InfoWatch Data Discovery. Руководство пользователя

10/03/2022

Тел./Факс +7 (495) 229-00-22

http://www.infowatch.ru

СОДЕРЖАНИЕ

В настоящем руководстве вы сможете найти сведения по работе и решению задач в InfoWatch Data Discovery – программном обеспечении, предназначенном для сканирования информационных ресурсов с последующей их отправкой в InfoWatch Traffic Monitor.

Веб-консоль управления (далее Консоль управления) имеет интуитивно понятный интерфейс, поэтому настоящее руководство содержит только общую информацию и ряд примеров, представляющих функциональность Системы.

1 Аудитория

Информация, содержащаяся в Руководстве, предназначена для пользователей, работающих с Системой (выполняющих настройку конфигурации, анализ информационных ресурсов и т. п.). Руководство рассчитано на пользователей, знакомых с основами работы в среде операционных систем Linux и СУБД PostgreSQL.

2 Комплект документов

Кроме «InfoWatch Data Discovery. Руководство пользователя» в комплект документации входит «InfoWatch Data Discovery. Руководство по установке, конфигурированию и администрированию». Документ содержит описание установки и настройки Системы.
Сопутствующая документация по комплексу InfoWatch Traffic Monitor включает в себя:

- «InfoWatch Traffic Monitor. Руководство по установке». Содержит описание порядка установки, настройки, обновления и удаления Системы InfoWatch Traffic Monitor.
- «InfoWatch Traffic Monitor. Руководство администратора». Содержит информацию по администрированию Системы InfoWatch Traffic Monitor (база данных, серверная часть).
- «InfoWatch Traffic Monitor. Руководство пользователя». Содержит описание порядка работы с InfoWatch Traffic Monitor (настройка конфигурации, экспорт/импорт данных, подготовка политик для обработки объектов).
- «InfoWatch Traffic Monitor. Справочник по конфигурационным файлам». Содержит пояснения к часто используемым конфигурационным файлам.

3 Техническая поддержка пользователей

При возникновении проблем и вопросов, связанных с работой Системы, вы можете обратиться в службу технической поддержки:

- если вы приобрели продукт у партнера компании InfoWatch, то обратитесь в службу технической поддержки партнера.
- если продукт приобретен у компании InfoWatch напрямую, то обратитесь в службу технической поддержки компании InfoWatch по адресу support@infowatch.com.

Часы работы Службы технической поддержки – с 7:00 до 21:00 по московскому времени с понедельника по пятницу, исключая официальные выходные и праздничные дни в РФ. Вы также можете посетить раздел технической поддержки на нашем сайте: www.infowatch.ru/services/support.

4 Функциональные возможности Data Discovery

Используя Data Discovery, Вы можете:

- сканировать общие сетевые ресурсы по протоколу SMB;
- сканировать рабочие станции под управлением Linux по протоколу SSH;
- создавать копии файлов;
- отправлять файлы на сервер Traffic Monitor;
- обнаруживать и обрабатывать новые и измененные файлы на ресурсах с последующей их отправкой в Traffic Monitor;
- подготавливать и отображать статистику о выполнении задач сканирования.

5 Интерфейс Data Discovery

Основная работа с Системой ведется в разделе Задачи. Раздел содержит список задач сканирования и подробную информацию о каждой из них.

Следующие действия доступны при работе с разделом:

- создание новой задачи сканирования
- запуск и остановка задачи сканирования
- редактирование, копирование, и удаление существующих задач сканирования
- просмотр информации о задачах

В рамках каждой задачи возможна настройка подключения к **Хосту** – адресу сервера, рабочей станции в сети, используемой для сканирования и загрузки с нее копий файлов для последующего их анализа. Одна задача может иметь несколько хостов. Хост содержит список ресурсов, которые называются **Пути сканирования**.

Важно!

Перед тем, как приступить к работе с задачами сканирования, необходимо настроить синхронизацию с Traffic Monitor, а также добавить хранилища для временного хранения скачанных файлов перед отправкой в Traffic Monitor. Необходимые настройки описаны в следующих тематических разделах:

Экспорт данных

Хранение

5.1 Экспорт данных

Для настройки интеграции с Traffic Monitor нажмите  в правой верхней части экрана и перейдите в раздел **Настройки продукта** -> **Экспорт данных**.

Укажите следующие параметры:

1. **Версию ТМ** (Traffic Monitor) на сервере, синхронизацию с которым необходимо настроить. Для этого выберите **Версия 6.10** или **Версия 7.1 - 7.3**.

   Примечание:

   Для того, чтобы узнать номер версии ТМ, перейдите в Консоли управления Traffic Monitor в раздел **Офицер безопасности** -> **О системе**.

2. **Адрес XAPI сервера** Traffic Monitor в формате IP-адреса IPv4: "xxx.xxx.xxx.xxx".
3. В поле **Токен** укажите токен для подключения.

   Примечание:

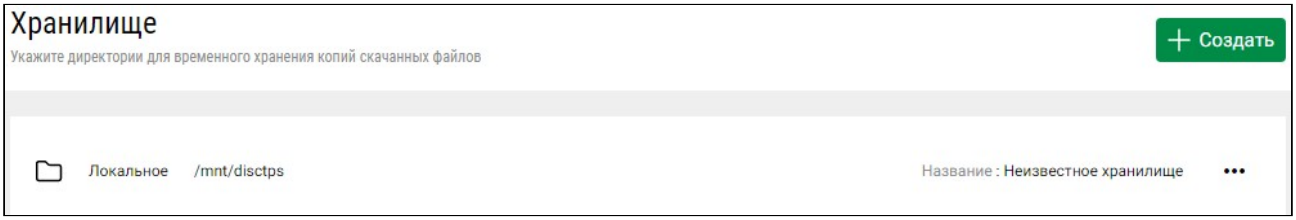
Чтобы скопировать токен для подключения, в Консоли управления Traffic Monitor перейдите в раздел **Управление** -> **Плагины**. Выберите в левой верхней части экрана предустановленный плагин InfoWatch Crawler и скопируйте предоставленный токен, нажав .

4. Укажите при необходимости комментарий.
5. Нажмите **Сохранить**.

5.2 Хранение

Для того чтобы настроить директории для временного хранения файлов перед отправкой в Traffic Monior, нажмите в правой верхней части экрана и перейдите в раздел **Настройки продукта** -> **Хранение**.

На экране вы увидите информацию о предустановленном локальном хранилище, созданном по умолчанию во время установки Системы. При необходимости данное хранилище может быть удалено.



