MaxPatrol VM версия 2.8

Руководство администратора

Дата редакции документа: 10.06.2025

Содержание

1. Об этом документе

Руководство администратора содержит справочную информацию и инструкции по администрированию Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM). Руководство не содержит инструкций по установке MaxPatrol VM и использованию основных функций продукта.

Руководство адресовано специалистам, администрирующим MaxPatrol VM.

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 и обновлению продукта.
- Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации.
- 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.

В этом разделе

Условные обозначения (см. раздел 1.1)

Другие источники информации о MaxPatrol VM (см. раздел 1.2)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

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

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

1.2. Другие источники информации о MaxPatrol VM

Вы можете найти дополнительную информацию о MaxPatrol VM на портале технической поддержки.

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

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 24).

См. также

О технической поддержке (см. раздел 24)

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.

В этом разделе

Архитектура MaxPatrol VM (см. раздел 2.1)

Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов (см. раздел 2.2)

2.1. Архитектура MaxPatrol VM

MaxPatrol VM состоит из программных компонентов, которые вы можете размещать как на одном сервере, так и на нескольких. Такая структура обеспечивает масштабирование и позволяет внедрять систему в компаниях любого размера.

В этом разделе

2.1.1. Компонент MaxPatrol 10 Core

Компонент MaxPatrol 10 Core (далее также — MP 10 Core) является основным компонентом системы, ее управляющим сервером. MP 10 Core устанавливается в центральном офисе компании или в крупных территориальных и функциональных подразделениях и выполняет следующие функции:

— централизованное хранение конфигурации активов;

— централизованное управление всеми компонентами системы;

— автоматизацию процесса управления уязвимостями;

— поддержку веб-интерфейса системы.

2.1.2. Компонент MaxPatrol 10 Collector

Компонент MaxPatrol 10 Collector (далее также — MP 10 Collector) имеет модульную структуру и сканирует активы системы в режимах черного и белого ящика. Модули сканирования позволяют обнаруживать узлы и их открытые сетевые сервисы и проводить специализированные проверки в режиме теста на проникновение.

MP 10 Collector в режиме активного и пассивного сканирования собирает следующую информацию об активах: название, версию и производителя операционной системы, установленные обновления ОС, список установленного ПО, параметры ОС и ПО, учетные записи пользователей и их привилегии, данные об аппаратном обеспечении, запущенных сетевых сервисах и службах ОС, параметрах сети и средств защиты.

Компонент MP 10 Collector управляет перечисленными модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и компонентом MP 10 Core. Собранные данные используются компонентом MP 10 Core для расчета уязвимости активов.

К одному компоненту MP 10 Core можно подключать несколько компонентов MP 10 Collector. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

2.1.3. Компонент PT Management and Configuration

Компонент PT Management and Configuration (далее также — PT MC) обеспечивает:

- сервис единого входа в продукты Positive Technologies, развернутые в инфраструктуре организации;
- управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;
- интеграцию с Microsoft Active Directory, включая аутентификацию пользователей и синхронизацию прав доступа;
- управление иерархией продуктов Positive Technologies;
- журналирование действий пользователей;
- управление лицензиями продуктов Positive Technologies;
- прием, анонимизацию, шифрование и отправку телеметрических данных.

2.1.4. Компонент PT Update and Configuration Service

Компонент PT Update and Configuration Service (PT UCS) выполняет следующие функции:

- проверку наличия, загрузку и установку новых версий модуля Pentest для коллекторов;
- проверку наличия и загрузку дистрибутива с новыми версиями компонентов с глобального сервера обновлений Positive Technologies.

Для доставки коллекторам новых версий модуля Pentest PT UCS использует ПО SaltStack: модуль Salt Master находится на сервере PT UCS, модуль Salt Minion — на серверах коллекторов. PT UCS загружает новые версии с глобального сервера обновлений Positive Technologies и с помощью модуля Salt Master отправляет их модулям Salt Minion для установки.

2.1.5. Локальный сервер обновлений

Локальный сервер обновлений загружает обновления с глобального сервера обновлений Positive Technologies и передает их в изолированный сегмент сети при отсутствии прямого доступа к интернету.

2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol VM:

1. Модули компонента MP 10 Collector сканируют IT-инфраструктуру предприятия и собирают сведения о сетевых узлах. Собранные данные коллекторы передают в MP 10 Core.
2. Компонент MP 10 Core обрабатывает и хранит результаты сканирования с подробной информацией об обнаруженных ОС, ПО, службах, портах и прочими сведениями об узлах и связях между ними. Также компонент хранит параметры задач на сбор данных, профилей сканирования и транспортов, данные и сценарии справочников и осуществляет контроль доступа к этим данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов.
3. Используя данные базы уязвимостей MaxPatrol VM, компонент MP 10 Core рассчитывает уязвимости на активах.
4. Компонент PT MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
5. Для управления системой, просмотра данных, построения отчетов и мониторинга пользователь подключается к компоненту MP 10 Core через веб-интерфейс в соответствии с правами, которые назначены в PT MC.
6. Компонент PT UCS обеспечивает обновление модуля Pentest для коллекторов и загрузку дистрибутивов с новыми версиями компонентов.
7. Локальный сервер обновлений обеспечивает загрузку и передачу обновлений с глобального сервера обновлений Positive Technologies при отсутствии прямого доступа к интернету.

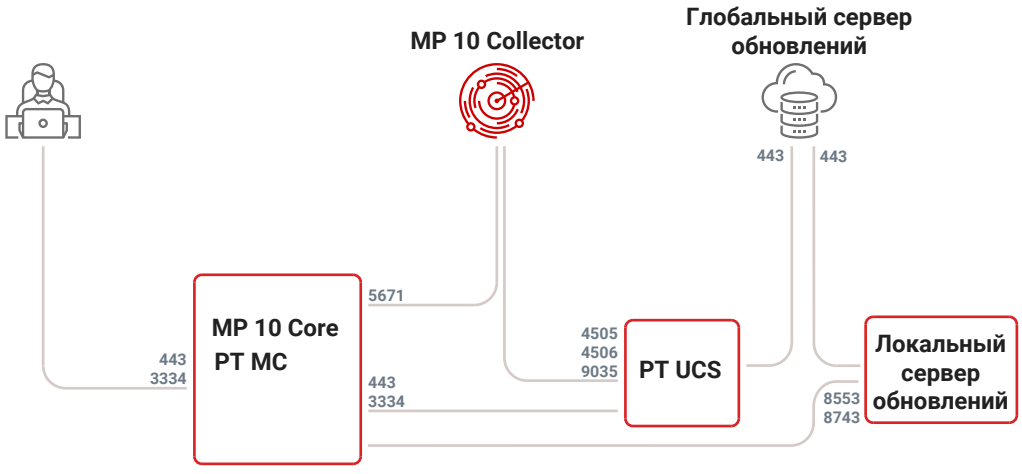

Рисунок 1. Взаимодействие компонентов MaxPatrol VM

Для получения обновлений межсетевой экран сервера компонента PT UCS не должен блокировать адреса глобальных серверов обновлений Positive Technologies — update.ptsecurity.ru и update.ptsecurity.com. Для обеспечения сетевого взаимодействия компонентов MaxPatrol VM должны быть доступны для входящих соединений перечисленные ниже порты.

Таблица 2. Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя	MP 10 Core	443
MP 10 Collector	MP 10 Core	5671
PT UCS	MP 10 Core	443, 3334
Рабочая станция пользователя	PT MC	3334
MP 10 Core, MP 10 Collector	PT UCS	4505, 4506, 9035
PT UCS, локальный сервер обновлений	Глобальный сервер обновлений	443
PT MC	Локальный сервер обновлений	8553, 8743

Внимание! На сервере, на который необходимо установить роль Deployer, порты 4505/TCP, 4506/TCP, 5000/TCP должны быть доступны для входящих соединений.

Для исходящих соединений не требуется создавать правила межсетевого экрана. Для удаленного доступа к серверам компонентов рекомендуется разрешить соединения от рабочих станций администратора через порт 3389/TCP к серверам на Microsoft Windows, через порт 22/TCP — к серверам на Linux.

> **Примечание.** По умолчанию локальный сервер обновлений использует для подключения по протоколам HTTP и HTTPS порты 8553 и 8743 соответственно. Вы можете изменить эти значения в параметрах сервиса получения обновлений.

3. Предоставление прав доступа

В MaxPatrol VM реализована ролевая модель управления доступом. В общем случае пользователю могут быть назначены одна или несколько ролей. Каждая роль содержит набор привилегий, которые определяют доступные для пользователя разделы интерфейса и операции в системе (например, доступность работы с активами). Также для роли можно определить активы, уязвимости и задачи на сбор данных, доступ к которым получат пользователи с этой ролью.

При развертывании системы ее компоненты передают в PT MC данные о доступных привилегиях и стандартных ролях. Роли и привилегии распределены по приложениям, которым соответствует определенный набор функций системы. Если пользователь имеет несколько ролей в приложении, права доступа суммируются.

PT MC обеспечивает механизм единого входа (технология single sign-on), поэтому другие продукты Positive Technologies в случае их интеграции с MaxPatrol VM также могут быть зарегистрованы в PT MC, а их роли и привилегии будут доступны для назначения пользователям.

При развертывании MaxPatrol VM автоматически создается учетная запись (логин — `Administrator`, пароль — `P@ssw0rd`), имеющая все возможные стандартные роли. Эту учетную запись невозможно заблокировать, также невозможно изменить ее логин. После входа в систему рекомендуется сменить пароль этой учетной записи на более сложный.

Для обеспечения выполнения пользователем производственных задач необходимо:

1. Создать для пользователя учетную запись.
2. Если набор привилегий стандартных ролей не подходит для выполнения производственных задач — создать пользовательские роли с нужным набором привилегий.
3. Назначить пользователю необходимые роли.
4. Настроить для ролей доступ к активам и уязвимостям (см. раздел 3.2), а также к задачам на сбор данных (см. раздел 3.3) в соответствии с производственными задачами пользователя.

Если учетные записи пользователей синхронизируются со службой каталогов, назначение им ролей в приложении Management and Configuration недоступно. В этом случае назначать роли пользователям необходимо в службе каталогов, добавляя пользователей в группы, соответствующие требуемым ролям.

В этом разделе приведена инструкция по предоставлению доступа к активам и связанным с ними уязвимостям, а также к задачам на сбор данных. Подробная информация об учетных записях пользователей, их ролях и привилегиях, а также инструкции по работе с ними приведены в руководстве администратора PT MC.

В этом разделе

См. также

Возможности привилегии «Расширенные полномочия» (см. приложение Д)

3.1. О приложениях PT MC

При развертывании MaxPatrol VM в PT MC регистрируются следующие приложения:

- Management and Configuration — предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления площадками и связями между ними. По умолчанию содержит стандартные роли **Администратор** (с полными правами), **Пользователь** (с правами на просмотр и изменение информации в личном профиле) и **Оператор** (с правами на просмотр всей информации в приложении). Приложение также предоставляет пользователю возможность регистрировать, переименовывать и удалять приложения из системы. Для этого роль пользователя должна содержать соответствующие привилегии — **Переименование приложений** и **Добавление и удаление приложений**. Для повышения безопасности вы можете настроить в системе обязательное подтверждение регистрации приложений, установленных неавторизованными пользователями, в соответствии с инструкцией «Включение подтверждения регистрации приложений» Руководства администратора PT MC.
- MaxPatrol 10 — предназначено для настройки сбора данных об IT-инфраструктуре предприятия и работы с активами и уязвимостями. По умолчанию приложение содержит стандартные роли **Администратор** (с полными правами на просмотр и изменение данных в приложении), **Оператор** (с ограниченными правами на просмотр и изменение данных) и **Наблюдатель** (с правами только на просмотр данных). Вы можете просмотреть список привилегий, доступных для этих ролей, на странице **Система** → **Права доступа**.

3.2. Предоставление доступа к активам и уязвимостям

- Чтобы предоставить доступ к активам:

  1. В главном меню в разделе **Система** выберите пункт **Права доступа**.

     Откроется страница **Права доступа**.

  2. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к активам.

  3. В панели **<Название роли>** в блоке параметров **Доступ к активам** нажмите .

4. В открывшемся окне в раскрывающемся списке **Доступ** выберите необходимый тип доступа.
5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы активов, к которым необходимо предоставить доступ.

   Примечание. Вы можете искать группы активов с помощью поля поиска и выбирать группы активов, устанавливая флажки напротив них.
6. Нажмите кнопку **Сохранить**.

Доступ к активам предоставлен.

3.3. Предоставление доступа к задачам на сбор данных

► Чтобы предоставить доступ к задачам на сбор данных:

1. В главном меню в разделе **Система** выберите пункт **Права доступа**.

   Откроется страница **Права доступа**.
2. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к задачам на сбор данных.
3. В панели **<Название роли>** в блоке параметров **Доступ к задачам на сбор данных** нажмите .
4. В открывшемся окне в раскрывающемся списке **Доступ** выберите необходимый тип доступа.
5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы задач на сбор данных, к которым необходимо предоставить доступ.

   Примечание. Вы можете искать группы задач с помощью поля поиска и выбирать группы задач, устанавливая флажки напротив них.
6. Нажмите кнопку **Сохранить**.

Доступ к задачам предоставлен.

4. Управление политиками

Специалистам по ИБ часто требуется анализировать состояние IT-инфраструктуры предприятия. При большом количестве сетевых узлов анализ, выполняемый вручную, может занимать значительное время, что замедлит реакцию на угрозы ИБ.

В MaxPatrol VM предусмотрен механизм для автоматизации процессов устранения уязвимостей и контроля за регулярностью сканирования активов — политики. Политика состоит из совокупности правил, которые автоматически изменяют параметры объектов системы (например, сроки актуальности данных об активах или статусы экземпляров уязвимостей).

Порядок применения правил

Политики содержат стандартные правила, которые по умолчанию отключены. Также вы можете создавать свои правила. Применение условий правила зависит от его номера по порядку внутри политики. Если объект системы может быть изменен несколькими правилами (например, один и тот же актив подходит под условия фильтрации нескольких правил), применятся условия первого по порядку правила. Вы можете менять порядок, перетаскивая правила в таблице.

Применение изменений в политиках

При создании, удалении, включении и отключении правил, а также при изменении их параметров или порядка система не изменяет политику сразу: она создает черновик политики и вносит в него все изменения. Пока изменения не применены, система работает с двумя версиями политики: измененная версия (черновик) отображается в веб-интерфейсе и не применяется к объектам системы, исходная версия (чистовик) применяется к объектам и недоступна для просмотра в веб-интерфейсе. При большом количестве объектов применение изменений может занимать продолжительное время (до нескольких суток).

Если политику изменяют одновременно несколько пользователей, они работают с одним черновиком. В результате применятся изменения, внесенные тем пользователем, который последним работал с черновиком.

Типы политик

В MaxPatrol VM доступны следующие политики.

— **Значимость активов** — правила политики автоматически изменяют значимость активов. Определение значимости активов позволяет упорядочить работу с ними, выделить значимые активы, уязвимости на которых могут нанести больше всего вреда IT-инфраструктуре организации, и уделять им повышенное внимание. Необходимо стремиться к тому, чтобы для всех активов была указана значимость.

— **Сроки актуальности** — правила политики автоматически устанавливают сроки актуальности и устаревания данных об активах, полученных в результате сканирования IT-инфраструктуры методами аудита и пентеста. Опасные уязвимости на активах, данные о

которых редко обновляются, могут быть выявлены слишком поздно. Вы можете оценить количество активов, данные о которых не были получены вовремя, с помощью виджета **Актуальность данных об активах**, а также найти их с помощью PDQL-запроса.

— **Статусы уязвимостей** — правила политики автоматически изменяют статус экземпляров уязвимостей, определяют срок их устранения или откладывают их обработку на определенный срок. Перечень запланированных к устранению уязвимостей можно выпускать в виде отчета по расписанию и отправлять по электронной почте системному администратору.

— **Отметка «важная»** — правила политики автоматически отмечают отдельные экземпляры уязвимостей как важные. Например, в качестве важных могут быть отмечены наиболее опасные для IT-инфраструктуры уязвимости. Вы можете найти активы с важными уязвимостями с помощью PDQL-запроса.

