MaxPatrol VM версия 2.0

Руководство оператора

Дата редакции документа: 22.09.2023

Содержание

1. Об этом документе

Руководство оператора содержит пошаговые инструкции и справочную информацию об использовании Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) для управления информационными активами организации. В руководстве вы также найдете инструкции по настройке ключевых и дополнительных функций системы для выполнения конкретных задач. Руководство не содержит инструкций по установке, первоначальной настройке и администрированию MaxPatrol VM.

Руководство адресовано специалистам, ответственным за обеспечение информационной безопасности.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.
- PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol VM.
- Руководство разработчика — содержит информацию о доступных в MaxPatrol VM функциях сервиса REST API.

2. О MaxPatrol VM

Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) обеспечивает комплексное управление уязвимостями в IT-инфраструктуре предприятия. MaxPatrol VM позволяет автоматизировать:

— управление активами;

— анализ защищенности активов ИБ;

— приоритизацию и проверку устранения уязвимостей на активах ИБ.

MaxPatrol VM можно развернуть и использовать как самостоятельно, так и в рамках единой интегрированной системы обеспечения информационной безопасности предприятия. В этом случае MaxPatrol VM поддерживает взаимодействие с другими продуктами (MaxPatrol SIEM, PT NAD), что позволяет полнее и своевременнее актуализировать модель IT-инфраструктуры предприятия, более точно оценивать защищенность предприятия и использовать эти данные при работе с сетевым трафиком.

MaxPatrol VM позволяет:

— в любой момент предоставлять пользователю и другим системам актуальную информацию об IT-инфраструктуре, полученную путем активного и пассивного сбора данных;

— объединять активы в группы по различным критериям, чтобы упростить управление активами;

— оценивать степень влияния активов на информационную безопасность предприятия в целом;

— на основе постоянно обновляемой со стороны Positive Technologies базы знаний предоставлять пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных на активах, и отображать степень защищенности активов;

— определять способы устранения уязвимостей и настраивать политики контроля;

— выбирать среди уязвимостей те, которые необходимо устранять в первую очередь;

— контролировать степень защищенности IT-инфраструктуры и отслеживать информацию об уязвимостях на интерактивных дашбордах;

— выгружать данные для внешних систем и выпускать отчеты для различных подразделений и должностных лиц.

3. Вход в MaxPatrol VM через PT MC

Сервис управления пользователями и доступом PT Management and Configuration (PT MC) обеспечивает механизм единого входа (технология single sign-on) в приложения Positive Technologies.

Перед входом в MaxPatrol VM запросите у администратора PT MC:

— ссылку для входа в интерфейс продукта;

— тип учетной записи (локальная или доменная);

— логин и пароль вашей учетной записи пользователя.

В MaxPatrol VM реализована ролевая модель управления доступом. Роли определяют доступные для пользователя операции (например, работу с активами), а также объекты (например, активы и уязвимости). Подробнее о ролевой модели см. Руководство администратора.

Перед выполнением инструкции нужно убедиться, что в браузере разрешены всплывающие окна.

► Чтобы войти в MaxPatrol VM:

1. В адресной строке браузера введите ссылку для входа в интерфейс MaxPatrol VM.

   Откроется страница входа в сервис PT MC.

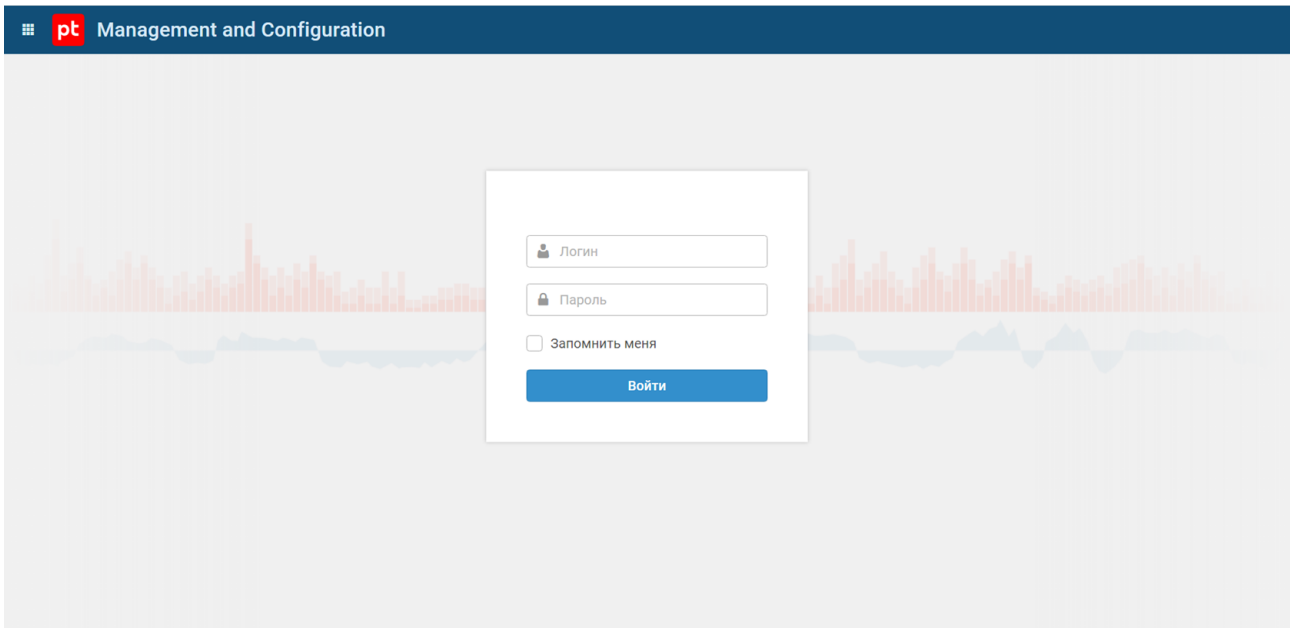

Рисунок 1. Ввод учетных данных

2. Выполните одно из следующих действий:

- Если вы входите под локальной учетной записью, то на вкладке **Локальный** укажите логин локальной учетной записи.
- Если вы входите под доменной учетной записью, то на вкладке **LDAP** укажите логин доменной учетной записи.

3. В поле **Пароль** введите пароль вашей учетной записи.

   Примечание. Стандартная сессия пользователя в MaxPatrol VM длится 12 часов. Вы можете продлить сессию, установив флажок **Запомнить меня**: тогда она завершится только через 7 дней бездействия.

4. Нажмите кнопку **Войти**.

PT MC проверяет введенные вами учетные данные. Если вы указали верные данные, откроется стартовая страница со стандартным дашбордом MaxPatrol VM. Если вы указали неверные данные, отобразится сообщение об ошибке.

4. Интерфейс MaxPatrol VM

Все действия в MaxPatrol VM вы можете выполнять с помощью графического пользовательского интерфейса. В этом разделе приводится описание основных элементов интерфейса MaxPatrol VM, доступных после входа в MaxPatrol VM.

В этом разделе

4.1. Главное меню

Главное меню расположено в верхней части страницы и обеспечивает доступ к основным функциям MaxPatrol VM.

Рисунок 2. Главное меню

Главное меню содержит название системы и следующие элементы:

— Кнопку . По кнопке открывается меню для перехода в базу знаний Knowledge Base и в сервис управления пользователями и доступом PT Management and Configuration.

— Кнопку для перехода на главную страницу с дашбордами.

— Разделы для перехода к страницам MaxPatrol VM. Если раздел объединяет несколько страниц, то у него есть меню. Выбирая пункт меню, вы переходите на нужную страницу.

— Индикатор состояния MaxPatrol VM. По нажатию на индикатор открывается список уведомлений о состоянии системы. Индикатор может показывать следующие состояния:

  — система работает корректно;

  — в системе есть предупреждения;

  — система работает с ошибками;

  — в системе происходит событие, не нарушающее ее работоспособность;

— не удалось выполнить диагностику системы.

— Значок для просмотра сообщений центра уведомлений MaxPatrol VM. По нажатию на значок открывается список уведомлений. Нажав на уведомление, вы можете открыть окно с подробным описанием. Вы можете удалить одно уведомление или уведомления за день, нажав . Также вы можете очистить список уведомлений, нажав кнопку **Удалить все**, или отключить все уведомления, нажав .

— Кнопку для перехода к справочной информации.

— Кнопку . По кнопке открывается меню с именем пользователя MaxPatrol VM и пунктами **Профиль** для перехода в личный кабинет пользователя в PT MC и **Выход** для выхода из системы.

4.2. Панель инструментов

Панель инструментов расположена в верхней части страницы под главным меню. Состав панели инструментов и содержимое рабочей области зависят от страницы.

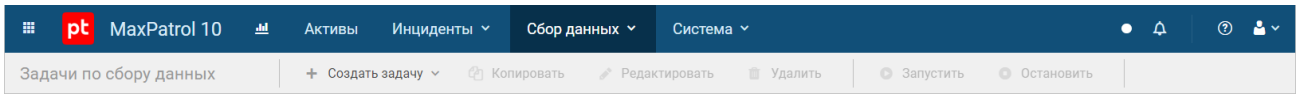

Рисунок 3. Панель инструментов

Панель инструментов содержит кнопки. С их помощью вы можете выполнять действия (в том числе групповые) с данными, представленными в рабочей области.

Кнопки могут иметь раскрывающееся меню, объединяющее группу пунктов.

4.3. Рабочая область

Рабочая область расположена на странице под панелью инструментов.

Рабочая область отображает различную информацию о работе системы одним из следующих способов:

— В виде списка. Списки бывают обычные и иерархические. Содержимое некоторых списков вы можете фильтровать.

— В виде таблицы. Например, информация об активах отображается в виде таблицы. Рабочая область может содержать таблицы, в которых вы можете настраивать состав колонок, а также сортировать, группировать и фильтровать записи.

Запрос: Все активы

@Host, Host.OsName, Host.@CreationTim… Выполнить

@Host ASC

Узел @Host	Операционная система Host.OsName	Дата и время создания а… Host.@CreationTime	Дата и время последнего… Host.@UpdateTime
10.0.164.16	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.27	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.31	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.33	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.35	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.36	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.40	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.58	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.63	null	Вчера, в 21:11	Вчера, в 21:11
10.0.164.65	null	Вчера, в 21:11	Вчера, в 21:11

Всего 948 записей, выбрана 1 запись (1 актив, 0 уязвимостей)

Рисунок 4. Таблица с данными

Для дополнительной группировки информации в рабочей области предусмотрены вкладки.

Рабочая область может содержать инструменты, позволяющие настраивать представление информации: панель группировки, панель фильтрации.

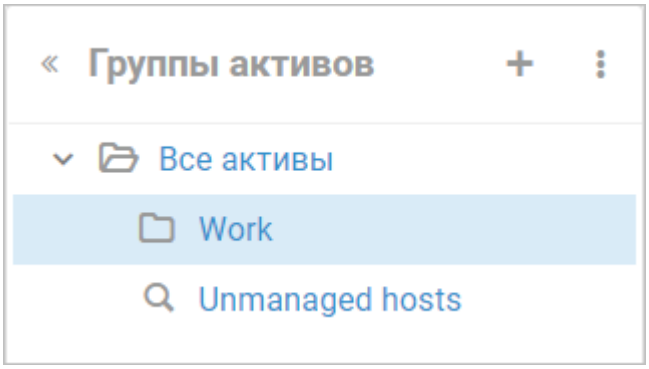

Рисунок 5. Панель группировки

4.4. Главная страница

При входе в MaxPatrol VM открывается главная страница.

На главной странице вам доступна информация, расположенная на виджетах и дашбордах. Виджет — это отдельный графический элемент представления данных, например гистограмма или таблица. Дашборд — это страница, содержащая набор виджетов. Вы можете:

- просматривать данные на виджетах, сохранять информацию, представленную на диаграммах, в PNG-файл;
- настраивать период времени, за который вам требуется просматривать информацию (по умолчанию каждый виджет содержит статистические данные за последние 24 часа);
- настраивать время автоматического обновления этих данных или обновлять их вручную (по умолчанию время автоматического обновления — 15 минут);
- настраивать виджеты в соответствии с видом представления информации (количественные показатели, диаграммы без распределения данных во времени, диаграммы с распределением данных во времени);
- переходить к просмотру детальной информации, нажимая на элементы виджетов;
- создавать пользовательские дашборды на основе стандартных шаблонов, содержащих разметку для размещения виджетов;
- настраивать состав и расположение пользовательских дашбордов, изменять их названия;
- настраивать состав виджетов на пользовательских дашбордах, выбирая их из библиотеки виджетов;
- менять расположение виджетов на дашборде.

В рабочей области главной страницы расположен стандартный дашборд **Управление уязвимостями**. Он помогает вам отслеживать, сколько активов и уязвимостей было в IT-инфраструктуре организации в тот или иной момент. Вы можете просматривать, как менялось их количество, приоритизировать уязвимые активы и контролировать распространение проблем.

Стандартный дашборд **Управление уязвимостями** содержит предустановленные виджеты. Вы можете настраивать их, изменять их расположение или добавлять на дашборд другие виджеты из специальной библиотеки, настраивать количество колонок, которые будет занимать виджет, перемещать виджеты по дашборду, копировать отдельные виджеты на другой дашборд.

> **Примечание.** При первом входе в систему после установки MaxPatrol VM виджеты стандартного дашборда будут пустыми, поскольку в системе не зарегистрированы активы и нет информации об уязвимостях.

Вы можете добавлять дашборды с нужной вам информацией.

Информация на виджетах обновляется автоматически (по умолчанию каждые 15 минут). Также вы можете обновить информацию вручную по кнопке .

См. также

Чек-лист настройки системы (см. раздел 11)

Работа с дашбордами и виджетами (см. раздел 8)

4.5. Страница «Активы»

На странице **Активы** отображается информация об активах, которые добавлены в систему, а также о группах активов и запросах для фильтрации активов. По умолчанию отображаются все активы, данные о которых есть в системе, из групп, к которым у вас есть доступ (включая вложенные группы). Данные об активах добавляются в систему с помощью задач по сбору данных.

В рабочей области страницы **Активы** расположены:

- Панель **Группы активов** с иерархическим списком групп для категоризации активов. В верхней части панели находятся следующие кнопки:

  + — для создания группы активов;

  ⋮ — для просмотра свойств, изменения и удаления группы активов.

- Панель **Запросы** со списком PDQL-запросов для фильтрации активов. Список содержит три вида запросов — стандартные, общие и пользовательские. В верхней части панели **Запросы** расположены следующие кнопки:

  🔍 — для поиска запроса по названию;

  + — для создания новой папки с запросами.

  > **Примечание.** Вы можете скрывать и раскрывать панели **Группы активов** и **Запросы**, используя « и » .

— Панель инструментов над таблицей активов. Вы можете обновить таблицу активов по нажатию или настроить автоматическое обновление таблицы по нажатию . Панель инструментов содержит следующие кнопки:

- **Добавить актив** — для добавления актива вручную или импорта данных об активе из файла;
- **Выпустить отчет** — для создания отчетов по активам в формате PDF;
- **Создать табличный список** — для экспорта данных об активах в табличный список.

— Панель фильтрации активов с возможностью формирования PDQL-запроса для фильтрации, сортировки и группировки активов в таблице активов. Вы можете как применять стандартные и общие запросы, так и создавать собственные, сохраняя их для повторного использования. Выбрать условия запроса можно по нажатию , и .

Вы можете вручную изменить сохраненный PDQL-запрос. Для выполнения такого запроса нужно нажать кнопку **Выполнить**.

В панели фильтрации активов также расположены следующие кнопки:

— для построения виджета, отображающего собранные данные об активах в виде таблицы, столбчатой диаграммы, графика или круговой диаграммы;

— для выбора способа ввода PDQL-запроса (текстом или с помощью графического интерфейса);

— Таблица активов, в которой отображаются данные об активах в соответствии с параметрами фильтрации, сортировки и группировки, заданными с помощью PDQL-запроса.

— Панель с подробной информацией об активе, который выбран в таблице активов. Панель содержит вкладки **Актив** и **Топология**. Если в таблице активов выбрана для отображения колонка **Уязвимость**, панель с подробной информацией об активе будет также содержать вкладку **Уязвимость**.

В центре вкладки **Актив** располагается график, отражающий изменения интегральной уязвимости в пределах выбранного периода и моменты получения новых сведений об активе.

В нижней части располагаются вкладки, которые содержат сводные данные об активе, информацию об уязвимостях, информацию о программном и аппаратном обеспечении актива, перечень и значения метрик CVSS (Common Vulnerability Scoring System).

В верхней части вкладки **Актив** отображаются сведения о жизненном цикле актива, показатель интегральной уязвимости, метрика значимости актива и следующие кнопки:

— для изменения паспорта актива и дополнительных сведений об активе;

— для просмотра и изменения расположения актива в группах активов;

— для присвоения активу значимости (не определена, низкая, средняя, высокая);

— для удаления актива из системы;

— для сравнения конфигураций актива, действовавших в разные дни;

— для экспорта истории конфигураций актива в XML-формате;

— для поиска задач по сбору данных;

— для создания задачи по сбору данных;

Расчет достижимости — для расчета достижимости актива (куда есть доступ у актива, откуда есть доступ к активу).

- **Проверки** — отображается для требований с несколькими проверками и содержит список проверок экземпляра требования с краткими описаниями и значками вердиктов. При выборе проверки на вкладке **Требование** отобразится карточка проверки, которая содержит название и идентификатор проверки, ее описание, рекомендации по устранению несоответствий актива требованию, а также раскрывающиеся блоки **Вердикт проверки**, **Как исправить** и **Команды и конфигурация** с информацией для выбранной проверки.

  Примечание. Вы можете перемещаться между карточками проверок, используя ^ и v в верхнем правом углу карточки.

— На вкладке **Топология** отображаются карта сети и связи выбранного актива с другими активами. По кнопке ⋮ можно выбрать параметры отображения карты сети. На вкладке **Топология** также расположены следующие кнопки:

— для расположения узлов на карте сети по умолчанию;

Расчет достижимости — для расчета достижимости актива (куда есть доступ у актива, откуда есть доступ к активу);

Скачать — для скачивания карты сети в формате PNG или SVG.

— На вкладке **Уязвимость** отображается основная информация об уязвимости, обнаруженной на активе (например, уровень опасности и статус, типы последствий эксплуатации уязвимости), количество активов с такими же уязвимостями, описание уязвимости, способ исправления уязвимости, оценка по CVSS и дополнительная информация. На вкладке **Уязвимость** также расположены следующие кнопки:

- **Изменить статус** — для изменения статуса уязвимости (новая, в работе, исправляется, требуется проверка, просрочено, исключена, устранена).
- **Отметить как важную** — для выделения важной уязвимости.
- **Изменить метки** — для присвоения ключевых слов для быстрого поиска, идентификации или категоризации уязвимостей.

4.6. Страницы раздела «Сбор данных»

Используя пункты раздела **Сбор данных** главного меню, вы можете открывать страницы для настройки сбора данных, аудита активов и тонкой настройки анализа полученных данных.

В этом разделе

4.6.1. Страница «Задачи по сбору данных»

На странице **Задачи по сбору данных** вы можете создавать, копировать, изменять и удалять задачи, запускать и останавливать их выполнение.

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать задачу** — по кнопке раскрывается меню, которое содержит пункт для создания задачи по сбору данных;
- **Копировать** — для копирования выбранной задачи;
- **Редактировать** — для изменения параметров выбранной задачи;
- **Удалить** — для удаления выбранной задачи;
- **Запустить** — для запуска выбранного задачи;
- **Остановить** — для остановки выбранной задачи;

В рабочей области страницы расположены:

- Панель **Статусы** со списком фильтров по статусам задач.
- Панель **Типы задач** со списком фильтров по типу задач.

  Примечание. Вы можете скрывать и раскрывать боковые панели, используя « и » .

- Панель **Все задачи** содержит таблицу с задачами.

  При нажатии в верхней части панели открывается поле для быстрого поиска задач по названию задачи, коллектора, учетной записи, профиля или модуля; по IP-адресу или FQDN цели задачи.

  При нажатии открывается панель для настройки фильтра задач.

  Примечание. Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию — пять минут).

В таблице в колонке **Статус** отображается статус задачи. Существуют следующие статусы:

- **Не запускалась**.

  — задача ни разу не запускалась.

- **Подготавливается**. Создается запуск задачи. Создаются подзадачи.
- **Ожидает выполнения**. Отправлен запрос о назначении подзадач на MP 10 Collector. Подзадачи будут запущены в порядке очереди.

  — все подзадачи назначены.

  — часть подзадач не назначены.

- **Выполняется**. Хотя бы одна подзадача запущена на MP 10 Collector. Идет процесс сбора данных.

  — нет подзадач, завершенных с ошибками.

  — часть подзадач завершены с ошибкой.

- **Завершается**. После остановки задачи вручную пользователем отправлен запрос об остановке подзадач на MP 10 Collector.

  — нет подзадач, завершенных с ошибками.

  — часть подзадач завершены с ошибкой.

- **Завершена**. Подзадачи завершены.

  — все подзадачи завершены без ошибок.

  — часть подзадач завершена с ошибками.

  — все подзадачи завершены с ошибками, задача не может быть выполнена.

— Панель **<Название задачи>** содержит информацию о выбранной задаче.

  По ссылке **История запусков** вы можете просматривать историю запусков задачи и журналы подзадач.

— Панель **<Количество задач>** с информацией о количестве выбранных задач и кнопками запуска, остановки и удаления задач, отмены выделения выбранных задач и сброса состояния источников. Отображается, когда в таблице выбрано несколько задач.

В этом разделе

Страница История запусков <Название задачи> (см. раздел 4.6.1.1)

Страница Журнал подзадачи <Время> (см. раздел 4.6.1.2)

4.6.1.1. Страница История запусков <Название задачи>

На странице **История запусков <Название задачи>** вы можете просматривать историю запусков задачи и список подзадач, созданных при каждом запуске.