Чтобы создать новое хранилище:

1. Нажмите **+Создать** в правой верхней области раздела.
2. Укажите Название хранилища.
3. В открывшемся окне укажите **тип** хранилища: **NFS** или **Локальное**.

> **Важно!**
>
> Создайте предварительно NFS хранилище для того, чтобы указать его в шаге 3 данной инструкции.

4. Если используете NFS хранилище, в строке **Адрес** укажите доменный или IP-адрес для подключения.
5. Укажите **Путь до папки временного хранения файлов** в формате /storage.
6. Нажмите **Сохранить**.

Вновь созданное хранилище будет добавлено в список.

Чтобы отредактировать хранилище:

1. Нажмите справа от хранилища, для которого требуется внести изменения.

> **Важно!**

Предустановленное локальное хранилище редактированию не подлежит.

2. Внесите все необходимые изменения.
3. Нажмите **Сохранить**.

Чтобы удалить хранилище:

1. Нажмите  справа от хранилища, которое требуется удалить и выберите **Удалить**.
2. Подтвердите действие.

6 Работа с задачами сканирования

Задача сканирования – уникальная и непрерывно повторяющаяся операция проверки указанных ресурсов (путей сканирования) на наличие конфиденциальных данных. О том, как определить конфиденциальные данные, см. "Traffic Monitor. Руководство пользователя", статья "Определение конфиденциальной информации".

Создав задачу, вы можете просканировать:

- общие сетевые ресурсы по протоколу SMB;
- файловые системы серверов и рабочих станций под управлением Linux по протоколу SSH.

> **Примечание:**
>
> Сканирование ресурсов возможно только при наличии соответствующих прав доступа у учетной записи, под которой Data Discovery подключается к ресурсу.

Следующие основные действия доступны при работе с задачами:

- Создание и запуск
- Редактирование
- Копирование
- Удаление

6.1 Создание и запуск задачи

> **Важно!**
>
> Перед созданием задачи сканирования необходимо убедиться, что в Системе выполнены настройки для отправки данных. Подробнее см. Экспорт данных.

Чтобы создать новую задачу сканирования:

1. Перейдите в раздел **Задачи**.
2. В левом верхнем углу нажмите **Создать задачу** ⊕ .
3. В открывшемся окне укажите параметры задачи:

Параметр	Описание
Название	Название задачи
Описание	Краткое описание задачи
Группа SMB	Домен или группа **Примечание:** Параметр используется для хостов с типом подключения SMB.

Параметр	Описание
Логин	Имя пользователя
Пароль	Пароль

Примечание:

Поля, обязательные к заполнению, отмечены значком *.

4. **Расширенные настройки** позволяют создать/настроить задачу сканирования с учетом особенностей вашей инфраструктуры, поэтому убедитесь, что указанные параметры корректны:

Параметр	Описание
Число сканеров	Количество сканеров (puller), используемых для выполнения задачи
Число передатчиков	Количество передатчиков (sender), используемых для завершения задачи по отправке данных в Traffic Monitor
Глубина обработки (в днях)	Размер окна сканирования ресурса. Если дата изменения файла не попадает в окно сканирования, то файл не будет обработан в текущую сессию. В первой сессии в рамках прохода в качестве окна сканирования устанавливается период от *Newest* до *Newest–Depth*, где: ▪ *Newest* – самая поздняя дата изменения у файлов на ресурсе; ▪ *Depth* – количество дней, указанное в параметре. В каждой следующей сессии в качестве окна сканирования устанавливается период от *Last* до *Last–Depth*, где: • *Last* – самая ранняя дата изменения у файлов, обработанных в предыдущую сессию; • *Depth* – количество дней, указанное в параметре. Новые файлы учитываются в **каждой** сессии. Параметр используется для равномерного сканирования ресурсов. Чем ниже значение, тем чаще сканер будет переключаться между ресурсами. **Пример использования параметра**

Параметр	Описание
	На ресурсе находятся 4 файла: • Файл A, дата изменения которого – 28.05.2021; • Файл B, дата изменения которого – 03.05.2021; • Файл C, дата изменения которого – 15.04.2021; • Файл D, дата изменения которого – 19.03.2021. Если значение параметра равно 30 дням, то: a. В первой сессии в рамках прохода в качестве окна сканирования устанавливается период 28.05.2021 – 28.04.2021. Обрабатывается файл A и файл B. Сканер переключается на другой ресурс. b. Во второй сессии в качестве в качестве окна сканирования устанавливается период 02.05.2021 – 02.04.2021. Обрабатывается файл C. Сканер переключается на другой ресурс. c. В третьей сессии в качестве окна сканирования устанавливается период 14.04.2021 – 15.03.2021. Обрабатывается файл D. Проход по ресурсу завершается.
Длительность обработки (в минутах)	Максимальная длительность сессии при обработке ресурса. По истечении времени, указанного в параметре, обработка ресурса будет приостановлена, сканер начнет обработку следующего ресурса. Параметр используется для равномерного сканирования ресурсов. Чем ниже значение, тем чаще сканер будет переключаться между ресурсами. **Примечание**: Когда сканер повторно дойдет до ресурса, обработка которого была приостановлена по истечении максимального времени, обработка продолжится с того места, где она была приостановлена в предыдущую сессию.
Хранилища	Директории для временного хранения копий сканированных файлов перед отправкой в Traffic Monitor. Доступен выбор директорий. Подробнее см. Хранение
Дополнительно проверять неизмененные файлы	По умолчанию для файлов, которые были обработаны во время предыдущего прохода, сканер проверяет только метаданные. Если метаданные файла не изменились, то файл не будет обработан повторно.

Параметр	Описание
	Если данный параметр включен (), то при каждой обработке ресурса сканер будет скачивать файл и проверять содержимое файла на наличие изменений. Это позволяет выявить файлы, у которых изменилось содержимое, но не изменились метаданные. **Примечание:** Если данный параметр включен (), то увеличится объем трафика и время, требуемое для повторной обработки ресурса.

5. Поле **Форматы файлов** содержит форматы файлов, которые будут просканированы и отправлены в Traffic Monitor. Определите те, которые вам нужны, удалив лишние. Это можно сделать, нажав  справа от ненужного формата. Также вы можете добавить необходимые вам форматы, нажав  и используя маску файлов "*.".

> **Важно!**
>
> Если в поле **Форматы файлов** не указать ни один из форматов файлов, Система станет сканировать все файлы в указанных директориях, включая системные файлы и пр. В результате отправки всех сканированных файлов на сервер Traffic Monitor нагрузка на Систему может значительно повыситься, что может сказаться на ее работоспособности.