Работа с правилами

На странице **Система** → **Политики** вы можете создавать, изменять и удалять ранее созданные правила. Если требуется изменить стандартное правило, вы можете создать его копию. Вы также можете включать и отключать любые правила, в том числе и стандартные.

Перетаскивая правила в таблице в центральной панели, вы можете настроить порядок применения правил.

Чтобы изменения вступили в силу, необходимо нажать **Применить изменения** под списком политик. Слева от названий измененных политик отобразятся значки .

В таблице в центральной панели отображаются состояния правил:

— правило работает;

— правило остановлено;

— правило работает с предупреждением;

— правило не работает из-за ошибки. Такой же значок отобразится слева от названия политики с этим правилом.

В этом разделе

Создание правила для значимости активов (см. раздел 4.1)

Создание правила для сроков актуальности данных (см. раздел 4.2)

Создание правила для статусов уязвимостей (см. раздел 4.3)

Создание правила для отметки «важная» (см. раздел 4.4)

4.1. Создание правила для значимости активов

- Чтобы создать правило:

  1. В главном меню выберите **Система** → **Политики**.
  2. Выберите политику **Значимость активов**.
  3. Нажмите **Создать правило**.
  4. Введите название правила.
  5. Выберите активы, для которых необходимо указывать значимость.

     Примечание. Вы можете указать группы активов и отфильтровать активы с помощью PDQL-запроса. По ссылке **Вставить условие** доступны стандартные фильтры.
  6. Выберите значимость, которую правило будет назначать активам.
  7. Нажмите **Сохранить**.

  Правило создано. Система начнет использовать его только после применения изменений в политике.

4.2. Создание правила для сроков актуальности данных

- Чтобы создать правило:

  1. В главном меню выберите **Система** → **Политики**.
  2. Выберите политику **Сроки актуальности** для аудита или пентеста.
  3. Нажмите **Создать правило**.
  4. Введите название правила.
  5. Выберите активы, для которых необходимо указывать сроки актуальности данных.

     Примечание. Вы можете указать группы активов и отфильтровать активы с помощью PDQL-запроса. По ссылке **Вставить условие** доступны стандартные фильтры.
  6. Нажмите **Сохранить**.

  Правило создано. Система начнет использовать его только после применения изменений в политике.

4.3. Создание правила для статусов уязвимостей

- Чтобы создать правило:

  1. В главном меню выберите **Система** → **Политики**.
  2. Выберите политику **Статусы уязвимостей**.

3. Нажмите **Создать правило**.
4. Введите название правила.
5. В поле **Фильтр уязвимостей** введите PDQL-запрос для поиска тех экземпляров уязвимостей, статусы которых необходимо изменять.

   Пример:

   ```
   Host.@Vulners.SeverityRating in ['Critical', 'High']
   ```

   Примечание. Вы можете указать группы активов и отфильтровать активы с помощью PDQL-запроса. По ссылке **Вставить условие** доступны стандартные фильтры.
6. Выберите действие, которое необходимо выполнять с экземплярами уязвимостей.
7. Если требуется исключать из мониторинга экземпляры уязвимостей, в раскрывающемся списке **Уточнение к статусу** выберите причину исключения.

   Примечание. По истечении срока исключения экземпляры уязвимостей будут по умолчанию запланированы к устранению в течение семи дней. Если требуется устранять экземпляры уязвимостей вручную, необходимо выбрать это действие в раскрывающемся списке **Устранение**.
8. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только после применения изменений в политике.

4.4. Создание правила для отметки «важная»

- Чтобы создать правило:

1. В главном меню выберите **Система** → **Политики**.
2. Выберите политику **Отметка важная**.
3. Нажмите **Создать правило**.
4. Введите название правила.
5. В поле **Фильтр уязвимостей** введите запрос на языке PDQL для поиска экземпляров уязвимостей, которые необходимо отмечать как важные.

   Пример:

   ```
   Host.@Vulners.IsTrend = True
   ```

   Примечание. Вы можете указать группы активов и отфильтровать активы с помощью PDQL-запроса. По ссылке **Вставить условие** доступны стандартные фильтры.
6. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только после применения изменений в политике.

5. Мониторинг состояния MaxPatrol VM

В MaxPatrol VM реализован автоматический мониторинг параметров жизнеспособности и целостности системы и ее компонентов. Источником для мониторинга служат статистические данные за определенные периоды. Результаты мониторинга отображаются по нажатию индикатора состояния системы. Предусмотрены также цветовые индикаторы уровня опасности события:

- красный — сообщает о неполадке или ошибке в работе системы или ее компонента (например, о том, что компонент недоступен);
- желтый — сообщает о проблеме в работе системы или ее компонента (например, о приближении к пороговому значению наблюдаемого параметра);
- зеленый — сообщает о том, что система работает корректно;
- синий — сообщает о каком-либо событии, не нарушающем жизнеспособность и целостность системы или ее компонента;
- белый — сообщает о том, что диагностику системы выполнить не удалось.

В этом разделе

5.1. Страница «Управление системой»

Страница **Управление системой** предназначена для управления коллекторами сбора данных, а также для просмотра информации об используемой базе знаний по уязвимостям и обновления этой базы вручную.

В рабочей области страницы расположены центральная панель и панель **Компоненты**, в которой доступны следующие разделы.

О системе

Раздел предназначен для просмотра информации о версиях системы и компонента MP 10 Core.

Коллекторы

Раздел предназначен для просмотра подробной информации о коллекторах, для обновления их версий и удаления недоступных коллекторов. При выборе раздела в центральной панели отобразится таблица с коллекторами. Для каждого коллектора в таблице указаны название, версия, статус, роли, а также имя, IP-адреса и семейство ОС сервера.

Примечание. В колонке **IP-адреса** для каждого MP 10 Collector отображаются все адреса сетевых интерфейсов сервера MP 10 Collector, которые доступны для внешнего подключения.

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 поиска параметр коллектора. При выборе коллектора система отображает подробную информацию о нем в боковой панели, в том числе перечень модулей коллектора.

В таблице отображаются следующие статусы коллектора:

- **Доступен** — коллектор работает в нормальном режиме;
- **С ограничениями** — коллектор работает в режиме ограниченной функциональности по причине нехватки свободного места на жестком диске;
- **Недоступен** — MP 10 Core не получает отклика от коллектора более 10 минут;
- **Обновляется** — коллектор обновляется;
- **Удаляется** — коллектор удаляется из списка.

В панели инструментов находятся следующие кнопки:

- **Удалить** — для удаления недоступного коллектора (см. раздел 5.2). Если после удаления коллектор начнет присылать данные, он снова будет отображаться в списке.
- **Обновить версию** — для обновления версии коллектора.

База знаний

Раздел предназначен для просмотра информации о базе знаний, используемой в MP 10 Core, а также для обновления базы знаний вручную. По умолчанию система автоматически проверяет наличие обновлений каждые пять минут.

Обработка активов

Раздел предназначен для просмотра информации 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.

См. также

Удаление недоступного коллектора (см. раздел 5.2)

5.2. Удаление недоступного коллектора

Коллектор, который был установлен в системе, а затем выведен из ее состава (например, по причине неисправности сервера коллектора), автоматически не удаляется из списка коллекторов и продолжает отображаться в интерфейсе со статусом **Недоступен**. После удаления коллектора будут автоматически остановлены:

— если удаленный коллектор был выбран в задаче автоматически — использующие его подзадачи;

— если удаленный коллектор был выбран вручную — использующие его задачи.

► Чтобы удалить коллектор из списка:

1. В главном меню в разделе **Система** выберите пункт **Управление системой**.

   Откроется страница **Управление системой**.

2. В панели **Компоненты** выберите пункт **Коллекторы**.

   В рабочей области страницы отобразится таблица со списком коллекторов.

3. Выберите коллектор со статусом **Недоступен**, который необходимо удалить.

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.

4. В панели управления нажмите кнопку **Удалить из списка** и подтвердите удаление.

   Примечание. Окно подтверждения удаления появляется в случае, когда удаляемый коллектор используется запущенными задачами.

   Статус удаляемого коллектора изменится на **Удаляется**. По завершении удаления коллектор не будет отображаться в списке.

Коллектор удален из списка.

5.3. Настройка количества подзадач, одновременно выполняемых модулем

В коллекторах существует ограничение на количество одновременно выполняемых подзадач для модулей (потоков). При достижении заданного максимального значения новые подзадачи ставятся в очередь. Вы можете настроить количество одновременно выполняемых подзадач для каждого модуля.

► Чтобы настроить количество одновременно выполняемых подзадач:

1. В главном меню в разделе **Система** выберите пункт **Управление системой**.

   Откроется страница **Управление системой**.

2. В панели **Компоненты** выберите пункт **Коллекторы**.

В рабочей области страницы отобразится таблица со списком коллекторов.

3. Выберите коллектор.
4. В панели **Модули и потоки** выберите модуль.
5. По ссылке **Настроить** выберите вариант **Вручную** и укажите значение.

   Внимание! Если указанное значение меньше, чем количество подзадач, выполняющихся в настоящий момент на коллекторе, то новые подзадачи не будут запущены, пока не завершатся уже запущенные подзадачи.

   Примечание. Вы можете отключить модуль от сбора данных, указав значение `0`.

Количество одновременно выполняемых подзадач настроено.

6. Сбор телеметрических данных

В MaxPatrol VM реализован сбор телеметрических данных о производительности микросервисов компонента MP 10 Core и действиях пользователя. Это необходимо для дальнейшего развития продукта и повышения качества экспертизы.

Телеметрические данные собираются на сервере компонента PT MC. Сбор данных о действиях пользователя осуществляется при регистрации действий в системе, а сбор данных о производительности микросервисов — по заданному расписанию (по умолчанию один раз в минуту). Собранные и обезличенные телеметрические данные хранятся в каталоге `/var/lib/deployed-roles/mc-application/observability/data/telemetry/files` в виде файлов в различных форматах.

Архивы файлов с телеметрическими данными хранятся в каталоге `/var/lib/deployed-roles/mc-application/observability/data/telemetry/packs`. Архив шифруется и отправляется на внешний сервер приема телеметрии. Данные из файла с ключом шифрования передаются на сервер с помощью HTTP-запроса.

Для отключения отправки телеметрических данных необходимо обратиться в службу технической поддержки Positive Technologies. Если отправка телеметрических данных в системе отключена, при необходимости вы можете вручную передать архивы файлов с телеметрическими данными в рамках запроса в службу технической поддержки.

Телеметрические данные отправляются на внешний сервер при достижении максимально разрешенного размера (по умолчанию 35 МБ) или один раз в сутки. Вы можете указать период разрешенной отправки данных. Рекомендуется настроить отправку данных в периоды наименьшей нагрузки системы. Отправленные данные автоматически удаляются с сервера. Если отправка данных на внешний сервер разрешена, но не удалась, сервер пытается отправить их повторно в заданное время. Неотправленные данные удаляются через заданный период времени (по умолчанию 30 дней).

7. Мониторинг ресурсов в Grafana

Grafana используется для построения графиков мониторинга и анализа метрик MaxPatrol VM с помощью дашбордов.

Grafana версии 7.5.17 под лицензией Apache 2.0 устанавливается вместе с ролью Observability компонента PT MC.

После установки роли веб-интерфейс Grafana доступен по адресу: `https://<IP-адрес или FQDN сервера PT MC>:3334/grafana`. Вместо `3334/grafana` вы можете использовать номер порта, заданного в параметре `GrafanaServerHttpPort` роли Observability (по умолчанию `9002`).

Для первого входа в веб-интерфейс Grafana необходимо ввести логин и пароль учетной записи, которые задаются в соответствующих параметрах при установке или обновлении роли Observability (по умолчанию `admin` и `P@ssw0rd`).

При установке MaxPatrol VM в Grafana добавляются несколько стандартных дашбордов для мониторинга состояния системы.

Вы можете просматривать метрики серверов, на которых установлены компоненты MaxPatrol VM, а также получать информацию о ключевых метриках СУБД PostgreSQL.

Для переключения между дашбордами необходимо использовать значок ☰ в правом верхнем углу страницы.

Вы не можете вносить изменения в дашборды и источники данных, поставляемые с Grafana. При необходимости вы можете создавать копии системных дашбордов или источников данных либо импортировать собственные, используя штатные инструменты Grafana. В случае переустановки системы эти дашборды будут сохранены.

Подробная информация о Grafana приведена на сайте grafana.com/docs.

В этом разделе

7.1. Работа с дашбордом хранилища событий LogSpace

В MaxPatrol VM реализован сбор данных из хранилища событий LogSpace. Это позволяет отслеживать состояние хранилища и оперативно реагировать на инциденты. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели хранилища, базы данных и операций с ее таблицами, а также показатели дискового пространства и кэша.

В верхней панели дашборда вы можете выбрать FQDN сервера, экземпляр роли Event Storage и период обновления виджетов в минутах.

Виджеты SERVICE SUMMARY

Секция содержит следующие виджеты для мониторинга основных показателей хранилища:

— **LogSpace Status.** Виджет отображает текстовое описание состояния хранилища. Могут отображаться следующие состояния:

  • **Active** — хранилище включено;

  • **Down** — хранилище выключено.

— **LogSpace Uptime.** Виджет отображает время работы хранилища событий с его последней перезагрузки в часах, минутах и секундах.

— **Database Size.** Виджет отображает размер базы данных хранилища LogSpace.

— **Threads.** Виджет отображает количество потоков в процессе LogSpace.

— **Disk Free.** Виджет отображает объем свободного места на диске, где установлено хранилище. Если хранилище LogSpace находится на нескольких дисках, значение будет неполным.

— **Connections.** Виджет представляет собой график, который показывает информацию о количестве соединений следующих типов:

  • **TCP** — открытые TCP-соединения от клиентов к хранилищу;

  • **HTTP** — открытые HTTP-соединения от клиентов к хранилищу;

  • **Interserver** — открытые HTTP-соединения типа «сервер — сервер» (кросс-доменных запросов).

— **Open and Seek.** Виджет представляет собой график, который показывает информацию о следующих показателях:

  • **Files Open** — количество файлов, открытых для чтения или записи;

  • **Seek** — количество установленных смещений файлового дескриптора для последующего чтения.

— **RAM Usage.** Виджет представляет собой график, который показывает информацию об объеме оперативной памяти сервера, используемой сервисами хранилища, за выбранный период времени.

— **Queries.** Виджет представляет собой график, который показывает информацию о количестве следующих типов принятых запросов за выбранный период времени:

  - **Query** — принятые SQL-запросы;
  - **Selectquery** — принятые SQL-запросы `SELECT`;
  - **Insertquery** — принятые SQL-запросы `INSERT`.

— **Cancellations.** Виджет представляет собой график, который показывает информацию о количестве операций следующих типов за выбранный период времени:

  - **RejectedInserts** — добавление информации в таблицу было отменено из-за превышения максимального количества партиций в сегменте;
  - **MergeInsteadInsert** — добавление информации в таблицу отложено из-за объединения партиций: слишком много партиций в одном из сегментов таблицы;
  - **QueryPostponed** — выполнение запроса отложено из-за запросов с более высоким приоритетом.

Виджеты DATABASE

Секция содержит следующие виджеты для мониторинга показателей базы данных:

— **Threads.** Виджет представляет собой график, который показывает информацию о количестве потоков в процессе LogSpace за выбранный период времени.

— **Buffer Read\Write.** Виджет представляет собой график, который показывает информацию о количестве следующих типов операций за выбранный период времени:

  - **Read** — данные файла прочитаны в буфер ввода;
  - **Write** — данные из буфера вывода записаны в файл.

— **Memory Tracking.** Виджет представляет собой график, который показывает информацию об объеме памяти, используемой конвейером обработки запросов, за выбранный период времени.

— **Buffer Read\Write, bytes.** Виджет представляет собой график, который показывает информацию об объеме следующих типов данных за выбранный период времени (в байтах):

  - **Read** — объем прочитанных данных;
  - **Write** — объем записанных данных.