В рабочей области страницы расположены:

— Панель **Сводка** с подробной информацией о задаче.

Примечание. Вы можете скрывать и раскрывать панель, используя « и » .

— Панель с историей запусков задачи.

В верхней части панели расположены кнопки — для выбора даты запуска и — для фильтрации запусков с ошибками.

— Панель **Подзадачи**, содержит таблицу с подзадачами, а также следующие кнопки:

- **Найти события** — по кнопке вы можете открыть страницу с событиями, собранными по выбранной подзадаче.
- **Скачать журнал** — по кнопке вы можете скачать файл с журналом выбранной подзадачи.
- **Журнал подзадачи** — по кнопке вы можете открыть страницу журнала выбранной подзадачи.

Примечание. Вы можете обновить данные в панели нажатием , настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию — пять минут).

В таблице в колонке **Статус** отображается статус подзадачи. Существуют следующие статусы:

Создана.

Назначена — назначен MP 10 Collector для выполнения.

Ожидает выполнения.

Выполняется.

Завершается.

Завершена — подзадача завершена без ошибок.

Завершена — подзадача завершена с ошибками.

Примечание. Подзадача завершается с ошибкой, если, например, указаны неверные учетные данные, цель сбора данных недоступна или не собрано никаких данных. Более подробная информация доступна в журнале подзадачи (см. раздел 7.4.7).

4.6.1.2. Страница Журнал подзадачи <Время>

На странице **Журнал подзадачи <Время>** вы можете просматривать сообщения и подробную информацию об ошибках подзадачи.

Панель инструментов содержит название страницы, а также следующие кнопку **Остановить задачу** для остановки задачи, для которой создана выбранная подзадача.

> **Примечание.** Вы можете обновить данные на странице нажатием ⟳, настроить период автоматического обновления данных в меню, открывающемся при нажатии ⋮ (по умолчанию — пять минут).

В рабочей области страницы расположены:

— Панель **Подзадача** с подробной информацией о выбранной задаче.

  Вы можете скрывать и раскрывать боковые панели, используя « и ».

— Панель **Журнал** со списком сообщений об ошибках подзадачи. По кнопке **Скачать журнал** вы можете скачать файл с журналом подзадачи.

— Панель **Сводка** с подробной информацией о выбранной ошибке.

4.6.2. Страница «Профили»

На странице **Профили** вы можете создавать пользовательские профили на базе стандартных, изменять и удалять их.

Панель инструментов содержит название страницы, а также следующие кнопки:

— **Создать** — по кнопке раскрывается меню, которое содержит пункты для создания пользовательского профиля на базе стандартного и для создания профиля для поиска выбранных уязвимостей;

— **Редактировать** — для изменения параметров выбранного пользовательского профиля;

— **Удалить** — для удаления выбранного пользовательского профиля.

В рабочей области страницы расположены:

— Панель **Профили** для фильтрации профилей по собираемым данным или названиям модулей, для которого они созданы.

  > **Примечание.** Вы можете открыть и скрыть панели **Профили** и **Сводка**, используя « и ».

— Панель **Список профилей** с таблицей профилей. Для каждого профиля в таблице указаны название, базовый профиль, название модуля и тип (стандартный или пользовательский).

— Панель **Сводка**, содержит информацию о выбранном профиле.

  По ссылке **Перейти** в строке **Задачи с этим профилем** вы можете просматривать список задач, созданных с выбранным профилем.

По кнопке **Параметры** вы можете просматривать параметры профиля.

См. также

Работа с профилями (см. раздел 7.3)

4.6.3. Страница «Учетные записи»

На странице **Учетные записи** вы можете добавлять, изменять и удалять учетные записи (см. раздел 7.1).

Панель инструментов содержит название страницы, а также следующие кнопки:

— **Добавить учетную запись** — по кнопке раскрывается меню, которое содержит пункты для создания учетных записей различных типов («логин—пароль», «пароль» или «сертификат»);

— **Редактировать** — для изменения параметров выбранной учетной записи;

— **Удалить** — для удаления выбранной учетной записи.

В рабочей области страницы расположены:

— Панель для выбора учетной записи, содержит список добавленных учетных записей с указанием их типа.

— Панель **Сводка**, содержит информацию о выбранной учетной записи.

  По ссылке **Перейти** в строке **Задачи с этой учетной записью** вы можете просматривать список задач, созданных с выбранной учетной записью.

  Примечание. Вы можете открыть и скрыть панель, используя « и » .

4.6.4. Страница «Справочники»

На странице **Справочники** вы можете создавать, изменять и удалять пользовательские справочники (см. раздел 7.2).

Панель инструментов содержит название страницы, а также следующие кнопки:

— **Создать** — для создания пользовательского справочника;

— **Редактировать** — для изменения выбранного пользовательского справочника;

— **Удалить** — для удаления выбранного пользовательского справочника.

В рабочей области страницы расположены:

— Панель **Группы справочников**. Содержит список групп справочников.

— Панель для выбора справочника. Содержит список справочников в выбранной группе.

— Панель **<Название справочника>**. В панели отображается содержимое выбранного справочника.

Примечание. Вы можете открыть и скрыть панели **Группы справочников** и **<Название справочника>**, используя « и » .

4.7. Страницы раздела «Система»

Используя пункты раздела **Система** главного меню, вы можете открывать страницы для работы со всеми отчетами, созданными в MaxPatrol VM; списками проверок, позволяющих правильно настроить MaxPatrol VM; информацию о состоянии MaxPatrol VM.

В этом разделе

4.7.1. Страница «Отчеты»

Все отчеты, созданные в системе, отображаются на странице **Отчеты** (**Система** → **Отчеты**). На этой странице вы можете:

- создавать, копировать, изменять или удалять задачи по выпуску отчетов;
- выпускать отчеты и настраивать расписание выпуска отчетов;
- скачивать отчеты (см. раздел 9.6).

Панель инструментов содержит название страницы, а также следующие кнопки:

- **Создать** — для создания задачи по выпуску отчета;
- **Копировать** — для копирования параметров выбранной задачи по выпуску отчета;
- **Редактировать** — для изменения параметров выбранной задачи по выпуску отчета;
- **Удалить** — для удаления выбранной задачи по выпуску отчета;
- **Выпустить** — для выпуска отчета;
- **Расписание** — по кнопке раскрывается меню, которое содержит пункты для управления расписанием выпуска отчета.

Рабочая область страницы **Отчеты** содержит:

— таблицу задач по выпуску отчетов, в которой отображается подробная информация обо всех таких задачах;

— панель **История выпусков**, в которой отображается информация о дате и времени выпуска отчета, а также о доступности отчета для скачивания;

— панель **Сводка** с подробной информацией о задаче по выпуску отчета, которая выбрана в таблице задач по выпуску отчетов.

Вы можете скрывать и раскрывать панель **Сводка**, используя » и « .

4.7.2. Страница «Уведомления»

Страница **Уведомления** позволяет работать с задачами для отправки уведомлений. В панели инструментов страницы находятся следующие кнопки:

— **Создать** — для создания задачи;

— **Копировать** — для создания задачи на основе существующей задачи (см. раздел 10.6);

— **Редактировать** — для изменения параметров задачи (см. раздел 10.7);

— **Удалить** — для удаления задачи (см. раздел 10.8);

— **Остановить** — для остановки задачи (см. раздел 10.5);

— **Запустить** — для запуска задачи после ее остановки (см. раздел 10.5).

Примечание. После создания задачи она запускается автоматически.

В рабочей области страницы расположены:

— Панель **Типы уведомлений**. Содержит перечень разделов по типам объектов, для которых доступно создание задач. При выборе типа в центральной панели отобразятся задачи, созданные для объектов этого типа.

— Центральная панель. Содержит таблицу с задачами.

— Панель **<Название задачи>**. Содержит данные о выбранной задаче.

4.7.3. Страница «Политики»

На странице **Политики** вы можете просматривать политики — наборы правил, по которым активы и уязвимости на активах проверяются и обрабатываются автоматически. Политики бывают следующих видов:

— для значимости активов — позволяют расставить приоритеты в работе с активами и отметить активы, уязвимости на которых представляют наибольшую опасность для IT-инфраструктуры организации;

— для сроков актуальности данных — позволяют указать сроки актуальности данных, полученных сканированием активов методом аудита или пентеста;

— для статусов уязвимостей — позволяют изменить тип устранения и статус уязвимостей, которые попадают под определенные правила политики;

— для отметки «важная» — позволяют настроить обработку уязвимостей, представляющих особую угрозу и поэтому отмеченных как важные.

В рабочей области страницы **Политики** отображается:

— Панель **Список политик**, содержащая перечень доступных политик. Политика может стать недействующей, если в правилах этой политики появились ошибки. Такое правило в таблице правил будет отмечено значком .

— Панель инструментов с возможностью создавать, изменять, копировать, удалять, включать и отключать правила.

Примечание. Для настройки политик требуются права администратора.

— Панель с таблицей правил выбранной политики. Правила внутри политики применяются согласно установленному порядку. Правила могут быть стандартными и пользовательскими.

— Панель **Сводка** со сводной информацией о состоянии правила, результатах его применения и о группах активов, для которых установлено правило.

Примечание. Вы можете скрывать и раскрывать боковые панели, используя « и » .

4.7.4. Страница «Управление системой»

На странице **Управление системой** отображается информация о состоянии компонентов MaxPatrol VM.

Рабочая область страницы **Управление системой** содержит панель **Компоненты** с разделами **О системе**, **Коллекторы**, **База знаний** и **Обработка активов**.

Раздел О системе

В разделе **О системе** вы можете просматривать информацию о лицензии и версии компонента MP 10 Core. Для корректной работы MaxPatrol VM необходима действующая лицензия.

Раздел Коллекторы

В разделе **Коллекторы** вы можете просматривать информацию о MP 10 Collector, который обеспечивает поступление данных в систему.

Панель инструментов содержит кнопку **Обновить версию** для обновления версии коллектора и кнопку **Удалить** для удаления недоступного коллектора из списка.

В рабочей области страницы отображается таблица со списком коллекторов. Для каждого коллектора в таблице указаны название, версия, статус, роли, а также IP-адреса и семейство ОС сервера. Вы можете сортировать список, нажимая на названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая ⚙ в правой верхней части таблицы. Для поиска коллектора в списке вы можете нажать 🔍 и ввести в поле для поиска параметр коллектора. При выборе коллектора система отображает подробную информацию о нем в боковой панели с названием коллектора.

> **Примечание.** Вы можете скрывать и раскрывать боковые панели, используя « и » .

В колонке **Статус** отображается статус коллектора:

- **Доступен** — коллектор работает в нормальном режиме;
- **С ограничениями** — коллектор работает в режиме ограниченной функциональности по причине нехватки свободного дискового пространства (величина свободного дискового пространства для каждого коллектора задается администратором системы);
- **Недоступен** — MP 10 Core не получает отклика от коллектора более 10 минут;
- **Обновляется** — коллектор обновляется с помощью компонента PT UCS;

Удаляется — коллектор удаляется из списка.

Раздел База знаний

В разделе **База знаний** вы можете просматривать информацию о подключенной базе знаний. Панель инструментов содержит кнопку **Обновить** для обновления версии базы знаний.

Настройка компонентов системы описана в Руководстве администратора.

Раздел Обработка активов

В разделе **Обработка активов** вы можете просматривать информацию о работе служб MP 10 Core на различных этапах обработки данных об активах.

Для каждого этапа в таблице указаны название используемой службы, длина очереди, время ожидания обработки, номера пакетов в очереди, номера последних обработанных пакетов и средняя скорость обработки пакетов за 5 минут. Вы можете обновить данные в таблице нажатием и настроить период автоматического обновления данных в меню, открывающемся при нажатии (по умолчанию — пять минут).

4.7.5. Страница «Чек-лист настройки системы»

После установки MaxPatrol VM на странице **Чек-лист настройки системы** вы можете уточнить, какие параметры необходимо настроить в системе с учетом специфики IT-инфраструктуры вашей организации. Также в процессе работы с MaxPatrol VM вы можете проверять, корректно ли настроена система.

В рабочей области страницы **Чек-лист настройки системы** отображается:

— панель **Список проверок** со списком и статусом всех проверок, с возможностью искать и фильтровать проверки;

— панель инструментов с возможностью запускать проверку или исключать ее из списка;

— описание отдельной проверки и необходимых шагов по настройке системы.

Для удобства проверки сгруппированы. Напротив каждой группы отображается количество пройденных в этой группе проверок.

5. Работа с активами

Работа с системой начинается со сбора сведений об активах. Это позволяет получить представление об информационной инфраструктуре предприятия.

Вы можете анализировать данные об активах и связях между ними, чтобы принимать решения по управлению IT-инфраструктурой.

В этом разделе

5.1. Инвентаризация активов

Актив в MaxPatrol VM — информация или оборудование, имеющие ценность для предприятия и подлежащие защите от киберугроз.

Основные типы активов — сетевой узел и служба каталогов Microsoft Active Directory.

Служба каталогов Microsoft Active Directory является хранилищем для логинов, паролей и групп пользователей, персональной и организационной информации. Количество служб зависит от количества инфраструктур, но в большинстве случаев на предприятии такая служба одна. Службу каталогов Microsoft Active Directory можно добавить в MaxPatrol VM только с помощью задачи на сбор данных (см. раздел 7.4.1), вручную это сделать невозможно.

> **Внимание!** Активы такого типа доступны в таблице активов после создания динамической группы активов (см. раздел 5.1.3.1) с фильтром `ActiveDirectory`.

Сведения, собранные об активе, составляют модель актива.

При сканировании IT-инфраструктуры организации MaxPatrol VM обнаруживает активы и создает о них записи.

Вы также можете добавлять активы вручную, импортировать из файла (см. раздел 5.1.2.2) или из MP8. Удаляется актив либо вручную, либо автоматически — при его устаревании (см. раздел 5.1.4).

Вы можете объединять активы в группы (см. раздел 5.1.3) для удобства работы с системой: для отображения в системе организационной структуры предприятия, планирования задач на сканирование узлов, генерации отчетов.

В этом разделе

Группы активов (см. раздел 5.1.3)

Устаревание актива (см. раздел 5.1.4)

Карточка актива (см. раздел 5.1.5)

Мини-карточка актива (см. раздел 5.1.6)

Изменение информации об активах (см. раздел 5.1.7)

Присвоение значимости активам (см. раздел 5.1.8)

Удаление активов (см. раздел 5.1.9)

См. также

Создание группы активов (см. раздел 5.1.3.1)

5.1.1. Идентификация активов

MaxPatrol VM обнаруживает активы при сканировании сети предприятия. Обнаруженные активы необходимо идентифицировать.

Степень полноты идентифицирующих данных, достаточных для создания записи о новом или обновления существующей записи об активе, зависит от контекста, например от метода сканирования актива.

Идентификация активов — это сравнение отдельных атрибутов актива (его идентификаторов) с атрибутами существующих активов, о которых есть записи в базе данных. В случае идентификации при обнаружении активов по итогам сравнения либо создается запись о новом активе, либо обновляются записи о существующих активах.

У актива могут быть следующие идентификаторы:

- Type — тип операционной системы;
- VMID — уникальный ключ виртуальной машины в контексте конкретной виртуальной инфраструктуры;
- IsVirtual — признак виртуальности узла;
- SystemId — уникальный идентификатор системы (способ формирования зависит от конкретной операционной системы);
- Hostname — имя узла, заданное на самом узле;
- FQDN — полное имя узла (значение, которое будет отображаться при аудите узла в режиме белого ящика, безотносительно внешних серверов имен);
- MAC — список доступных MAC-адресов (исключая виртуальные, такие как MAC-адреса протоколов отказоустойчивости);
- IP — список доступных IP-адресов (только маршрутизируемых за пределы сегмента);
- Failover — список серийных номеров участников failover-группы (для Cisco ASA).

В этом разделе

5.1.1.1. Обнаружение активов

Под обнаружением актива подразумевается получение набора данных, идентифицирующих актив, достаточного для создания новой или обновления существующей записи об активе.

Для составления и поддержания полного и актуального представления об IT-инфраструктуре предприятия в системе используются методы как непосредственного обнаружения — путем сканирования самого актива, так и косвенного обнаружения активов — при анализе информации о других активах, которую содержит сканируемый актив.

К непосредственным методам обнаружения активов относятся сканирование сетевых узлов аудитом и пентестом, добавление активов вручную и импорт активов из файла.

Активы также могут быть импортированы из MP8. Подробнее см. Руководство по настройке источников.

Результаты сканирования активов получает служба управления сканированием (Core Scanning), эта же служба получает результаты ручного ввода и импорта активов.

Косвенный метод обнаружения активов — обнаружение на основе данных других активов. Обнаруженные активы поступают на вход службы управления сканированием.

В обоих случаях обнаруженные активы поступают на вход службы управления сканированием. Таким образом, независимо от метода обнаружения активов их дальнейшая обработка происходит единообразно.

На основе данных других активов, полученных сканированием в режиме белого ящика, могут быть обнаружены следующие активы:

- При сканировании контроллера домена Active Directory обнаруживаются активы-участники домена с операционной системой Windows.
- При сканировании сервера Microsoft System Center Configuration Manager (SCCM) обнаруживаются активы-клиенты SCCM с операционной системой Windows, информацией о сетевых интерфейсах и установленном программном обеспечении.
- При сканировании сервера Kaspersky Security Center обнаруживаются активы-клиенты с операционной системой Windows.
- При сканировании гипервизоров VMware ESXi и Microsoft Hyper-V обнаруживаются активные виртуальные машины, если гипервизор предоставляет достаточную информацию об их сетевых интерфейсах и установленной операционной системе (полнота информации, доступной гипервизору, зависит от гостевой операционной системы и наличия установленного набора утилит VMware Tools).

— При сканировании сетевых устройств анализируется полученная по протоколам CDP и LLDP информация о соседних устройствах, их типе, IP-адресах и операционной системе и обнаруживаются соответствующие активы.

— При сканировании сетевых устройств анализируется полученная информация об актуальных связках «MAC-адрес — IP-адрес» в базе DHCP snooping и обнаруживаются активы — сетевые узлы с данными адресами.

— При сканировании актива на основе динамических записей из его ARP-таблицы обнаруживаются активы — сетевые узлы (за исключением записей proxy ARP, local proxy ARP и записей с виртуальными MAC-адресами).

— При сканировании актива на основе информации о шлюзах, полученной из его таблицы маршрутизации, обнаруживаются активы с указанным IP-адресом и ролью «маршрутизатор».

Обнаружение активов на основе данных другого актива производится не на этапе сканирования, а на этапе обработки данных исходного актива агрегатором (исключение — обнаружение клиентских активов SCCM, которое производится на этапе сканирования SCCM).

5.1.1.2. Алгоритмы идентификации активов

При сканировании сетевых узлов площадки требуется правильно идентифицировать активы.

Сканирование одним коллектором сетевых сегментов, активы в которых имеют одни и те же IP-адреса, может привести к неверной агрегации активов: вместо нескольких активов система может идентифицировать один актив. Также наличие в списке активов с одинаковым IP-адресом может затруднить поиск необходимого актива. При наличии в составе площадки таких сегментов сети для каждого из них создается отдельная инфраструктура. В задаче сканирования указывается инфраструктура (если их несколько), соответственно для сканирования разных инфраструктур создаются разные задачи.

> **Примечание.** После развертывания MaxPatrol VM имеет одну инфраструктуру **Инфраструктура** по умолчанию.

Подробнее о работе с инфраструктурами см. Руководство администратора.

Псевдонимы параметров инфраструктур, к которым принадлежат активы, вы можете использовать для фильтрации, настройки представления данных в таблице активов и для создания динамических групп активов. Подробное описание см. в документе Синтаксис языка запросов PDQL.

Алгоритм идентификации при обнаружении активов

При обнаружении активов идентификация происходит следующим образом: обнаруженные активы поступают в службу управления сканированием от одного из источников (модулей сканирования, ручного ввода, импорта из файла).

Затем в системе сравниваются идентификаторы просканированных активов (в первую очередь идентификатор Type) с идентификаторами существующих в инфраструктуре активов. В зависимости от результатов происходит обновление базы данных активов по одному из сценариев:

— если совпадений нет — создается новая запись об активе, в которую заносятся входящие модельные данные;

— если входящему набору идентификаторов соответствует один существующий актив — входящие модельные данные заносятся в существующую запись об активе;

— если входящему набору идентификаторов соответствует несколько существующих активов — совпавшие записи объединяются в одну, и в эту запись заносятся входящие модельные данные.

5.1.2. Добавление активов в систему

Система обнаруживает активы при сканировании сети предприятия.

Вы также можете добавлять активы вручную или импортировать из CSV-файла. При импорте из файла вы можете задавать пользовательские поля активов и их значения, которые необходимы вам для их идентификации.

Кроме того, при добавлении активов вы можете задавать время, в течение которого данные об активе будут считаться актуальными, для сканирования в режиме аудита и пентеста. Это поможет вам контролировать устаревание активов (см. раздел 5.1.4).

В этом разделе

5.1.2.1. Добавление актива вручную

► Чтобы добавить актив в систему:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

   Примечание. Если это первый запуск MaxPatrol VM, то вам необходимо создать пользовательскую группу активов.

2. В панели инструментов нажмите + и в раскрывшемся меню выберите пункт **Добавить актив**.

   Откроется окно **Создание актива**.

3. В раскрывающемся списке **Расположение** выберите группу, в которую будет помещен актив.

4. Если вы знаете название операционной системы, установленной на активе, в раскрывающемся списке **ОС** выберите тип операционной системы и в поле **OsName** введите ее название.
5. Укажите идентификаторы актива:
   - если вы выбрали тип операционной системы Windows, в поле **FQDN** введите полное доменное имя актива;
   - если вы выбрали тип операционной системы Cisco IOS, в поле **FQDN** введите полное доменное имя актива или в поле **Hostname** введите имя узла актива;
   - если вы не выбрали тип операционной системы или выбрали другой тип, в поле **Hostname** введите имя узла актива.
6. В поле **IP-адрес** введите IP-адрес актива.
7. Если вы указали название операционной системы, установленной на активе, нажмите кнопку **Далее**.