> **Примечание:**
>
> Фильтр по форматам файлов не учитывает регистр.

6. При необходимости укажите пороговые значения для сканируемых файлов, заполнив поля **Минимальный размер** и **Максимальный размер** (в байтах).
7. Нажмите **Сохранить**.

Чтобы добавить хост / импортировать список хостов:

1. Нажмите левой клавишей мыши в области созданной задачи.
2. На открывшейся странице в левом верхнем углу меню **Управление хостами** нажмите:
   a.  , если требуется добавить новый хост;
   b.  , если необходимо импортировать список существующих хостов. Для этого в открывшемся окне укажите файл, содержащий список хостов.

> **Примечание:**
>
> Для импорта списка хостов используйте файл с расширением .txt, в котором данные о каждом хосте указаны на отдельной строке. Данные о хосте могут быть представлены в формате IP-адреса рабочей станции или, как полное имя домена (FQDN).

Важно!

При импорте всем хостам указывается тип подключения SMB по умолчанию.

3. При добавлении хоста в открывшемся окне укажите его параметры:

Параметр	Описание
Тип подключения	Доступные значения: • SMB – для сканирования общих сетевых ресурсов; • SSH – для сканирования серверов и рабочих станций под управлением Linux. **Примечание:** Изменение данного параметра недоступно при редактировании хоста.
Адрес	Доменное имя или IP-адрес рабочей станции
Порт	Порт подключения Если порт подключения не указан, то используется значение по умолчанию: • для SMB подключения – 445; • для SSH подключения – 22.
Описание	Краткое описание хоста

4. В **Параметрах авторизации** укажите следующее:

Параметр	Описание
Группа SMB	Домен или группа **Примечание:** Параметр доступен, если тип подключения хоста – SMB.
Логин	Имя пользователя
Пароль	Пароль

Примечание:

В случае если не указаны параметры авторизации для хоста, то при выполнении задачи сканирования будут учитываться параметры, указанные при создании задачи.

5. **Расширенные настройки** позволяют создать/настроить задачу сканирования с учетом особенностей вашей инфраструктуры, поэтому убедитесь, что указанные параметры корректны:

Параметр	Описание
Тайм-аут (мс)	Тайм-аут подключения к хосту
Попыток повторения	Максимальное количество попыток соединения
Уровень отладки	Степень подробности представления отладочной информации в библиотеке smbclient. Принимает значения от 0 до 10. Чем выше значение, тем подробнее отладочная информация. Для повседневного использования рекомендуется значение 1. Для изучения возникающих проблем рекомендуется использовать значение 2. Подробнее см. документацию smbclient (параметр debuglevel). **Примечание:** Параметр используется для хостов с типом подключения SMB.
Пауза до повтора (сек)	Временной интервал между попытками соединения
Размер чанка (байт)	Размер фрагмента передаваемых данных

6. Чтобы добавить **Путь сканирования**, укажите его в поле, после чего нажмите  :
   - Для хоста с типом подключения SMB укажите имя общего сетевого ресурса, например: **share**.

     Примечание:

     Для SMB хостов не поддерживается возможность указать поддиректорию сетевого ресурса (например: /share/folder) в качестве пути сканирования.

   - Для хоста с типом подключения SSH укажите полный путь к директории, например: **/home/username/Documents**.
7. В случае, когда пути сканирования неизвестны, вы можете воспользоваться функцией их определения. Для этого после выполнения шага 8 нажмите  в меню **Управление хостами**.

   Важно!

   Определение путей сканирования недоступно для хостов с типом подключения SSH.

   Определение путей сканирования выполняется только для тех хостов, у которых пути сканирования не указаны.

8. Нажмите **Сохранить**.

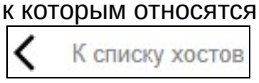
Возможности работы с хостами

Хост – адрес сервера, рабочей станции в сети. Для просмотра хоста или списка хостов задачи, нажмите на задачу левой клавишей мыши.

> **Примечание:**
>
> К действиям с хостами относятся редактирование  и удаление  . Они могут быть доступны только если задача не выполняется.

Для вашего удобства в верхней части экрана со списком хостов доступно управление задачей, к которой относятся хосты: ее можно остановить для редактирования, отредактировать и удалить.

Нажав на хост левой клавишей мыши, вы сможете видеть список **Путей сканирования** хоста.

В верхней части экрана со списком путей сканирования доступно меню управления хостом и задачей, к которым относятся пути сканирования из списка. Для возвращения к списку хостов нажмите 

в левой верхней части экрана.

Чтобы запустить задачу сканирования:

Для запуска новой задачи нажмите  в меню управления задачей. При этом статус задачи Новая изменится на Выполняется, индикатор с желтого цвета изменится на зеленый, а кнопка запуска задачи изменится на  , что позволит остановить выполнение задачи для редактирования.

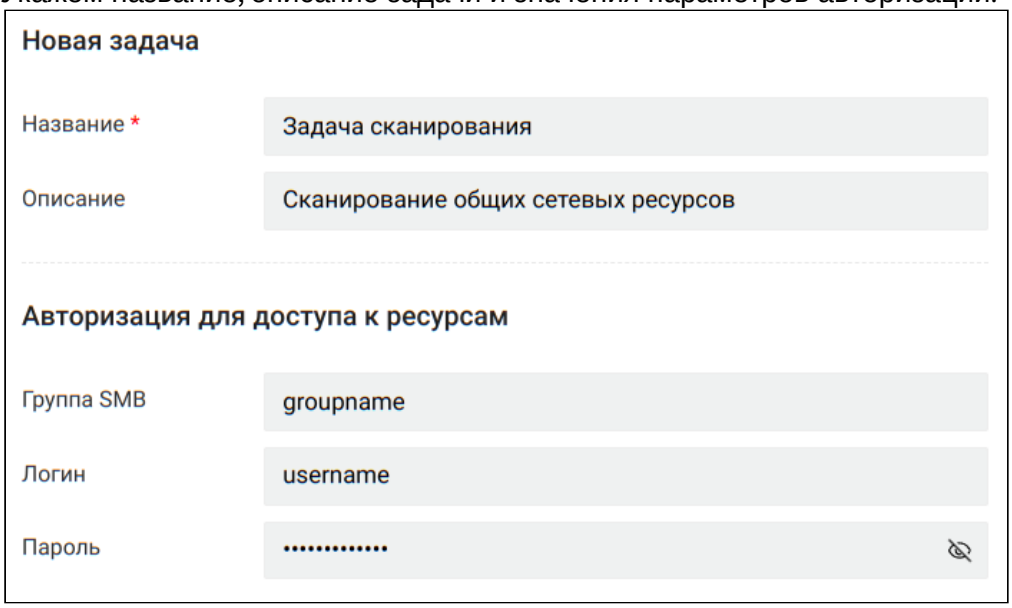
> **Примечание:**
>
> Выполнение задачи сканирования после ее запуска происходит циклично. Т.е. после сканирования хоста/пути задача не завершается, а начинается повторное сканирование с целью обнаружения новых и/или измененных файлов. Повторное сканирование будет продолжаться до тех пор пока вы не остановите задачу, нажав  .