Виджеты DISK

Секция содержит следующие виджеты для мониторинга показателей дискового пространства:

— **File Descriptors.** Виджет представляет собой график, который показывает информацию о количестве файловых дескрипторов, открытых процессами LogSpace, за выбранный период времени.

— **Read Details.** Виджет представляет собой график, который показывает информацию о количестве следующих типов данных за выбранный период времени:

- **SelectedParts** — секции, из которых были запущены процессы чтения;
- **SelectedRanges** — диапазоны ячеек, прочитанных из таблицы;
- **SelectedMarks** — ячейки, прочитанные из таблицы.

— **Size.** Виджет представляет собой графическое и текстовое отображение следующих типов данных:

- **Database Size** — общий размер базы данных LogSpace;
- **Data + stack size** — общий размер данных и стека процесса LogSpace;
- **Text size** — размер секции исполняемых инструкций процесса LogSpace.

Если объем оперативной памяти, занятой процессом LogSpace, приблизится к физическому объему оперативной памяти, работа сервиса замедлится (в некоторых случаях до полной остановки).

— **Opened files for Read\Write.** Виджет представляет собой график, который показывает информацию о количестве следующих типов файлов за выбранный период времени:

- **Read** — файлы, открытые для чтения;
- **Write** — файлы, открытые для записи.

— **Read\Write to files.** Виджет представляет собой график, который показывает информацию о количестве следующих типов файлов за выбранный период времени:

- **Read** — прочтения из файла;
- **Write** — записи в файл.

Виджеты TABLE OPERATIONS

Секция содержит следующие виджеты для мониторинга показателей операций с таблицами БД:

— **Queries.** Виджет представляет собой график, который показывает информацию о количестве следующих типов запросов за выбранный период времени:

- **SQL query accepted** — принятые SQL-запросы;
- **SelectQuery** — принятые SQL-запросы `SELECT`;
- **InsertQuery** — принятые SQL-запросы `INSERT`.

— **Merge.** Виджет представляет собой график, который показывает информацию о следующих показателях таблиц MergeTree за выбранный период времени:

- **Merge** — количество слияний в таблицах MergeTree;
- **MergeTreeDataWriterRows** — размер данных, записанных в строках;
- **MergeTreeDataWriterBlocks** — размер данных, записанных в блоках;
- **MergeTreeDataWriterBlocksAlreadySorted** — размер записанных блоков предварительно отсортированной информации. В таблицу добавлен блок данных, отсортированный в естественном для таблицы порядке: дополнительная сортировка не требуется. Блоки, добавленные в таблицы UnsortedMergeTree, не учитываются;
- **MergedRows** — размер слияний в строках.

— **External Aggregation.** Виджет представляет собой график, который показывает информацию о следующих показателях внешней агрегации за выбранный период времени:

- **ExternalSortWritePart** — ресурсоемкое слияние с использованием внешней сортировки; при этом части сортированных данных выгружаются на диск;
- **ExternalSortMerge** — ресурсоемкое слияние с использованием внешней сортировки; при этом данные с диска загружаются для дальнейшего слияния;
- **ExternalAggregationWritePart** — ресурсоемкая двухуровневая агрегация с выгрузкой данных или части данных на диск (внешняя агрегация, аналогичная внешней сортировке). При этом данные первого уровня агрегации выгружаются на диск;
- **ExternalAggregationMerge** — ресурсоемкая внешняя агрегация. Второй уровень агрегации с загрузкой частично агрегированых данных с диска.

— **Merge, bytes.** Виджет представляет собой график, который показывает информацию о следующих показателях слияний за выбранный период времени (в байтах):

  - **MergeTreeDataWriterUncompressedBytes** — исходный размер записанных данных (до сжатия, размер данных в памяти);
  - **MergeTreeDataWriterCompressedBytes** — конечный размер записанных данных (после сжатия, размер данных на диске);
  - **MergedUncompressedBytes** — размер слияния. В счетчиках слияний заложено усиление записи; средний коэффициент усиления можно оценить как соотношение количества записанных строк и объединенных строк.

— **External Aggregation, bytes.** Виджет представляет собой график, который показывает информацию о следующих показателях внешней агрегации за выбранный период времени (в байтах):

  - **ExternalAggregationCompressedBytes** — размер выгруженных на диск данных после сжатия (расход дискового пространства);
  - **ExternalAggregationUncompressedBytes** — размер выгруженных на диск данных (высвобождение оперативной памяти).

Виджеты CACHE

Секция содержит следующие виджеты для мониторинга показателей кэша:

— **Hits and misses.** Виджет представляет собой график, который показывает информацию о попаданиях и промахах при чтении из кэша для следующих показателей за выбранный период времени:

  - **MarkCacheHits** — попадание при чтении из кэша маркеров;
  - **IdDictCacheHits** — попадание при чтении из кэша словарей;
  - **IndexCacheHits** — попадание при чтении из кэша индексов;
  - **FullTxtCacheHits** — попадание при чтении из кэша полнотекстовых индексов;
  - **MarkCacheMisses** — промах при чтении из кэша маркеров;
  - **IdDictCacheMisses** — промах при чтении из кэша словарей;
  - **IndexCacheMisses** — промах при чтении из кэша индексов;
  - **FullTxtCacheMisses** — промах при чтении из кэша полнотекстовых индексов.

— **Size and limits.** Виджет представляет собой график, который показывает информацию о размере и ограничениях кэша за выбранный период времени:

  - **MarkCacheSize** — размер кэша маркеров;
  - **IdDictCacheSize** — размер кэша словарей;
  - **IndexCacheSize** — размер кэша индексов;

- **FullTxtCacheSize** — размер кэша полнотекстовых индексов;
- **MarkCacheLimit** — ограничение кэша маркеров;
- **IdDictCacheLimit** — ограничение кэша словарей;
- **IndexCacheLimit** — ограничение кэша индексов;
- **FullTxtCacheLimit** — ограничение кэша полнотекстовых индексов.

— **Items.** Виджет представляет собой график, который показывает информацию о количестве записей в кэше следующих типов за выбранный период времени:

- **MarkCacheItems** — записи в кэше маркеров;
- **IdDictCacheItems** — записи в кэше словарей;
- **IndexCacheItems** — записи в кэше индексов;
- **FullTxtCacheItems** — записи в кэше полнотекстовых индексов.

8. Удаление истории изменения активов

MaxPatrol VM хранит историю изменений каждого актива в базе данных сервиса Temporal Read Model (далее также — TRM). Такие данные могут занимать большой объем дискового пространства и приводить к переполнению базы данных. Причинами могут быть большое количество активов в организации и продолжительный жизненный цикл активов.

Для освобождения дискового пространства в MaxPatrol VM реализован механизм автоматического удаления из базы данных TRM записей о версиях активов с момента обнаружения до нужной даты. Процесс автоматического удаления таких записей и связанных с ними объектов называется ротацией. Дата окончания периода, исторические данные за который необходимо удалять, определяется с помощью параметра `HistoryRotationDepth` (глубина ротации в днях). В ходе ротации для каждого актива определяется его версия, ближайшая к дате, определяемой глубиной ротации. В результате удаляются записи с историческими данными обо всех версиях актива, кроме первой и ближайшей к дате, определяемой глубиной ротации.

В ходе ротации удаляются:

— конфигурации активов и данные о состоянии активов до даты ротации;

— информация о вхождении активов в группы до даты ротации;

— данные о состоянии уязвимостей, найденных на активах до даты ротации.

После ротации выполняется оптимизация оставшихся исторических данных, необходимая для сохранения связей между объектами оставшихся версий.

При оптимизации исторических данных об активах в свойствах объектов (групп активов), созданных в первой версии актива, связи с удаленными версиями заменяются на связи с версией, ближайшей к дате ротации. В свойствах объектов, созданных в удаленных версиях актива, дата создания заменяется датой создания версии актива, ближайшей к дате ротации.

Возможные последствия

В результате оптимизации исторических данных, оставшихся после ротации, возможны следующие ситуации:

— Сведения об активе могут заменяться значениями из версии, ближайшей к дате ротации.

— Данные об уязвимостях на активе будут соответствовать последнему актуальному состоянию. Например, открытая уязвимость может отображаться сразу в статусе **В работе**.

— Если актуальный статус уязвимости изменился в удаляемой версии актива, информация об уязвимости на дату обнаружения будет отсутствовать, но будет отображаться при выборе текущей даты.

— Данные о привязке актива к группе будут содержать только последнее актуальное состояние.

— Если перед датой ротации актив в последний раз изменялся вручную, а не по результатам аудита, в качестве даты последнего обновления в жизненном цикле на карточке актива будет отображаться дата последнего аудита актива, но состояние актива на эту дату отображаться не будет.

Настройка ротации истории изменения активов

По умолчанию ротация истории изменения активов в MaxPatrol VM выключена. Включить и настроить ротацию вы можете с помощью конфигурационных параметров роли MP 10 Core.

Внимание! Исторические данные удаляются безвозвратно, поэтому перед включением ротации настоятельно рекомендуется создать резервную копию базы данных assets_temporal_rm. Инструкцию по созданию резервной копии вы можете найти на сайте postgresql.org.

► Чтобы включить и настроить ротацию истории изменения активов:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz` из комплекта поставки:
   ```
   tar xzf pt_core_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_core_<Номер версии>/install.sh
   ```
3. Выберите вариант с идентификатором приложения роли.
4. Выберите вариант с идентификатором экземпляра роли.

   Откроется окно для выбора набора параметров.
5. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение Б).
6. Установите флажок `HistoryRotationEnabled`.
7. В качестве значения параметра `HistoryRotationDepth` укажите глубину ротации — период истории изменения активов, данные за который необходимо удалять:
   ```
   <Дни>.<Часы>:<Минуты>:<Секунды>
   ```

   Например:
   ```
   110.00:00:00
   ```

   Внимание! Минимально допустимое значение параметра `HistoryRotationDepth` — 14 дней (`14.00:00:00`).
8. В качестве значения параметра `HistoryRotationCronSchedule` укажите периодичность запуска ротации с помощью планировщика заданий cron:
   ```
   <Минута> <Час> <Число> <Месяц> <День недели>
   ```

Например, для запуска ротации каждые 6 месяцев в 1 час 30 минут необходимо указать:
`30 1 1 */6 *`

Примечание. Скорость ротации исторических данных об активах напрямую зависит от количества активов в организации и заданной глубины ротации. При этом новая ротация по расписанию будет пропущена, если не завершена предыдущая. Это необходимо учитывать при выборе значения параметра `HistoryRotationCronSchedule`.

9. Нажмите кнопку **OK**.
10. Нажмите **Submit**.

    Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
11. Нажмите кнопку **OK**.
12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

Ротация истории изменения активов включена и настроена.

В случае остановки ротации из-за нехватки объема свободного дискового пространства или из-за возникновения ошибок будет выполнена повторная попытка запуска ротации. Если после трех попыток запустить ротацию не удастся, следующий запуск будет выполнен в соответствии с заданным расписанием.

9. Изменение сроков актуальности данных сканирования активов

- Чтобы изменить сроки актуальности данных сканирования активов:

  1. В главном меню выберите **Активы**.
  2. Выберите активы.
  3. В панели инструментов нажмите → **Паспорт**.
  4. В блоке параметров **Статусы актуальности данных** нажмите **Настроить вручную** для нужного режима сканирования.
  5. Установите новые сроки актуальности данных по ссылкам.
  6. Нажмите **Сохранить**.

10. Ротация результатов сканирования, импорта и ручного ввода активов

MaxPatrol VM хранит результаты сканирования, импорта и ручного ввода активов в базе данных сервиса Assets.Scans. Для хранения таких данных за длительное время требуется большой объем дискового пространства. Если же глубина хранения этих данных недостаточна, вы можете потерять важную информацию.

Для освобождения дискового пространства в MaxPatrol VM реализован механизм ротации. Результаты сканирования, импорта и ручного ввода активов автоматически удаляются по достижении указанного срока хранения. Глубина хранения определяется в днях с помощью параметра `ScansRotationDepth`.

Рекомендуемая глубина хранения результатов — 90 дней. Если указана глубина хранения меньше 90 дней, индикатор состояния MaxPatrol VM отображает предупреждение. Если указана глубина хранения меньше 30 дней — ошибку.

В ходе ротации устаревшие результаты удаляются пакетами указанного размера.

> **Внимание!** Чтобы освободить дисковое пространство, после выполнения ротации необходимо запустить утилиту pgcompacttable для БД сервиса Assets.Scans.

Настройка ротации результатов сканирования, импорта и ручного ввода активов

Ротация результатов включена в MaxPatrol VM по умолчанию. Настроить ротацию вы можете с помощью конфигурационных параметров роли MP 10 Core.

- Чтобы настроить ротацию результатов сканирования, импорта и ручного ввода активов,

  измените конфигурацию роли MP 10 Core, указав значения следующих параметров:

  `ScansRotationEnabled`: `True`

  `ScansRotationDepth`: `<Глубина хранения в формате дд.чч:мм:сс>`

  `ScansRotationBatchSize`: `<Количество результатов сканирования в одном пакете в интервале от 1 до 10 000>`

  Примечание. Если указано значение `ScansRotationBatchSize` меньше 1, ротация запускаться не будет. Если указано значение больше 10 000, то будет использовано значение 10 000.

  `ScansRotationBatchDelay`: `<Задержка между началом обработки пакетов в одной процедуре ротации в формате чч:мм:сс>`

  `ScansRotationRotationDelay`: `<Задержка между процедурами ротации в формате чч:мм:сс>`

11. Максимальный размер собранных данных

Для повышения производительности и устойчивости MaxPatrol VM рекомендуется ограничить размер данных, которые могут быть собраны в одной подзадаче.

Некоторые задачи, например аудит Active Directory, могут возвращать данные сканирования такого объема, который превышает доступную память сервера MP 10 Core. С помощью параметра `MaxScanSizeKb` в MP 10 Core вы можете настроить максимальный размер собранных данных в соответствии с памятью сервера MP 10 Core.

Рекомендуемое значение `MaxScanSizeKb` — примерно 1% от размера памяти сервера MP 10 Core. Значение `MaxScanSizeKb` по умолчанию — 716 800 КБ.

Если собранные в подзадаче данные превышают максимальный размер, в MaxPatrol VM сохраняется запись о выполнении подзадачи, но собранные данные не обрабатываются.

> **Внимание!** При выборе значения `MaxScanSizeKb` следует учитывать связанные с этим ограничения на размер Active Directory. Например, при значении `MaxScanSizeKb`, равном 600 000 КБ, поддерживается аудит служб каталогов Active Directory, включающих до 100 000 пользователей и 5000 групп.
>
> **Примечание.** Чтобы снизить требования к размеру памяти при аудите Active Directory, вы можете ограничить количество собираемых активов. Подробности см. в разделе «Microsoft Active Directory в Windows Server 2003—2022: настройка MaxPatrol SIEM» Руководства по настройке источников.

Таблица 3. Максимальный размер собранных данных

Память (ОЗУ)	**Рекомендуемое значение MaxScanSizeKb, КБ**
80 ГБ	800 000
90 ГБ	900 000
100 ГБ	1 000 000

- Чтобы указать максимальный размер собранных данных,

  измените конфигурацию роли MP 10 Core, указав значение параметра `MaxScanSizeKb` в килобайтах.

12. Оптимизация выполнения PDQL-запросов для высоконагруженных систем

Для оптимизации выполнения PDQL-запросов в высоконагруженных системах вы можете изменить способ фильтрации по времени для сервиса Temporal Read Model (TRM).

При первом включении нового способа фильтрации по времени сервис TRM выполняет миграцию данных. В ходе миграции создаются новые индексы, что приводит к увеличению размера БД сервиса TRM (`assets_temporal_rm`). Для таблиц с данными автоматически выполняется операция vacuum.

Внимание! В процессе миграции могут возникать задержки обработки запросов на получение и вставку данных.

Существуют следующие режимы оптимизации:

- **IdAndPeriod.** Скорость обработки PDQL-запросов возрастает в несколько десятков раз. Увеличение размера БД сервиса TRM может составить до 100%.

  Внимание! Миграция данных в этом режиме может занимать более 10 часов для базы данных размером 100 ГБ.