   Откроется страница с блоком параметров **Программное обеспечение**.

   Примечание. С помощью раскрывающегося списка **Название ПО** вы можете выбрать название программного обеспечения, установленного на активе.
8. Если требуется, в блоке **Статусы актуальности данных** настройте время, в течение которого данные об активе будут считаться актуальными, отдельно для сканирования аудитом и пентестом.

   Примечание. Вы можете выбрать время в раскрывающемся списке или ввести его с помощью языка PDQL.
9. Нажмите кнопку **Сохранить**.

Актив добавлен в указанную группу активов.

5.1.2.2. Импорт активов из файла

Вы можете импортировать в MaxPatrol VM данные об активах типа Host из файла формата CSV. Имя файла может быть любым, файл должен быть представлен в кодировке UTF-8 с BOM.

В первой строке файла должны содержаться названия полей в порядке, в котором во второй и последующих строках будут содержаться их значения. Вторая и последующие строки описывают импортируемые активы (одна строка должна соответствовать одному активу). Значения текстовых полей должны быть заключены в кавычки (`" "`). Значения полей должны быть разделены точкой с запятой (`;`).

Примечание. Вы можете скачать пример файла в окне импорта активов по кнопке **?**.

В состав полей должны входить обязательные поля, необходимые для идентификации актива:

— TypeAlias — псевдоним (см. документ Синтаксис языка запроса PDQL);

— FQDN — для активов, на которых развернута операционная система семейства Windows или ESXi;

— FQDN или Hostname — для активов, на которых развернута операционная система семейства Cisco IOS;

— Hostname — для прочих активов;

— IP-адрес. Поле может содержать несколько значений, которые должны быть разделены вертикальной чертой (|).

Вы можете также добавить в файл необязательные поля: поле MAC, содержащее список доступных через сеть MAC-адресов актива, и поле IsVirtual (признак виртуальности узла). Значения поля MAC должны быть разделены вертикальной чертой (|). Кроме того, вы можете добавить в файл пользовательские поля, которые необходимы вам для работы с активами (см. Руководство администратора).

Примечание. Если в двух классах активов есть одинаковые по названию и разные по типу поля, вам необходимо указать в списке полей в файле оба поля, предваряя их названием класса с точкой. Например, для инвентаризационных номеров активов, на которых установлены операционные системы семейств Windows и Linux, укажите поля WindowsHost.UF_InvNum и LinuxHost.UF_InvNum.

► Чтобы импортировать из файла данные об активах:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели инструментов нажмите + и в раскрывшемся меню выберите пункт **Импортировать данные**.

   Откроется окно **Импорт активов**.

3. В раскрывающемся списке **Инфраструктура** выберите инфраструктуру, к которой будут привязаны активы.

   Примечание. Список отображается, если в системе создано более одной инфраструктуры.

4. В раскрывающемся списке **Расположение** выберите группу, в которую будут помещены активы.

5. Перетащите или выберите файл в формате CSV.

6. Нажмите кнопку **Импортировать**.

Данные об активах импортированы.

5.1.3. Группы активов

Пользователь может объединять активы в группы для удобства работы с системой: для отображения в системе организационной структуры предприятия, планирования задач на сканирование узлов, генерации отчетов.

Группировка активов также используется:

— при фильтрации данных для отчетов, графиков, отображения данных;

— привязке ролей пользователей (назначении пользователю определенных полномочий на выполнение тех или иных действий в рамках группы, назначении роли пользователя в группе; подробнее о ролях пользователей см. Руководство администратора);

— сборе данных.

Группа может содержать активы и другие группы. Отображение групп и содержащихся в этих группах активов зависит от роли пользователя, который авторизован в MaxPatrol VM. Пользователь не может настраивать или удалять вложенные группы активов, если у него нет прав на родительскую группу.

Группы активов бывают пользовательскими и стандартными. Стандартные группы предустановлены в MaxPatrol VM, их невозможно изменить или удалить.

По умолчанию MaxPatrol VM имеет две стандартные группы:

— группа **Все активы** — в ней выводятся все активы, которые доступны роли пользователя;

— группа **Unmanaged hosts** — в ней выводятся все активы, не привязанные ни к одной из групп (расположение этих активов не указано).

Пользовательские группы делятся на динамические и статические. В динамическую группу MaxPatrol VM добавляет актив автоматически, если он удовлетворяет определенному условию — запросу на языке PDQL.

> **Примечание.** Динамические группы наполняются всеми подходящими под PDQL-запрос активами, независимо от расположения и уровня вложенности этих групп.

Сложные PDQL-запросы могут обрабатываться долго. В списке групп медленные динамические группы отмечаются специальным значком.

Пользователь, у которого нет доступа ко всем активам, не может создавать динамические группы или изменять в динамической группе запрос для фильтрации активов.

В статической группе располагаются активы, которые вручную выбирает пользователь.

Для группы активов пользователь может выпустить отчет, построить статистику, просмотреть карту сети. По нажатию кнопки мыши пользователь может просматривать во всплывающей подсказке полный путь к группе, если роль пользователя предполагает доступ к нескольких группам с одинаковыми названиями, а доступ к родительским группам отсутствует. Также пользователь может воспользоваться поиском по группам активов.

Группы иерархически связаны друг с другом и отображаются в интерфейсе системы в виде дерева. На иерархию групп накладываются следующие ограничения:

— возможны не более 9 уровней вложенности;

— каждая создаваемая группа должна быть привязана к какой-либо другой группе;

— группа не может быть для другой группы одновременно родительской и вложенной в нее (например, если Группа 3 входит в Группу 1, то Группа 1 не может входить в Группу 3);

— динамическая группа не может содержать в себе вложенные группы.

В этом разделе

5.1.3.1. Создание группы активов

► Чтобы создать группу активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Группы активов** нажмите + .

   Откроется страница **Создание группы**.

3. В поле **Название** введите название группы активов.

4. В раскрывающемся списке **Расположение** выберите группу активов, в которую войдет новая группа.

5. Выберите тип группы активов.

   Примечание. Если у вас нет доступа ко всем активам, вы не сможете создать динамическую группу.

6. Если вы выбрали тип группы активов **Динамическая**, в поле **Фильтр** введите запрос для фильтрации активов на языке PDQL.

   Примечание. Вы также можете настроить метрики CVSS. Описание метрик CVSS см. на сайте first.org.

7. Нажмите кнопку **Сохранить**.

Группа активов создана.

5.1.3.2. Создание группы активов из карточки актива

Вы можете создавать группы активов из карточки актива.

► Чтобы создать группу активов из карточки актива:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Активы** выберите актив.
3. На карточке актива выберите вкладку **Актив**.
4. Во всплывающем окне выберите условие фильтрации.

   Условие будет добавлено в PDQL-запрос в нижней части карточки актива.

   Примечание. Вы можете выбрать несколько условий фильтрации.

5. В правом нижнем углу страницы нажмите **Перейти к созданию группы**.

   Откроется страница **Создание группы**. Сформированный PDQL-запрос будет автоматически добавлен в поле **Фильтр**.

   Примечание. Вы можете сформировать PDQL-запрос вручную.

6. В поле **Название** введите название группы активов.
7. В раскрывающемся списке **Расположение** выберите группу активов, в которую войдет новая группа.
8. Выберите тип группы активов.

   Примечание. Вы также можете настроить метрики CVSS. Описание метрик CVSS см. на сайте first.org.

9. Нажмите кнопку **Сохранить**.

Группа активов создана.

5.1.3.3. Настройка группы активов

► Чтобы настроить группу активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Группы активов** выберите группу активов.
3. В панели **Группы активов** нажмите ⋮ и в раскрывшемся меню выберите пункт **Редактировать**.

   Откроется страница **Редактирование группы <Название группы>**.

4. Внесите изменения.

   Примечание. Вы можете изменить тип группы. Если сделать группу динамической, из нее поначалу будут удалены все активы. Если группа содержит вложенные группы, сделать ее динамической невозможно. Если сделать группу статической, все активы, которые соответствуют фильтру, будут привязаны к ней.

   Примечание. Если у вас нет доступа ко всем активам, вы не сможете изменить запрос для фильтрации активов.

5. Нажмите кнопку **Сохранить**.

Группа активов настроена.

5.1.3.4. Удаление группы активов

Вы можете удалять группы активов, при этом будут удалены все вложенные группы. Вы не можете удалять стандартные группы активов.

► Чтобы удалить группу активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Группы активов** выберите группу активов.

   Примечание. Вы можете выбрать несколько групп, удерживая клавишу Ctrl.

3. В панели **Группы активов** нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить** и подтвердите удаление.

Выбранная группа активов удалена.

5.1.4. Устаревание актива

Сведения об активах со временем устаревают и приводят к ошибкам при выполнении задач. Чтобы не допускать таких ошибок, система выявляет и удаляет устаревшие активы. За это отвечает служба идентификации активов. Она принимает решение о том, что актив устарел и затем создает событие о его удалении.

Устаревшим считается актив, после последнего обновления которого прошло определенное время. Время устаревания для всех активов устанавливает администратор.

О том, когда ожидается устаревание конкретного актива, вы можете узнать в карточке актива.

Актив не устареет, если:

— от него будет получен ответ при сканировании сети;

— данные о нем будут обновлены вручную;

— данные о нем будут обновлены при импорте из файла.

5.1.5. Карточка актива

Карточка актива содержит полную информацию об активе. Перейти в карточку можно из таблицы активов, щелкнув по названию актива. Также вам доступен быстрый просмотр карточки в боковой панели **Актив**.

Под именем актива располагаются сведения о его жизненном цикле, а также указаны интегральная уязвимость и метрика значимости актива (низкая, средняя, высокая или не определена). Вы можете вручную установить значимость для актива из таблицы или из его карточки.

Интегральная уязвимость представляет собой сумму оценок опасности всех уязвимостей актива. Уровень опасности оценивается по стандарту Common Vulnerability Scoring System (CVSS). Если есть оценка опасности по стандарту CVSS версии 3, то для расчета интегральной уязвимости будет взята она, если нет — то оценка опасности по стандарту CVSS версии 2.

График отражает изменения интегральной уязвимости актива в пределах выбранного периода. Также на графике отмечены моменты, когда были получены новые данные об активе.

По умолчанию на графике отображается история актива за последние 7 дней. Вы можете изменить период для просмотра истории актива по кнопке .

Под графиком расположено несколько вкладок.

Для сетевых узлов и служб каталогов Microsoft Active Directory отображаются вкладки **Сводка**, **Уязвимости**, **Конфигурация** и **Метрики CVSS**. Для учетных записей отображаются вкладки **Сводка**, **Конфигурация** и **Метрики CVSS**.

Сводка. В карточке актива типа «сетевой узел» отображается краткая информация об аппаратном и программном обеспечении актива, 10 самых опасных уязвимостей, сетевая конфигурация, а также список с оценками уязвимостей сетевых служб, ОС и ПО. Из этих оценок складывается интегральная уязвимость всего актива.

В карточке актива типа «служба каталогов Microsoft Active Directory» информация отсутствует.

Уязвимости. Для карточки актива типа «сетевой узел» вкладка содержит блоки **Уязвимости ОС и ПО** и **Уязвимости сетевых служб** с подробной информацией об уязвимостях актива. Для каждой уязвимости указана оценка опасности и приведена ссылка на публичную базу данных Common Vulnerabilities and Exposures. Вы можете перейти в карточку уязвимости, щелкнув по названию уязвимости.

В карточке актива типа «служба каталогов Microsoft Active Directory» информация отсутствует.

Уровни опасности уязвимостей отмечены специальными значками:

- **Критический**;
- **Высокий**;
- **Средний**;

- **Низкий**;
- **Не определен**.

Уязвимости ОС и ПО 1079 | Уязвимости сетевых служб 32

Уязвимость	Интегральная уязвимость	CVE
Уязвимости операционной системы (632)	**3 780,8**	
Уязвимости программного обеспечения (447)	**2 725,8**	
Microsoft Internet Explorer 11.0 (113)	**655,7**	
Microsoft Internet Explorer 11.0 (113)	**655,7**	
OpenSSL 1.0.2f (41)	**245,4**	
OpenSSL 1.0.2g (34)	**197,2**	
OpenSSL 1.0.1p (29)	**190,5**	
Окончание поддержки продукта	10,0	
Отказ в обслуживании	8,5	CVE-2016-2177
Отказ в обслуживании	8,5	CVE-2016-2182
Разглашение информации	8,5	CVE-2016-0799
Отказ в обслуживании	8,5	CVE-2016-2842
Целочисленное переполнение	8,5	CVE-2016-6303
Двойное освобождение	8,5	CVE-2016-0705
Разглашение информации	7,1	CVE-2016-2176
Отказ в обслуживании	6,5	CVE-2016-6302

Рисунок 6. Вкладка **Уязвимости**

Конфигурация. Вкладка содержит подробную информацию об аппаратном и программном обеспечении актива.

Сводка | Уязвимости | Конфигурация | Метрики CVSS

Обновления
updates

- KB2958429
- KB2565063
- KB2919355
- KB3139929
- KB3148198
- KB3170106
- KB3172614

Идентификатор обновления updateId: KB2958429

Рисунок 7. Вкладка **Конфигурация**

Метрики CVSS. На вкладке отображаются контекстные метрики CVSS. Описание метрик CVSS см. на сайте first.org.

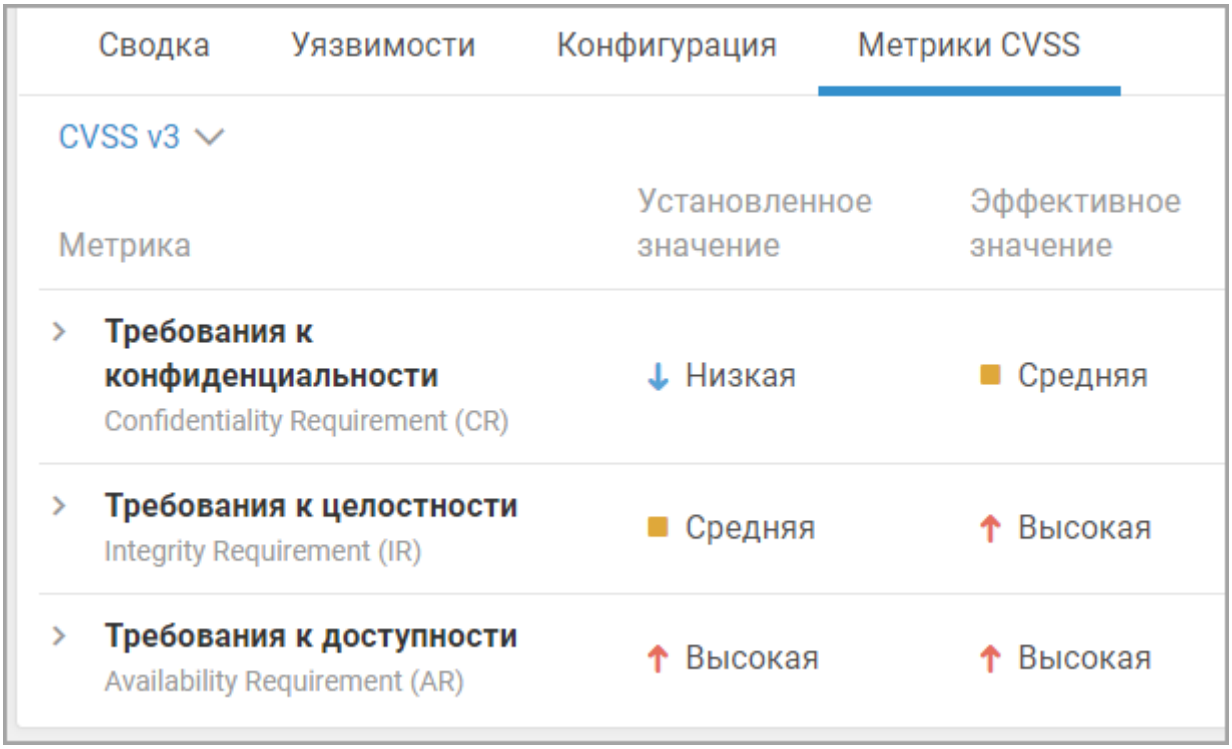

Рисунок 8. Вкладка **Метрики CVSS**

Вы можете устанавливать и изменять значения для метрик, в том числе при настройке группы, в которую входит актив. Эффективное значение определяется автоматически и является максимальным для данной метрики из всех установленных значений (для актива и групп, в которые входит актив). Максимальные значения метрик наследуются от родительской группы к вложенной группе и от вложенной группы к активу.

Кроме того, в карточке актива могут отображаться пользовательские поля, добавленные в модель актива, и их значения.

5.1.6. Мини-карточка актива

В мини-карточке актива вы можете получать базовую информацию об активе. Мини-карточка позволяет переходить к созданию задачи на сбор данных с актива, а также к просмотру:

— актива на карте сети;

— детальной информации об активе.

Открыть мини-карточку актива вы можете по ссылке с названием актива.

В верхней части мини-карточки содержится название актива. Под названием актива находятся вкладки **Сводка** и **Интерфейсы**.

> **Примечание.** Вкладка **Интерфейсы** доступна только при работе с мини-карточкой актива на карте сети.

На вкладке **Сводка** отображаются краткая информация о программном обеспечении актива, роли, указатель метрики значимости, дата последнего обновления, а также признак виртуальности (если есть).

Вкладка **Интерфейсы** содержит список интерфейсов актива с их IP- и MAC-адресами.

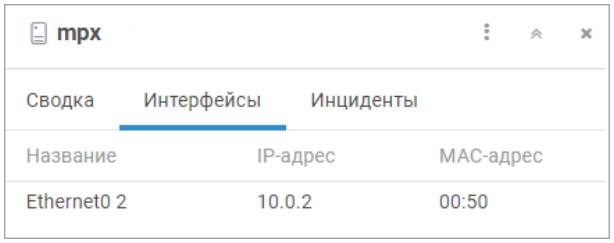

Рисунок 9. Просмотр интерфейсов актива

5.1.7. Изменение информации об активах

При сканировании сети предприятия система обновляет информацию об активах. Вы также можете изменять информацию об активах вручную. Например, если на активе была установлена новая версия операционной системы или новое программное обеспечение.

> **Примечание.** Вы не можете изменить ранее заданную операционную систему на систему другого семейства. Также вы не можете изменять дополнительные сведения одновременно для нескольких активов.

► Чтобы изменить информацию об одном или о нескольких активах:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В таблице активов выберите один или несколько активов.

3. В панели инструментов нажмите и в раскрывшемся меню выберите один из пунктов:

   - Если вы хотите изменить данные паспорта одного или нескольких активов, выберите пункт **Паспорт**.
   - Если вы хотите изменить другую информацию (например, значения пользовательских полей) об одном активе, выберите пункт **Дополнительные сведения**.

4. Измените информацию об активах.

5. Нажмите кнопку **Сохранить**.

Информация изменена.

Также вы можете изменить информацию об одном активе из его карточки по кнопке **Редактировать**.

5.1.8. Присвоение значимости активам

В MaxPatrol VM для новых активов уровень значимости не определяется автоматически.

Вы можете вручную присвоить активу значимость (низкую, среднюю или высокую), например чтобы расставить приоритеты во время устранения уязвимостей.

► Чтобы присвоить активам уровень значимости:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. Выберите активы в таблице.

3. В панели инструментов нажмите .

   Откроется окно **Изменение значимости <N> активов**.

4. В раскрывающемся списке выберите уровень значимости.

5. Нажмите кнопку **Применить**.

Активам присвоен уровень значимости.

Также вы можете перейти к присвоению уровня значимости одному активу из его карточки по кнопке **Установить значимость** или по кнопке **Редактировать** → **Паспорт**.

5.1.9. Удаление активов

При работе с системой может возникнуть ситуация, когда вы выявили неактуальные активы (например, была неправильно настроена задача сбора данных).

► Чтобы удалить активы:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. Выберите активы в таблице.

3. В панели инструментов нажмите и подтвердите удаление.

Выбранные активы удалены.

Также вы можете удалить один актив из его карточки по кнопке **Удалить**.

5.2. Аналитика по активам

По умолчанию на странице **Активы** отображаются все активы, данные о которых есть в системе, из групп, к которым у вас есть доступ (включая вложенные группы).

Информация об активах в системе представлена в виде модели активов, то есть структурированной совокупности всех атрибутов активов. В модель актива также могут быть добавлены пользовательские поля. Для удобства работы вы можете использовать табличное представление данных об активах и любых их атрибутах. В этом случае поля модели активов преобразуются в поля таблицы активов, а атрибуты активов — в значения. В таблице активов вы можете:

— фильтровать записи;

— изменять состав колонок;

— группировать записи;

— анализировать данные;

— ограничивать количество записей;

— отображать только уникальные записи;

— выбирать порядок сортировки.

После группировки вы можете анализировать данные об активах с помощью математических операций.

Вы можете изменять список отображаемых данных об активах с помощью панели фильтрации — последовательно выбирая операции, а также с помощью поля поиска — указав название актива, его описание, MAC- или IP-адрес. Способы фильтрации сочетаются друг с другом: ввод значения в поле поиска дает возможность перейти к созданию запроса на языке PDQL по кнопке ⌨.

Подробнее фильтрация активов описана в документе Синтаксис языка запросов PDQL.

В этом разделе

5.2.1. Фильтрация активов по группе

Вы можете использовать стандартные и пользовательские группы активов, чтобы фильтровать активы. Иерархический список групп активов отображается на странице **Активы** в панели **Группы активов**.

► Чтобы отфильтровать активы по группе:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Группы активов** выберите группу активов.