Подробнее о запущенной задаче можно узнать, просмотрев Статистику выполнения.

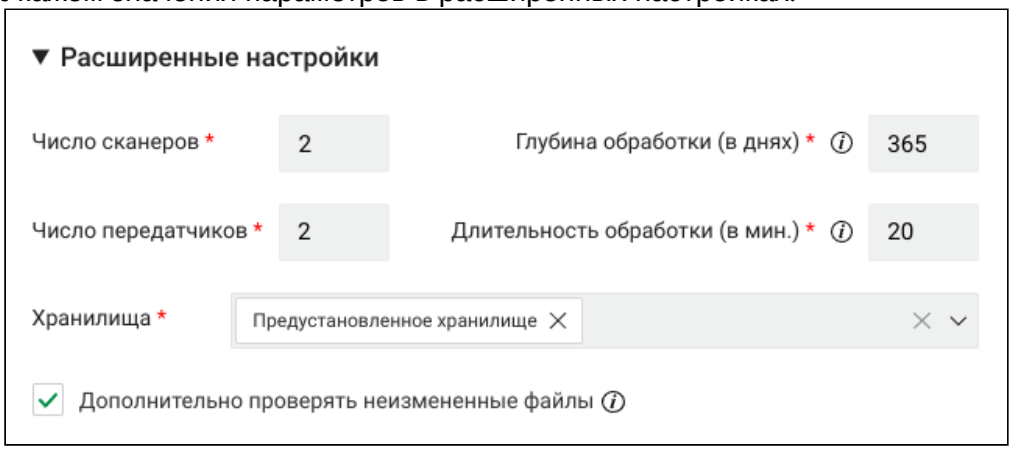
Пример создания задачи и добавления хоста

Создадим задачу, для этого:

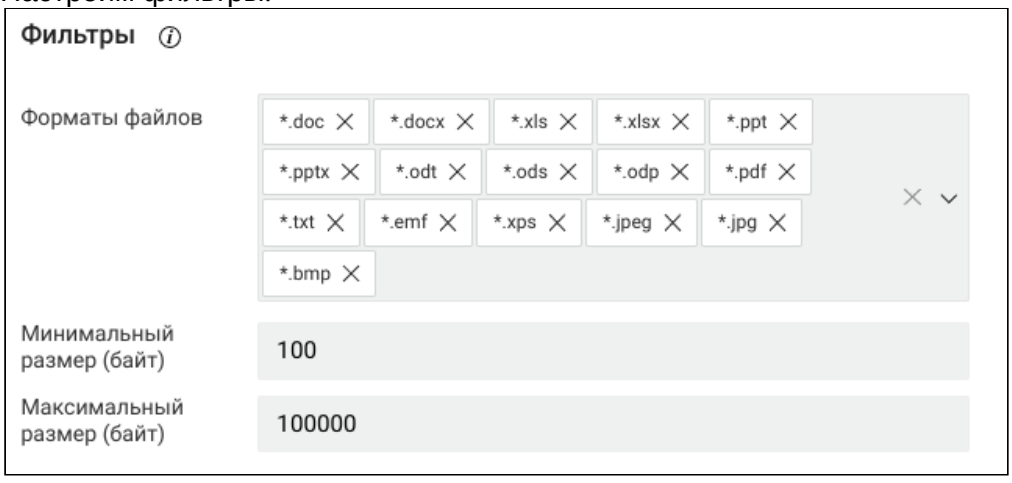
1. Укажем название, описание задачи и значения параметров авторизации:



2. Укажем значения параметров в расширенных настройках:



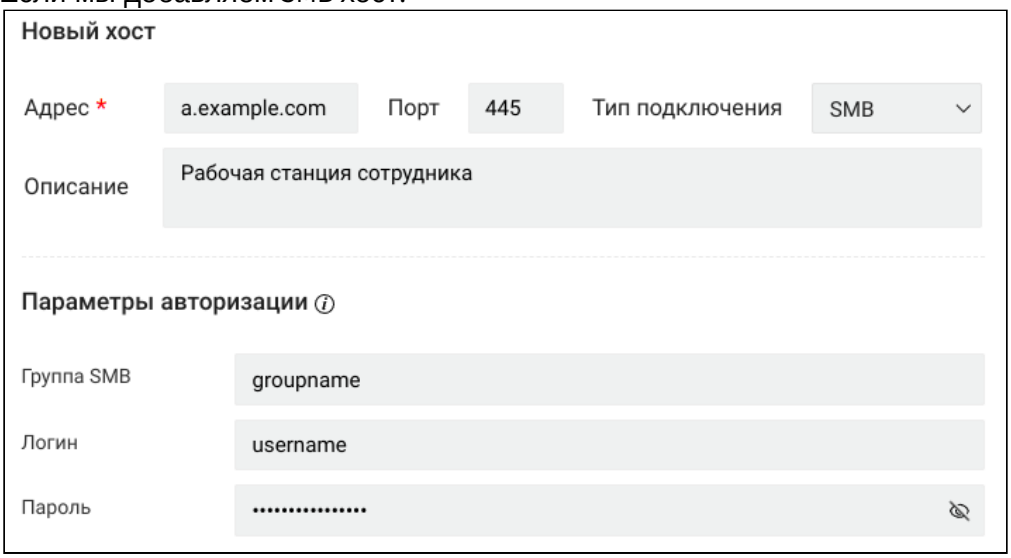
3. Настроим фильтры:



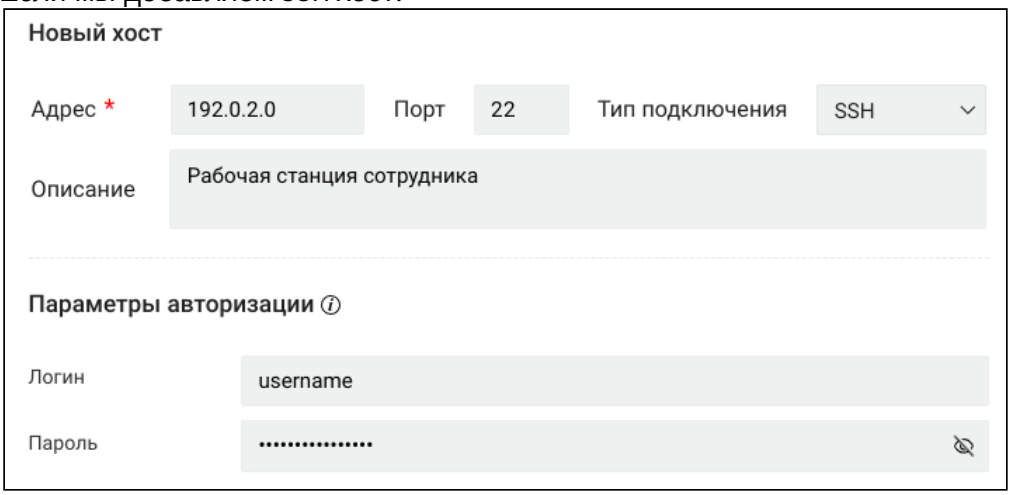
Добавим хост, для этого:

1. Укажем значения параметров для подключения к хосту:

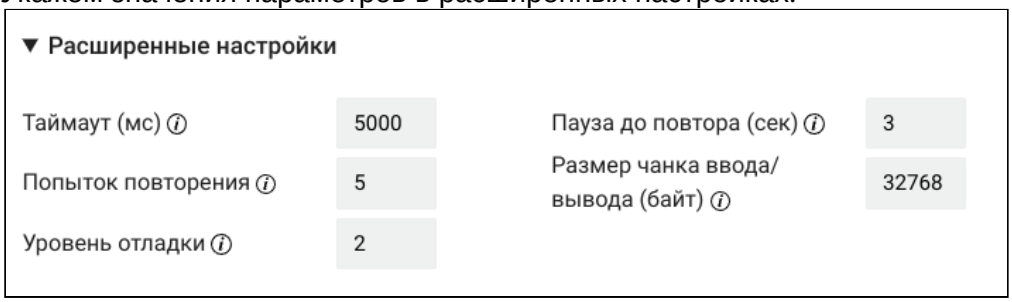
- Если мы добавляем SMB хост:



- Если мы добавляем SSH хост:



2. Укажем значения параметров в расширенных настройках:

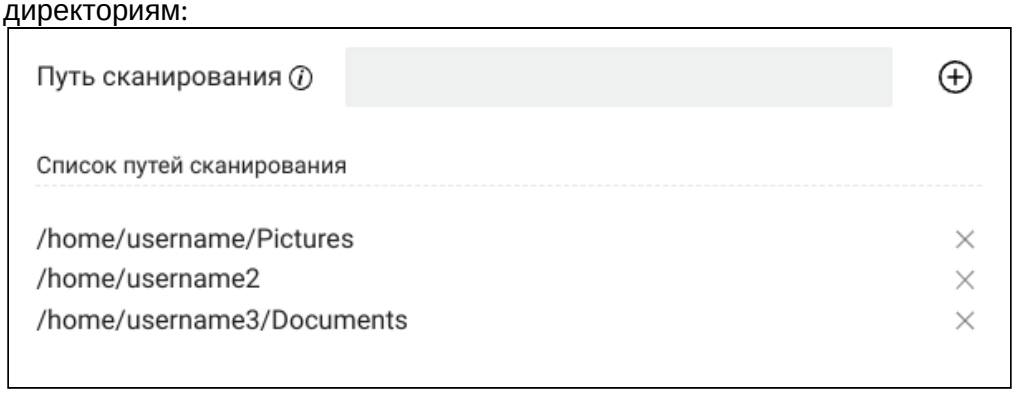


3. Добавим пути сканирования:
   - Если мы добавляем SMB хост, то в качестве путей сканирования укажем имена сетевых ресурсов:

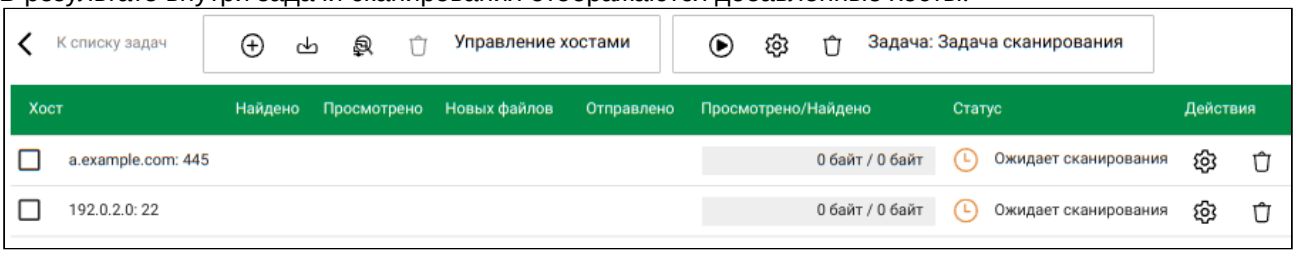
Примечание:

Не поддерживается возможность указать поддиректорию сетевого ресурса (например: /share/folder) в качестве пути сканирования.

- Если мы добавляем SSH хост, то в качестве путей сканирования укажем пути к директориям:



В результате внутри задачи сканирования отображаются добавленные хосты:



6.2 Редактирование задачи и хоста

Перед тем как приступить к редактированию задачи, убедитесь, что задача остановлена. Вновь созданную задачу можно редактировать до момента запуска сканирования.

Важно!

Для задач со статусом Выполняется функция редактирования недоступна.

Чтобы отредактировать задачу:

1. Перейдите в раздел **Задачи**.
2. Справа напротив задачи, которую требуется отредактировать, нажмите  .
3. При редактировании ранее созданной задачи, как и при создании новой, отображается диалоговое окно, в котором вы можете изменить параметры задачи, где это необходимо.

> **Важно!**
>
> Если при редактировании задачи в поле **Форматы файлов** не указать ни один из форматов файлов, Система станет сканировать все файлы в указанных директориях, включая системные файлы и пр. В результате отправки всех сканированных файлов на сервер Traffic Monitor нагрузка на Систему может значительно повыситься, что может сказаться на ее работоспособности.

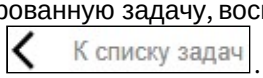
4. Нажмите **Сохранить** после внесения изменений.

Чтобы отредактировать хост в задаче:

1. Нажмите левой клавишей мыши на задаче, хост которой подлежит редактированию.

> **Примечание:**
>
> Вы можете отредактировать хост только при условии, что задача **не выполняется**.