- **PeriodOnly.** Скорость обработки PDQL-запросов возрастает в несколько раз. Размер БД сервиса TRM увеличивается на 10—20%.

  Внимание! Миграция данных в этом режиме может занимать более одного часа для базы данных размером 100 ГБ.

  Внимание! Перед выполнением миграции необходимо убедиться, что свободного места на диске достаточно.

► Чтобы определить размер базы данных сервиса TRM:

1. Откройте веб-интерфейс Grafana по адресу: `https://<IP-адрес или FQDN сервера PT MC>:3334/grafana`.
2. Выберите дашборд **Postgresql**.
3. В поле **database** выберите `assets_temporal_rm`.

Размер базы данных показан на виджете **Database size**.

► Чтобы включить и настроить оптимизацию выполнения PDQL-запросов,

измените конфигурацию роли Core, указав значения следующих параметров:

`AssetGridVersionRangeModeEnabled`: `True`

`AssetGridValidTimePeriodIndexFormat`: `<Режим оптимизации выполнения PDQL-запросов>`

13. Резервное копирование данных

Вы можете создавать резервные копии данных компонентов MP 10 Core и PT MC с помощью сценариев. При создании резервной копии данных и при их последующем восстановлении из резервной копии должны совпадать конфигурации MaxPatrol VM, версии компонента MaxPatrol VM и языки интерфейса ОС.

Во время создания резервной копии сценарий останавливает службы компонентов, поэтому веб-интерфейс системы будет недоступен. Данные, собираемые коллекторами во время создания копии, не отправляются другим компонентам системы и накапливаются на серверах коллекторов. По завершении создания копии эти данные будут отправлены одновременно всеми коллекторами, что создаст повышенную нагрузку на систему и может привести к появлению ошибок в ее работе. Поэтому перед созданием резервной копии рекомендуется остановить все задачи по сбору данных, а также убедиться, что на период создания резервной копии не запланирован запуск задач по расписанию.

Для резервного копирования данных компонентов на Linux необходимо создать резервные копии данных ролей в следующем порядке: Core → SqlStorage → Deployer. Для резервного копирования данных каждой роли вам потребуется отдельный сценарий `backup.sh`, который после установки роли находится в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/`. Сценарий необходимо запускать в интерфейсе терминала Linux от имени суперпользователя (root).

Если роль RMQ Message Bus содержит пользовательские определения, вы можете создать их резервную копию для сохранения определений при обновлении роли до версии 27.0 или выше.

Сценарии резервного копирования не создают копию цифрового сертификата, заверенного подписью удостоверяющего центра, а также не сохраняют пароли служебных учетных записей, отличные от паролей по умолчанию.

В этом разделе

Создание резервной копии данных роли на Linux (см. раздел 13.1)

Создание резервной копии пользовательских определений роли RMQ Message Bus (см. раздел 13.2)

13.1. Создание резервной копии данных роли на Linux

Если вы используете пользовательские цифровые сертификаты, перед созданием резервной копии необходимо сохранить:

- копии файлов корневых и промежуточных пользовательских сертификатов центра сертификации для роли Deployer, расположенных в каталогах `/opt/deployer/pki/` и `/opt/deployer/pki/trusted_ca/`;
- копии файлов пользовательских сертификатов для остальных ролей из каталогов `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`;
- пути к каталогам, в которых хранятся файлы сертификатов.

  Примечание. Вы можете получить список каталогов, в которых хранятся сертификаты, с помощью команды `deployer params get | grep CertificatesDir | uniq`.

В ходе восстановления данных из резервной копии (см. раздел 14.1) необходимо добавить:

- файлы сертификатов роли Deployer — в каталоги `/opt/deployer/pki/` и `/opt/deployer/pki/trusted_ca/`;
- файлы сертификатов для остальных ролей — в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.

  Примечание. Чтобы избежать ошибок в ходе восстановления данных из резервной копии, при сохранении копий файлов пользовательских сертификатов их необходимо отличать от системных. Для этого вы можете воспользоваться поиском пользовательских сертификатов (см. раздел 23.17).

Перед созданием резервной копии данных роли необходимо остановить все задачи на сбор данных, а также убедиться, что на период создания резервной копии не запланирован запуск задач по расписанию.

► Чтобы создать резервную копию данных,

запустите сценарий резервного копирования:

```
/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/backup.sh
<Путь к каталогу для резервной копии>
```

Например:

```
/var/lib/deployed-roles/mc-application/sqlstorage/backup.sh /home
```

Архив `backup.tar` с резервной копией будет сохранен в каталоге `/<Путь к каталогу для резервной копии>/<Идентификатор приложения>/<Название экземпляра роли>/`.

Например:

`/home/mc-application/sqlstorage`.

13.2. Создание резервной копии пользовательских определений роли RMQ Message Bus

Резервная копия пользовательских определений создается в Docker-контейнере роли RMQ Message Bus.

- Чтобы создать резервную копию,

  на каждом из серверов с установленной ролью RMQ Message Bus выполните следующие команды:

  ```
  docker exec -it $(docker ps -aqf name=messagebus-rabbitmq) rabbitmqctl export_definitions /tmp/rmq_definitions.json
  docker cp $(docker ps -aqf name=messagebus-rabbitmq):/tmp/rmq_definitions.json <Путь к каталогу с резервной копией данных роли на соответствующем сервере>/
  ```

Все пользовательские определения роли будут сохранены в файл `<Путь к каталогу с резервной копией данных роли на соответствующем сервере>/rmq_definitions.json`.

14. Восстановление данных из резервной копии

Вы можете восстанавливать данные компонентов MP 10 Core и PT MC из резервных копий с помощью сценариев. При создании резервной копии данных и при их последующем восстановлении из резервной копии должны совпадать конфигурации MaxPatrol VM, версии компонента MaxPatrol VM и языки интерфейса ОС.

Данные компонентов на Linux необходимо восстанавливать в следующем порядке: Deployer → SqlStorage → Core. Для восстановления данных каждой роли вам потребуется отдельный сценарий `restore.sh`, который после установки роли находится в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/`. Сценарий необходимо запускать в интерфейсе терминала Linux от имени суперпользователя (root).

Инструкции по восстановлению данных содержат шаги по установке компонентов. Поэтому данные компонентов необходимо восстанавливать на сервере с чистой операционной системой.

В этом разделе

14.1. Восстановление данных компонентов MaxPatrol VM на Linux из резервной копии

Для восстановления данных вам потребуются архивы с дистрибутивами ролей. Их версии должны совпадать с версиями дистрибутивов, которые были использованы при создании резервной копии.

Перед восстановлением данных необходимо разместить резервную копию на сервере роли Deployer, а также распаковать на этом сервере архивы с дистрибутивами ролей.

> **Примечание.** Каталоги с резервными копиями должны иметь структуру вида `/<Имя каталога>/<Идентификатор приложения>/<Название экземпляра роли>/backup.tar`, полученную при резервном копировании, например `/backup/mc-application/sqlstorage/backup.tar`.
>
> **Примечание.** Устанавливать роли в процессе восстановления данных необходимо в соответствии с инструкциями из раздела «Развертывание MaxPatrol VM» Руководства по внедрению. При установке всех ролей, кроме Deployer, необходимо выбирать идентификатор восстанавливаемого приложения и название экземпляра восстанавливаемой роли.

- Чтобы восстановить данные компонентов на Linux:

  1. Установите роль Deployer.
  2. Для каждой роли в следующей последовательности SqlStorage → LogConnector → Observability → Management and Configuration → RMQ Message Bus → Core → Collector выполните сценарий:

     ```
     deployer package install -Path /home/<Имя пользователя>/<Путь к файлам дистрибутива роли>/
     pt_<Название роли>_<Номер версии>.tar.gz
     ```

     Например:

     ```
     deployer package install -Path /home/username/pt_MP10-Application_distro_27.3.16568.1980/
     MP10-Application_27.3.16568/pt_agent-linux_27.3.16568.tar.gz
     ```

  3. Восстановите данные роли Deployer:

     ```
     /var/lib/deployed-roles/<Идентификатор приложения Deployer>/<Название экземпляра роли
     Deployer>/restore.sh <Путь к архиву с файлами резервной копии>
     ```

     Например:

     ```
     /var/lib/deployed-roles/Deployment-Application/Deployer/restore.sh /home/deploy-app/
     Deployer/backup.tar
     ```

  4. Если вы используете пользовательские сертификаты, добавьте файлы корневых и промежуточных пользовательских сертификатов центра сертификации для роли Deployer, сохраненные на этапе резервного копирования (см. раздел 13.1), в каталог `/opt/deployer/pki/trusted_ca/`.
  5. Измените конфигурацию (см. раздел 17.2) роли Deployer.
  6. Для каждой роли в каталоге `/var/lib/deployer/role_instances/<Название роли>` в файле `instance.yaml` в качестве значения параметра `HostId` укажите идентификатор Salt Minion.
  7. Для каждой роли в каталоге `/var/lib/deployer/role_instances/<Название роли>` в файлах `params.yaml` и `params.default.yaml` в качестве значений параметров, содержащих FQDN, укажите FQDN серверов, на которые будут установлены соответствующие роли.

     Примечание. Для быстрой замены значений параметров можно использовать команду `find /var/lib/deployer/ -name "params*.yaml" -exec sed -i 's/<FQDN сервера, на который была установлена роль>/<FQDN сервера, на который будет установлена роль>/' {} \;`

  8. Создайте каталоги, в которых хранились файлы сертификатов.

     ```
     mkdir -p <Путь к каталогу сертификатов>
     ```

     Например:

     ```
     mkdir -p /var/lib/deployed-roles/mp10-application/core-1/certs
     ```

  9. Скопируйте в эти каталоги файлы сертификатов, сохраненные при создании резервной копии:

     ```
     cp <Путь к каталогу резервной копии сертификатов>/* <Путь к каталогу сертификатов>
     ```

Например:

```
cp backup/certs/core/certs/* /var/lib/deployed-roles/mp10-application/core-1/certs
```

10. Установите роль SqlStorage.
11. Восстановите данные роли SqlStorage:

    ```
    /var/lib/deployed-roles/<Идентификатор приложения SqlStorage>/<Название экземпляра роли SqlStorage>/restore.sh <Путь к каталогу с файлами резервной копии>
    ```

    Например:

    ```
    /var/lib/deployed-roles/mc-application/sqlstorage/restore.sh /home/mc-application/sqlstorage/
    ```

12. Установите роль LogConnector.
13. Установите роль Observability.
14. Установите роль Management and Configuration.
15. Установите роли RMQ Message Bus и Core.
16. Восстановите данные роли Core:

    ```
    /var/lib/deployed-roles/<Идентификатор приложения Core>/<Название экземпляра роли Core>/restore.sh <Путь к каталогу с файлами резервной копии>
    ```

17. Если вы используете пользовательские сертификаты, добавьте файлы пользовательских сертификатов для остальных ролей:

    Внимание! В случае если резервная копия была создана на сервере с IP-адресом или FQDN, отличным от IP-адреса и FQDN сервера, на котором выполняется восстановление, пользовательские доверенные сертификаты, сохраненные в резервной копии, перестанут быть валидными.

    - Если резервная копия была создана на том же сервере, на котором выполняется восстановление, добавьте файлы пользовательских сертификатов, сохраненные на этапе резервного копирования (см. раздел 13.1), в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.
    - Если резервная копия была создана на одном сервере, а восстановление выполняется на другом, для доверенного сертификата в расширении Subject Alternative Name (SAN) должен быть указан IP-адрес или FQDN того сервера, на котором выполняется восстановление.

18. Выполните команду для восстановления экземпляров роли Collector:

    ```
    deployer instance reconfigure -type AgentLinux
    ```

19. Если ключ инсталляции PT MC уже использовался для активации PT MC на другом устройстве, деактивируйте (см. раздел 23.11) PT MC.
20. Если вы сбросили активацию PT MC, повторно активируйте PT MC по инструкции «Активация PT MC» Руководства по внедрению.

Внимание! Количество активаций ключа инсталляции PT MC ограничено. Если лимит активаций превышен, ваш экземпляр PT MC отключится через 30 дней с момента активации. Чтобы избежать этого, обратитесь в службу технической поддержки Positive Technologies.

21. Если вы сбросили активацию PT MC, повторно активируйте MaxPatrol VM по инструкции «Активация лицензии MaxPatrol VM» Руководства по внедрению.

См. также

Создание резервной копии данных роли на Linux (см. раздел 13.1)

14.2. Восстановление пользовательских определений роли RMQ Message Bus

Вы можете восстановить пользовательские определения роли RMQ Message Bus из резервной копии в Docker-контейнере роли после обновления до версии 27.0 и выше.

- Чтобы восстановить данные из резервной копии,

  на каждом из серверов с установленной ролью RMQ Message Bus выполните следующие команды:

  ```
  docker cp <Путь к каталогу с резервной копией данных роли на соответствующем сервере>/rmq_definitions.json $(docker ps -aqf name=messagebus-rabbitmq):/tmp/
  docker exec -it $(docker ps -aqf name=messagebus-rabbitmq) rabbitmqctl import_definitions /tmp/rmq_definitions.json
  ```

15. Смена паролей служебных учетных записей

Для выполнения своих функций компоненты MaxPatrol VM могут использовать служебные учетные записи. Такие учетные записи не предназначены для выполнения пользователем действий в системе и необходимы для доступа компонентов к ее ресурсам. При развертывании MaxPatrol VM логины и пароли служебных учетных записей устанавливаются в значения по умолчанию.

Вы можете сменить пароли служебных учетных записей. Команды для смены паролей необходимо вводить в интерфейсе терминала Linux от имени суперпользователя (root).

В этом разделе

15.1. Смена пароля служебной учетной записи в PostgreSQL

При развертывании MaxPatrol VM в PostgreSQL создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи — `pt_system`, пароль — `P@ssw0rdP@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи в PostgreSQL на Linux:

  1. Измените конфигурацию (см. раздел 17.2) роли SqlStorage:
     `PgPassword: <Новый пароль>`
  2. Измените конфигурации ролей LogConnector, Observability, Management and Configuration и Core:
     `PostgrePassword: <Новый пароль>`

  Внимание! Не рекомендуется использовать в паролях служебных учетных записей в PostgreSQL следующие символы: `\`, `/`, `'`, `"`, `;`, `$`.

15.2. Смена паролей служебных учетных записей в RabbitMQ

Для обмена данными между службами компонентов MaxPatrol VM используется брокер сообщений RabbitMQ.

В этом разделе

15.2.1. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Core на Linux

По умолчанию логин служебной учетной записи компонента MP 10 Core на Linux — `core`, пароль — `P@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи MP 10 Core:

  1. На сервере MP 10 Core измените конфигурации (см. раздел 17.2) ролей Core и RMQ Message Bus:

     ```
     RMQPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
     docker-compose down
     docker-compose up -d
     ```

  Пароль изменен.

15.2.2. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Microsoft Windows

По умолчанию логин служебной учетной записи компонента MP 10 Collector на Microsoft Windows для доступа к RabbitMQ — `mpx_agent`, пароль — `P@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи для доступа к RabbitMQ, установленному на сервер MP 10 Core под управлением Linux:

  1. Измените конфигурацию ролей RMQ Message Bus и Core, установленных на сервере MP 10 Core:

     ```
     RMQAgentPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
     docker-compose down
     docker-compose up -d
     ```

  3. На сервере каждого компонента MP 10 Collector выполните команду:

     ```
     coreagentcfg set -p RMQUser agent RMQPassword <Новый пароль>
     ```

  Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 17.2)

15.2.3. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Linux

По умолчанию логин служебной учетной записи компонента MP 10 Collector на Linux для доступа к RabbitMQ — `agent`, пароль — `P@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи для доступа к RabbitMQ, установленному на сервер MP 10 Core под управлением Linux:

  1. Измените конфигурацию ролей RMQ Message Bus и Core, установленных на сервере MP 10 Core:

     ```
     RMQAgentPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
     docker-compose down
     docker-compose up -d
     ```

  3. На сервере каждого компонента MP 10 Collector измените конфигурацию роли Collector:

     ```
     AgentRMQPassword: <Новый пароль>
     ```

  Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 17.2)

16. Настройка журналирования работы MaxPatrol VM

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

В этом разделе

16.1. Настройка журналирования работы компонента MP 10 Core на Linux

Настройка выполняется отдельно для каждой службы компонента.