Активы отфильтрованы.

Для удобства анализа вы можете настроить отображение не всех активов из выбранных, а только их части, фильтруя активы с помощью запросов на языке PDQL.

Кроме того, вы можете настроить представление данных в таблице активов. Например, чтобы отсортировать записи об активах в таблице.

5.2.2. Фильтрация активов с помощью PDQL-запроса

Вы можете использовать запросы на языке PDQL, чтобы фильтровать активы.

► Чтобы отфильтровать активы с помощью PDQL-запроса:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Фильтрация**.

   Откроется окно PDQL-запроса.

3. В поле **Фильтр** введите запрос на языке PDQL (см. документ Синтаксис языка PDQL).
4. Нажмите кнопку **Применить**.

Активы отфильтрованы.

Кроме того, вы можете перейти к созданию и изменению PDQL-запроса по нажатию на значок ⌨.

В открывшемся окне вы можете настроить представление данных в таблице активов (см. документ Синтаксис языка PDQL).

Если вы хотите регулярно фильтровать данные по заданному набору атрибутов и их значений, вы можете сохранить этот набор как запрос.

5.2.3. Представление данных об активах

По умолчанию на странице **Активы** представлены все активы, к которым у вас есть доступ.

Для каждого актива в таблице отображаются:

— название и графическое обозначение его типа;

— название операционной системы;

— дата и время создания актива;

— дата и время последнего изменения данных.

Вы можете изменить состав колонок таблицы и настроить отображение данных в ней:

— ограничить количество записей;

— отобразить только уникальные записи;

— выбрать порядок сортировки.

Кроме того, вы можете сгруппировать данные об активах и проанализировать их с помощью математических функций.

Если вы хотите регулярно настраивать представление данных в таблице с помощью набора атрибутов и их значений, вы можете сохранить этот набор как запрос.

В этом разделе

Выбор колонок для таблицы активов (см. раздел 5.2.3.1)

Ограничение количества записей в таблице активов (см. раздел 5.2.3.2)

Отображение уникальных записей в таблице активов (см. раздел 5.2.3.3)

Сортировка записей в таблице активов (см. раздел 5.2.3.4)

См. также

Группировка и анализ данных об активах с помощью математических операций (см. раздел 5.2.4)

Работа с пользовательскими и общими запросами (см. раздел 5.2.6)

5.2.3.1. Выбор колонок для таблицы активов

► Чтобы выбрать колонки для таблицы активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт ||| **Выбор полей**.

3. В открывшемся окне **Выбор полей** выберите колонки для таблицы активов.

   Если требуется, включите отображение только уникальных записей в таблице.

Примечание. Вы можете отобразить только уникальные записи в таблице позднее (см. раздел 5.2.3.3).

4. Нажмите кнопку **Применить**.

В таблице активов отображены выбранные колонки с данными.

5.2.3.2. Ограничение количества записей в таблице активов

► Чтобы ограничить количество записей в таблице активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Ограничение**.

3. В открывшемся окне в поле **Максимальное количество строк** введите количество строк таблицы.

4. Если требуется, включите отображение всех записей.

5. Нажмите кнопку **Применить**.

Количество записей в таблице активов ограничено.

5.2.3.3. Отображение уникальных записей в таблице активов

► Чтобы отобразить уникальные записи в таблице активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Уникальность**.

В таблице активов отображены уникальные записи.

Кроме того, вы можете включить отображение только уникальных записей в таблице при выборе колонок для таблицы активов (см. раздел 5.2.3.1).

5.2.3.4. Сортировка записей в таблице активов

► Чтобы отсортировать данные в таблице активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Сортировка**.

3. В открывшемся окне в поле **Сортировка по полям** укажите колонки таблицы активов.

4. Если требуется, измените направление сортировки.

5. Нажмите кнопку **Применить**.

Данные в таблице активов отсортированы.

5.2.4. Группировка и анализ данных об активах с помощью математических операций

Вы можете анализировать сгруппированные данные об активах с помощью математических операций над данными в таблице активов. Для выполнения операций используются функции (см. приложение А).

► Чтобы сгруппировать и проанализировать данные об активах:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Группировка и агрегация**.

   Откроется окно группировки и анализа данных.

3. В раскрывающемся списке **Группировка** выберите поля, по которым требуется сгруппировать активы.

   Примечание. Вы можете выбрать не более десяти полей.

4. В раскрывающемся списке выберите функцию.

5. В раскрывающемся списке выберите название колонки таблицы, над данными которой требуется выполнить математическую операцию.

6. Если требуется, укажите псевдоним.

   Вы можете проанализировать данные об активах, выбрав несколько математических операций по нажатию + .

Вы можете удалять математические операции по нажатию 🗑 в строке операции.

7. Нажмите кнопку **Применить**.

В таблице отображены результаты группировки и анализа данных об активах.

Вы также можете выполнить группировку и анализ данных отдельно.

Если вы хотите регулярно группировать и анализировать данные в таблице с помощью набора атрибутов и их значений, вы можете сохранить этот набор как запрос (см. раздел 5.2.6).

См. также

Работа с пользовательскими и общими запросами (см. раздел 5.2.6)

5.2.5. Фильтрация активов с помощью объединения запросов

Для подготовки аналитики по активам часто требуется получать данные об их атрибутах, которые связаны между собой, но находятся на разных уровнях иерархии в модели активов или относятся к активам разных типов. Чтобы получать все эти данные в одной таблице, вы можете объединять результат ранее выполненного PDQL-запроса с результатом выполнения другого PDQL-запроса.

Избежать повторения названий колонок таблиц при объединении запросов можно с помощью псевдонимов. В качестве псевдонима для PDQL-запроса вы можете использовать один или несколько символов, которые будут добавлены к названиям всех колонок в таблице с результатами объединения запроса. Например, при использовании псевдонима A колонки таблицы будут иметь названия 1, 2, ..., n, A.1, A2, ..., A.n.

► Чтобы объединить результат выполненного запроса с результатом выполнения другого запроса:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. Введите запрос на языке PDQL (см. документ Синтаксис языка PDQL).

3. В панели фильтрации нажмите + и в раскрывшемся меню выберите пункт **Объединение**.

   Откроется окно **Объединение с результатом другого запроса**.

4. В поле **Запрос** введите запрос на языке PDQL.

   С результатом выполнения этого запроса будет объединен результат ранее выполненного PDQL-запроса.

   Примечание. Вы можете скопировать условие фильтрации, нажав ссылку **Вставить условие из сохраненного запроса** и выбрав условие из списка.

5. Если требуется, в поле **Псевдоним запроса** введите псевдоним.

   Примечание. Псевдоним запроса может содержать латинские и русские буквы, цифры, знак подчеркивания и дефис; не может начинаться с дефиса.

   В списке **Колонки, доступные для объединения** отобразятся названия всех колонок таблиц.

6. В поле **Условие объединения запроса** введите условие объединения (см. документ Синтаксис языка PDQL).

   Для создания условия надо использовать только названия колонок таблиц из списка **Колонки, доступные для объединения**.

7. Нажмите кнопку **Применить**.

Запросы объединены, результат отобразится в таблице активов.

Если вы хотите регулярно искать и анализировать данных об активах с помощью двух запросов, вы можете сохранить объединенный запрос.

5.2.6. Работа с пользовательскими и общими запросами

Вы можете фильтровать активы в MaxPatrol VM с помощью запросов на языке PDQL.

В системе предусмотрены готовые запросы для фильтрации активов и настройки представления данных о них в таблице. Эти запросы расположены в папках, вложенных в стандартную папку **Стандартные запросы**.

Примечание. Вы не можете изменять или удалять стандартные папки и запросы.

Для решения рабочих задач вы можете создавать свои пользовательские запросы и папки и помещать их в стандартную папку **Пользовательские запросы**. К пользовательским запросам и папкам не имеет доступа никто, кроме их создателя. Кроме того, вы можете создавать в стандартной папке **Общие запросы** вложенные папки (или перемещать туда пользовательские папки) и запросы, к которым будут иметь доступ все пользователи системы.

На странице **Активы** вы можете работать с пользовательскими и общими вложенными папками и запросами.

В этом разделе

Изменение названия и расположения запроса (см. раздел 5.2.6.7)

Удаление запроса (см. раздел 5.2.6.8)

5.2.6.1. Создание папки запросов

Для удобства работы вы можете создавать папки, чтобы помещать туда запросы для фильтрации активов по выбранным критериям.

► Чтобы создать папку запросов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** нажмите + .

   Откроется окно **Новая папка**.

3. В поле **Название** введите название папки запросов.
4. В раскрывающемся списке **Расположение** выберите папку, внутри которой требуется создать папку запросов.

   По умолчанию папка создается внутри папки **Пользовательские запросы**.

5. Нажмите кнопку **Создать**.

Папка запросов создана.

Кроме того, вы можете перейти к созданию папки внутри уже созданной папки запросов, наведя курсор на созданную папку и нажав ⋮ .

5.2.6.2. Изменение папки запросов

Вы можете изменять названия папок запросов или перемещать их в другие папки.

► Чтобы изменить папку запросов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** наведите курсор на папку, нажмите ⋮ и в раскрывшемся меню выберите пункт **Переместить или переименовать**.

   Откроется окно **<Название папки>**.

3. В поле **Новое название** введите название папки запросов.

4. В раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить папку запросов.
5. Нажмите кнопку **Сохранить**.

Папка запросов изменена.

5.2.6.3. Удаление папки запросов

Вы можете удалять папки запросов. При удалении папки все вложенные папки и запросы также будут удалены.

► Чтобы удалить папку запросов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** наведите курсор на папку, нажмите ⋮, в раскрывшемся меню выберите пункт **Удалить папку** и при необходимости подтвердите удаление.

Папка запросов удалена.

5.2.6.4. Сохранение запроса

Вы можете сохранять условия запросов для фильтрации активов, чтобы использовать их повторно.

Условие запроса может включать в себя:

— условие фильтрации активов на языке PDQL (см. раздел 5.2.2);

— настроенное представление данных об активах в таблице (см. раздел 5.2.3);

— условие группировки данных об активах и параметры их анализа с помощью математических функций (см. раздел 5.2.4).

► Чтобы сохранить условие запроса:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. Добавьте условие запроса в панель фильтрации.
3. В панели фильтрации нажмите ⋮ и в раскрывшемся меню выберите пункт **Сохранить как новый**.

   Откроется окно **Новый запрос**.

4. В поле **Название** введите название пользовательского запроса.

5. Если требуется, в раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить этот запрос.
6. Нажмите кнопку **Сохранить**.

Условие запроса сохранено.

5.2.6.5. Создание запроса на основе существующего

Вы можете создавать новые запросы на основе имеющихся запросов — стандартных, общих или пользовательских.

► Чтобы создать запрос на основе имеющегося:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** наведите курсор на запрос, нажмите ⋮ и в раскрывшемся меню выберите пункт **Сохранить как новый**.

   Откроется окно **Новый запрос**.

3. В поле **Название** введите название пользовательского запроса.
4. Если требуется, в раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить этот запрос.
5. Нажмите кнопку **Сохранить**.

Запрос создан.

5.2.6.6. Изменение условия запроса

► Чтобы изменить условие запроса:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** выберите запрос.

   Условие запроса будет добавлено в панель фильтрации.

3. Измените условие запроса.
4. В панели фильтрации нажмите ⋮ и в раскрывшемся меню выберите пункт **Сохранить**.

Условие запроса изменено.

5.2.6.7. Изменение названия и расположения запроса

Вы можете изменять названия запросов или перемещать их в другие папки.

Примечание. После перемещения пользовательского запроса в папку **Общие запросы** другие пользователи смогут изменять, перемещать или удалить его.

► Чтобы изменить запрос:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** наведите курсор на запрос, нажмите ⋮ .
3. В раскрывшемся меню выберите пункт **Переместить или переименовать**.

   Откроется окно **<Название запроса>**.

4. В поле **Новое название** введите название запроса.
5. В раскрывающемся списке **Расположение** выберите папку, в которую требуется переместить запрос.
6. Нажмите кнопку **Сохранить**.

Запрос изменен.

Кроме того, вы можете перемещать запросы, нажав ⋮ и в раскрывшемся меню выбрав пункт **Перенести в общие** или **Перенести в личные**.

5.2.6.8. Удаление запроса

► Чтобы удалить запрос:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Запросы** наведите курсор на запрос, нажмите ⋮ .
3. В раскрывшемся меню выберите пункт **Удалить запрос** и подтвердите удаление.

Запрос удален.

5.2.7. Экспорт данных об активах в CSV-файл

Данные об активах в системе могут быть представлены в виде таблицы. Вы можете экспортировать отфильтрованные и сгруппированные данные об активах из таблицы в файл формата CSV для последующего анализа.

► Чтобы экспортировать данные об активах в файл:

1. В главном меню выберите раздел **Активы**.

Откроется страница **Активы**.

2. Выберите записи об активах.

3. Внизу таблицы активов в сообщении о количестве выбранных записей нажмите .

   Система сформирует CSV-файл и выгрузит его в локальную папку, указанную в свойствах браузера.

См. также

Фильтрация активов с помощью PDQL-запроса (см. раздел 5.2.2)

Фильтрация активов по группе (см. раздел 5.2.1)

Представление данных об активах (см. раздел 5.2.3)

Группировка и анализ данных об активах с помощью математических операций (см. раздел 5.2.4)

5.3. Работа с конфигурацией актива

В ряде случаев (например, при анализе результатов сканирования) вам нужно видеть, различались ли конфигурации выбранного актива в два разных момента времени. Также вам может потребоваться история изменений, произошедших с активом, чтобы найти в заданном промежутке времени опасные, подозрительные или интересные изменения актива.

В этом разделе

5.3.1. Экспорт истории конфигурации актива

В ряде случаев (например, при анализе результатов сканирования) вам может потребоваться история изменений, произошедших с активом.

Примечание. Вы можете экспортировать историю изменений только одного актива.

► Чтобы экспортировать историю изменений актива:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В таблице активов выберите актив.

3. В панели инструментов нажмите .

   Откроется окно **Параметры для экспорта**.

4. Выберите период времени, за который вы хотите получить историю изменений конфигурации актива.
5. Установите флажки для нужных вам параметров конфигурации актива.
6. Нажмите кнопку **Экспортировать**.

Система сформировала XML-файл и выгрузила его в локальную папку, указанную в свойствах браузера. Файл содержит структурированное представление истории изменений, произошедших с активом за выбранный период времени, с учетом выбранных параметров конфигурации актива.

5.3.2. Сравнение конфигураций актива

В ряде случаев (например, при анализе результатов сканирования) вам может потребоваться информация о том, различались ли конфигурации одного или нескольких выбранных активов в два разных момента времени.

Примечание. Если на любой из выбранных вами моментов времени актив не существовал, то система будет считать, что в этот момент времени актив не содержал ни одного элемента.

► Чтобы сравнить конфигурации одного или нескольких активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите ⇄.

   Откроется окно **Сравнение конфигураций для <N> активов**.
4. Выберите моменты времени, на которые будет производиться сравнение конфигураций.
5. Нажмите кнопку **Сравнить**.

   Откроется страница со списком активов.
6. Если требуется, в панели инструментов включите **Только изменения**, чтобы исключить из просмотра те активы, по которым не было изменений.

Примечание. Вы можете просмотреть подробный результат сравнения конфигураций, выбрав интересующий вас актив.

Примечание. Также вы можете экспортировать в XML-файл результаты сравнения конфигураций по кнопке **Экспорт**.

5.4. Топология сети. Работа с картой сети

Реальные связи между активами в сети представлены в виде карты сети. Она строится на основе информации об активе или группе активов. Топология сети отображается на странице **Активы** на вкладке **Топология**. Вершинами графа являются активы сети, а ребрами — связи между ними.

Связи между активами отображаются на карте на основе данных об активе, полученных при сканировании сети в режиме белого ящика (модулем audit). Если данные актива изменились, то после сканирования карта обновится.

С помощью карты сети вы можете выявлять:

— связи между активами;

— отсутствие необходимых связей между активами;

— ошибки настройки активов (например, объединенные в кластер маршрутизаторы имеют разные параметры);

— проблемы архитектуры сети (например, активы из одной сети имеют разные сетевые маски);

— постороннее оборудование, подключенное к внутренним сетям.

Для удобства каждый тип актива на карте сети имеет свое графическое обозначение.

Таблица 1. Графические обозначения активов на карте сети

Тип актива	Графическое обозначение
Рабочая станция	
Сервер	
Маршрутизатор	
Сетевой коммутатор	
Межсетевой экран	
Точка доступа	
Неизвестное сетевое устройство	
Сетевой принтер	
Узел	
Сеть	
Служба каталогов Microsoft Active Directory	
Гипервизор	

Тип актива	Графическое обозначение
Контроллер удаленного управления сервером (iDRAC или iLO)	

В этом разделе

5.4.1. Настройка отображения активов на карте сети

На вкладке **Топология** вы можете:

— изменять число активов в сети, отображаемых на карте сети;

— изменять отображение карты сети в рабочей области;

— отображать или скрывать названия активов на карте сети.

Вы можете настраивать отображение активов на карте сети для одной или нескольких групп активов. Для удобства работы с системой вид карты сети сохраняется для каждой учетной записи пользователя.

Кроме того, вы можете изменять расположение активов на карте сети курсором.

► Чтобы вернуть вид карты сети по умолчанию,

в панели инструментов нажмите кнопку **Расположить узлы по умолчанию**.

Выбор количества активов

По умолчанию на карте сети отображаются не более 20 активов, входящих в одну сеть. Вы можете изменить это максимальное число активов. Например, если необходимо просмотреть все активы, входящие в сеть.

► Чтобы выбрать максимальное число активов, отображаемых для одной сети:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели инструментов выберите вкладку **Топология**.

   Отобразится карта сети.

3. В панели инструментов нажмите .

Откроется окно настройки вида карты сети.

4. Укажите число активов в поле **Уменьшать узлы в сетях больше <число> узлов**.

На карте для каждой сети отображено выбранное число активов.

Выбор отображения карты сети

Вы можете выбрать отображения карты сети в рабочей области — с прокруткой или без прокрутки.

Если выбран вариант без прокрутки, то на карте сети вы видите все активы и связи между ними. Карта сети занимает всю рабочую область, ее масштаб зависит от количества активов.

Если выбран вариант с прокруткой, то масштаб отображения активов на карте сети увеличивается. Карта сети выходит за пределы рабочей области.

► Чтобы выбрать отображение карты сети в рабочей области:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели инструментов выберите вкладку **Топология**.

   Отобразится карта сети.

3. В панели инструментов нажмите ⋮ .

   Откроется окно настройки вида карты сети.

4. Выберите один из вариантов:

   · Если вы хотите видеть сразу все активы на карте сети, выключите прокрутку.

   · Если вы хотите увеличить масштаб отображения активов на карте сети, включите прокрутку.

Карта сети отображается в рабочей области в соответствии с выбранным вариантом.

Выключение отображения названий активов

По умолчанию на карте сети отображаются названия активов. Вы можете выключить отображение названий активов. Например, если на экране слишком много активов и их названия затрудняют восприятие информации и работу с картой сети.

► Чтобы выключить отображение названий активов на карте:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели инструментов выберите вкладку **Топология**.

   Отобразится карта сети.

3. В панели инструментов нажмите ⋮ .

   Откроется окно настройки вида карты сети.

4. Выключите отображение названий узлов и сетей.

Отображение названий активов на карте выключено.

5.4.2. Просмотр информации об активе

На карте сети отображаются активы, удовлетворяющие условиям фильтра. Вы можете выбрать любой актив или связь между активами, чтобы просмотреть подробную информацию о них.

Активы, удовлетворяющие условиям фильтра, но не выбранные на карте, не изменяют цвет . Активы, выбранные на карте, выделены синим цветом . Активы и связи между активами, не удовлетворяющими условиям фильтра, изменяют цвет на серый .

Кнопки ↙↗ и ↙↗ позволяют сворачивать и разворачивать содержимое активов типа «Сеть».

По нажатию на актив открывается окно с базовой информацией о нем — мини-карточка актива. По ссылке **Карточка актива** вы можете перейти к просмотру состояния актива.

Для актива типа «Сеть» в окне с информацией на вкладке **Свойства** отображаются параметры, а на вкладке **Активы** — список активов.

