdpi (см. раздел A.4).

В этом разделе

A.1. Обновление драйвера сетевой карты Intel

Для работы модуля ptdpi подсистемы захвата с механизмом захвата трафика AF_PACKET на сетевой карте Intel на сервере PT NAD должна быть установлена последняя версия драйвера сетевой карты.

Вы можете узнать название драйвера для вашей сетевой карты, выполнив команду `ptdpictl devlist`. В выводе команды название нужного вам драйвера пишется в поле `Driver`. Вы можете скачать драйверы igb, ixgbe и i40e с сайта Intel.

Скачанный архив драйвера нужно загрузить на сервер PT NAD.

- Чтобы обновить драйвер сетевой карты Intel:

  1. Распакуйте загруженный архив драйвера:

     ```
     tar pxf ./<Название архива>.tar.gz
     ```

Например:

```
tar pxf ./igb-5.3.6.tar.gz
```

2. Перейдите в каталог `src` распакованного архива:

   ```
   cd <Каталог с распакованным архивом>/src
   ```

   Например:

   ```
   cd igb-5.3.6/src
   ```

3. Установите пакет linux-headers для сборки драйвера:

   ```
   sudo apt-get install linux-headers-$(uname -r)
   ```

4. Скомпилируйте драйвер:

   ```
   make
   ```

5. Установите драйвер:

   ```
   sudo make install
   ```

6. Добавьте драйвер в инициализацию пользовательского пространства:

   ```
   sudo update-initramfs -u
   ```

7. Перезагрузите сервер PT NAD:

   ```
   sudo reboot now
   ```

Драйвер сетевой карты Intel обновлен.

Внимание! После каждого обновления ядра Linux нужно заново компилировать и устанавливать драйвер (для этого повторите инструкцию с шага 4).

A.2. Смена механизма захвата трафика на AF_PACKET

Модуль ptdpi подсистемы захвата PT NAD использует один из двух механизмов захвата трафика, по умолчанию — DPDK. Для использования AF_PACKET нужно сменить механизм захвата трафика в конфигурации продукта.

- Чтобы сменить механизм захвата трафика на AF_PACKET:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:

     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```

  2. В секции `Capture settings` в значении параметра `capture_type` укажите `af-packet`:

     ```
     capture_type: af-packet
     ```

  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.

  Механизм захвата трафика изменен.

A.3. Задание сетевых интерфейсов для захвата трафика при использовании AF_PACKET

Вам нужно указать названия сетевых интерфейсов, с которых модуль ptdpi будет захватывать трафик. Каждый подключаемый сетевой интерфейс должен принадлежать совместимой с модулем ptdpi сетевой карте (см. раздел «Требования модуля ptdpi к процессору и сетевой карте» в Руководстве по проектированию). Список сетевых интерфейсов можно получить с помощью команды `ptdpictl devlist`. В выводе команды название интерфейса пишется в поле `Linux if name`. В данном разделе приводится инструкция для механизма захвата трафика AF_PACKET.

- Чтобы задать сетевые интерфейсы для захвата трафика при использовании AF_PACKET:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
  2. В секции `Capture settings` в значении параметра `capture_if` через пробел задайте названия сетевых интерфейсов, трафик с которых нужно захватывать, например:
     ```
     capture_if: ens32 ens34
     ```
  3. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  4. Если захват трафика осуществляется при помощи технологии ERSPAN, в файле `/etc/network/interfaces` укажите IP-адрес сетевого интерфейса, на котором PT NAD должен принимать трафик, например:
     ```
     auto ens32
     iface ens32 inet static
     address 198.51.100.10
     netmask 255.255.255.0
     ```
     Внимание! После изменения файла `/etc/network/interfaces` перезапустите указанный сетевой интерфейс для применения новой конфигурации.
  5. Перезапустите модуль ptdpi:
     ```
     sudo ptdpictl restart
     ```

  Сетевые интерфейсы для захвата трафика заданы.