- Чтобы настроить журналирование:

  1. На сервере MP 10 Core в файл `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol VM>/<Название экземпляра роли Core>/images/<Название службы>/config/custom.env` добавьте параметр:

     ```
     Logging_Threshold=<Уровень журналирования>
     ```

     Примечание. Возможны значения FATAL, ERROR, WARN, INFO, DEBUG и TRACE.

  2. Выполните команды:

     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol VM>/<Название экземпляра роли Core>/images/<Название службы>/
     docker-compose down
     docker-compose up -d
     ```

  Журналирование настроено.

16.2. Настройка журналирования работы компонента MP 10 Collector на Microsoft Windows

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию в журнал записываются события уровня `DEBUG`. Размер каждого файла журнала ограничен 100 МБ, сохраняются последние 50 файлов. Для настройки журналирования вам потребуется файл `C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\agent.log.xml`, который находится на сервере MP 10 Collector.

Примечание. Не рекомендуется изменять уровень журналирования без указания службы технической поддержки Positive Technologies.

- Чтобы настроить журналирование:

  1. В файле `agent.log.xml` измените значение атрибута `level` параметра `config` → `root`:

     ```
     <Название журналируемого компонента коллектора> level="<Уровень журналирования>"
     ```

     Примечание. Возможные значения NOTSET, FATAL, ERROR, WARN, INFO, DEBUG и TRACE.

  2. Измените значения атрибутов `max_file_size` и `max_backup_index` параметра `config` → `params`:

     ```
     params max_file_size="<Максимальный размер файла журнала (в мегабайтах)>"
     max_backup_index="<Максимальное количество сохраняемых файлов журналов>"
     ```

  3. Перезапустите службу Core Agent.

  Журналирование настроено.

Эта инструкция не предназначена для настройки журналирования работы модулей MP 10 Collector и их компонентов. Оно настраивается с помощью справочников MaxPatrol VM (подробное описание см. в Руководстве по настройке источников).

17. Просмотр и изменение параметров конфигурации MaxPatrol VM

В этом разделе приведены инструкции по просмотру и изменению параметров конфигурации компонентов MaxPatrol VM. Описания параметров приведены в приложениях.

Конфигурация компонента включает в себя параметры конфигураций ролей, с помощью которых компонент был установлен. Для изменения конфигурации компонента необходимо изменить конфигурацию той или иной роли.

В результате просмотра или изменения конфигурации роли в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы изменений. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

В этом разделе

17.1. Просмотр конфигурации роли

- Чтобы просмотреть конфигурацию роли:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_<Название роли>_<Номер версии>.tar.gz` из комплекта поставки:
     ```
     tar -xf pt_<Название роли>_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_<Название роли>_<Номер версии>/install.sh
     ```
  3. В открывшемся окне нажмите кнопку **Yes**.
  4. Выберите вариант с идентификатором приложения роли.
  5. Выберите вариант с идентификатором экземпляра роли.

     Откроется окно для выбора набора параметров.

6. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение Б).

7. По завершении просмотра нажмите кнопку **Cancel**.
8. В окне для выбора набора параметров нажмите кнопку **Cancel**.

17.2. Изменение конфигурации роли

Вы можете изменить конфигурацию роли с помощью сценария `install.sh`, который необходимо запускать в интерфейсе терминала от имени суперпользователя (root), а также с помощью утилиты `deployer`, поставляемой с ролью Deployer.

- Чтобы изменить конфигурацию роли с помощью сценария `install.sh`:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_<Название роли>_<Номер версии>.tar.gz` из комплекта поставки:
     ```
     tar -xf pt_<Название роли>_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_<Название роли>_<Номер версии>/install.sh
     ```
  3. В открывшемся окне нажмите кнопку **Yes**.
  4. Выберите вариант с идентификатором приложения роли.
  5. Выберите вариант с идентификатором экземпляра роли.

     Откроется окно для выбора набора параметров.

  6. Выберите вариант **Advanced configuration**.

     Откроется страница со списком параметров (см. приложение Б).

  7. Измените значения параметров.
  8. Нажмите кнопку **OK**.
  9. Нажмите **Submit**.

     Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.

  10. Нажмите кнопку **OK**.
  11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

  Конфигурация роли изменена.

► Чтобы изменить конфигурацию роли с помощью утилиты `deployer`:

1. На сервере с установленной ролью Deployer выполните команду:
   `deployer instance configure -type <Тип роли>`
2. Выберите вариант с идентификатором приложения роли.
3. Выберите вариант с идентификатором экземпляра роли.

   Примечание. Вы можете узнать идентификатор экземпляра роли с помощью утилиты `deployer`.

   Откроется окно для выбора набора параметров.
4. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение Б).
5. Измените значения параметров.
6. Нажмите **Submit**.

   Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
7. Нажмите кнопку **OK**.
8. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

Конфигурация роли изменена.

Примечание. Вы можете установить значение любого из параметров экземпляра роли, а также можете сбросить значение любого параметра до значения по умолчанию с помощью команды `deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр, значение которого необходимо установить>=<Значение> <Параметр, значение которого необходимо сбросить>=`. Кроме того, с помощью команды `deployer instance clearparam -Id <Идентификатор экземпляра роли>` вы можете сбросить значения всех параметров экземпляра роли до значений по умолчанию. После внесения этих изменений необходимо изменить конфигурацию роли, выполнив команду `deployer instance reconfigure -type <Тип роли>`.

17.3. Управление изменением конфигурации ролей с помощью манифеста

Начиная с версии 2.8 для оптимизации работы вы можете выбрать необходимые роли и внести изменения в их конфигурацию одновременно. Для этого необходимо создать манифест (см. раздел 17.3.2) — файл формата YAML, который задает параметры изменения конфигурации.

В этом разделе

17.3.1. Изменение конфигурации ролей с помощью манифеста

- Чтобы изменить конфигурацию ролей с помощью манифеста:

  1. Обновите роль Deployer.
  2. Создайте манифест (см. раздел 17.3.2).
  3. Если требуется, добавьте параметры в файл манифеста или измените значения существующих.

     Структура файла манифеста и описание его параметров приведены в разделе «Авторазвертывание MaxPatrol VM с помощью манифеста» Руководства по внедрению.
  4. Выполните команду для изменения конфигурации ролей:

     ```
     deployer application deploy ./export_manifest.yaml --accepteula
     ```

В консоли появится информация о результатах изменения конфигурации:

- Если конфигурация экземпляра роли была изменена успешно, рядом с его идентификатором будет добавлен комментарий `Instance installation is successful`.
- Если конфигурация экземпляра роли не была изменена, рядом с его идентификатором будет добавлен комментарий с причиной неудачи.
- Если конфигурация экземпляра роли не была изменена из-за отсутствия соединения с модулем Salt Minion, появится сообщение об ошибке `There are no SCM hosts available`.

  Примечание. Вы можете проверить соединение с модулями с помощью команды `salt-run manage.status`.

Отчет о работе сценария будет сохранен в каталоге `./installReports`.

См. также

Создание манифеста для обновления компонентов или изменения конфигурации ролей (см. раздел 17.3.2)

17.3.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей

Для обновления компонентов или изменения конфигурации ролей MaxPatrol VM вы можете использовать манифест — файл формата YAML. Для создания манифеста необходимо использовать сценарий `deployer instance export`.

- Чтобы создать манифест:

  1. На сервере с установленной ролью Deployer запустите сценарий:
     `deployer instance export`
  2. Выберите вариант с идентификатором приложения MaxPatrol 10.

     Значение по умолчанию — `mp10-application`.
  3. Нажмите **Select**.
  4. Выберите экземпляры ролей, информацию о которых необходимо добавить в манифест.
  5. Нажмите **Select**.

В текущем каталоге появится файл `export_manifest.yaml` с информацией о выбранных экземплярах ролей.

Вы можете использовать сценарий `deployer instance export` со следующими аргументами.

Таблица 4. Аргументы сценария

Аргумент	Описание	Пример использования
`AppId`	Добавление в манифест информации об идентификаторе приложения. Для добавления информации обо всех приложениях после аргумента необходимо добавить `"*"`	`deployer instance export -AppId "*"`
`Id`	Добавление в манифест информации об идентификаторе экземпляра роли. Для добавления информации обо всех ролях после аргумента необходимо добавить `"*"`	`deployer instance export -Id "*"`
`Type`	Добавление в манифест информации о типе экземпляра роли. Для добавления информации обо всех ролях после аргумента необходимо добавить `"*"`	`deployer instance export -Type "*"`

Аргумент	Описание	Пример использования
`ExcludeType`	Исключение из манифеста информации о типе экземпляра роли. Чтобы исключить информацию о нескольких типах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -ExcludeType "rmqmessagebus,core,siemserver,agentlinux"`
`ExcludeId`	Исключение из манифеста информации об идентификаторе экземпляра роли. Чтобы исключить информацию о нескольких идентификаторах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -ExcludeId "rmq-1,kb-1"`
`IncludeType`	Добавление в манифест информации о типе экземпляра роли. Чтобы добавить информацию о нескольких типах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux"`
`IncludeId`	Добавление в манифест информации о идентификаторе экземпляра роли. Чтобы добавить информацию о нескольких идентификаторах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeId "rmq-1,kb-1"`
`IncludeParam`	Добавление в манифест информации о параметрах экземпляра роли. Чтобы добавить информацию о нескольких параметрах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParam "RmqPassword"`
`IncludeParamValue`	Добавление в манифест определенных значений параметров экземпляра роли. Чтобы добавить несколько значений, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParamValue "P@ssw0rd"`
`NotExportParams`	Исключение из манифеста параметров экземпляров ролей. Параметры, к которым применены аргументы `IncludeParam` или `-IncludeParamValue`, не будут исключены из манифеста	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -NotExportParams "RmqPassword"`

Аргумент	Описание	Пример использования
`ExportVersion`	Сохранение текущих версий экземпляров ролей и компонентов. Аргумент применяется, если необходимо изменить конфигурацию ролей без обновления их версий	`deployer instance export -AppId "*" -ExportVersion`

Примечание. Рекомендуется использовать сценарий с одним из аргументов `AppId`, `Id` или `Type`. Если указать несколько аргументов, фильтрация будет применена в следующем порядке: `AppId`, `Type`, `Id`.

Для параметров экземпляров ролей, не указанных в сценарии, будет применяться ранее заданное значение. Если значения не были заданы, то в качестве параметров роли будут определены автоматически рассчитанные динамические значения или статические значения по умолчанию.

Примеры сценариев создания манифеста

Вы можете использовать следующие примеры сценариев создания манифеста для изменения конфигурации ролей:

- `deployer instance export -Type "agentlinux" -ExportVersion`

  Манифест будет включать информацию обо всех экземплярах роли Collector.

- `deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -ExportVersion`

  Манифест будет включать информацию обо всех экземплярах ролей RMQ Message Bus, Core, SIEM Server, Collector.

- `deployer instance export -AppId "*" -ExcludeType "agentlinux" -ExportVersion`

  Манифест будет включать информацию об экземплярах всех ролей, кроме Collector.

- `deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParam "RmqPassword" -ExportVersion`

  Манифест будет включать информацию об экземплярах ролей RMQ Message Bus, Core, SIEM Server, Collector и пароле служебной учетной записи для подключения к брокеру сообщений RMQ Message Bus.

- `deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParamValue "P@ssw0rd" -ExportVersion`

  Манифест будет включать информацию обо всех экземплярах ролей RMQ Message Bus, Core, SIEM Server, Collector и всех параметрах, которые имеют значение `P@ssw0rd`.

Вы можете использовать следующие примеры сценариев создания манифеста для обновления компонентов:

— `deployer instance export -Type "agentlinux"`

  Манифест будет включать информацию обо всех экземплярах роли Collector.

— `deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux"`

  Манифест будет включать информацию обо всех экземплярах ролей RMQ Message Bus, Core, SIEM Server, Collector.

— `deployer instance export -AppId "*" -ExcludeType "agentlinux"`

  Манифест будет включать информацию об экземплярах всех ролей, кроме Collector.

— `deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParam "RmqPassword"`

  Манифест будет включать информацию об экземплярах ролей RMQ Message Bus, Core, SIEM Server, Collector и пароле служебной учетной записи для подключения к брокеру RMQ Message Bus.

— `deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParamValue "P@ssw0rd"`

  Манифест будет включать информацию обо всех экземплярах ролей RMQ Message Bus, Core, SIEM Server, Collector и всех параметрах, которые имеют значение `P@ssw0rd`.

17.4. Настройка SMTP-сервера для отправки уведомлений по электронной почте

Уведомления MaxPatrol VM содержат информацию об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных и состоянии системы. Вы можете настроить отправку уведомлений по электронной почте, указав при создании задачи адреса получателей уведомления. Подробнее о создании задач для отправки уведомлений см. Руководство оператора. Перед созданием задачи необходимо настроить SMTP-сервер.

► Чтобы настроить SMTP-сервер для отправки уведомлений по электронной почте:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_core_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_core_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Выберите вариант с идентификатором приложения роли.
5. Выберите вариант с идентификатором экземпляра роли.

Откроется окно для выбора набора параметров.

6. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение Б).

7. Укажите значения параметров:

   ```
   SmtpHost: <IP-адрес или FQDN SMTP-сервера>
   SmtpPassword: <Пароль служебной учетной записи для подключения MP 10 Core к SMTP-серверу>
   SmtpPort: <Порт SMTP-сервера для входящих подключений от MP 10 Core>
   SmtpSender: <Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте>
   SmtpUser: <Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу>
   ```

   Примечание. Для публичных почтовых сервисов значения параметров `SmtpSender` и `SmtpUser` должны совпадать.

8. Чтобы отключить проверку валидности сертификата при подключении к SMTP-серверу, в качестве значения параметра `SmtpIgnoreCertificateValidation` выберите `True`.

9. В качестве значения параметра `SmtpSecureSocketOptions` выберите вариант шифрования при подключении к SMTP-серверу.

10. Нажмите кнопку **OK**.

11. Нажмите **Submit**.

    Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.

12. Нажмите кнопку **OK**.

13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

SMTP-сервер настроен.

17.5. Настройка прокси-сервера для онлайн-активации PT MC

- Чтобы настроить прокси-сервер,

  измените конфигурацию роли Management and Configuration, указав значения следующих параметров:

  ```
  ProxyPassword: <Пароль для доступа к прокси-серверу>
  ProxyUrl: <URL прокси-сервера>
  ProxyUserName: <Логин для доступа к прокси-серверу>
  UseProxy: True
  ```

17.6. Включение AI-поиска по запросам

- Чтобы включить AI-поиск по PDQL-запросам,

  измените конфигурацию роли Core, указав для параметра `Text2PdqlEnabled` значение `True`.

Подробности об этой возможности см. в разделе «Фильтрация активов с помощью AI-поиска по запросам» Руководства оператора.

17.7. Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol VM

Для повышения уровня безопасности Docker-контейнеров ролей рекомендуется включить в них профили безопасности.

- Чтобы включить профиль безопасности в Docker-контейнерах ролей:

  1. Измените конфигурацию роли Deployer, указав для параметра `SeccompEnabled` значение `True`.
  2. Измените конфигурацию остальных ролей, указав для параметра `SeccompEnabled` значение `True`.

17.8. Изменение времени устаревания активов

По умолчанию время устаревания активов — 90 дней.

- Чтобы установить другое время,

  измените конфигурацию роли Core, указав для параметра `DefaultAssetTtl` новое значение в формате `<Дни>.<Часы>:<Минуты>:<Секунды>`, например `30.00:00:00`.

18. Удаление экземпляра роли Collector

Вы можете удалить экземпляры роли Collector с помощью утилиты Remove-RoleInstance, поставляемой с ролью Deployer. Утилита удаляет пакеты коллектора и его модулей, файлы из каталогов для хранения данных роли, а также экземпляр роли из веб-интерфейса.

Внимание! Для удаления экземпляра роли Collector вам потребуются логин и пароль учетной записи, которой доступна привилегия «Управление системой».