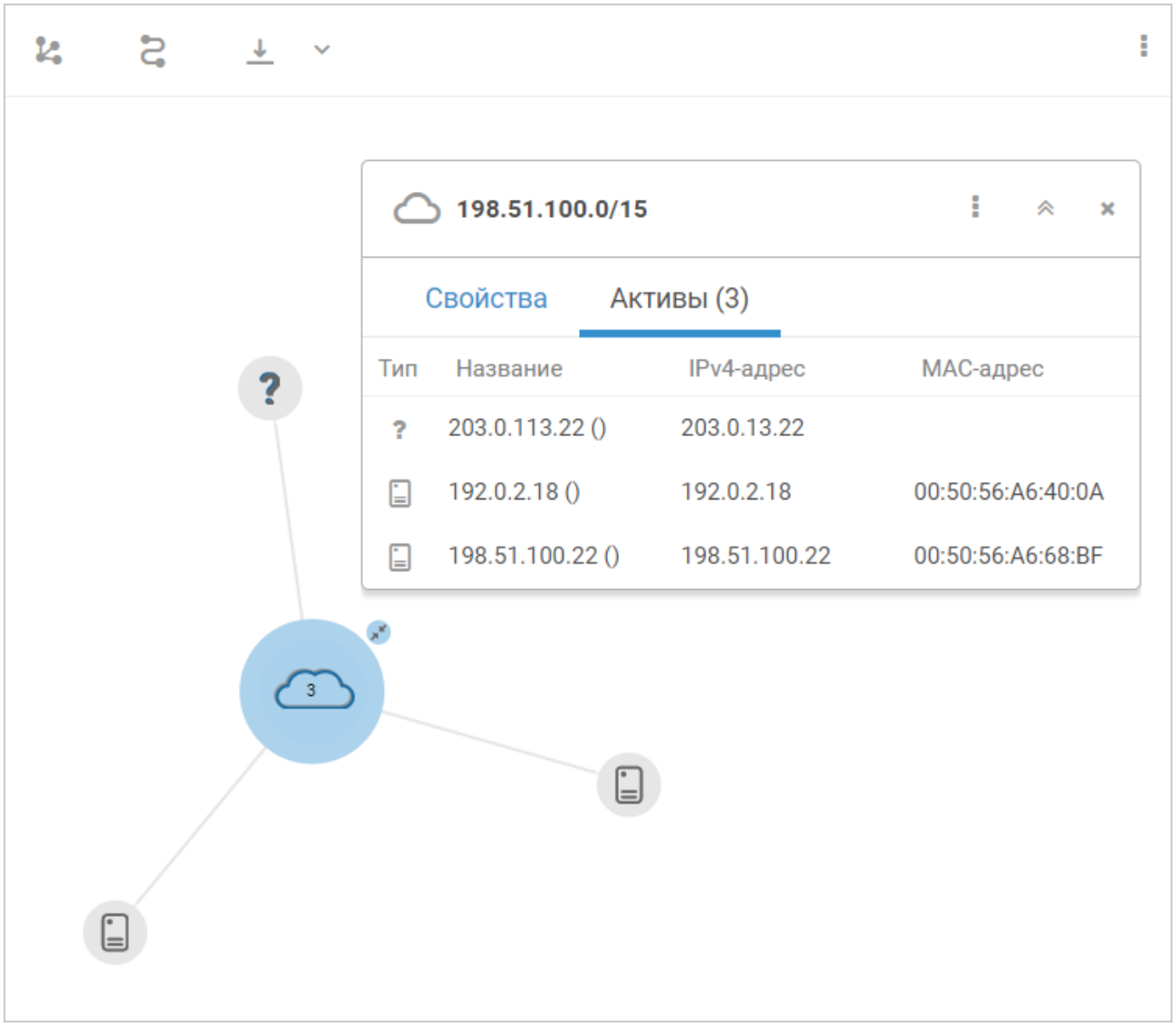

Рисунок 10. Просмотр списка активов для актива типа «Сеть»

По нажатию на связь между активами открывается окно с информацией о типе активов, их параметрах и о связи между ними.

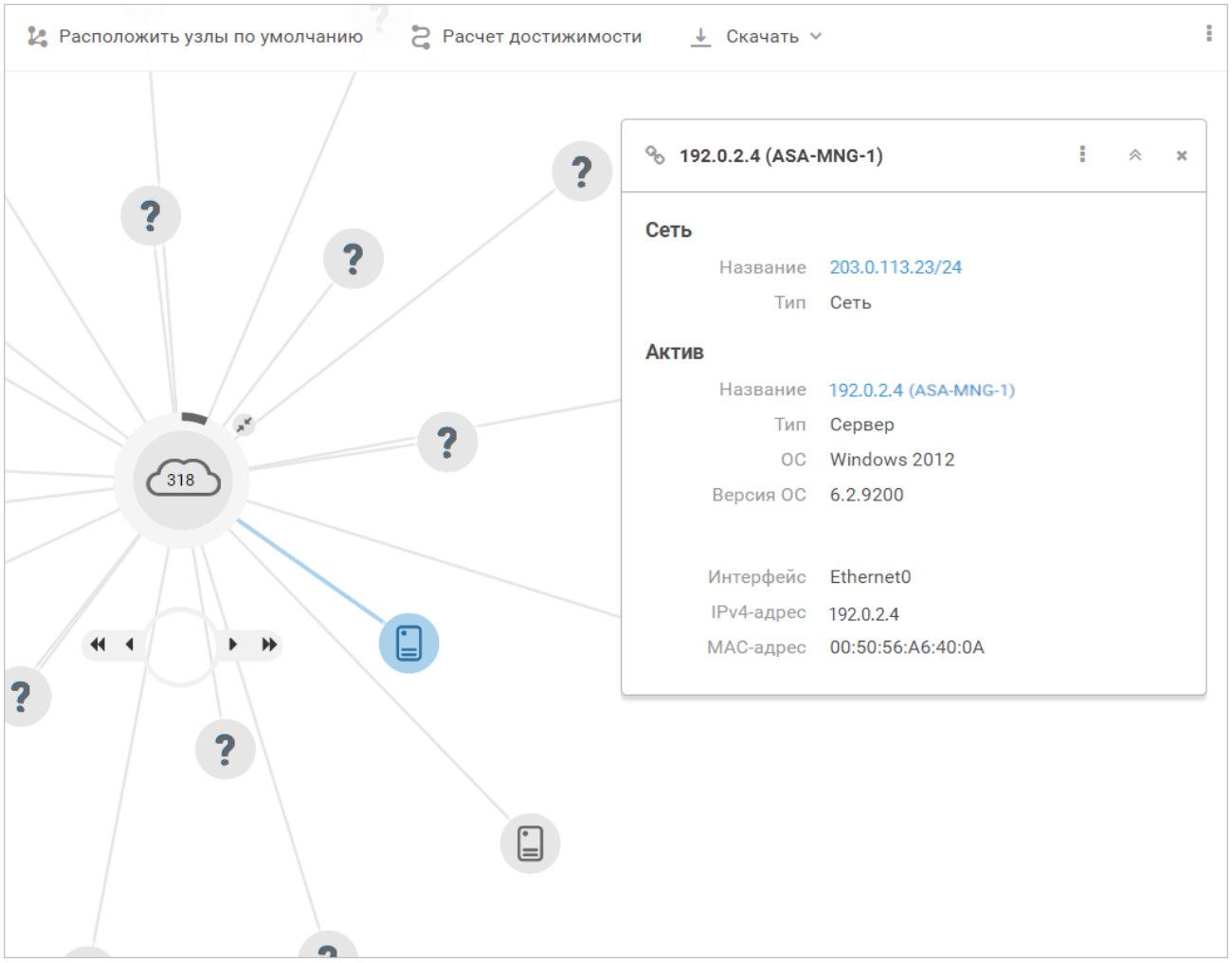

Рисунок 11. Просмотр информации о связи между активами

- Чтобы свернуть окно с информацией об активе или связи между активами,

  нажмите ⌃ .

- Чтобы закрыть окно с информацией об активе или связи между активами,

  нажмите ✖ .

5.4.3. Достижимость между активами

Достижимость — это свойство актива и группы активов, означающее возможность их взаимодействия с другими активами и группами активов в сети. Путь между достижимыми активами и группами активов (маршрут) определяется выбранными параметрами достижимости.

С помощью расчета достижимости вы можете:

— контролировать доступность активов и групп активов в сети;

— проверять правильность установки и настройки сетевых устройств;

— проверять работу политик доступа к активам и группам активов;

— уточнять список активов и групп активов, которые нужно проанализировать во время аудита;

— выявлять активы и группы активов, представляющие угрозу ИБ, и их связи с другими активами и группами активов.

Вы можете рассчитать достижимость от одного актива и (или) группы активов или всех активов и сетевых адресов к активу и (или) группе активов, сетевому адресу, диапазону сетевых адресов.

Вы можете перейти к расчету достижимости по кнопке **Расчет достижимости** в панели инструментов.

В этом разделе

Расчет достижимости от актива (см. раздел 5.4.3.1)

Расчет достижимости к активу (см. раздел 5.4.3.2)

5.4.3.1. Расчет достижимости от актива

Вы можете рассчитать достижимость от выбранного актива и (или) группы активов к другому активу и (или) группе активов, сетевому адресу, диапазону сетевых адресов.

► Чтобы рассчитать достижимость от актива:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. Выберите активы в таблице.

3. В панели инструментов нажмите кнопку **Расчет достижимости** и в раскрывшемся меню выберите пункт **Куда открыт доступ**.

   В новой вкладке браузера откроется страница **Активы**, в таблице активов будут отображаться выбранные активы. В панели **Топология** откроется окно **Расчет достижимости**.

   Активы, от которых рассчитывается достижимость, указаны в блоке параметров **Источники**.

4. В блоке параметров **Цели** выберите конечные точки маршрутов.

5. Если требуется, укажите дополнительную информацию о протоколах и портах цели по ссылке **Уточнить протоколы и порты цели**.
6. Нажмите кнопку **Рассчитать маршруты**.

   Система сформирует списки доступных целей и маршрутов к ним.

   Доступные сетевые адреса и маршруты к ним отобразятся на вкладке **Доступные**.
7. Если требуется, по кнопке выберите способ группировки маршрутов.
8. Выберите конечную точку маршрута.

В раскрывающемся блоке отображаются маршруты достижимости выбранной цели, сгруппированные по парам «протокол — порт». Для маршрутов также могут отображаться правила маршрутизации, трансляции сетевых адресов (NAT) и списков управления доступом (ACL).

Маршрут достижимости отображается также на карте сети.

Кроме того, вы можете перейти к расчету достижимости по кнопке **Расчет достижимости** на вкладке **Топология**.

5.4.3.2. Расчет достижимости к активу

Вы можете рассчитать достижимость от актива и (или) группы активов или всех активов и сетевых адресов к выбранному активу и (или) группе активов.

► Чтобы рассчитать достижимость к активу:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.
2. Выберите активы в таблице.
3. В панели инструментов нажмите кнопку **Расчет достижимости** и в раскрывшемся меню выберите пункт **Откуда открыт доступ**.

   В новой вкладке браузера откроется страница **Активы**, в таблице активов будут отображаться выбранные активы. В панели **Топология** откроется окно **Расчет достижимости**.

   Активы, от которых рассчитывается достижимость, указаны в блоке параметров **Цели**.
4. Если требуется, укажите дополнительную информацию о протоколах и портах цели по ссылке **Уточнить протоколы и порты цели**.
5. В блоке параметров **Источники** выберите начальные точки маршрутов. Начальными точками маршрутов могут быть активы, группы активов или все активы и сетевые адреса.
6. Нажмите кнопку **Рассчитать маршруты**.

Система сформирует списки доступных источников и маршрутов к выбранным активам.

7. Если требуется, по кнопке выберите способ группировки маршрутов.
8. Выберите начальную точку маршрута.

В раскрывающемся блоке отображаются маршруты достижимости выбранной цели, сгруппированные по парам «протокол — порт». Для маршрутов также могут отображаться правила маршрутизации, трансляции сетевых адресов (NAT) и списков управления доступом (ACL).

Маршрут достижимости отображается также на карте сети.

Кроме того, вы можете перейти к расчету достижимости по кнопке **Расчет достижимости** на вкладке **Топология**.

5.4.4. Экспорт топологии активов

MaxPatrol VM собирает информацию об активах в сети и представляет ее в виде карты. Вы можете экспортировать настроенную топологию сети в виде графического файла для последующего анализа.

► Чтобы экспортировать топологию сети:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели инструментов выберите вкладку **Топология**.

   Отобразится карта сети.

3. В панели инструментов нажмите кнопку **Скачать** и в раскрывшемся меню выберите формат графического файла: PNG или SVG.

Топология сети экспортирована.

6. Работа с уязвимостями

Уязвимость — это недостаток, обнаруженный в IT-системе. Используя этот недостаток, злоумышленник может нарушить конфиденциальность, целостность или доступность данных. Уязвимости могут возникать, например, в результате ошибок программирования.

MaxPatrol VM предназначен не только для поиска уязвимостей на активах, но и для управления ими. Процесс работы с уязвимостями в MaxPatrol VM состоит из следующих этапов:

1. Инвентаризация активов.
2. Классификация и оценка активов.
3. Выявление и приоритизация уязвимостей.
4. Устранение уязвимостей.
5. Проверка результатов.

Инвентаризация активов

Цель этапа: обнаружить и идентифицировать активы в вашей IT-инфраструктуре.

При сканировании IT-инфраструктуры организации MaxPatrol VM обнаруживает активы и создает о них записи. Вы также можете добавлять активы вручную, импортировать из файла или из MP8. Обнаруженные активы необходимо идентифицировать, чтобы избежать их дублирования. И не менее важно поддерживать информацию об активах в актуальном состоянии, иначе вы можете пропустить часть уязвимостей в IT-инфраструктуре. Вы можете использовать виджет **Актуальность данных об активах**, чтобы отслеживать, сколько у вас активов с отсутствующими или неактуальными данными сканирования.

Результат этапа: вы обладаете актуальными данными о том, какие активы есть в IT-инфраструктуре и какая у них конфигурация. На основании этих данных MaxPatrol VM будет обновлять информацию об обнаруженных уязвимостях.

Классификация и оценка активов

Цель этапа: выделить значимые активы, уязвимости на которых могут нанести больше всего вреда.

Вы можете использовать виджет **Значимость активов**, чтобы понять, сколько у вас активов, для которых не указана значимость. Затем вам нужно присвоить значимость максимально возможному количеству активов вручную или с помощью правил специальной политики. Это поможет отсортировать активы по приоритету и оптимизировать сроки устранения уязвимостей на них.

В MaxPatrol VM предусмотрена возможность использовать стандартные и пользовательские группы активов, чтобы было удобнее фильтровать активы. Это поможет вам быстрее проверить их на наличие конкретной уязвимости.

Результат этапа: вы присвоили значимость максимальному количеству активов в IT-инфраструктуре.

Выявление и приоритизация уязвимостей

Цель этапа — приоритизировать уязвимости и настроить автоматическую обработку для максимально возможного их количества.

В MaxPatrol VM выявление уязвимостей происходит автоматически на основании данных об инфраструктуре, постоянно актуализируемой информации об активах. По результатам сканирования в режимах аудита и пентеста (в режимах белого и черного ящика) MaxPatrol VM выявляет открытые сетевые порты и доступные службы, уязвимости в ПО, а также недостатки конфигурации оборудования, серверов и средств защиты. Актуализация данных об уязвимостях в MaxPatrol VM происходит при обновлении Knowledge Base в части уязвимостей, а также при актуализации информации об активах. В результате может быть выявлено значительное количество уязвимостей. Вам необходимо максимально автоматизировать процесс их обработки, чтобы устранять вручную только самые сложные и опасные уязвимости.

В MaxPatrol VM для этих целей используются политики — наборы правил, в соответствии с которыми уязвимости на активах проверяются и обрабатываются. Вы можете просматривать список политик на странице **Система** → **Политики**. Для каждой политики можно создавать и использовать правила обработки уязвимостей (для уязвимостей в статусе «Новая») или правила, по результатам применения которых уязвимости будут отмечены как важные.

> **Примечание.** Управлять политиками может только пользователь с правами администратора. Подробное описание политик см. в Руководстве администратора.

Если уязвимость активно используется в атаках злоумышленников (или будет использоваться в ближайшем будущем), эксперты Positive Technologies относят ее к числу трендовых и об этом появляется соответствующая отметка. На такие уязвимости необходимо обращать повышенное внимание и устранять их в первую очередь.

Вы можете отслеживать отметку **Трендовая** в карточке уязвимости. С помощью политик вы можете отметить все трендовые уязвимости как важные. Также вы можете использовать виджеты **Трендовые уязвимости** и **Трендовые уязвимости на активах**, чтобы оценить количество найденных трендовых уязвимостей (см. раздел 8.1).

Кроме того, вы можете присваивать уязвимостям ключевые слова (метки) для их быстрого поиска, идентификации или категоризации.

Результат этапа: максимальное количество уязвимостей приоритизировано.

Устранение уязвимостей

Цель этапа — оперативно устранять уязвимости на активах.

Если в вашей организации принято регулярно устанавливать патчи и обновления ОС и ПО, вам необходимо лишь проверять отсутствие уязвимостей через определенное количество дней после публикации информации о них в Knowledge Base. Вы можете использовать виджеты по

уязвимостям (например, **Последние добавленные уязвимости**, **Трендовые уязвимости**, **Уязвимости на важных активах**), чтобы контролировать количество уязвимостей в IT-инфраструктуре.

В противном случае вам необходимо после обнаружения уязвимостей обновить версии определенного ПО и установить нужные патчи в определенные сроки. Затем вам нужно использовать политики:

— по плановому устранению уязвимостей — чтобы установить сроки устранения и статус устранения;

— по исключению уязвимостей — чтобы исключить уязвимости, которые, например, появились в результате ложных срабатываний или которые невозможно устранить;

— по устранению уязвимостей вручную — если вы не сможете устранить найденные уязвимости автоматически;

— по отметке «важная» — чтобы самые опасные уязвимости были отмечены как приоритетные.

В MaxPatrol VM вы можете создать задачу на выпуск отчета, чтобы все сотрудники, вовлеченные в процесс устранения уязвимостей, регулярно получали актуальную информацию об активах и уязвимостях.

Уязвимостям могут быть присвоены следующие статусы:

1. **Новая**. MaxPatrol VM обнаружил уязвимость на активе. Необходимо ее классифицировать и понять, как ее устранять.
2. **В работе**. Вы взяли уязвимость в работу и планируете ее устранить. В устранении могут участвовать сотрудники IT-подразделений, например ответственные за установку патчей.
3. **Исправляется**. Устранение уязвимости запланировано — вручную или политикой. Если плановый срок исправления истечет, то уязвимость автоматически перейдет в статус **Требуется проверка**.
4. **Требуется проверка**. Необходимо проверить, удалось ли исправить уязвимость. Для этого нужно выполнить сканирование актива. Если наличие уязвимости подтвердилось, она автоматически перейдет в статус **Просрочено**. Если не подтвердилось — в статус **Устранена**. Если нужно исключить уязвимость из числа подлежащих проверке, вы можете перевести ее в статус **Исключена**.
5. **Просрочено**. Истек запланированный срок исправления уязвимости, и в результате сканирования актива ее присутствие подтвердилось.
6. **Исключена**. Вы можете исключить уязвимость из числа подлежащих устранению. Причины могут быть разными: например, ее обнаружили на активе с низкой значимостью или же заведомо известно, что на всех активах с подобными уязвимостями уже приняты защитные меры.
7. **Устранена**. Уязвимость была устранена или актив был удален.

Результат этапа: все выявленные уязвимости на активах запланированы к устранению, исключены из рассмотрения или устранены. Вы можете оперативно получать и передавать информацию о том, сколько у вас уязвимостей и в каких статусах.

Доступ к информации о найденных, запланированных к устранению, исключенных из рассмотрения, просроченных и устраненных уязвимостях обеспечивается с помощью запросов на языке PDQL. Он позволяет гибко запрашивать данные, фильтруя их как по параметрам уязвимостей, так и по параметрам активов, на которых эти уязвимости присутствуют. На базе этих данных строятся виджеты, с помощью которых можно отслеживать состояние защищенности IT-инфраструктуры организации и планировать работу по управлению уязвимостями.

Подробное описание псевдонимов уязвимостей см. в документе Синтаксис языка запросов PDQL.

Проверка результатов

Цель этапа: проверить, как быстро устраняются критически опасные уязвимости и соблюдаются ли политики устранения уязвимостей.

Вы можете использовать виджеты по активам и уязвимостям, расположенные на главной странице MaxPatrol VM. Например, если за выбранный период количество активов без указанной значимости выросло, стало больше важных и трендовых уязвимостей, не исправленных в срок, вам необходимо проверить, как настроены политики устранения уязвимостей. Если количество уязвимостей на значимых активах уменьшилось, то вы можете запланировать устранение уязвимостей на менее приоритетных активах.

В этом разделе

6.1. Карточка уязвимости

MaxPatrol VM может обнаруживать уязвимости на активах. Найденная уязвимость отображается в таблице активов в столбце **Уязвимость**. По ссылке в этом столбце вы можете перейти в карточку уязвимости, где доступна структурированная информация о ней: уровень опасности, описание уязвимости и способов ее устранения, метрики CVSS, а также ссылки на публичные базы данных, в которых описаны уязвимости такого типа (в частности, на Common Vulnerabilities and Exposures и банк данных угроз ФСТЭК). Все эти сведения помогают понять, какой приоритет имеет уязвимость при ее устранении.

Если уязвимость активно используется в атаках злоумышленников (или будет использоваться в ближайшем будущем), эксперты Positive Technologies относят ее к числу трендовых и об этом появляется соответствующая отметка. На такие уязвимости необходимо обращать повышенное внимание и устранять их в первую очередь.

Также необходимо отслеживать уязвимости в программном обеспечении, для использования которых существуют опубликованные эксплойты. Эксплойты позволяют даже неопытному злоумышленнику воспользоваться уязвимостями, автоматизировать атаку и получить контроль над важными ресурсами. Такие уязвимости имеют в MaxPatrol VM дополнительную отметку **Эксплойт**. Кроме того, дополнительными отметками обозначены уязвимости, которые могут эксплуатироваться удаленно, и уязвимости, которые можно исправить, выполнив определенные условия (например, обновив программное обеспечение).

В карточке уязвимости также отображаются типы последствий, к которым может привести эксплуатация уязвимости: удаленное выполнение кода (RCE), повышение привилегий (LPE), отказ в обслуживании (DoS).

Активы / important asset (192.0.1.1) Состояние на сейчас

3,6 **Уязвимость, связанная с распределением пула ядра Windows** | CVE-2014-4064

Изменить статус Отметить как важную Изменить метки

Обнаружена 16 октября, 01:46

Основная информация

Опасность	Низкий уровень
Эксплойт	Есть
Удаленная эксплуатация	Да
Статус	Новая
Устранение	Нет политики
Актив	important asset (192.0.1.1)

Описание

Уязвимость, позволяющая получить доступ к конфиденциальной информации, существует в Windows и связана с обработкой памяти ядра. Эксплуатация данной уязвимости позволяет злоумышленнику получить информацию об адресах памяти или другие сведения о ядре.