2. При редактировании ранее созданного хоста, как и при добавлении нового, отображается диалоговое окно, в котором вы можете изменить параметры, где это необходимо.
3. Нажмите **Сохранить** после внесения изменений.

Вы можете запустить отредактированную задачу, воспользовавшись меню в верхней части экрана или вернуться к списку задач, нажав 

.

6.3 Копирование задачи

Чтобы скопировать задачу:

1. Перейдите к списку задач в разделе **Задачи**.
2. Нажмите  в правой части экрана напротив задачи, копия которой вам нужна.

В списке задач сразу же отобразится скопированная задача, содержимое которой будет соответствовать оригинальной, а название будет отличаться добавлением "Копия".

Скопированная задача будет иметь статус **Новая** с индикатором желтого цвета до момента ее запуска.

> **Важно!**
>
> При запуске скопированной задачи осуществляется полное (повторное) сканирование ресурсов.

6.4 Удаление задачи и хоста

Чтобы удалить задачу:

1. Перейдите к списку задач в разделе **Задачи**.
2. Нажмите  в правой части экрана напротив задачи, которую необходимо удалить.

   > **Важно!**
   >
   > Для задач со статусом Выполняется функция удаления недоступна.

3. Подтвердите удаление, нажав **Ok**.

Чтобы удалить хост в задаче:

1. Перейдите к списку хостов, нажав левой клавишей мыши на задаче сканирования.
2. Нажмите  справа от хоста, который необходимо удалить.
3. Если требуется удалить несколько хостов одновременно, отметьте слева от каждого из них  и нажмите  в меню **Управление хостами**.

   > **Важно!**
   >
   > Вы можете удалить хост только при условии, что задача не выполняется.

4. Подтвердите удаление, нажав **Ok**.

Для возврата к списку задач, нажмите 

в верхней части экрана.

7 Статистика выполнения задач

Для представления полной информации о выполнении каждой задачи в Системе представлена статистика, которая доступна в разделе Задачи. Навигация по страницам списка задач осуществляется с помощью панели навигации, расположенной внизу экрана. Статистика по задачам включает в себя следующие данные:

Параметр	Описание
Имя	Отображает название задачи
Описание	Краткое описание задачи сканирования
Дата запуска	Дата и вермя запуска задачи, отображается в формате DD.MM.YY HH.MM.SS
Дата остановки	Дата и время остановки задачи, отображается в формате DD.MM.YY HH.MM.SS. Данные отсутствуют для задачи в статусе Выполняется
Найдено	Число файлов, найденных на всех ресурсах задачи / общий объем найденных файлов (с учетом фильтра)
Отправлено	Число файлов, отправленных в Traffic Monitor / общий объем отправленных файлов
Статус	Текущий статус задачи: • Новая • Выполняется • Остановлена • Определение путей сканирования
Действия	Следующие действия доступны для задач:  - Запустить задачу (доступно для задач со статусами Новая и Остановлена)  - Копировать задачу (доступно для задач с любым статусом)  - Редактировать (доступно для задач со статусами Новая и Остановлена, после запуска задачи вы можете ее Оставить для редактирования, нажав )  - Удалить (доступно для задач с любым статусом, кроме Выполняется)

Сортировка списка задач возможна по следующим столбцам: *Имя, Дата запуска, Дата остановки, Статус*. Чтобы изменить порядок сортировки строк в списке задач, щелкните левой клавишей мыши по заголовку того столбца, по которому нужно выполнить сортировку.

Для просмотра статистики по **Хостам**, нажмите левой клавишей мыши на задачу. Навигация по страницам списка хостов осуществляется с помощью панели навигации, расположенной внизу экрана. Статистика содержит информацию вида:

Параметр	Описание
Хост	Отображает адрес хоста
Найдено	Число файлов, найденных на каждом хосте задачи / общий объем файлов, найденных на хосте (с учетом фильтра)
Просмотрено	Число обработанных файлов / общий объем обработанных файлов
Новых файлов	Число новых или измененных файлов на ресурсах хоста (с учетом фильтра, с момента последней сессии подключения)
Отправлено	Число файлов, отправленных в Traffic Monitor / общий объем отправленных файлов
Просмотрено/Найдено	Отображает соотношение найденных и обработанных файлов
Статус	Текущий статус хоста:  - Ожидает сканирования  - Нет доступа  - Идет сканирование
Действия	 - Редактировать (доступно для задач со статусами Новая и Остановлена, после запуска задачи вы можете ее Оставить для редактирования, нажав)  - Удалить (доступно для задач с любым статусом, кроме Выполняется)

Сортировка списка хостов возможна по следующим столбцам: *Хост, Статус*. Чтобы изменить порядок сортировки строк в списке хостов, щелкните левой клавишей мыши по заголовку того столбца, по которому нужно выполнить сортировку.

Для просмотра статистики по **Путям сканирования**, нажмите левой клавишей мыши на хост. Навигация по страницам списка путей сканирования осуществляется с помощью панели навигации, расположенной внизу экрана. Для пути сканирования статистика содержит информацию вида:

Параметр	Описание
Точка подключения	Отображает имя ресурса
Дата последнего сканирования	Дата и время последнего подключения к ресурсу, отображается в формате DD.MM.YY HH.MM.SS
Найдено	Число файлов, найденных по указанному пути сканирования / общий объем найденных файлов (с учетом фильтра)
Просмотрено	Число обработанных файлов / общий объем обработанных файлов
Новых файлов	Число новых или измененных файлов на ресурсе (с учетом фильтра, с момента последней сессии подключения)
Отправлено	Число файлов, отправленных в Traffic Monitor / общий объем отправленных файлов
Просмотрено/Найдено	Отображает соотношение найденных и обработанных файлов
Статус	Текущий статус пути сканирования:  - Ожидает сканирования  - Нет доступа  - Идет сканирование

Сортировка списка путей сканирования возможна по следующим столбцам: *Точка подключения, Статус*. Чтобы изменить порядок сортировки строк в списке путей сканирования, щелкните левой клавишей мыши по заголовку того столбца, по которому нужно выполнить сортировку.

8 Лицензионная информация

Лицензионная информация для Системы доступна в разделе "Пользовательское лицензионное соглашение".

8.1 Пользовательское лицензионное соглашение

ВНИМАНИЕ! Внимательно ознакомьтесь с условиями лицензионного соглашения перед началом работы с программным обеспечением.
Нажатие Вами кнопки подтверждения согласия в окне с текстом лицензионного соглашения при установке программного обеспечения или использование устанавливаемого программного обеспечения означает Ваше безоговорочное согласие с условиями настоящего лицензионного соглашения. Если Вы не согласны с условиями настоящего лицензионного соглашения, Вы должны прервать установку и/или использование программного обеспечения.