- Чтобы удалить экземпляр роли Collector:

  1. На сервере с установленной ролью Deployer запустите утилиту Remove-RoleInstance: `/opt/deployer/bin/Remove-RoleInstance.ps1`
  2. Если в системе есть несколько коллекторов, в открывшемся окне выберите экземпляр роли для удаления и нажмите кнопку **Yes**.
  3. В открывшемся окне подтвердите удаление экземпляра роли.
  4. В открывшемся окне введите логин учетной записи, которой доступна привилегия «Управление системой», и нажмите кнопку **OK**.
  5. В открывшемся окне введите пароль учетной записи, которой доступна привилегия «Управление системой», и нажмите кнопку **OK**.

     Начнется процесс удаления экземпляра роли.

Удаленный экземпляр роли будет отсутствовать в списке коллекторов на странице **Система** → **Управление системой** на вкладке **Коллекторы**. Также будут удалены каталоги `/var/log/core-agent` и `/opt/core-agent`. Вы можете проверить корректность удаления пакетов коллектора и его модулей с помощью команды `dpkg -l | grep agent`.

Если при первом запуске утилиты не удалось удалить экземпляр роли (например, отсутствует связь с модулем Salt Minion на сервере коллектора), вы можете запускать утилиту повторно до удаления экземпляра.

19. Настройка очереди выпуска отчетов

По умолчанию в MaxPatrol VM одновременно может быть запущено не более пяти задач на выпуск отчетов. При необходимости вы можете изменить это ограничение с помощью параметра `PrintingQueueJobsLimit` роли Core.

- Чтобы настроить очередь выпуска отчетов:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz` из комплекта поставки:
     ```
     tar xzf pt_core_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_core_<Номер версии>/install.sh
     ```
  3. Выберите вариант с идентификатором приложения роли.
  4. Выберите вариант с идентификатором экземпляра роли.
  5. Выберите вариант **Advanced configuration**.
  6. В качестве значения параметра `PrintingQueueJobsLimit` укажите максимальное количество одновременно выпускаемых отчетов.

     Примечание. Чем больше это количество, тем выше будет нагрузка на аппаратные ресурсы сервера MaxPatrol VM.
  7. Нажмите **OK**.
  8. Нажмите **Submit**.

     Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
  9. Нажмите **OK**.
  10. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

  Примечание. В результате настройки текущие задачи на выпуск отчетов будут остановлены со статусом **Выпуск отменен** и пропадут из очереди. После настройки необходимо перезапустить остановленные задачи вручную по кнопке **Выпустить отчет**.

20. Пользовательские поля в модели актива

После развертывания системы в модели актива присутствуют только стандартные поля (например, «Полное имя узла», «Тип устройства», «Операционная система»). Вы можете добавлять в модель актива пользовательские поля (например, «Инвентаризационный номер актива в реестре», «Ответственный за актив») и их описание, изменять имена добавленных ранее полей или удалять их из модели актива.

После добавления полей и ввода их значений пользователи системы смогут:

— просматривать значения добавленных полей в карточке и миникарточке актива;

— вводить поисковые запросы с учетом добавленных полей;

— осуществлять выборку, группировку и отбор по значениям добавленных полей (PDQL-запрос).

Перед работой с пользовательскими полями необходимо создать файл `UserModel.xml` в кодировке UTF-8:

```
<model Version="0.0.0.0">
    <layer id="UserModel" version="">
        <Dsl Version="">
            <Entities/>
            <Migrations>
            </Migrations>
        </Dsl>
    </layer>
    <layer id="UserDescriptions" locale="ru-RU" version="">
        <Entities>
        </Entities>
    </layer>
</model>
```

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла `UserModel.xml` не игнорируется регистр символов.

Файл `UserModel.xml` необходимо разместить на сервере MP 10 Core в каталоге `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли Core>/config/user_model/`.

В этом разделе

20.1. Добавление пользовательских полей в модель актива

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла `UserModel.xml` не игнорируется регистр символов.

Если вы добавляете пользовательские поля впервые, вам потребуется файл `ModelMigrations.xml`, который находится в каталоге `/usr/local/share/microservice/layers/ModelMigrations.xml` в Docker-контейнере службы Core Assets Processing.

> **Примечание.** Вы можете войти в Docker-контейнер службы Core Assets Processing с помощью команды `docker exec -t -i $(docker ps | awk '/assets-processing/ {print $NF}') /bin/bash`.

Первичное добавление пользовательских полей в модель актива

- Чтобы впервые добавить пользовательские поля в модель актива:

1. В файле `ModelMigrations.xml` скопируйте значение атрибута `Version` элемента `Dsl` и добавьте единицу к последней цифре скопированного значения версии пользовательской модели (например, `version="19.0.20206.1"`).
2. В файле `UserModel.xml` укажите полученное значение в качестве значения атрибута `Version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl`.

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="19.0.20206.1">
    <Dsl Version="19.0.20206.1">
      <Entities/>
      <Migrations>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="19.0.20206.1">
    <Entities>
    </Entities>
  </layer>
</model>
```

3. Для элемента `layer id="UserModel"` → `Dsl` → `Migrations` добавьте дочерний элемент `Group` с атрибутом `Version`. В качестве значения атрибута `Version` укажите версию пользовательской модели, например:

```
<Group Version="19.0.20206.1">
</Group>
```

4. Для элемента `Group` добавьте дочерний элемент `ChangeEntity` с атрибутом `Type`. В качестве значения атрибута `Type` укажите `Core.Host`:

```
<ChangeEntity Type="Core.Host">
</ChangeEntity>
```

5. Для элемента `ChangeEntity` добавьте дочерние элементы `AddProperty` (по количеству добавляемых пользовательских полей) с атрибутами `Property` и `PropertyType`. В качестве значения атрибута `Property` укажите имя поля, значения атрибута `PropertyType` — тип поля.

   Примечание. Имена полей должны начинаться с префикса `UF_`. Допускаются также следующие типы полей: `Int`, `Bool`, `String`, `DateTime`, `Double`, `Network.IP`.

   Например:

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="19.0.20206.1">
    <Dsl Version="19.0.20206.1">
      <Entities/>
      <Migrations>
        <Group Version="19.0.20206.1">
          <ChangeEntity Type="Core.Host">
            <AddProperty Property="UF_InformationSystem" PropertyType="String"/>
            <AddProperty Property="UF_Purpose" PropertyType="String"/>
            <AddProperty Property="UF_ProdTest" PropertyType="String"/>
            <AddProperty Property="UF_Segment" PropertyType="String"/>
            <AddProperty Property="UF_Tag" PropertyType="String"/>
          </ChangeEntity>
        </Group>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="19.0.20206.1">
    <Entities>
    </Entities>
  </layer>
</model>
```

6. Если требуется, добавьте описание пользовательских полей (см. раздел 20.2).

7. Перезапустите службы.

```
docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|
assets.compliancecontrol|assets-identity|assets.input|assets.groups|assets-projections|
assets-scans|core.scanning|core-tables|core-topology|core-topology-analyzer/ {print $NF}')
```

Повторное добавление пользовательских полей в модель актива

- Чтобы повторно добавить пользовательские поля в модель актива:

1. В файле `UserModel.xml` добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.2"`) в качестве значения атрибута `Version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl`.

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="19.0.20206.2">
```

```
    <Dsl Version="19.0.20206.2">
      <Entities/>
      <Migrations>
        <Group Version="19.0.20206.1">
          <ChangeEntity Type="Core.Host">
            <AddProperty Property="UF_InformationSystem" PropertyType="String"/>
            <AddProperty Property="UF_Purpose" PropertyType="String"/>
            <AddProperty Property="UF_ProdTest" PropertyType="String"/>
            <AddProperty Property="UF_Segment" PropertyType="String"/>
            <AddProperty Property="UF_Tag" PropertyType="String"/>
          </ChangeEntity>
        </Group>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="19.0.20206.2">
    <Entities>
    </Entities>
  </layer>
</model>
```

2. Для элемента `layer id="UserModel"` → `Dsl` → `Migrations` добавьте дочерний элемент `Group` с атрибутом `Version`. В качестве значения атрибута `Version` укажите версию пользовательской модели, например:

   ```
   <Group Version="19.0.20206.2">
   </Group>
   ```

3. Для элемента `Group` добавьте дочерний элемент `ChangeEntity` с атрибутом `Type`. В качестве значения атрибута `Type` укажите `Core.Host`:

   ```
   <ChangeEntity Type="Core.Host">
   </ChangeEntity>
   ```

4. Для элемента `ChangeEntity` добавьте дочерние элементы `AddProperty` (по количеству добавляемых пользовательских полей) с атрибутами `Property` и `PropertyType`. В качестве значения атрибута `Property` укажите имя поля, значения атрибута `PropertyType` — тип поля.

   Примечание. Имена полей должны начинаться с префикса `UF_`. Допускаются также следующие типы полей: `Int`, `Bool`, `String`, `DateTime`, `Double`, `Network.IP`.

   Например:

   ```
   <model Version="0.0.0.0">
     <layer id="UserModel" version="19.0.20206.2">
       <Dsl Version="19.0.20206.2">
         <Entities/>
         <Migrations>
           <Group Version="19.0.20206.1">
             <ChangeEntity Type="Core.Host">
               <AddProperty Property="UF_InformationSystem" PropertyType="String"/>
               <AddProperty Property="UF_Purpose" PropertyType="String"/>
               <AddProperty Property="UF_ProdTest" PropertyType="String"/>
   ```

```
            <AddProperty Property="UF_Segment" PropertyType="String"/>
            <AddProperty Property="UF_Tag" PropertyType="String"/>
          </ChangeEntity>
        </Group>
        <Group Version="19.0.20206.2">
          <ChangeEntity Type="Core.Host">
            <AddProperty Property="UF_ISOwner" PropertyType="String"/>
            <AddProperty Property="UF_ ISOwnerLogin" PropertyType="String"/>
          </ChangeEntity>
        </Group>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="19.0.20206.2">
    <Entities>
    </Entities>
  </layer>
</model>
```

5. Если требуется, добавьте описание пользовательских полей (см. раздел 20.2).
6. Перезапустите службы.