A.4. Изменение количества потоков выполнения модуля ptdpi при использовании AF_PACKET

Вы можете изменить количество потоков выполнения модуля ptdpi в соответствии с расчетами. В этом разделе приводится инструкция для механизма захвата трафика AF_PACKET.

- Чтобы изменить количество потоков выполнения модуля ptdpi:

  1. Откройте файл `/opt/ptsecurity/etc/ptdpi.settings.yaml`:
     ```
     sudo nano /opt/ptsecurity/etc/ptdpi.settings.yaml
     ```
     Дальнейшая настройка выполняется в секции `Capture settings`. Если необходимых параметров нет в этой секции, вам нужно будет их добавить.
  2. Если нужно изменить количество потоков захвата и обработки трафика, укажите новое количество в параметре `capture_channels`, например:
     ```
     capture_channels: 4
     ```
     Внимание! При использовании технологии ERSPAN совместно с механизмом захвата AF_PACKET сетевые пакеты от одного источника-коммутатора обрабатываются только одним логическим ядром процессора независимо от значения параметра `capture_channels`. Чтобы задействовать больше ядер, используйте технологию SPAN или смените механизм захвата на DPDK.

     Примечание. Максимально допустимое значение параметра при использовании AF_PACKET — 16.
  3. Если нужно изменить количество потоков обработки соединений, укажите новое количество в параметре `management_threads`, например:
     ```
     management_threads: 2
     ```
  4. Сохраните изменения в файле `/opt/ptsecurity/etc/ptdpi.settings.yaml`.
  5. Примените сетевые параметры модуля ptdpi:
     ```
     sudo ptdpictl restart-net
     ```
  6. Перезапустите модуль ptdpi:
     ```
     sudo ptdpictl restart
     ```

  Количество потоков выполнения модуля ptdpi изменено.

Глоссарий

PT NAD Sensor

Упрощенная версия PT NAD, которая используется для интеграции с MaxPatrol 10. Позволяет снизить требования к аппаратным ресурсам за счет отключения или ограничения функций, не имеющих значения для работы в MaxPatrol 10.

актив

Информация, ресурсы (финансовые, людские, вычислительные, информационные, телекоммуникационные и прочие), процессы, выпускаемая продукция, услуги или оборудование, имеющие ценность для организации и подлежащие защите от киберугроз.

атака

То же, что и кибератака.

вредоносное программное обеспечение

Программное обеспечение, которое разрабатывается для получения несанкционированного доступа к вычислительным ресурсам и данным, а также для нанесения ущерба путем копирования, искажения, удаления или подмены данных.

инвентаризация IT-активов

Сбор сведений об IT-активах для получения представления об IT-инфраструктуре организации.

инцидент ИБ

Событие (группа событий) информационной безопасности, которое может привести к нарушению функционирования IT-инфраструктуры или возникновению угроз безопасности обрабатываемой в ней информации.

исходная копия трафика

Сетевые данные, которые были захвачены модулем ptdpi и сохранены в хранилище файлов PCAP. Исходную копию трафика можно экспортировать в формате PCAP для ретроспективного анализа в PT NAD и импорта во внешние программы.

кибератака

Целенаправленное воздействие программных и (или) программно-аппаратных средств на IT-инфраструктуру и ее компоненты с целью нарушения (прекращения) ее функционирования или создания угрозы безопасности обрабатываемой в ней информации. Целями кибератаки могут быть, например, несанкционированный перевод денежных средств, нарушение или блокировка работы системы, получение несанкционированного доступа к инфраструктуре или хищение персональных данных.

ретроспективный анализ

Анализ данных с учетом изменения во времени, начиная от текущего момента времени к какому-либо прошедшему, для выявления закономерностей и построения гипотез.

угроза ИБ

Возможность нарушения информационной безопасности, в результате которого может быть нанесен ущерб организации или пользователю.