1. Предоставление лицензии.

1.1. Вам предоставляется неисключительная лицензия на использование программного обеспечения (далее — ПО) (Правообладатель прав на ПО — ООО «Лаборатория ИнфоВотч») в рамках функциональности, описанной в Документации к ПО (Руководство Пользователя, Руководство Администратора, Руководство по Установке), при условии соблюдения Вами всех технических требований, описанных в Документации к ПО, а также всех ограничений и условий использования ПО, указанных в настоящем Соглашении и Договоре, заключенном между Вами и Вашим лицензиаром.

1.2. В случае если Вы получили, загрузили и/или установили ПО, предназначенное для ознакомительных целей, Вы имеете право использовать ПО только в целях ознакомления и только в течение ознакомительного периода. Любое использование ПО для других целей или по завершении ознакомительного периода запрещено.

1.3. Если Вы используете ПО разных версий или версии ПО для разных языков, если Вы получили ПО на нескольких носителях, если Вы иным способом получили несколько копий ПО или получили ПО в составе пакета другого программного обеспечения, то общее число используемых вами лицензий, не должно превышать их количества определенного Договором между Вами и Вашим лицензиаром;

1.4. Вы имеете право изготовить копию ПО при условии, что эта копия предназначена только для архивных целей и для замены правомерно приобретенного экземпляра в случаях, когда оригинал утерян, уничтожен или стал непригоден для использования. Такая копия не может быть использована для иных целей и должна быть уничтожена в случае, если владение экземпляром ПО перестанет быть правомерным.

1.5. Вы самостоятельно несете ответственность и обеспечиваете соблюдение применимого экспортного и импортного законодательства, а также применимых торговых санкций и эмбарго в отношении передачи прав и использования ПО.

2. Ограничения.

2.1. Вы не вправе декомпилировать, дизассемблировать, модифицировать или выполнять производные работы, основанные на ПО, целиком или частично, за исключением случаев, предусмотренных законодательством РФ.

2.2. Вам запрещается передавать право на использование ПО третьим лицам.

2.3. Запрещается передавать и предоставлять доступ к лицензионному ключу третьим лицам в нарушение положений настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром. Лицензионный ключ является конфиденциальной информацией. Правообладатель оставляет за собой право использовать средства для проверки подлинности установленного у Вас лицензионного ключа.

2.4. Запрещается сдавать ПО в аренду, прокат или во временное пользование, а также разглашать результаты стендовых испытаний ПО.

2.5. Правообладатель имеет право заблокировать лицензионный ключ в случае нарушения Вами условий настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром.

2.6. За нарушение интеллектуальных прав на ПО нарушитель несет гражданскую, административную или уголовную ответственность в соответствии с законодательством.

2.7. Вы не вправе использовать ПО для любых целей или способом, ограниченным или запрещенным применимым законодательством. Вы самостоятельно несете ответственность за неправомерное использование ПО.

2.8. В случае нарушения Вами какого-либо из условий данного Соглашения или Договора, заключенного между Вами и Вашим лицензиаром, Правообладатель или Ваш лицензиар вправе прервать действие лицензии на использование ПО в любое время без уведомления Вас и без возмещения стоимости ПО или его части.

3. Ограниченная гарантия и отказ от предоставления гарантий.

3.1. Правообладатель гарантирует работу ПО в соответствии с описанием, изложенным в Документации к ПО.

3.2. Вы соглашаетесь с тем, что никакое ПО не свободно от ошибок и Вам рекомендуется регулярно создавать резервные копии своих файлов.

3.3. Правообладатель не гарантирует работоспособность ПО при нарушении условий, описанных в Документации к ПО, а также в случае нарушения пользователем условий настоящего Соглашения и Договора, заключенного между Вами и Вашим лицензиаром.

3.4. За исключением устанавливаемой в настоящем пункте ограниченной гарантии, ПО поставляется «как есть». Правообладатель не дает никаких гарантий и не несет никакой ответственности перед Вами в случае любых изменений в программном обеспечении третьих лиц, произошедшее после установки/внедрения ПО и повлекшее потерю функциональности ПО (включая, но не ограничиваясь, изменением протокола передачи данных, формата хранения данных, логике работы стороннего программного обеспечения, обновлением программного обеспечения, которое перестает поддерживать работу с ПО). Правообладатель не дает никаких гарантий, условий, представлений или положений (выражаемых в явной или в подразумеваемой форме) на все, включая без ограничений нарушения прав третьих лиц, коммерческое качество, интеграцию или пригодность для определенных целей. Пользователь соглашается с тем, что он несет ответственность за выбор ПО для достижения нужных результатов, за установку и использование ПО, а также за результаты, полученные с его помощью.

4. Ограничение и пределы ответственности Правообладателя.

Правообладатель не несет ответственности за какие-либо убытки, ущерб, независимо от причин его возникновения (включая, но не ограничиваясь этим, особый, случайный или косвенный ущерб, убытки связанные с недополученной прибылью, прерыванием коммерческой или производственной деятельности, утратой деловой информации, небрежностью, или какие-либо иные убытки), возникшие вследствие использования или невозможности использования ПО. Основанием ответственности Правообладателя будет вина, при этом убытки будут ограничиваться только доказанным в судебном порядке реальным ущербом.

5. Права на интеллектуальную собственность.

5.1. Вы соглашаетесь с тем, что исключительные права на любые объекты интеллектуальной собственности, воплощенные в ПО и /или любой предоставленной Вам документации, принадлежат Правообладателю. Ничто в данном Соглашении не предоставляет Вам никаких прав на указанные объекты интеллектуальной собственности иные, чем предоставленные Вам по Договору, заключенному между Вами и Вашим лицензиаром.

5.2. Вы соглашаетесь с тем, что исходный код, лицензионный ключ для ПО являются собственностью Правообладателя.

5.3. Вы не можете удалять или изменять уведомления об авторских правах или другие проприетарные уведомления на любой копии ПО.

6. Права на информацию, доступ к которой получен Вами в рамках осуществления настоящего Соглашения.

6.1. Вы соглашаетесь с тем, что Вам не принадлежат никакие права на любую информацию, не являющуюся объектом интеллектуальной собственности в соответствии с разделом 6, доступ к которой получен Вами в рамках осуществления настоящего Соглашения.

6.2. К указанной информации, включая, но не ограничиваясь, относятся системы, методы работы, другая информация.