Как исправить

Используйте рекомендации производителя:

http://technet.microsoft.com/en-us/security/bulletin/ms14-045

Метрики CVSS v2

Общая оценка	3.6
Базовый вектор	4.9 — AV:L/AC:L/Au:N/C:C/I:N/A:N
Временной вектор	3.6 — E:U/RL:OF/RC:C

Ссылки

http://technet.microsoft.com/en-us/security/bulletin/ms14-045

Дополнительная информация

Дата публикации	12 августа 2014, 07:00
Идентификатор	CVE-2014-4064
Пентест-проверка	Неприменима
Уязвимое ПО	Windows
Способ обнаружения	Расчет

Найдена уязвимость в ОС Microsoft Windows

ОС на узле

Класс	OperatingSystem.Windows.WindowsHost
Название	Microsoft Windows
Операционная система	Windows 7
Архитектура	x86
Пакет обновления	1

Свернуть подробности

Активы с такими же уязвимостями

Значимость	Активы
Высокая	0
Средняя	0
Низкая	0
Не определена	18
Всего	18

Группы с такими же уязвимостями

Группа	Активы
Unmanaged hosts	18

Идентификаторы в базах данных

Идентификатор	Активы
CVE-2014-4064	18
BDU:2015-00752	18
MP8ID: MP8ID-413493	18

Рисунок 12. Карточка уязвимости

Уязвимость может быть рассчитана на основе данных об активе или обнаружена во время сканирования IT-инфраструктуры модулем pentest. Подробнее см. Руководство по настройке источников.

Карточка уязвимости заполняется информацией из Knowledge Base, но в случае если расчет уязвимости был выполнен на основе бюллетеня безопасности, рекомендации по исправлению уязвимости будут заполнены информацией из этого бюллетеня. В карточке можно изменять статус уязвимости, отмечать уязвимость как важную или проставлять метки.

Все уязвимости на активах типизированы. У каждого типа есть паспорт, который содержит общую справочную информацию обо всех уязвимостях, которые к нему принадлежат. Паспорт выглядит так же и содержит ту же информацию, что и карточка уязвимости, за исключением того, что в паспорте нет информации об уязвимостях на конкретных активах (не указаны даты и способы обнаружения, контекстные метрики CVSS).

Вы можете группировать активы с одинаковыми уязвимостями с помощью псевдонимов на языке PDQL (см. документ Синтаксис языка запроса PDQL).

См. также

Виджеты по активам (см. раздел 8.1)

6.2. Массовые операции над уязвимостями

Для удобства и экономии времени вы можете выполнять массовые операции над уязвимостями: менять статусы, отмечать уязвимости как важные, применять правила обработки уязвимостей.

В этом разделе

6.2.1. Использование правил

Для уязвимостей, параметры которых менялись вручную, перестают действовать правила политик. Вы можете сбросить параметры и снова применить правила к этим уязвимостям.

► Чтобы применить правила:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите ☰.

   Откроется окно **Выбор полей**.

3. Добавьте поле `Host.@Vulners` и нажмите кнопку **Выполнить**.

В таблице активов отобразятся уязвимости.

Примечание. Подробное описание запросов см. в документе Синтаксис языка запросов PDQL.

4. В таблице активов выберите уязвимости.
5. Выберите вкладку **Уязвимость**.
6. В панели инструментов нажмите кнопку **Использовать правила** и подтвердите применение правил.

Параметры, настроенные вручную, сброшены. Когда закончится перерасчет, на уязвимости начнут распространяться условия политик.

6.2.2. Изменение статуса уязвимостей

► Чтобы изменить статус уязвимостей:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите .

   Откроется окно **Выбор полей**.

3. Добавьте поле `Host.@Vulners` и нажмите кнопку **Выполнить**.
4. В таблице активов выберите уязвимости.
5. Выберите вкладку **Уязвимость**.
6. В панели инструментов нажмите кнопку **Изменить статус** и в раскрывшемся меню выберите статус.

   Откроется окно изменения статуса уязвимостей.

7. Укажите необходимые параметры и нажмите кнопку **Изменить**.

Статус уязвимостей изменен.

6.2.3. Выделение важных уязвимостей

► Чтобы отметить уязвимости как важные:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели фильтрации нажмите .

   Откроется окно **Выбор полей**.

3. Добавьте поле `Host.@Vulners` и нажмите кнопку **Выполнить**.
4. В таблице активов выберите уязвимости.
5. Выберите вкладку **Уязвимость**.
6. В панели инструментов нажмите кнопку **Отметить как важную**.

Уязвимости отмечены как важные.

► Чтобы снять отметку «важная» с уязвимостей:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.
2. В таблице активов выберите уязвимости.
3. Выберите вкладку **Уязвимость**.
4. В панели инструментов нажмите кнопку **Снять отметку важная**.

С уязвимостей снята отметка «важная».

6.2.4. Изменение меток для уязвимостей

Вы можете присваивать уязвимостям ключевые слова для их быстрого поиска, идентификации или категоризации. Такие слова называются метками.

► Чтобы добавить или изменить метки для уязвимостей:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.
2. В панели фильтрации нажмите .

   Откроется окно **Выбор полей**.
3. Добавьте поле `Host.@Vulners` и нажмите кнопку **Выполнить**.
4. В таблице активов выберите уязвимости.
5. Выберите вкладку **Уязвимость**.
6. В панели инструментов нажмите кнопку **Изменить метки**.

   Откроется окно изменения меток.
7. Выберите метки для уязвимостей.
8. Нажмите кнопку **Применить**.

Метки для уязвимостей изменены.

6.3. Оценка уровня опасности уязвимостей на активах по методике ФСТЭК

Предварительно необходимо определить активы в IT-инфраструктуре предприятия, подверженные уязвимостям, и собрать данные об этих активах методом аудита. После этого необходимо создать в соответствии с инструкцией (см. раздел 5.1.3.1):

— группу для активов, для которых нужно рассчитать уровень опасности уязвимостей;

— группу «Периметр» для активов на периметре IT-инфраструктуры предприятия, подверженных уязвимостям и доступных из интернета;

— группу «Критически важные активы» для подверженных уязвимостям активов, которые обеспечивают реализацию критически важных функций и процессов.

Примечание. Если вы создали статические группы, необходимо вручную добавить в них соответствующие активы.

► Чтобы рассчитать уровень опасности уязвимостей на активах:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели **Группы активов** выберите созданную ранее группу активов, для которых нужно рассчитать уровень опасности уязвимостей.

3. В панели фильтрации нажмите ⌨.

4. В открывшемся поле введите следующий PDQL-запрос:

```
select(@Host, Host.HostType, compact(Host.@Groups) as groups, Host.@Vulners,
Host.@Vulners.KB as kb, Host.@Vulners.Score) |
filter(Host.@Vulners) |
join(select(Host.@Vulners.KB as kb, countunique(@Host) as alikeHostsCount) as Q1, kb =
Q1.kb) |
join(select(count(Host.@Id) as hostsCount) as Q2, True) |
calc(Q1.alikeHostsCount/Q2.hostsCount as alikePercent) |
calc(if groups contains "Критически важные активы" then 0.4 else if Host.HostType in
["Server", "Server Controller"] then 0.32 else if Host.HostType = "Network Device" then
0.32 else if Host.HostType = "Desktop" then 0.2 else 0.2 as kK) |
calc(if alikePercent < 0.1 then 0.1 else if alikePercent < 0.5 then 0.12 else if
alikePercent < 0.7 then 0.16 else 0.2 as lL) |
calc(if groups contains "Периметр" then 0.4 else 0.2 as pP) |
calc(kK + lL + pP as I) |
calc(Host.@Vulners.Score*I as total) |
calc(if total >= 7 then "Critical" else if total >= 4.5 then "High" else if total >=1.5
then "Medium" else "Low" as criticality) |
select(@Host, Host.@Vulners, total as "Оценка уязвимости", criticality as "Уровень
опасности уязвимости") |
sort("Оценка уязвимости" desc)
```

Примечание. Расчет по этому запросу выполняется в соответствии с документом ФСТЭК России «Методика оценки уровня критичности уязвимостей программных, программно-аппаратных средств».

5. Нажмите кнопку **Выполнить**.

   В таблице активов отобразятся оценка и уровень опасности уязвимостей. Записи в таблице будут отсортированы по уменьшению уровня опасности.

7. Сбор данных

Примечание. MP 10 Collector может одновременно проводить аудит не более чем на 1000 клиентских компьютерах.

Аудит активов проводится компонентом MP 10 Collector. Компонент имеет модульную структуру и, в зависимости от используемых модулей, может выполнять различные задачи по сбору данных о IT-инфраструктуре организации. Для настройки модуля и указания особенностей сбора информации для модулей создаются шаблоны настройки — профили. Для доступа к активу в параметрах профиля можно выбрать учетную запись.

В этом разделе

7.1. Работа с учетными записями

Учетные записи используются для авторизации на активе для проведения аудита. При добавлении учетной записи вы можете указать одну или несколько меток, соответствующих методу сбора данных, при котором она будет использоваться. Добавлять, изменять и удалять учетные записи вы можете на странице **Учетные записи**.

В этом разделе

См. также

7.1.1. Добавление учетной записи типа «логин — пароль»

► Чтобы добавить учетную запись типа «логин — пароль»:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Логин — пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.

5. В поле **Логин** введите логин учетной записи.

6. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

   Примечание. При вводе различаются заглавные и строчные буквы.

7. Если для доступа к источнику используется доменная учетная запись, в поле **Домен** введите имя домена.

8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.1.2. Добавление учетной записи типа «пароль»

► Чтобы добавить учетную запись типа «пароль»:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Пароль**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.

5. В поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

Примечание. При вводе различаются заглавные и строчные буквы.

6. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.1.3. Добавление учетной записи типа «сертификат»

► Чтобы добавить учетную запись типа «сертификат»:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **Сертификат**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.

   Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.

5. В поле **Сертификат** введите путь к файлу сертификата.

   Вы можете указать расположение файла сертификата по ссылке **Выбрать** или перетащить файл в поле **Сертификат**.

   Внимание! Размер файла сертификата должен быть меньше 100 КБ.

6. Если требуется, в поле **Логин** введите логин учетной записи.

7. Если требуется, в поле **Пароль** введите пароль и подтвердите его в поле **Подтверждение пароля**.

   Примечание. При вводе различаются заглавные и строчные буквы.

8. Нажмите кнопку **Сохранить**.

Учетная запись добавлена.

7.1.4. Добавление учетной записи типа LAPS

MaxPatrol VM позволяет использовать Local Administrator Password Solution (LAPS) в сочетании со службой каталогов Active Directory для сбора данных с активов.

► Чтобы добавить учетную запись типа LAPS:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. В панели инструментов нажмите кнопку **Добавить учетную запись** и в раскрывшемся меню выберите пункт **LAPS**.

   Откроется страница **Добавление учетной записи**.

3. В поле **Название** введите название учетной записи.
4. Если учетная запись добавляется для определенных методов сбора данных, в раскрывающемся списке **Метки** установите флажки у этих методов.
5. В блоке параметров **Параметры подключения** в поле **Адрес** введите FQDN или IP-адрес контроллера домена Active Directory.
6. В блоке параметров **Параметры подключения** в поле **Порт** введите номер TCP-порта для подключения к контроллеру домена.
7. Если требуется, в поле **База поиска активов** введите фильтры для ускорения поиска активов в домене Active Directory.
8. В раскрывающемся меню **Учетная запись Active Directory** укажите учетную запись с правами на просмотр атрибутов объектов типа «Компьютер».
9. Введите логин для подключения к целевым активам.

   Логин по умолчанию — `Administrator`.

10. Нажмите кнопку **Создать**.

Учетная запись типа LAPS добавлена.

7.1.5. Изменение учетной записи

► Чтобы изменить учетную запись:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

   Откроется страница **Учетные записи**.

2. Выберите учетную запись.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. Измените параметры учетной записи.
5. Нажмите кнопку **Сохранить**.

Учетная запись изменена.

7.1.6. Удаление учетной записи

► Чтобы удалить учетную запись:

1. В главном меню в разделе **Сбор данных** выберите пункт **Учетные записи**.

Откроется страница **Учетные записи**.

2. Выберите учетную запись.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Учетная запись удалена.

7.2. Работа со справочниками

В справочниках могут храниться дополнительные данные и сценарии, необходимые для работы модулей. Например, справочники `example_collect_process_changes`, `example_collect_tabular`, `example_collect_text` содержат сценарии на языке программирования Python.

Справочники бывают стандартные и пользовательские. Стандартные справочники предустановлены, вы не можете их изменять и удалять. Создавать, изменять и удалять пользовательские справочники вы можете на странице **Справочники**.

В этом разделе

См. также

Страница «Справочники» (см. раздел 4.6.4)

7.2.1. Создание справочника

► Чтобы создать справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.

   Откроется страница **Справочники**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание справочника**.

3. В поле **Название** введите название справочника.
4. В поле **Содержимое** введите текст для справочника.

Для деления текста на колонки вы можете использовать табуляцию (комбинация клавиш Alt+009). Вы также можете написать текст в любом текстовом редакторе и скопировать в поле **Содержание**.

5. Нажмите кнопку **Сохранить**.

Справочник создан.

7.2.2. Копирование справочника

► Чтобы скопировать справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.

   Откроется страница **Справочники**.

2. Выберите справочник.
3. В панели инструментов нажмите кнопку **Копировать**.

   Откроется окно **Создание справочника**.

4. Если требуется, измените справочник.
5. Нажмите кнопку **Сохранить**.

Справочник скопирован.

7.2.3. Изменение пользовательского справочника

► Чтобы изменить пользовательский справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.

   Откроется страница **Справочники**.

2. Выберите пользовательский справочник.
3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница **Редактирование справочника**.

4. В поле **Название** измените название справочника.
5. В поле **Содержимое** измените содержимое справочника.
6. Нажмите кнопку **Сохранить**.

Пользовательский справочник изменен.

7.2.4. Удаление пользовательского справочника

► Чтобы удалить пользовательский справочник:

1. В главном меню в разделе **Сбор данных** выберите пункт **Справочники**.

   Откроется страница **Справочники**.

2. Выберите пользовательский справочник.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Пользовательский справочник удален.

7.3. Работа с профилями

Профиль — шаблон настройки модуля, описывающий особенности сбора событий с источников или аудита активов.

Профили используются для сохранения параметров модулей. Профили бывают стандартные и пользовательские. Стандартные профили предустановлены, вы не можете их изменять и удалять. На базе стандартных вы можете создавать пользовательские профили и настраивать параметры сбора данных. Создавать, изменять и удалять пользовательские профили вы можете на странице **Профили**.

В этом разделе

См. также

Страница «Профили» (см. раздел 4.6.2)

7.3.1. Создание пользовательского профиля на базе стандартного

► Чтобы создать пользовательский профиль на базе стандартного:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.

2. В панели **Список профилей** выберите профиль.

3. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **На базе выбранного профиля**.

   Откроется страница **Новый профиль**.

4. В поле **Название** введите название профиля.

5. Если требуется, в панели **Параметры профиля** в раскрывающемся списке **Учетная запись** выберите учетную запись для сбора данных.

   В зависимости от профиля для выбора учетной записи вам может потребоваться указать другие параметры профиля или выбрать другой пункт в иерархическом списке.

   Примечание. В раскрывающемся списке **Учетная запись** отображаются учетные записи, при добавлении которых была выбрана метка используемого профилем метода сбора данных или не было выбрано никаких меток.

6. Если требуется, настройте другие параметры профиля.

   Примечание. Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

7. Нажмите кнопку **Сохранить**.

Пользовательский профиль создан.

7.3.2. Создание профиля для поиска уязвимостей

► Чтобы создать профиль для поиска уязвимостей пентестом:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.

2. В панели инструментов нажмите кнопку **Создать** и в раскрывшемся меню выберите пункт **Поиск выбранных уязвимостей в режиме BlackBox**.

   Откроется окно выбора уязвимостей.

3. В поле **Выбрать уязвимости** введите номер CVE уязвимости или другой идентификатор в базе знаний.

   Примечание. Вы можете просмотреть полный список CVE-идентификаторов уязвимостей, для которых доступны проверки в MaxPatrol VM, выполнив на странице **Активы** запрос `select(@VulnerPassport, VulnerPassport.HasPentestCheck, VulnerPassport.CVEs) | filter(VulnerPassport.HasPentestCheck = true and VulnerPassport.CVEs)`.

4. Выберите используемые порты.

5. Нажмите кнопку **Создать**.

   Откроется страница **Новый профиль**.

6. В поле **Название** введите название профиля.

Примечание. В поле **Описание** вы можете ввести любой текстовый комментарий.

7. Нажмите кнопку **Сохранить**.

Профиль для поиска уязвимостей создан.

7.3.3. Изменение пользовательского профиля

► Чтобы изменить пользовательский профиль:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.

2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница **Профили / <Название профиля>**.

4. Измените параметры профиля.

   Примечание. Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

5. Нажмите кнопку **Сохранить**.

Пользовательский профиль изменен.

7.3.4. Экспорт параметров профиля

При экспорте параметров пользовательского профиля в файле формата JSON сохраняются название и GUID стандартного профиля, на базе которого создан пользовательский профиль, и параметры, отличающиеся от указанных по умолчанию.

► Чтобы экспортировать параметры пользовательского профиля:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.

2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Редактировать**.
4. В панели **Параметры профиля** нажмите кнопку **Экспорт**.

   Примечание. Кнопка **Экспорт** доступна, если параметры пользовательского профиля отличаются от параметров стандартного профиля, на базе которого он создан.

Параметры пользовательского профиля экспортированы и сохранены в файле `<Название профиля>_<Дата и время экспорта>.json`.

7.3.5. Удаление пользовательского профиля

► Чтобы удалить пользовательский профиль:

1. В главном меню в разделе **Сбор данных** выберите пункт **Профили**.

   Откроется страница **Профили**.

2. В панели **Список профилей** выберите профиль.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Пользовательский профиль удален.

7.4. Работа с задачами

Для получения данных с IT-инфраструктуры организации в MaxPatrol VM необходимо создать задачу. В задаче необходимо указать цели, с которых нужно получить данные, например IP-адреса или добавленные в систему активы (группы активов). Вы можете запускать задачу вручную или настроить запуск по расписанию. В рамках задачи система создает подзадачи, которые выполняются автоматически. В зависимости от выбранного в задаче профиля с помощью компонента MP 10 Collector запускается соответствующий модуль для сбора данных. Задачи могут использоваться для:

— Обнаружения узлов. Система вносит информацию обо всех обнаруженных в IT-инфраструктуре организации активах в хранилище активов.

— Сканирования активов методом черного ящика. Система обнаруживает открытые порты и сетевые сервисы на этих портах. Затем обнаруживает уязвимости на сетевых сервисах.

— Аудита активов методом белого ящика. Система определяет детальную конфигурацию операционной системы, установленной на активе, перечень установленного на активе программного обеспечения, список открытых портов, перечень пользователей, которые зарегистрированы на активе. Формирует перечень уязвимостей и карту сети.

— Сканирования веб-приложения. Система обнаруживает параметры веб-приложения, выявляет уязвимые параметры, формирует перечень уязвимых библиотек.

— Поиска уязвимостей на активах в режиме пентест. Система выполнит поиск на активах уязвимостей с указанными CVE-идентификаторами.

Вы можете создавать, изменять, удалять, запускать и останавливать задачи на странице **Задачи по сбору данных**. Кроме того, вы можете перейти к просмотру истории запусков подзадач по ссылке **История запусков**.

Задачи на сбор данных об активах, созданные на основе профилей Windows Audit, Windows Audit Vulnerabilities Discovery и Unix Audit, поддерживают обновления экспертизы для аудита, получаемые с сервера Positive Technologies. Данные из обновлений позволяют обнаруживать ПО, которого нет в модели актива, чтобы впоследствии быстрее находить трендовые уязвимости. В уже существующих и новых задачах на сбор данных с указанными профилями использование обновлений экспертизы включено по умолчанию.

В этом разделе

7.4.1. Создание задачи на сбор данных

► Чтобы создать задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.

3. В поле **Название** введите название задачи.

4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.

5. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите профиль.

6. Если требуется, в раскрывающемся списке **Учетная запись** выберите учетную запись для сбора данных.

   В зависимости от профиля для выбора учетной записи вам может потребоваться указать другие параметры профиля или выбрать другой пункт в иерархическом списке.

   Примечание. В раскрывающемся списке **Учетная запись** отображаются учетные записи, при добавлении которых была выбрана метка используемого профилем метода сбора данных или не было выбрано никаких меток. По умолчанию выбрана учетная запись, указанная в профиле.

7. Если требуется, настройте другие параметры профиля.

Примечание. Профили Windows Audit, Windows Audit Vulnerabilities Discovery и Unix Audit поддерживают получение обновлений экспертных данных для аудита с сервера Positive Technologies. Обновления хранятся в справочнике audit_expertise_extension. Вы можете отключить использование этого справочника в пункте **Дополнительная экспертиза для аудита** иерархического списка.

Примечание. Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

8. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
9. Если в системе заведено больше одной инфраструктуры, в раскрывающемся списке **Инфраструктура** выберите инфраструктуру.
10. В панели **Цели сбора данных** на вкладке **Включить** укажите цели:
    - Если вы хотите сканировать группу активов, укажите ее в поле **Группы активов**.
    - Если вы хотите сканировать отдельные активы, укажите их в поле **Активы**.
    - Если вы хотите сканировать конкретные сетевые узлы, укажите их IP-адреса, FQDN или маски подсетей в поле **Сетевые адреса**.

    Примечание. Вы также можете изменить приоритетный способ подключения к активам — по полному доменному имени (FQDN) или по IP-адресу. По умолчанию выбран приоритет подключения по FQDN актива, так как вероятность его изменения ниже, чем у IP-адреса. Подключение по FQDN позволяет увеличить согласованность результатов сбора данных и реализовать поддержку протокола Kerberos. При невозможности подключения к активу по FQDN используется подключение по IP-адресу, и наоборот.

    Примечание. В поле **Сетевые адреса** вы также можете указывать локальные сетевые адреса, например `localhost`, `127.0.0.1`, `::1`. Это может потребоваться для сбора данных о конфигурации MP 10 Collector, журналов MP 10 Collector или для использования модуля RemoteExecutor.
11. Если требуется, установите флажок **Выполнить обнаружение узлов до начала сбора данных**.

    Обнаружение узлов до начала сбора данных позволяет сократить общее время сканирования.
12. Если требуется исключить отдельные цели сбора данных, укажите их на вкладке **Исключить**.

    Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
13. Нажмите кнопку **Сохранить**.

Задача создана.

7.4.2. Создание задачи на поиск уязвимостей

Перед созданием задачи на поиск уязвимостей в режиме пентест необходимо создать профиль для поиска уязвимостей (см. раздел 7.3.2).

► Чтобы создать задачу на поиск уязвимостей в режиме пентест:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.
2. В панели инструментов нажмите кнопку **Создать задачу** и в раскрывшемся меню выберите пункт **Сбор данных**.

   Откроется страница **Создание задачи на сбор данных**.
3. Если требуется, в поле **Название** измените название задачи.
4. Если требуется, добавьте подробное описание задачи по ссылке **Добавить описание**.
5. В панели **Параметры сбора данных** в раскрывающемся списке **Профиль** выберите профиль, созданный ранее.
6. Если требуется, в раскрывающемся списке **Коллекторы** выберите коллекторы для сбора данных.
7. В панели **Цели сбора данных** на вкладке **Включить** укажите цели:
   - Если вы хотите сканировать группу активов, укажите ее в поле **Группы активов**.
   - Если вы хотите сканировать отдельные активы, укажите их в поле **Активы**.

   Примечание. В панели **Расписание** вы можете включить и настроить автоматический запуск задачи по расписанию.
8. Нажмите кнопку **Сохранить**.

Задача создана.

7.4.3. Поиск и фильтрация задач

Вы можете настроить фильтр по статусам задач, их целям, используемым в них модулям, профилям, транспортам и учетным записям; по коллекторам, которые выполняют задачи или инфраструктурам (если их несколько).

► Чтобы настроить фильтр задач:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.
2. В панели **Все задачи** нажмите кнопку .

   Откроется панель фильтрации.
3. Нажмите кнопку с названием параметра задачи.

Откроется окно для выбора значений параметра.

4. Если вы настраиваете фильтр по коллекторам, модулям, профилям, статусам задач, учетным записям или инфраструктурам, в открывшемся окне установите флажки напротив значений параметров.

   Примечание. Вы можете использовать поле поиска в верхней части окна для поиска значения параметра.

5. Если вы настраиваете фильтр по целям задачи, укажите цели следующими способами:

   - в раскрывающемся списке **Группы активов** установите флажки напротив групп активов;
   - в поле **Активы** укажите один или несколько активов;
   - в поле **Сетевые адреса** введите IP-адрес, диапазон IP-адресов, маску подсети или FQDN.

6. Нажмите кнопку с названием параметра задачи.

   Примечание. Вы можете очистить значения для одного параметра задачи, нажав рядом с его названием ✖ , или очистить фильтры, нажав ✖ в панели фильтрации.

Задачи отфильтрованы в соответствии с условием.

7.4.4. Запуск задачи вручную

► Чтобы запустить задачу вручную:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.

   Примечание. Для выбора нескольких задач подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных задач — клавишу Ctrl, для выбора всех задач в списке — комбинацию клавиш Ctrl+A.

3. В панели инструментов нажмите кнопку **Запустить**.

Задача запущена.

7.4.5. Остановка задачи

Вы можете останавливать задачи, например чтобы снизить нагрузку на оборудование в сети.

► Чтобы остановить задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.

   Примечание. Для выбора нескольких задач подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных задач — клавишу Ctrl, для выбора всех задач в списке — комбинацию клавиш Ctrl+A.

3. В панели инструментов нажмите кнопку **Остановить**.

Задача остановлена.

7.4.6. Просмотр истории запусков задачи

При каждом запуске задачи (по расписанию или вручную) автоматически создается подзадача.

► Чтобы просмотреть историю запусков задачи:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.
3. По ссылке **История запусков** откройте страницу **История запусков <Название задачи>**.

   В панели **Подзадачи** отображается история запусков задачи.

   Примечание. Вы можете настроить период для просмотра запусков задачи, указав его по ссылке **за все время**, или настроить фильтр (по статусам подзадач, их целям или по коллекторам, которые выполняют подзадачи), нажав в панели **Подзадачи**.

Вы можете просмотреть журнал подзадачи по кнопке **Журнал подзадачи** или экспортировать его в текстовый файл по кнопке **Скачать журнал**.

7.4.7. Просмотр журнала подзадачи

► Чтобы просмотреть журнал подзадачи:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.
3. По ссылке **История запусков** откройте страницу **История запусков <Название задачи>**.
4. В панели **Подзадачи** выберите подзадачу.

Примечание. Вы можете настроить фильтр подзадач, нажав .

5. Нажмите кнопку **Журнал подзадачи**.

   Откроется страница **Журнал подзадачи от <Период журнала>**.

Вы можете экспортировать журнал подзадачи в текстовый файл по кнопке **Скачать журнал**.

7.4.8. Копирование задачи

► Чтобы скопировать задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.
3. В панели инструментов нажмите кнопку **Копировать**.

   Откроется страница **Создание задачи на сбор данных**.

4. Если нужно, измените параметры задачи.
5. Нажмите кнопку **Сохранить**.

Задача скопирована.

7.4.9. Настройка задачи

► Чтобы настроить задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.
3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница **Задачи / <Название задачи>**.

4. Измените параметры задачи и выбранного профиля.

   Примечание. Вы можете импортировать сохраненные ранее параметры профиля, указав по кнопке **Импорт** файл с параметрами.

5. Нажмите кнопку **Сохранить**.

Задача настроена.

7.4.10. Экспорт параметров профиля

Вы можете экспортировать измененные параметры профиля, выбранного в задаче. При экспорте параметров в файле формата JSON сохраняются название и GUID стандартного профиля и параметры, отличающиеся от указанных по умолчанию.

► Чтобы экспортировать параметры профиля, выбранного в задаче:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.

3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница **Задачи / <Название задачи>**.

4. В панели **Параметры сбора данных** нажмите кнопку **Экспорт**.

   Примечание. Кнопка **Экспорт** доступна, если профиль отличается от стандартного.

Параметры профиля экспортированы и сохранены в файле `<Название задачи>_<Дата и время экспорта>.json`.

7.4.11. Удаление задачи

► Чтобы удалить задачу:

1. В главном меню в разделе **Сбор данных** выберите пункт **Задачи**.

   Откроется страница **Задачи по сбору данных**.

2. В панели **Все задачи** выберите задачу.

   Примечание. Для выбора нескольких задач подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных задач — клавишу Ctrl, для выбора всех задач в списке — комбинацию клавиш Ctrl+A.

3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача удалена.

8. Работа с дашбордами и виджетами

На главной странице MaxPatrol VM располагаются дашборды. На дашбордах размещаются виджеты — модули с данными, полученными в процессе мониторинга информационной безопасности. При первом запуске MaxPatrol VM стандартный дашборд формируется автоматически и содержит предустановленный набор виджетов. Вы можете:

— Просматривать статистическую информацию на дашбордах. Виджеты отображают информацию об активах и связанных с ними уязвимостях, а также о включенных проверках системы.

— Создавать, переименовывать, изменять, перемещать и удалять дашборды.

— Создавать шаблоны дашбордов.

— Создавать, изменять, копировать, перемещать и удалять виджеты, а также настраивать их размер.

Примечание. Если вы хотите иметь возможность настраивать размер виджетов, при создании дашборда вам нужно выбирать динамическую сетку.

— Выгружать данные с виджетов в PNG- или CSV-файл.

В этом разделе

8.1. Виджеты по активам

Набор стандартных виджетов по активам показывает, сколько активов есть в системе, как изменялось их количество за выбранный период, а также как распределяются уязвимости по уровням опасности. Эти виджеты отображаются на дашборде **Общая информация**.

Количество активов

Виджет **Количество активов** представляет собой тренд и число. Число означает количество активов в системе. Если выбрана точная дата, то отображается количество активов на эту дату. Если выбран период, то отображается количество активов на конец периода. Тренд показывает, как менялось это количество.

Значимость активов

Своевременно полученная информация о том, что в IT-инфраструктуре есть уязвимости, позволяет вовремя устранять их. Поскольку постоянное сканирование всех активов может создать большую нагрузку на систему, необходимо выделять самые значимые активы, уязвимости на которых могут нанести больше всего вреда.

Виджет **Значимость активов** представляет собой числа и график. Первое число означает количество активов, для которых не указана значимость. Второе число означает общее количество активов в системе. Если выбрана точная дата, то отображается количество активов на эту дату. Если выбран период, то отображается количество активов на конец периода. График показывает, как менялось количество всех активов.

Актуальность данных об активах

Важно поддерживать информацию об активах в актуальном состоянии, иначе вы можете пропустить часть уязвимостей в IT-инфраструктуре организации.

Виджет представляет собой график, отображающий количество активов и состояние данных сканирования (например, данные отсутствуют, неактуальны, сканирование не проводилось). Под графиком отображается количество активов, у которых не определена операционная система.

Также указано количество активов, для которых отсутствуют базовые сведения для расчета уязвимостей.

Уязвимости на важных активах

Важно контролировать состояние наиболее значимых активов. Для этого нужно вовремя отслеживать появление уязвимостей на таких активах и то, как происходит их устранение.

Виджет представляет собой графики, отображающие изменение количества уязвимых активов и актуальных уязвимостей. Можно настроить отображение только одного графика или двух сразу. График для уязвимых активов отображает изменение общего количества активов и количества уязвимых активов за тот или иной период. График актуальных уязвимостей отображает изменение количества уязвимостей, которые не были исключены или устранены.

При наведении курсора на точку графика отображается подробная информация. Также вы можете перейти в таблицу активов, чтобы ознакомиться с подробными данными об активах и уязвимостях.

Для графика вы можете изменять фильтры активов и уязвимостей, выбирать период и настраивать данные, включать счетчики.

Последние добавленные уязвимости

При добавлении новых типов уязвимостей важно сразу получать информацию об обнаруженных экземплярах таких уязвимостей.

Виджет представляет собой список типов уязвимостей. Каждый из типов отмечен значком, который показывает степень опасности. Также может быть указан идентификационный номер в публичной базе данных, в которой описаны уязвимости такого типа (в частности, в Common Vulnerabilities and Exposures). Если же уязвимости обнаружены в IT-инфраструктуре, будут показаны их количество и статусы.

Плановое устранение и новые без политики

Виджет состоит из четырех диаграмм для новых уязвимостей без политики и для уязвимостей, предполагающих плановое устранение. Каждая диаграмма разбита по статусам устранения этих уязвимостей. Две верхних диаграммы отображают количество уязвимостей с отметкой «важная» на активах высокой значимости и активах средней значимости. Две нижних диаграммы отображают количество критически опасных уязвимостей на активах высокой и средней значимости.

Устранение вручную

Виджет состоит из четырех диаграмм для уязвимостей, запланированных к устранению вручную. Каждая диаграмма разбита по статусам устранения этих уязвимостей. Две верхних диаграммы отображают количество уязвимостей с отметкой «важная» на активах высокой значимости и активах средней значимости. Две нижних диаграммы отображают количество остальных уязвимостей на активах высокой и средней значимости.

Трендовые уязвимости на активах

Трендовые уязвимости — это такие уязвимости, которые активно используются в атаках злоумышленников или будут использоваться в ближайшем будущем. На них необходимо обращать повышенное внимание и устранять их в первую очередь. Виджет позволяет оценить защищенность вашей системы и состояние обработки найденных уязвимостей.

Виджет состоит из четырех графиков. По умолчанию два верхних графика отображают состояние актуальных уязвимостей на активах высокой значимости и на остальных активах, два нижних графика — состояние обработки исправленных уязвимостей (исключенные и устраненные уязвимости). Также по нажатию на цифры вы можете перейти в таблицу активов, чтобы ознакомиться с подробными данными об активах и уязвимостях.

Вы можете настраивать графики, например отключать отдельные блоки, фильтровать активы по значимости, отбирать только актуальные уязвимости.

Трендовые уязвимости

Трендовые уязвимости — это такие уязвимости, которые активно используются в атаках злоумышленников или будут использоваться в ближайшем будущем. На них необходимо обращать повышенное внимание и устранять их в первую очередь. Виджет позволяет оценить защищенность вашей системы и состояние обработки найденных уязвимостей.

Виджет представляет собой список типов уязвимостей. Каждый из типов отмечен значком, который показывает степень опасности. Также может быть указан идентификационный номер в публичной базе данных, в которой описаны уязвимости такого типа (в частности, в Common Vulnerabilities and Exposures). Если же уязвимости обнаружены в IT-инфраструктуре, будут показаны их количество и статусы.

Вы можете настраивать сортировку данных об уязвимостях, которые будут отображаться в виджете: по дате публикации, по дате добавления уязвимости в трендовые, по количеству актуальных уязвимостей. Также вы можете перейти к списку найденных трендовых уязвимостей.

Уязвимости с эксплойтом

Эксплойты — это специальные программы, фрагменты программного кода или последовательности команд, применяемые для атаки на вычислительную систему. Важно отслеживать уязвимости в программном обеспечении, для использования которых созданы эксплойты. Эксплойты позволяют даже неопытному злоумышленнику воспользоваться уязвимостями, автоматизировать атаку и получить контроль над важными ресурсами.

Этот виджет показывает, как меняется количество уязвимостей с эксплойтом. При наведении курсора на точку графика отображается детальная информация. Также вы можете перейти в таблицу активов, чтобы ознакомиться с подробными данными об активах и уязвимостях с эксплойтом.

Последние добавленные опасные уязвимости в ПО Microsoft

Важно отслеживать уязвимости в программном обеспечении Microsoft, поскольку Windows является одной из самых распространенных операционных систем и, следовательно, привлекательной мишенью для атак злоумышленников.

Виджет представляет собой список типов уязвимостей. Каждый из типов отмечен значком, который показывает степень опасности. Также может быть указан идентификационный номер в публичной базе данных, в которой описаны уязвимости такого типа (в частности, в Common Vulnerabilities and Exposures). Если же уязвимости обнаружены в IT-инфраструктуре, будут показаны их количество и статусы.

Базовый список уязвимостей

Виджет содержит список типов уязвимостей, обнаруженных в системе. В правой части списка для каждого типа отображается количество обнаруженных уязвимостей, разбитое по статусам уязвимостей. Под списком показаны паспорта уязвимостей с подробной информацией.

Уязвимости в списке могут быть сгруппированы по паспорту, активу, уязвимому компоненту, а также по активу и уязвимому компоненту одновременно. В зависимости от выбранной группировки, уязвимости можно дополнительно отсортировать: в случае группировки по активу или активу и уязвимому компоненту — по дате публикации паспорта, оценке CVSS, статусу или дате и времени обнаружения, в случае группировки по паспорту или уязвимому компоненту можно сортировать паспорта уязвимостей по оценке CVSS или дате публикации паспорта, а сами уязвимости — по статусу или дате и времени обнаружения.

См. также

Мини-карточка актива (см. раздел 5.1.6)

8.2. Виджет по проверкам

Виджет **Проверки по чек-листу** представляет собой список групп включенных проверок системы (см. раздел 11) с индикаторами состояния.

Вы можете настраивать период обновления данных. Также вы можете перейти из виджета на страницу **Чек-лист настройки системы**, чтобы ознакомиться с подробной информацией о проверках и действиях, которые необходимо выполнить, чтобы настроить систему.

См. также

Страница «Чек-лист настройки системы» (см. раздел 4.7.5)

Изменение виджета на дашборде (см. раздел 8.10)

8.3. Создание дашборда

На главной странице MaxPatrol VM на дашбордах представлены данные, полученные в процессе мониторинга информационной безопасности. При первом запуске MaxPatrol VM стандартный дашборд формируется автоматически и содержит предустановленный набор виджетов. Вы можете создавать дашборды и добавлять на них виджеты самостоятельно. При создании дашборда можно использовать как стандартные шаблоны, так и шаблоны, созданные другими пользователями.

> **Примечание.** Дашборд, созданный по шаблону, сохраняет с ним связь. Это означает, что если изменяется шаблон, изменяются и все дашборды, созданные на его основе.

► Чтобы создать дашборд:

1. На главной странице в панели инструментов нажмите + .

   Откроется окно **Создание дашборда**.

2. В поле **Название** введите название дашборда.

3. Выберите вариант сетки, по которой будут располагаться виджеты.
4. Нажмите кнопку **Создать**.

Дашборд создан.

► Чтобы создать дашборд на основе шаблона:

1. На главной странице в панели инструментов нажмите + .

   Откроется окно **Создание дашборда**.
2. Выберите одну из вкладок с шаблонами и щелкните левой кнопкой мыши по полю с описанием шаблона.

   Отобразятся параметры дашборда.

   Примечание. Вы можете изменить название дашборда или отвязать его от шаблона.
3. Нажмите кнопку **Создать**.

Дашборд создан.

По умолчанию новый дашборд отображается справа от уже существующих, но вы можете его перетащить.

8.4. Создание шаблона дашборда

В MaxPatrol VM вы можете создавать шаблоны дашбордов и хранить их в базе шаблонов. При этом можно использовать стандартные шаблоны и шаблоны, созданные другими пользователями. Дашборд, созданный по шаблону, сохраняет с ним связь. Это означает, что если изменяется шаблон, изменяются и все дашборды, созданные на его основе.

► Чтобы создать шаблон дашборда:

1. На главной странице выберите дашборд.
2. В панели инструментов нажмите и в раскрывшемся меню нажмите кнопку **Сохранить как новый шаблон**.

   Откроется окно создания шаблона дашборда.
3. В поле **Название** введите название шаблона.
4. Если требуется, в поле **Описание** введите информацию о шаблоне.

   Примечание. Дополнительная информация может помочь другим пользователям выбрать наиболее удобный и полезный для них шаблон.
5. Нажмите кнопку **Сохранить**.

Шаблон дашборда создан.

8.5. Изменение дашборда

Вы можете переименовывать дашборды, а также отвязывать дашборд от шаблона, чтобы дашборд не изменялся автоматически при изменении шаблона.

► Чтобы изменить название дашборда:

1. На главной странице выберите дашборд.
2. В панели инструментов нажмите и в открывшемся окне введите новое название дашборда.
3. Нажмите кнопку **Сохранить**.

Название дашборда изменено.

Также вы можете отвязать дашборд от шаблона по кнопке **Сохранить и отвязать от шаблона**.

8.6. Удаление дашборда

► Чтобы удалить дашборд:

1. На главной странице выберите дашборд.
2. В панели инструментов нажмите и подтвердите удаление дашборда.

Дашборд удален.

8.7. Создание виджета по активам

Вы можете создавать виджеты по отфильтрованным активам.

► Чтобы создать виджет по отфильтрованным активам:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.
2. Сгруппируйте и проанализируйте данные об активах (см. раздел 5.2.4).
3. В панели инструментов нажмите .
4. Выберите и настройте графическое представление виджета — таблицу, столбчатую диаграмму, график, круговую диаграмму.
5. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.
6. В открывшемся окне введите название виджета и название запроса.
7. Укажите папку запроса и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

См. также

Сохранение запроса (см. раздел 5.2.6.4)

8.8. Создание табличного виджета по активам

Вы можете создавать табличные виджеты, построенные на основе данных обо всей совокупности активов, представленной в таблице активов.

► Чтобы создать табличный виджет по активам:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. В панели инструментов нажмите .

3. В панели инструментов нажмите кнопку **Сохранить в библиотеку виджетов**.

4. В открывшемся окне введите название виджета и название запроса.

5. Укажите папку запроса и подтвердите сохранение.

Виджет создан и сохранен в библиотеку виджетов.

См. также

Группировка и анализ данных об активах с помощью математических операций (см. раздел 5.2.4)

Сохранение запроса (см. раздел 5.2.6.4)

8.9. Добавление виджета на дашборд

Вы можете добавлять виджеты только в пустые ячейки пользовательских дашбордов. Если пустых ячеек на дашборде нет, необходимо сначала удалить один виджет, затем добавить другой.

Для поиска виджета с необходимой статистической информацией в библиотеке предусмотрена фильтрация виджетов.

► Чтобы добавить виджет на дашборд:

1. На главной странице выберите пользовательский дашборд.

2. В свободной ячейке нажмите кнопку **Добавить виджет**.

   Откроется окно **Добавить виджет**.

3. В окне выберите хотя бы один виджет.
4. Нажмите кнопку **Добавить**.

Виджет добавлен на дашборд.

8.10. Изменение виджета на дашборде

В процессе работы со статистическими данными, представленными на виджетах, вы можете изменять виджеты с учетом решаемых задач.

► Чтобы изменить виджет:

1. На главной странице выберите дашборд.
2. В панели инструментов виджета нажмите ⋮ и в раскрывшемся меню выберите пункт **Настроить**.

   Откроется страница **Настройка виджета**.
3. Внесите изменения и нажмите кнопку **Сохранить**.

Виджет изменен.

8.11. Удаление виджета с дашборда

► Чтобы удалить виджет с дашборда:

1. На главной странице выберите пользовательский дашборд.
2. В панели инструментов виджета нажмите ⋮ и в раскрывшемся меню выберите пункт **Удалить**.

Виджет удален с дашборда.

8.12. Экспорт статистических данных

Информация о текущем состоянии информационной инфраструктуры организации может быть вам полезна при проведении аудитов и формировании отчетности. Вы можете экспортировать статистические данные с графического виджета в файл формата PNG или с табличного виджета в файл формата CSV.