6.3. Указанная выше информация будет использоваться Вами только в целях осуществления предоставленных Вам по договору прав на ПО без права использования указанной информации в собственных интересах и за пределами Договора, заключенного между Вами и Вашим лицензиаром.

7. Вы проинформированы о том, что ПО содержит открытое программное обеспечение, распространяемое под определенными лицензиями, с которыми вы можете ознакомиться в файле licenses.inf, распространяемом с ПО в составе дистрибутива.

8. Контактная информация Правообладателя ООО «Лаборатория ИнфоВотч».

Тел./факс: +7(495)229-00-22

Коммерческий департамент: sales@infowatch.com

Служба технической поддержки: support@infowatch.com

Веб-сайт: www.infowatch.ru

9 Глоссарий

Термин	Определение
Администратор	Администратор – пользователь Системы, выполняющий установку, настройку и поддерживающий работу Системы. См. также: Офицер безопасности, Пользователь.
Группа SMB	Параметр, позволяющий использовать систему как часть определенной рабочей группы для сетевого управления папками, расположенными на рабочих станциях, терминальных серверах, файловых хранилищах и т.д. (например, домен).
Задача сканирования	Уникальная и непрерывно повторяющаяся операция проверки указанных ресурсов (путей сканирования) на наличие конфиденциальных данных. Каждая задача содержит описание ресурсов сканирования, загрузки и передачи файлов с них в Traffic Monitor. Содержит список хостов, список путей сканирования, фильтр по форматам сканируемых файлов.
Интеграция	Описание интеграции с Traffic Monitor для отправки скачанных с ресурсов файлов и их дальнейшего анализа. Указывает на конкретную инсталляцию Traffic Monitor, требуется токен авторизации и список адресов XAPI. В меню Консоли управления Системы относится к разделу Экспорт данных.
Интерфейс пользователя	Совокупность средств и методов, при помощи которых пользователь взаимодействует с системой.
Консоль управления	Графический интерфейс пользователя, предназначенный для управления системой Data Discovery (администрирование и настройка Системы, работа с задачами сканирования).
Лицензия	Право на использование Системы. Получается при приобретении Системы и определяет допустимые действия с системой относительно количества пользователей и т.п.
Маска	Шаблон поиска – метод описания поискового запроса с использованием метасимволов. Маски используют для поиска файлов нужных форматов.
Офицер безопасности	Основной пользователь Консоли управления. Также – предустановленная роль пользователя Консоли управления, имеющая привилегии на все действия в системе, за исключением административных.

Термин	Определение
План выполнения задачи	Формируемый сервисом Execution Controller порядок действий для сервиса сканнера (Puller). Определяет последовательность обработки ресурсов.
Пользователь	Пользователь системы Data Discovery – администратор, офицер безопасности и др. См. также: Администратор, Офицер безопасности.
Продуктовая платформа	Принципиальная конструкцию продукта – комплекс частей, подсистем, интерфейсов и производственных процессов, изменяемых о времени. Продуктовая платформа выступает в качестве базы для развертывания выпуска семейства продуктов и сборки готовых изделий из стандартизированных компонентов.
Проход	Сканирование одного ресурса полностью (т.е. все файлы на ресурсе должны быть обработаны сервисом сканнера (Puller)). Проход может состоять из нескольких сессий.
Рабочая станция/Компьютер	В терминах Системы подразумевается контролируемая рабочая станция или терминальное устройство.
Ресурс (Resource)	Путь сканирования/точка подключения к хосту, используемая для загрузки с него файлов. Обычно представляет из себя сетевую (или локальную) папку. Требует указания параметров для подключения.
Сессия	Подключение к ресурсу в рамках прохода. Длительность сессии сканирования (параметр Длительность обработки) задается в дополнительных (расширенных) настройках задачи.
Сервис ClickHouse	Распределенная аналитическая столбцовая СУБД, предназначенная для проведения анализа по хранящимся данным в реальном времени. Компонент продуктовой платформы.
Сервис PostgreSQL	СУБД, которая используется в продукте Data Discovery для хранения настроек и конфигураций задач, а также статистики о задачах. Компонент продуктовой платформы.
Сервис Tarantool	Используется для реализации очереди задач, которые сервисы ставят друг другу. Компонент продуктовой платформы.
Фильтры (Filters)	Набор условий для загрузки файлов с ресурсов. Представляет из себя список масок для фильтрации по

Термин	Определение
	форматам файлов, а также фильтры по максимальному и минимальному размеру файлов.
Хост (Host)	IP-адрес или DNS-имя компьютера/сервера, к которому осуществляется подключение для сканирования и загрузки с него файлов для дальнейшего анализа. Содержит список ресурсов для сканирования.
Хранилище (Storage)	Временное место хранения скачанных файлов. Файл хранится здесь до момента отправки его в Traffic Monitor.
Docker	Набор программ использующих виртуализацию на уровне операционной системы для развертывания специально упакованных приложений, называемых контейнерами.
InfoWatch Traffic Monitor	Traffic Monitor: программный комплекс, предназначенный для осуществления контроля различных видов трафика (SMTP, IMAP, POP3, HTTP, HTTPS, IMAP, XMPP, ICQ, NRPC) и теневых копий данных, копируемых на съемные носители и отправляемых на печать.
Kubernetes	Программное обеспечение для оркестрации контейнеризированных приложений – автоматизации их развертывания, масштабирования и координации в условиях кластера.
NATS	Система обмена сообщениями для компонентов.
Operator	Сервис представляет из себя бэкенд и настраивает работу всех остальных сервисов в Kubernetes.
Puller	Сервис для сканирования ресурсов и загрузки файлов с них. Помещает загруженные файлы в хранилище.
Sender	Сервис для отправки загруженных файлов в Traffic Monitor. Берет загруженные файлы из хранилища и передает в Traffic Monitor для дальнейшего анализа.
SMB (Server Message Block)	Сетевой протокол для удаленного доступа к файлам, принтерам и другим сетевым ресурсам, а также для межпроцессного взаимодействия.
SSH (Secure Shell)	Сетевой протокол, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов).

Термин	Определение
Storage Coordinator	Сервис для управления работой нескольких хранилищ. Управляет работой TPS Agentов, предоставляет статистику по всем хранилищам.
Task Execution Controller	Сервис для управления выполнением задачи. Контролирует работу над задачей всех остальных сервисов.
TPS Agent	Сервис для мониторинга состояния хранилища. Помогает работе с хранилищем Pullerов и Senderов, предоставляет статистику по этому хранилищу.
XAPI	Приватный API для передачи файлов в Traffic Monitor.