► Чтобы экспортировать данные с графического виджета:

1. На главной странице выберите дашборд.
2. В панели инструментов графического виджета нажмите ⋮, в раскрывшемся меню выберите пункт **Скачать в PNG** и подтвердите сохранение.

Файл сохранен на ваш компьютер.

► Чтобы экспортировать записи с табличного виджета:

1. На главной странице выберите дашборд.
2. В панели инструментов табличного виджета нажмите ⋮ и в раскрывшемся меню выберите один из вариантов:
   - если вы хотите экспортировать только выбранные записи — **Экспортировать выбранные записи в CSV-файл**;
   - если вы хотите экспортировать все отображаемые записи — **Экспортировать отображаемые записи в CSV-файл**.
3. Подтвердите сохранение.

Файл сохранен на ваш компьютер.

9. Работа с отчетами

При работе с большим количеством данных необходимо, чтобы они были хорошо организованы и наглядно представлены. Данные, полученные в процессе мониторинга информационной безопасности и представленные на дашбордах на главной странице MaxPatrol VM, вы можете выгружать в PDF-файлы. Такие файлы называются отчетами и дают вам возможность:

— исследовать данные об активах;

— изучить данные об уязвимостях различного типа, обнаруженных в системе (например, динамику среднего времени жизни важных уязвимостей);

— оценить процесс управления уязвимостями в организации (например, соотношение количества важных уязвимостей, обрабатываемых автоматически на основе политик, и обрабатываемых вручную);

— определить наиболее значимые данные;

— находить в данных закономерности и аномалии, которые невозможно выявить при ручном анализе (например, понять, как защита периметра сети влияет на защищенность конкретного узла).

Вы можете управлять отчетами на странице **Отчеты** (**Система** → **Отчеты**).

Рабочая область страницы **Отчеты** содержит:

— таблицу задач по выпуску отчетов, в которой отображается подробная информация обо всех таких задачах;

— панель **История выпусков**, в которой отображается информация о дате и времени выпуска отчета, а также о доступности отчета для скачивания;

— панель **Сводка** с подробной информацией о задаче по выпуску отчета, которая выбрана в таблице задач по выпуску отчетов.

Вы можете создавать отчеты самостоятельно или использовать отчеты с предустановленными параметрами на основе шаблонов; копировать, изменять и удалять отчеты. Также вы можете настроить выпуск отчетов по расписанию или выпускать отчеты вручную.

В этом разделе

Управление выпуском отчетов (см. раздел 9.6)

Выпуск отчета по активам (см. раздел 9.7)

9.1. Создание задачи по выпуску пользовательского отчета

При создании задачи по выпуску пользовательского отчета вы можете:

— задавать последовательность объектов (текстов, изображений, виджетов), из которых будет состоять отчет;

— выбирать для отчета различные типы визуализации, например диаграммы, графики или гистограммы;

— настраивать внешний вид отчета: добавить колонтитулы, легенды и подписи для диаграмм.

► Чтобы создать задачу по выпуску пользовательского отчета:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание задачи**.

3. В списке шаблонов отчетов выберите пункт **Без шаблона** и нажмите кнопку **Далее**.

   Откроется страница **Редактирование задачи <Название отчета>**.

4. В панели **Настройка задачи** на вкладке **Параметры отчета** настройте внешний вид отчета.

   Примечание. Вы можете изменить название задачи по выпуску отчета, если требуется, а также настроить отображение информации в колонтитулах.

5. Выберите вкладку **Параметры выпуска**.

6. Настройте формат и частоту выпуска отчета, укажите получателя отчета.

7. В рабочей области нажмите + и выберите объект.

   На страницу отчета добавится новый объект.

   Примечание. Вы можете добавить несколько объектов.

8. Выберите объект.

   Откроется панель настройки объекта.

9. Настройте выбранный объект.

10. Нажмите кнопку **Сохранить** и в раскрывшемся меню выберите пункт **Сохранить задачу**.

11. Нажмите кнопку **Обновить**.
12. Нажмите кнопку **Закрыть**.

Задача по выпуску пользовательского отчета создана и отображается в таблице задач по выпуску отчетов.

9.2. Создание задачи по выпуску отчета на основе шаблона

Отчеты удобнее всего создавать на основе шаблонов. Шаблоны — это готовые типовые отчеты, в совокупности предоставляющие наиболее полную информацию о состоянии безопасности системы. Они позволяют провести инвентаризацию операционной системы, программного или аппаратного обеспечения. С их помощью вы можете понять, насколько хорошо выстроен процесс обработки уязвимостей.

► Чтобы создать задачу на выпуск отчета на основе шаблона:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание задачи**.
3. Выберите шаблон отчета из списка и нажмите кнопку **Далее**.

   Откроется окно **Создание задачи** с описанием выбранного шаблона и информацией о расписании его запуска.
4. Нажмите кнопку **Далее**.

   Откроется страница **Редактирование задачи <Название отчета>**.
5. В панели **Настройка задачи** на вкладке **Параметры отчета** настройте внешний вид отчета.

   Примечание. Вы можете изменить название задачи по выпуску отчета, если требуется, а также настроить отображение информации в колонтитулах.
6. Выберите вкладку **Параметры выпуска**.
7. Настройте формат и частоту выпуска отчета, укажите получателя отчета.

► Чтобы добавить дополнительные объекты в отчет, если это необходимо:

1. В рабочей области нажмите + и выберите объект.

   На страницу отчета добавится новый объект.

   Примечание. Вы можете добавить несколько объектов.
2. Выберите объект.

Откроется панель настройки объекта.

3. Настройте выбранный объект.
4. Нажмите кнопку **Сохранить** и в раскрывшемся меню выберите пункт **Сохранить задачу**.

Задача по выпуску отчета на основе шаблона создана и отображается в таблице задач по выпуску отчетов.

В этом разделе

Создание задачи по выпуску отчета по активам (см. раздел 9.2.1)

Создание задачи по выпуску отчета по уязвимостям (см. раздел 9.2.2)

9.2.1. Создание задачи по выпуску отчета по активам

► Чтобы создать задачу по выпуску отчета по активам:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.
2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание задачи**.
3. В списке шаблонов выберите **Отчеты по активам и инцидентам**.
4. Нажмите кнопку **Далее**.

   Откроется окно **Создание задачи**.
5. В поле **Название** введите название отчета.
6. В раскрывающемся списке **Источник** выберите **Активы**.
7. В раскрывающемся списке **Отчет** выберите шаблон отчета.
8. Если требуется, в поле **Получатели отчета** укажите адреса электронной почты для доставки отчета.
9. В раскрывающемся списке **В группе** выберите группу активов, данные о которых должны войти в отчет.
10. Если вы хотите, чтобы в отчет попадали также данные об активах из вложенных групп, установите флажок **Включая вложенные**.
11. Настройте расписание, в соответствии с которым отчет будет автоматически выпускаться в указанное время с заданной периодичностью.
12. Нажмите кнопку **Сохранить**.

Задача по выпуску отчета по активам создана.

9.2.2. Создание задачи по выпуску отчета по уязвимостям

Отчеты по уязвимостям используются для сбора структурированный информации о скорости обнаружения и устранения уязвимостей в инфраструктуре организации и на отдельных группах активов. Отчеты по уязвимостям можно использовать для отчета о выполненных работах, планирования устранения уязвимостей и оценки качества управления уязвимостями.

Для создания задач по выпуску отчетов по уязвимостям доступны группы шаблонов **Важные уязвимости** и **Показатели управления уязвимостями**. Формат файла отчета — PDF.

► Чтобы создать задачу по выпуску отчета по уязвимостям:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание задачи**.

3. Выберите в группах шаблонов **Важные уязвимости** или **Показатели управления уязвимостями** нужный шаблон отчета.

4. Нажмите кнопку **Далее**.

   Откроется окно с кратким описанием отчета и расписанием выпуска, установленным по умолчанию.

5. Нажмите кнопку **Далее**.

   Откроется окно **Редактирование задачи**.

6. В панели **Настройка задачи** выберите вкладку **Параметры отчета**.

7. Если требуется, в поле **Название** введите название отчета.

8. Если требуется, в поле **Описание** введите описание отчета.

9. Если требуется, в блоке параметров **Внешний вид отчета** выберите ориентацию страниц отчета.

10. Если требуется, в раскрывающемся меню **Шрифт по умолчанию** выберите шрифт, которым будет набран отчет.

11. Если требуется, включите и настройте верхний и нижний колонтитулы.

    Примечание. Колонтитул может содержать номер страницы, дату публикации отчета и загруженное изображение в формате PNG, JPG, BMP, GIF, SVG, ICO.

12. Для отображения внесенных в отчет изменений без сохранения нажмите кнопку **Обновить**.

13. В панели **Настройка задачи** выберите вкладку **Параметры выпуска**.

14. Если требуется, в поле **Получатели отчета** укажите адреса электронной почты для доставки отчета.

15. Если требуется, в блоке параметров **Расписание** включите и настройте расписание выпуска отчета.
16. В панели инструментов нажмите кнопку **Сохранить** и в раскрывшемся меню выберите пункт **Сохранить задачу**.

Задача по выпуску отчета по уязвимостям создана.

9.3. Создание задачи по выпуску отчета на основе существующей

Если вам необходимы несколько похожих задач по выпуску отчета, вы можете создать их на основе существующей задачи, изменив отдельные параметры.

► Чтобы создать задачу по выпуску отчета на основе существующей:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.
2. Выберите задачу по выпуску отчета.
3. В панели инструментов нажмите кнопку **Копировать**.

   Откроется страница **Редактирование задачи <Название отчета> (копия)**.
4. Внесите изменения и нажмите кнопку **Сохранить**.

Задача по выпуску отчета создана.

9.4. Изменение задачи по выпуску отчета

► Чтобы изменить задачу по выпуску отчета:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.
2. Выберите задачу по выпуску отчета.
3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется страница с параметрами задачи по выпуску отчета.
4. Внесите изменения и нажмите кнопку **Сохранить**.

Задача по выпуску отчета изменена.

9.5. Удаление задачи по выпуску отчета

► Чтобы удалить задачу по выпуску отчета:

1. В главном меню в разделе **Система** выберите пункт **Отчеты**.

   Откроется страница **Отчеты**.

2. Выберите задачу по выпуску отчета.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача по выпуску отчета удалена.

9.6. Управление выпуском отчетов

В MaxPatrol VM на странице **Отчеты** вы можете настроить автоматический выпуск отчетов по расписанию или выпустить отдельный отчет вручную. При выпуске отчета по расписанию MaxPatrol VM отправляет указанным адресатам электронное письмо с выпущенным отчетом во вложении.

MaxPatrol VM хранит последние два файла отчета. Вы можете скачать их в панели **История выпусков**.

Выпуск отчетов осуществляется поочередно. Это означает, что пока MaxPatrol VM не завершит выпуск одного отчета, вы не сможете выпустить еще один отчет.

См. также

Страница «Отчеты» (см. раздел 4.7.1)

9.7. Выпуск отчета по активам

► Чтобы выпустить отчет по выбранной группе активов:

1. В главном меню выберите раздел **Активы**.

   Откроется страница **Активы**.

2. Выберите активы в таблице.
3. В панели инструментов нажмите кнопку **Выпустить отчет**.

   Откроется окно **Выпуск отчета**.

4. Выберите шаблоны отчетов по активам.
5. В поле **Формат** выберите формат отчета.
6. Нажмите кнопку **Выпустить отчет**.

Отчеты по активам используются для инвентаризации операционной системы, программного или аппаратного обеспечения.

Отчет состоит из нескольких разделов:

— **Параметры отчета** — список активов, на основании которых сформирован отчет.

— **Общая статистика** — отображение информации отчета в виде таблицы или графической диаграммы.

— **Свойства объектов** — более подробное описание параметров каждого из объектов (только для отчетов по активам).

10. Работа с уведомлениями

Уведомления MaxPatrol VM содержат информацию об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных и состоянии системы.

Вы можете автоматизировать отправку уведомлений, создавая задачи на странице **Уведомления**.

В этом разделе

10.1. Создание задачи для отправки уведомления об изменении общего числа активов

► Чтобы создать задачу для отправки уведомления об изменении общего числа активов:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.

3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об изменении общего числа активов**.
5. Если необходимо, снимите флажок **Создание активов** или **Удаление активов**.
6. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:

- Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
- Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.

7. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
8. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об изменении общего числа активов создана.

10.2. Создание задачи для отправки уведомления об изменениях в группах активов

► Чтобы создать задачу для отправки уведомления об изменениях в группах активов:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об изменениях в группах активов**.
5. Если необходимо, снимите флажок **Добавление активов в группу** или **Исключение активов из группы**.
6. В раскрывающемся списке **В группах** выберите те группы активов, об изменениях которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.

8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об изменениях в группах активов создана.

10.3. Создание задачи для отправки уведомления о состоянии MaxPatrol VM

► Чтобы создать задачу для отправки уведомления о состоянии MaxPatrol VM:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся блоке **Сообщать** выберите **О состоянии системы**.
5. В раскрывающемся списке **Опасность** выберите тип сообщений, отправляемых системой самодиагностики.
6. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
7. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
8. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о состоянии системы создана.

10.4. Создание задачи для отправки уведомления о выполнении задач сбора данных

► Чтобы создать задачу для отправки уведомления о выполнении задач сбора данных:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.

3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **О задачах сбора данных**.
5. Если необходимо, снимите флажок **О начале выполнения** или **О завершении**.
6. В раскрывающемся списке **Задачи** выберите те задачи сбора данных, о начале и (или) завершении которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о выполнении задач сбора данных создана.

10.5. Остановка и повторный запуск задачи для отправки уведомления

► Чтобы остановить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

Откроется страница **Уведомления**.

2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Остановить**.

Задача для отправки уведомления остановлена.

► Чтобы запустить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.

2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Запустить**.

Задача для отправки уведомления запущена.

10.6. Создание новой задачи на основе существующей задачи

► Чтобы создать новую задачу на основе существующей:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.

2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Копировать**.

   Откроется окно **Новое уведомление**.

4. Внесите изменения и нажмите кнопку **Сохранить**.

Новая задача создана на основе существующей.

10.7. Изменение задачи для отправки уведомления

► Чтобы изменить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.

2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Редактировать**.

Откроется окно **Редактировать уведомление**.

4. Внесите изменения и нажмите кнопку **Сохранить**.

Задача для отправки уведомлений изменена.

10.8. Удаление задачи для отправки уведомления

► Чтобы удалить задачу для отправки уведомления:

1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

   Откроется страница **Уведомления**.

2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача для отправки уведомлений удалена.

11. Чек-лист настройки системы

После установки MaxPatrol VM необходимо его настроить, поскольку часть параметров зависит от специфики IT-инфраструктуры организации. Также в процессе работы часть параметров может изменяться, поэтому возникает необходимость периодически проверять, корректно ли настроен MaxPatrol VM. Для решения этих задач вы можете использовать чек-лист (**Система** → **Чек-лист настройки системы**), который содержит список проверок, помогающих вам правильно выполнить необходимые действия.

Для удобства проверки сгруппированы. Напротив каждой группы отображается количество пройденных в этой группе проверок. Для каждой проверки дано краткое описание, объясняющее, что именно и почему требуется настроить и какие шаги необходимо выполнить. Вы можете исключить те проверки, которые не являются для вас важными.

Отдельные параметры проверок можно изменять с помощью файла конфигурации. Подробнее о параметрах проверок см. Руководство администратора.

Для некоторых проверок приведены примеры PDQL-запросов. Такие запросы составлены с учетом значений по умолчанию параметров проверки. Если параметры проверки были изменены, вам необходимо будет внести изменения и в PDQL-запрос (см. документ Синтаксис языка запроса PDQL).

Кроме того, в MaxPatrol VM реализованы уведомления о непройденных проверках.

12. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

— решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;

— диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;

— разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;

— устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

12.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

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.

Техническая поддержка на портале предоставляется на русском и английском языках.

12.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

12.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

12.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

12.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

12.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 2).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 2. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

12.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

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

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Математические функции для работы с данными в системе

В MaxPatrol VM вы можете использовать математические функции для анализа данных.

Функция Avg

Функция с аргументом All используется для подсчета среднего значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Avg ([All] [Поле 1]) Where [Условие фильтрации] Group by
[Поле 2] Over time [Период]
```

Функция Compact

Функция используется для компактного представления данных о выбранном объекте. Применяется к данным любого типа. Возвращает для каждой группы единственную строку с указанием значения объекта [Поле 2] (тип данных String) и количества (тип данных Number).

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select ([Поле 1], Compact [Поле 2]) Where [Условие фильтрации]
```

Функция Compactunique

Функция используется для компактного представления данных о выбранном объекте. Применяется к данным любого типа. Возвращает для каждой группы единственную строку с указанием уникального значения объекта (тип данных String) и количества (тип данных Number).

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], (Compactunique [Поле 2]) Where [Условие фильтрации]
```

Функция Count

Функция используется для подсчета количества значений за указанный период. Применяется к данным любого типа. Возвращает для каждой группы единственное значение с типом данных Number.

Функция с аргументом All используется для подсчета количества всех значений с любым типом данных, кроме Null, в выбранной колонке [Поле 1] за указанный период.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Count ([All] [Поле 1]) Where [Условие фильтрации] Group
by [Поле 2] Over time [Период]
```

Функция с аргументом Distinct используется для подсчета количества уникальных значений с любым типом данных, кроме Null, в выбранной колонке [Поле 1] за указанный период.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Count ([Distinct] [Поле 1]) Where [Условие фильтрации]
Group by [Поле 2] Over time [Период]
```

Функция Count (*) используется для подсчета количества всех значений (в том числе повторяющихся и с типом данных Null) в таблице.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Count (*) Where [Условие фильтрации] Group by [Поле 2]
Over time [Период]
```

Функция Countunique

Функция используется для подсчета количества уникальных значений в выбранной колонке [Поле 1] за указанный период. Также функция может использоваться для подсчета количества уникальных записей исходной таблицы, сформированных из указанных колонок [Поле 1], ..., [Поле N]. Применяется к данным любого типа. Возвращает для каждой группы единственное значение с типом данных Number.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Countunique ([Поле 1], …, [Поле N]) Where [Условие
фильтрации] Group by [Поле 2] Over time [Период]
```

Функция Max

Функция с аргументом All используется для поиска максимального значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Max ([All] [Поле1]) Where [Условие фильтрации] Group by
[Поле 2] Over time [Период]
```

Функция Median

Функция с аргументом All используется для поиска медианного значения в выбранной колонке [Поле 1] за указанный период. Данные в колонке сортируются. Для наборов с нечетным числом элементов медианным считается значение центрального элемента, а для наборов с четным числом элементов — среднее значение двух центральных элементов. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Median ([All] [Поле1]) Where [Условие фильтрации] Group
by [Поле 2] Over time [Период]
```

Функция Min

Функция с аргументом All используется для поиска минимального значения в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Min ([All] [Поле 1]) WHERE [Условие фильтрации] Group by
[Поле 2] Over time [Период]
```

Функция Sum

Функция с аргументом All используется для подсчета суммы всех значений в выбранной колонке [Поле 1] за указанный период. Применяется к данным типа Number. Возвращает для каждой группы единственное значение с типом данных Number.

> **Примечание.** При подсчете не учитываются пустые значения с типом данных Null. Если все значения в выбранной колонке имеют тип данных Null, функция возвращает 0.

Синтаксис:

```
Select [Поле 1], …, [Поле N] Sum ([All] [Поле 1]) Where [Условие фильтрации] Group by
[Поле 2] Over time [Период]
```

Приложение Б. Клавиши и комбинации клавиш для работы в интерфейсе

Для удобства работы в интерфейсе MaxPatrol VM вы можете использовать клавиши и их комбинации.

Таблица 3. Клавиши и их комбинации для работы в интерфейсе MaxPatrol VM

Функция	**Клавиши и их комбинации**
Общие	
Войти в систему со страницы входа	Enter
Переключаться между разделами главного меню, кнопками, полями ввода	Tab
Переместиться на первую строку	Home
Переместиться на первую строку на странице	PgUp
Переместиться на последнюю строку	End
Переместиться на последнюю строку на странице	PgDn
Переместиться на предыдущую строку	↑
Переместиться на предыдущую строку с сохранением уже выделенных строк	Shift+ ↑
Переместиться на следующую строку	↓
Переместиться на следующую строку с сохранением уже выделенных строк	Shift+ ↓
Переключаться между разделами главного меню, кнопками в обратном порядке	Shift+Tab
Выбрать вариант	↓ и ↑
Установить или снять флажок	Space
Выполнить множественную сортировку	Shift + щелчок левой кнопкой мыши по названию колонки
Динамические группы активов	
Узнать количество активов, соответствующих условию PDQL-запроса, при создании динамической группы активов в поле **Фильтр**	Ctrl+Enter

Функция	Клавиши и их комбинации
Группы и фильтры	
Развернуть группу, папку фильтров или запросов	* на цифровой клавиатуре
Развернуть группу, папку фильтров или запросов до следующего уровня вложенности	→
Свернуть группу, папку фильтров или запросов	←
Свернуть группу, папку фильтров или запросов	– на цифровой клавиатуре
Свернуть или развернуть панель **Группы и запросы**	[
Свернуть или развернуть панель **Сводка**	]
Меню выбора периода	
Переместиться на предыдущий вариант	←, ↑
Переместиться на следующий вариант	→, ↓
Конструктор шаблонов отчетов: текстовые объекты	
Отменить (для Windows)	Ctrl+Z
Отменить (для Mac)	Control-Z
Вернуть изменения	Ctrl+Y
Присоединить содержимое элемента списка к элементу списка выше	Alt+ ↑
Присоединить содержимое элемента списка к элементу списка ниже	Alt+ ↓
Выделить параграф	Esc
Выделить полужирным	Ctrl+B
Выделить курсивом	Ctrl+I
Увеличить уровень вложенности списка	Ctrl+]
Уменьшить уровень вложенности списка	Ctrl+[

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.