```
docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|
assets.compliancecontrol|assets-identity|assets.input|assets.groups|assets-projections|
assets-scans|core.scanning|core-tables|core-topology|core-topology-analyzer/ {print $NF}')
```

См. также

Добавление описания пользовательских полей (см. раздел 20.2)

20.2. Добавление описания пользовательских полей

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла `UserModel.xml` не игнорируется регистр символов.

- Чтобы добавить описание пользовательских полей:

1. В файле `UserModel.xml` для элемента `layer id="UserDescriptions"` → `Entities` добавьте дочерний элемент `Entity` с атрибутом `Name`.
2. В качестве значения атрибута `Name` укажите алиас типа актива.

   Например, для активов на Windows необходимо указать:

   ```
   <Entity Name="OperatingSystem.Windows.WindowsHost">
   </Entity>
   ```

   Примечание. Названия алиасов по типу актива содержатся в Docker-контейнере службы Core Assets Processing в файле `/usr/local/share/microservice/layers/AssetAliases.xml`. Для входа в Docker-контейнер вы можете использовать команду `docker exec -t -i $(docker ps | awk '/assets-processing/ {print $NF}') /bin/bash`.

Примечание. При добавлении описания пользовательских полей значение атрибута `version` элемента `layer id="UserDescriptions"` несущественно. Вы можете оставить текущее значение или изменить его на любое другое.

3. Для элемента `Entity` добавьте дочерний элемент `Properties`:
   ```
   <Properties>
   </Properties>
   ```
4. Для элемента `Properties` добавьте дочерние элементы `Property` (по числу пользовательских полей с описанием) с атрибутом `Name`. В качестве значения атрибута `Name` укажите имя поля, например:
   ```
   <Property Name="UF_AssetNumber">
   </Property>
   ```
5. Для каждого элемента `Property` добавьте дочерний элемент `Title`. В качестве значения элемента `Title` укажите описание пользовательского поля.

   Например:
   ```
   <Entity Name="OperatingSystem.Windows.WindowsHost">
       <Properties>
           <Property Name="UF_AssetNumber">
               <Title>Инвентарный номер актива в реестре</Title>
           </Property>
           <Property Name="UF_AssetOwner">
               <Title>Ответственный за актив:</Title>
           </Property>
           <Property Name="UF_DeploymentEnviroment">
               <Title>Среда dev, test, stage, prod</Title>
           </Property>
           <Property Name="UF_NetworkSegment">
               <Title>Сегмент сети LAN, DMZ</Title>
           </Property>
           <Property Name="UF_Countour">
               <Title>Контур</Title>
           </Property>
           <Property Name="UF_AssetRevisionDate">
               <Title>Дата последней ревизии актива</Title>
           </Property>
       </Properties>
   </Entity>
   ```

   Описание пользовательских полей добавлено.

Вы можете изменять значения элементов `Title` без изменения значения атрибута `version` для элемента `layer id="UserDescriptions"`.

20.3. Изменение имен пользовательских полей

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла `UserModel.xml` не игнорируется регистр символов.

- Чтобы изменить имена пользовательских полей:

1. В файле `UserModel.xml` в качестве значения атрибута `version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели. Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.3"`).
2. Для элемента `layer id="UserModel"` → `Dsl` → `Migrations` добавьте дочерний элемент `Group` с атрибутом `Version`. В качестве значения атрибута `Version` укажите версию пользовательской модели, например:
   ```
   <Group Version="19.0.20206.3">
   </Group>
   ```
3. Для элемента `Group` добавьте дочерний элемент `ChangeEntity` с атрибутом `Type`. В качестве значения атрибута `Type` укажите `Core.Host`:
   ```
   <ChangeEntity Type="Core.Host">
   </ChangeEntity>
   ```
4. Для элемента `ChangeEntity` добавьте дочерние элементы `RenameProperty` (по количеству изменяемых пользовательских полей) с атрибутами `Property` и `NewName`. В качестве значения атрибута `Property` укажите старое имя поля, значения атрибута `NewName` — новое имя поля.

   Примечание. Имена полей должны начинаться с префикса `UF_`.

   Например:
   ```
   <Group Version="19.0.20206.3">
       <ChangeEntity Type="Core.Host">
           <RenameProperty Property="UF_AssetNamber" NewName="UF_AssetNumber"/>
           <RenameProperty Property="UF_AssetOuner" NewName="UF_AssetOwner"/>
       </ChangeEntity>
   </Group>
   ```
5. Перезапустите службы:
   ```
   docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|
   assets.compliancecontrol|assets-identity|assets.input|assets.groups|assets-projections|
   assets-scans|core.scanning|core-tables|core-topology|core-topology-analyzer/ {print $NF}')
   ```

Имена пользовательских полей изменены.

20.4. Удаление пользовательских полей из модели актива

Внимание! Имена элементов и атрибутов регистрозависимы, то есть при обработке файла `UserModel.xml` не игнорируется регистр символов.

- Чтобы удалить пользовательские поля из модели актива:

  1. В файле `UserModel.xml` в качестве значения атрибута `version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели. Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.4"`).
  2. Для элемента `layer id="UserModel"` → `Dsl` → `Migrations` добавьте дочерний элемент `Group` с атрибутом `Version`. В качестве значения атрибута `Version` укажите версию пользовательской модели, например:

     ```
     <Group Version="19.0.20206.4">
     </Group>
     ```
  3. Для элемента `Group` добавьте дочерний элемент `ChangeEntity` с атрибутом `Type`. В качестве значения атрибута `Type` укажите `Core.Host`:

     ```
     <ChangeEntity Type="Core.Host">
     </ChangeEntity>
     ```
  4. Для элемента `ChangeEntity` добавьте дочерние элементы `RemoveProperty` (по количеству удаляемых пользовательских полей) с атрибутом `Property`. В качестве значения атрибута `Property` укажите имя удаляемого поля.

     Например:

     ```
     <Group Version="19.0.20206.4">
         <ChangeEntity Type="Core.Host">
             <RemoveProperty Property="UF_AssetNumber"/>
             <RemoveProperty Property="UF_AssetOwner"/>
         </ChangeEntity>
     </Group>
     ```
  5. Перезапустите службы:

     ```
     docker restart $(docker ps | awk '/assets-processing|assets-temporalreadmodel|
     assets.compliancecontrol|assets-identity|assets.input|assets.groups|assets-projections|
     assets-scans|core.scanning|core-tables|core-topology|core-topology-analyzer/ {print $NF}')
     ```

  Пользовательские поля удалены из модели актива.

21. Работа с инфраструктурами

При сканировании IT-инфраструктуры предприятия важно 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 оператору поиск необходимого актива.

При наличии в составе площадки таких сегментов сети рекомендуется для каждого из них создать в MaxPatrol VM отдельную инфраструктуру и сканировать такие инфраструктуры одним коллектором по отдельности.

После развертывания система имеет одну инфраструктуру **Инфраструктура по умолчанию**. Вы можете создавать другие инфраструктуры, изменять их названия и удалять их на странице **Сбор данных** → **Инфраструктура**.

В этом разделе

21.1. Создание инфраструктуры

- Чтобы создать инфраструктуру:

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

     Откроется страница **Инфраструктура**.
  2. В панели инструментов нажмите кнопку **Добавить инфраструктуру**.

     Откроется страница **Создание инфраструктуры**.
  3. Введите название инфраструктуры.
  4. Нажмите кнопку **Создать**.

  Инфраструктура создана.

21.2. Изменение названия инфраструктуры

- Чтобы изменить название инфраструктуры:

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

     Откроется страница **Инфраструктура**.
  2. В панели инструментов нажмите кнопку **Редактировать**.

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

3. Измените название инфраструктуры.
4. Нажмите кнопку **Сохранить**.

Название инфраструктуры изменено.

21.3. Удаление инфраструктуры

- Чтобы удалить инфраструктуру:

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

   Откроется страница **Инфраструктура**.
2. В списке инфраструктур выберите инфраструктуру, которую необходимо удалить.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

   Примечание. Если к удаляемой инфраструктуре привязаны активы, они тоже будут удалены. Задачи, собиравшие данные с активов удаленной инфраструктуры, не будут автоматически остановлены, их необходимо остановить вручную.

Инфраструктура удалена.

22. Изменение проверок по чек-листу

- Чтобы изменить проверки на Linux:

  1. На сервере MP 10 Core в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/config/usagemonitoring` создайте копию файла `check_settings.default.yaml` — файл `check_settings.yaml`.
  2. В файле `check_settings.yaml` измените необходимые параметры (см. приложение B).
  3. Перезапустите контейнер core-usage-monitoring:

     ```
     docker restart $(docker ps | awk '/core-usage-monitoring/ {print $NF}')
     ```

  Проверки изменены.

См. также

Параметры проверок по чек-листу (см. приложение B)

23. Диагностика и решение проблем

В MaxPatrol VM реализован автоматический мониторинг параметров жизнеспособности и целостности системы и ее компонентов. Источником для мониторинга служат статистические данные за определенные периоды. Результаты мониторинга отображаются по нажатию индикатора состояния.

Предусмотрены следующие цветовые индикаторы уведомлений:

— синий — информирует о каком-либо событии, не связанном с ошибками в работе системы (например, об остановке служб);

— желтый — предупреждает о проблеме в работе системы или ее компонента (например, о приближении к пороговому значению наблюдаемого параметра) или уведомляет об инициализации компонента;

— красный — сигнализирует об ошибке в работе системы или ее компонента (например, о том, что компонент недоступен).

В этом разделе приводятся инструкции по диагностике и решению проблем и устранению ошибок, возникающих при работе с MaxPatrol VM. Шаги инструкций необходимо выполнять в порядке их перечисления. После того как один из шагов инструкции привел к решению проблемы или устранению ошибки, выполнять следующие за ним шаги не нужно.

В этом разделе

23.1. Вход в RabbitMQ

Перед входом в RabbitMQ необходимо убедиться, что правила межсетевого экрана разрешают входящее соединение от рабочей станции администратора к серверу RabbitMQ через порт 15672/TCP.

- Чтобы войти в RabbitMQ:

  1. В адресной строке браузера введите:
     `http://<IP-адрес или FQDN сервера RabbitMQ>:15672`

     Откроется страница входа в RabbitMQ.
  2. Введите логин `siem` и пароль.

     Примечание. По умолчанию пароль служебной учетной записи — `P@ssw0rd`.
  3. Нажмите кнопку **Login**.

     Отобразится страница **Overview**.

  Вход в RabbitMQ выполнен.

23.2. Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога»

Перед появлением ошибки система отображает предупреждение «Заканчивается свободное место на диске, выделенном для Core Messaging Service».

Возможные причины

Причиной ошибки является уменьшение свободного места на логическом диске, занимаемом виртуальным узлом RabbitMQ.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что аппаратные характеристики сервера MP 10 Core соответствуют минимальным требованиям к конфигурации.
  2. Определите, на какой логический диск установлен RabbitMQ.

     ```
     df -h /var/lib/deployed-roles/mp10-application/rmqmessagebus/
     ```

     Консоль отобразит информацию о диске, на который установлен RabbitMQ.
  3. Убедитесь, что этот логический диск занят только файлами, необходимыми для работы ОС и MaxPatrol VM. Если диск содержит другие файлы и каталоги, удалите их.
  4. Перезапустите службу Core Health Monitoring.

Если проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файл журнала службы Core Health Monitoring;

— снимок экрана, отображающий свободное место на логическом диске.

23.3. Задача аудита не собирает сведения об активах

Возможные причины

Возможными причинами проблемы являются сбор сведений от неподдерживаемых источников, отсутствие необходимых для сканирования инфраструктуры прав, а также ошибки в работе модуля аудита.

Решение

- Чтобы решить проблему:

  1. Проверьте, что версия сканируемого источника данных поддерживается системой (см. Руководство по настройке источников). Если источник не поддерживается, система не сможет получать от него данные.
  2. Убедитесь, что учетная запись для аудита имеет необходимые права доступа к источнику (см. Руководство по настройке источников).

Если проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файлы журналов задачи аудита, собранные с уровнем журналирования debug;

— название и версию источника;

— снимки экрана с данными о правах доступа и привилегиях учетной записи, используемой для аудита.

23.4. Не приходят уведомления, отправляемые по электронной почте

- Чтобы решить проблему:

  1. Откройте файлы журналов `Notifications.log` и `Triggers.log`, расположенные на серверах PT MC и MP 10 Core соответственно.
  2. Если журналы содержат сообщения об ошибках (например, `Can't send email to <Адрес электронной почты>. Reason: Failure sending mail.; Unable to connect to the remote server; No connection could be made because the target machine actively refused it`), убедитесь, что значения параметров `SmtpHost, SmtpPort, SmtpUser` и `SmtpPassword` роли Core соответствуют значениям параметров для подключения к серверу электронной почты.
  3. Если журналы содержат сообщения об отправке (например, `Email ["Название задачи"] "Название события" was sent to "Адрес электронной почты"`), обратитесь к системному администратору предприятия для проверки параметров сервера электронной почты и просмотра его журналов на наличие ошибок.

23.5. Расположение файлов журналов

Для анализа возникшей проблемы службе технической поддержки могут потребоваться файлы журналов. Для сбора файлов необходимо их скопировать, создать из скопированных файлов архив (со сжатием) и отправить его в службу технической поддержки.

Таблица 5. Расположение файлов журналов компонентов на Linux

Компонент	**Путь к файлам**
MP 10 Core, PT MC, MP 10 Collector	Файлы журналов MP 10 Core и PT MC находятся в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/log`, а файл журнала MP 10 Collector — в каталоге `/var/log/core-agent`. Журнал установки находится в файле `<Каталог со сценарием установки install.sh>/install_<Название роли>_<Номер версии>.log`
RabbitMQ	Файлы журналов находятся в каталоге `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли RMQ Message Bus>/log`, журнал установки — в файле `<Каталог со сценарием установки install.sh>/install_RmqMessagebus_<Номер версии>.log`
СУБД PostgreSQL	Файлы журналов находятся в каталоге `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли SqlStorage>/log`, журнал установки — в файле: `<Каталог со сценарием установки install.sh>/install_<Название роли>_<Номер версии>.log`

23.6. Настройка компонентов после изменения IP-адресов или FQDN их серверов

Для взаимодействия между собой компоненты системы используют IP-адреса или FQDN серверов, на которых они установлены. Эти сетевые параметры указываются администратором при установке компонента и сохраняются в его конфигурации. Если во время работы системы IP-адрес или FQDN сервера изменился, взаимодействие между компонентами нарушится, поскольку в конфигурации компонента будет храниться прежнее значение параметра. Для восстановления взаимодействия необходимо в качестве значений параметров компонентов указать актуальные IP-адреса или FQDN серверов.

> **Внимание!** После указания новых IP-адресов или FQDN серверов в параметрах компонентов необходимо деактивировать PT MC по инструкции (см. раздел 23.11).

Если был изменен IP-адрес или FQDN сервера, на котором установлена роль Deployer, на сервере каждого Salt Minion в файле `/etc/salt/minion.d/deployer.conf` необходимо указать в качестве значения параметра `master` актуальный IP-адрес или FQDN сервера с ролью Deployer и выполнить команду `systemctl restart salt-minion`.

> **Внимание!** Использование сценария `deploy_minion.sh` или утилиты `deploy_minion.ps1` для изменения конфигурации Salt Minion сделает работу MaxPatrol VM невозможной и потребует переустановки всей системы.

Если был изменен IP-адрес или FQDN сервера компонентов MP 10 Core и PT MC необходимо указать актуальные значения следующих параметров:

- `HostAddress` и `MCAddress` компонента MP 10 Core;
- `HostAddress` компонента PT MC;
- `RMQHost` компонента MP 10 Collector, установленного для отдельного сегмента сети.

> **Внимание!** Если компоненты MaxPatrol VM развернуты на нескольких площадках, перед сменой IP-адресов необходимо разорвать связи между площадками. После смены IP-адресов связи можно восстановить.

23.7. Подсеть Docker-контейнера MaxPatrol VM совпадает с одной из подсетей предприятия

Решение

Необходимо изменить подсеть Docker-контейнера MaxPatrol VM.

Команды из инструкции необходимо выполнять в интерфейсе терминала Linux.

► Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol VM остановите Docker-контейнеры:
   `docker stop $(docker ps -qa)`
2. На всех серверах с установленным MaxPatrol VM удалите Docker-контейнеры:
   `docker rm $(docker ps -qa)`
3. На всех серверах с установленным MaxPatrol VM удалите действующие параметры сети Docker:
   `docker network prune`
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz`:
   `tar -xf pt_deployer_<Номер версии>.tar.gz`
5. На сервере с установленной ролью Deployer запустите сценарий:
   `pt_deployer_<Номер версии>/install.sh`
6. В открывшемся окне нажмите кнопку **Yes**.
7. Выберите вариант с идентификатором приложения роли.
8. Выберите вариант с идентификатором экземпляра роли.

   Откроется окно для выбора набора параметров.
9. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение Б).
10. В качестве значения параметра `CustomDockerAddressPool` укажите подсеть для Docker-контейнеров MaxPatrol VM, отличную от подсетей, используемых в вашей организации.

    Внимание! Значение параметра должно содержать адрес подсети с маской /21 или шире (например, /20, /19 или /18) в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Например: 10.1.16.0/20 или 172.19.64.0/20.
11. В качестве значения параметра `CustomDockerNetworkSize` введите размер подсетей, которые будут выделяться из диапазона, указанного в параметре `CustomDockerAddressPool`.

    Примечание. Рекомендуется использовать значение, не превышающее 25 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра `CustomDockerAddressPool`, минимум на 4 бита.
12. Нажмите кнопку **OK**.
13. Нажмите **Submit**.

    Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
14. Нажмите кнопку **OK**.

15. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
16. На сервере с установленной ролью Deployer запустите обновление конфигурации установленных компонентов MaxPatrol VM:
    ```
    deployer instance reconfigure '*' -Verbose
    ```

Подсеть Docker-контейнера изменена.

Вы можете проверить изменение подсети Docker-контейнера, выполнив команды вывода информации о сетевых интерфейсах:

```
ip r
ip a | grep docker
iptables -L
```

Изменение подсети Docker-контейнера при обновлении компонентов

Возможна ситуация, когда изменить подсеть Docker-контейнера MaxPatrol VM необходимо во время обновления компонентов MaxPatrol VM. В этом случае необходимо воспользоваться инструкцией, приведенной ниже.

- Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol VM остановите Docker-контейнеры:
   ```
   docker stop $(docker ps -qa)
   ```
2. На всех серверах с установленным MaxPatrol VM удалите Docker-контейнеры:
   ```
   docker rm $(docker ps -qa)
   ```
3. На всех серверах с установленным MaxPatrol VM удалите действующие параметры сети Docker:
   ```
   docker network prune
   ```
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz` с новой версией роли:
   ```
   tar -xf pt_deployer_<Номер версии>.tar.gz
   ```
5. Запустите сценарий:
   ```
   pt_deployer_<Номер версии>/install.sh
   ```
6. В открывшемся окне нажмите кнопку **Yes**.

   Начнется распаковка и подготовка пакетов. По завершении подготовки откроется окно для проверки и изменения параметров обновления.
7. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение Б).
8. Убедитесь, что в качестве значения параметра `HostAddress` указан IP-адрес или FQDN сервера, на который установлена роль Deployer.

9. В качестве значения параметра `CustomDockerAddressPool` укажите подсеть для Docker-контейнеров MaxPatrol VM, отличную от подсетей, используемых в вашей организации.

   Внимание! Значение параметра должно содержать адрес подсети с маской /21 или шире (например, /20, /19 или /18) в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Например: 10.1.16.0/20 или 172.19.64.0/20.

10. В качестве значения параметра `CustomDockerNetworkSize` введите размер подсетей, которые будут выделяться из диапазона, указанного в параметре `CustomDockerAddressPool`.

    Примечание. Рекомендуется использовать значение, не превышающее 25 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра `CustomDockerAddressPool`, минимум на 4 бита.

11. Нажмите кнопку **OK**.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.

12. Нажмите кнопку **OK**.

13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

14. Обновите остальные роли согласно инструкциям в Руководстве по внедрению.

Подсеть Docker-контейнера изменена.

Вы можете проверить изменение подсети Docker-контейнера, выполнив команды вывода информации о сетевых интерфейсах:

```
ip r
ip a | grep docker
iptables -L
```

23.8. Не удается получить обновления с сервера Positive Technologies

Проблема

Не удается получить пакеты с обновлениями экспертных данных с сервера Positive Technologies.

Возможные причины

Возможными причинами проблемы являются ошибки в работе компонента PT MC или локального сервера обновлений, неправильная настройка этих компонентов, а также недоступность сервера Positive Technologies.

Решение

Для решения проблемы рекомендуется обратиться в службу технической поддержки Positive Technologies. До решения проблемы вы можете получать актуальные пакеты обновлений у специалистов службы технической поддержки и вручную добавлять их в MaxPatrol VM.

- Чтобы добавить пакет обновлений в систему:

  1. Извлеките файлы пакетов обновлений из архива, полученного от службы технической поддержки.

     Примечание. Файлы пакетов обновлений имеют расширение `.pkg`.

  2. Скопируйте файлы пакетов обновлений в каталог `/var/lib/deployed-roles/mc-application/managementandconfiguration/data/resources/local-packages/` на сервере с ролью Management and Configuration.

     Система автоматически установит пакеты обновлений из каталога `local-packages`.

Вы можете найти информацию об установленных пакетах обновлений на странице **Система** → **Управление системой** → **База уязвимостей**.

23.9. Ошибка при установке, переконфигурации или обновлении компонентов в высоконагруженных системах

Проблема

При установке, переконфигурации или обновлении компонентов в высоконагруженных системах появляется ошибка с кодом 137 (например, `Kill process '<Название операции>' on timeout WARNING: Process '<Название операции>' (args: '<Аргументы операции>') (pid:<Идентификатор процесса>) did not complete within 2400 sec. VERBOSE: Exit code: 137`).

Возможные причины

Возможной причиной проблемы является неуспешная попытка выполнения сервисной операции за установленный в MaxPatrol VM тайм-аут.

Решение

Вы можете увеличить тайм-аут выполнения сервисных операций.

- Чтобы изменить тайм-аут:

  1. На сервере с установленной ролью Deployer откройте файл `/etc/opt/deployer/deployer.yaml`.
  2. Измените значения параметров `SaltTimeoutSec` и `WaitTimeoutSec` (в секундах).

23.10. Экспорт и импорт пользовательских профилей

Вы можете экспортировать и импортировать пользовательские профили, а также справочники и учетные записи, относящиеся к этим профилям, с помощью скрипта unitmigrator.

Для запуска скрипта необходимы следующие конфигурационные файлы:

— `enabled_profiles.yaml` — содержит список профилей, которые необходимо экспортировать (импортировать);

— `hosts` — содержит параметры подключения к узлу, с которого необходимо экспортировать (или на который импортировать) профили.

Перед первым запуском скрипта необходимо создать файлы `enabled_profiles.yaml` и `hosts` в каталоге `/var/lib/deployed-roles/mp10-application/core/data/unitmigrator/config/` на сервере с MP 10 Core.

Приведенные ниже инструкции необходимо выполнять на сервере компонента MP 10 Core.

Экспорт профилей

► Чтобы экспортировать пользовательские профили:

1. В конфигурационный файл `enabled_profiles.yaml` добавьте строки с названиями профилей, которые необходимо экспортировать:

   ```
   - "<Название профиля 1>"
   - "<Название профиля 2>"
   ...
   - "<Название профиля N>"
   ```

   Примечание. Для экспорта всех профилей конфигурационный файл `enabled_profiles.yaml` необходимо оставить пустым.

2. В конфигурационный файл `hosts` добавьте строки с параметрами подключения к узлу, с которого необходимо экспортировать профили:

   ```
   [export]
   <IP-адрес или FQDN сервера MP 10 Core> ansible_user=<Логин> ansible_password=<Пароль>
   ```

3. Перейдите в каталог `core.unitmigrator`:

   ```
   cd /var/lib/deployed-roles/mp10-application/core/images/core.unitmigrator
   ```

4. Запустите скрипт с помощью команды:

   ```
   docker-compose run --rm core.unitmigrator export
   ```

   Начнется процесс экспорта профилей, по завершению которого в каталоге `/var/lib/deployed-roles/mp10-application/core/data/unitmigrator/export/` появится JSON-файл с названием вида `Профили_<Дата начала экспорта>.json`.

JSON-файл с результатами экспорта содержит следующие объекты:

— `hash` — хеш-сумма файла без учета пробелов;

— `microservice_version` — версия микросервиса, из которого экспортировались профили;

— `scanning_api_version` — версия API (ресурса), из которого экспортировались профили;

— `dictionaries_api_version` — версия API (ресурса), из которого экспортировались справочники;

— `credentials_api_version` — версия API (ресурса), из которого экспортировались учетные записи;

— `profiles` — список экспортируемых профилей;

— `dictionaries` — список пользовательских справочников, которые относятся к экспортируемым профилям;

— `credentials` — список учетных записей, которые относятся к экспортируемым профилям.

Импорт профилей

► Чтобы импортировать пользовательские профили:

1. В конфигурационный файл `enabled_profiles.yaml` добавьте строки с названиями профилей, которые необходимо импортировать:

   ```
   - "<Название профиля 1>"
   - "<Название профиля 2>"
   ...
   - "<Название профиля N>"
   ```

   Примечание. Для импорта всех профилей конфигурационный файл `enabled_profiles.yaml` необходимо оставить пустым.

2. В конфигурационный файл `hosts` добавьте строки с параметрами подключения к узлу, на который необходимо импортировать профили:

   ```
   [import]
   < IP-адрес или FQDN сервера MP 10 Core> ansible_user=<Логин> ansible_password=<Пароль>
   ```

3. Скопируйте в каталог `/var/lib/deployed-roles/mp10-application/core/data/unitmigrator/import/` JSON-файл, полученный при экспорте профилей.

4. Перейдите в каталог `core.unitmigrator`:

   ```
   cd /var/lib/deployed-roles/mp10-application/core/images/core.unitmigrator
   ```

5. Запустите скрипт с помощью команды с параметрами импорта:

   ```
   docker-compose run --rm core.unitmigrator import "profiles_strategy=<Значение>
   dictionaries_strategy=<Значение> credentials_strategy=<Значение> importable_file_name=<Имя
   файла с профилями>"
   ```

Например:

```
docker-compose run --rm core.unitmigrator import "profiles_strategy=Update
dictionaries_strategy= Update credentials_strategy=CreateNew
importable_file_name=Профили_2023-12-18-18-39-57Z.json"
```

Примечание. Описание и допустимые значения параметров `profiles_strategy`, `dictionaries_strategy`, `credentials_strategy` и `importable_file_name` приведены в таблице ниже.

Профили импортированы.

Журналы скрипта хранятся в каталоге `/var/lib/deployed-roles/mp10-application/core/log/unitmigrator/`.

Таблица 6. Параметры запуска скрипта при импорте профилей

Параметр	Описание	Значение по умолчанию
`profiles_strategy`	Действие скрипта при совпадении импортируемого профиля с существующим в системе. Допустимые значения: `CreateNew` — импортировать профиль как копию с уникальным именем; `Update` — заменить существующий профиль импортируемым; `Abort` — не импортировать профиль и сохранить существующий. Необязательный параметр. Если параметр не указан, скрипт использует значение по умолчанию	`CreateNew`
`dictionaries_strategy`	Действие скрипта при совпадении импортируемого справочника с существующим в системе. Допустимые значения: `CreateNew` — импортировать справочник как копию с уникальным именем; `Update` — заменить существующий справочник импортируемым; `Abort` — не импортировать справочник и сохранить существующий. Необязательный параметр. Если параметр не указан, скрипт использует значение по умолчанию	`CreateNew`

Параметр	Описание	Значение по умолчанию
`credentials_strategy`	Действие скрипта при совпадении импортируемой учетной записи с существующей в системе. Допустимые значения: `CreateNew` — импортировать учетную запись как копию с уникальным именем; `Abort` — не импортировать учетную запись и сохранить существующую. Необязательный параметр. Если параметр не указан, скрипт использует значение по умолчанию	`Abort`
`importable_file_name`	Название JSON-файла с импортируемыми профилями. Обязательный параметр	—

23.11. Деактивация PT MC

Чтобы деактивировать PT MC с помощью сценария,

на сервере с установленной ролью Management and Configuration запустите сценарий деактивации:

```
/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли Management and Configuration>/tools/clear-activation.sh
```

Например:

```
/var/lib/deployed-roles/mc-app/managementandconfiguration-1/tools/clear-activation.sh
```

Если для PT MC была выполнена деактивация с помощью сценария, при повторной активации PT MC может потребоваться повторная регистрация (см. раздел 23.12) MaxPatrol VM в системе лицензирования.

Внимание! Если при повторной активации в PT MC отображается сообщение «Ваш ключ инсталляции активирован слишком много раз», обратитесь в службу технической поддержки.

23.12. Повторная регистрация MaxPatrol VM в системе лицензирования

При повторной активации PT MC может потребоваться повторная регистрация MaxPatrol VM в системе лицензирования в случае, если ранее для PT MC была выполнена деактивация (см. раздел 23.11) с помощью сценария.

- Чтобы повторно зарегистрировать MaxPatrol VM в системе лицензирования:

  1. На сервере с установленной ролью Management and Configuration выполните команду:

     ```
     docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}') psql -U
     pt_system -d core_application_registration -c "UPDATE public.
     \"ApplicationRegistrationRecords\" SET \"Value\"=md5(random()::text) WHERE
     \"Id\"='RegistrationHash' OR \"Id\"='ClientDataHash';"
     ```

  2. Перезапустите контейнер:

     ```
     docker restart $(docker ps -aqf name=core.deployment.configuration)
     ```

23.13. Задача на сбор данных с коллектором на Windows завершается с ошибкой

Журнал выбранной подзадачи содержит следующую информацию об ошибке:

```
ERROR Agent.JobService: Failed to start module! Descr: Can't start process!
 [Nested error] = Can't start child process
  [Nested error] = CreateProcess failed: The system cannot find the file specified.
```

Возможные причины

Возможной причиной проблемы является то, что запускаемый файл процесса ModuleHost.exe помещен в карантин антивирусной программой Microsoft Defender.

Решение

- Чтобы решить проблему,

  восстановите файл из карантина.

Подробную инструкцию см. на сайте learn.microsoft.com в разделе «Восстановление файлов в карантине в антивирусной программе Microsoft Defender».

23.14. На коллекторах, установленных на Linux, задачи на сбор данных с профилем Microsoft Active Directory завершаются ошибкой

Проблема

Задача на сбор данных с Windows XP или Windows Server 2003 с профилем Microsoft Active Directory Audit для коллектора, установленного на Linux, завершается ошибкой.

Возможные причины

Для аутентификации на активе с помощью протокола Kerberos используется библиотека MIT Kerberos версии 1.18 или выше, которая содержит ошибку, приводящую к невозможности аутентификации.

Решение

Необходимо установить пакет libkrb5-3 с библиотекой MIT Kerberos версии ниже 1.18 или пакет libkrb5-26-heimdal с библиотекой Heimdal Kerberos, которые вы можете скачать на сайте debian.org.

- Чтобы решить проблему:

  1. Удалите пакет с библиотекой Kerberos, установленный в системе.

     Внимание! При удалении пакета система предложит удалить коллектор. Необходимо отклонить это действие.

  2. Установите пакет libkrb5-3 или libkrb5-26-heimdal.
  3. Откройте на редактирование файл `/etc/krb5.conf`.
  4. В блоке параметров `libdefaults` замените строки, которые ограничивают допустимые алгоритмы шифрования и подписи:

     - Если вы установили библиотеку MIT Kerberos:

       ```
       default_tgs_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 rc4-hmac
       default_tkt_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 rc4-hmac
       permitted_enctypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 rc4-hmac
       ```

- Если вы установили библиотеку Heimdal Kerberos:

```
default_etypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 rc4-hmac
default_tgs_etypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 rc4-hmac
default_as_etypes = aes256-cts-hmac-sha1-96 aes128-cts-hmac-sha1-96 aes128-cts-hmac-sha256-128 rc4-hmac
```

5. Сохраните изменения в файле `krb5.conf`.

23.15. Большое количество запросов к DNS-серверу от Docker-контейнеров сервера MP 10 Core

Проблема

Повышение нагрузки на DNS-сервер из-за большого количества запросов от Docker-контейнеров сервера MP 10 Core.

Решение

Необходимо внести изменения в конфигурационный файл `/var/lib/deployer/role_packages/docker/docker-compose.common.yaml` на сервере с установленной ролью Deployer. Перед выполнением инструкции рекомендуется создать резервную копию файла.

► Чтобы решить проблему:

1. Откройте файл `/var/lib/deployer/role_packages/docker/docker-compose.common.yaml`.
2. Раскомментируйте строки:

```
#    extra_hosts:
#      - "fqdn:ip"
```

3. Вместо элемента `fqdn:ip` добавьте строки для всех серверов инсталляции в формате <FQDN сервера>:<IP-адрес сервера>.

   Внимание! При редактировании файла необходимо соблюдать синтаксис языка YAML.

   Например:

```
    extra_hosts:
      - "core.test.example:10.10.10.10"
      - "siem.test.example:10.10.10.120"
```

4. Запустите обновление конфигураций установленных компонентов MaxPatrol VM:

```
deployer instance reconfigure '*'
```

В результате выполнения команды в конфигурационные файлы `docker-compose.common.yaml` всех ролей будет добавлена информация о серверах инсталляции.

Внимание! После обновления роли Deployer потребуется заново внести изменения в файл.

23.16. Установка модуля Salt Minion завершается с ошибкой

Решение

- Чтобы решить проблему:

  1. На сервере с установленной ролью Deployer перейдите в каталог `/opt/deployer/bin/`:
     ```
     cd /opt/deployer/bin/
     ```
  2. Запустите утилиту Get-MinionDistrib.ps1:
     ```
     /opt/deployer/bin/Get-MinionDistrib.ps1
     ```
  3. Укажите IP-адрес или FQDN сервера, на который необходимо установить модуль Salt Minion.
  4. Выберите одну или несколько операционных систем, на которые необходимо установить модуль, и нажмите **Select**.

     По завершении работы утилиты в каталоге появится архив `minion_dist_<IP-адрес или FQDN сервера, на который необходимо установить модуль Salt Minion>_<версия роли Deployer>.gz`.
  5. Скопируйте архив на сервер, на котором необходимо установить модуль Salt Minion.
  6. Распакуйте архив:
     ```
     tar -xf minion_dist_<IP-адрес или FQDN сервера, на который необходимо установить модуль Salt Minion>_<версия роли Deployer>.gz
     ```
  7. Запустите сценарий:
     ```
     minion_dist_< IP-адрес или FQDN сервера, на который необходимо установить модуль Salt Minion>_<версия роли Deployer>/install.sh
     ```
  8. На сервере с установленной ролью Deployer выполните команду:
     ```
     salt-key -A
     ```
  9. В строке `Proceed? [n/Y]` введите `y` и нажмите **Enter**.

23.17. Расположение пользовательских сертификатов

При резервном копировании и восстановлении данных вам может потребоваться найти файлы пользовательских сертификатов.

Для этого необходимо отобразить список параметров для всех установленных ролей.

- Чтобы отобразить параметры ролей,

  на сервере с установленной ролью Deployer выполните команду:
  ```
  deployer params get
  ```

В полученном списке параметров требуется найти разделы с заголовком `UserDefined` для каждой роли. Если в разделах есть файлы с расширениями `.key`, `.pem` или `.crt`, это файлы пользовательских сертификатов.

> **Примечание.** Список параметров роли может не содержать файлов пользовательских сертификатов, если пользовательские сертификаты для нее не создавались.

Сервер, на котором сохранен сертификат, указан в начале каждого из списков параметров в строке вида: `<Название роли> (<Название роли> <Версия системы>) on <Название сервера> params`.

Путь к найденным файлам сертификатов указан в подразделе `InstanceDefined` в значении параметра `CertificatesDir` каждой роли, для которой был добавлен сертификат. Например, для роли Core: `CertificatesDir=/var/lib/deployed-roles/mp10-application/core-1/certs`.

23.18. Ошибка при загрузке шаблона для экспорта записей в формате XLSX

Проблема

При загрузке шаблона для экспорта записей в формате XLSX появляется сообщение «Не удалось загрузить шаблон».

Возможные причины

Поле шаблона автоматически преобразовано в формулу средствами Microsoft Excel. Например, поле шаблона содержит символ `@`, из-за чего в него автоматически добавлена функция `HYPERLINK`.

Решение

- Чтобы решить проблему,

  проверьте поля шаблона: если поле содержит ненужную формулу, удалите ее.

23.19. Настройка мандатного контроля целостности для Astra Linux

Если MaxPatrol VM устанавливается на Astra Linux и включен мандатный контроль целостности (МКЦ), для учетной записи, которая используется при установке компонентов системы, необходим максимальный уровень целостности (63). Вы можете проверить, включен ли МКЦ, с помощью команды `astra-mic-control status`. Также вы можете просмотреть уровень МКЦ пользователя с помощью команды `sudo pdpl-user <Имя пользователя>`.

- Чтобы изменить уровень целостности,

  выполните команды:

  ```
  sudo gpasswd -a <Имя пользователя> astra-admin
  sudo pdpl-user <Имя пользователя> -i <Уровень целостности>
  ```

После установки MaxPatrol VM рекомендуется установить прежнее значение уровня целостности.

24. О технической поддержке

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

Предоставление доступа к обновленным версиям продукта

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

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

Восстановление работоспособности продукта

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

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

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

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

Рассмотрение предложений по доработке продукта

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

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

Портал технической поддержки

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

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

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

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

— номер лицензии на использование продукта;

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

— снимки экрана.

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

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

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

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

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

Время реакции и приоритизация заявок

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

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

Таблица 7. Время реакции на заявку

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

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

Обработка и закрытие заявок

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

— о ходе диагностики по заявленной проблеме и ее результатах;

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

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

Специалист закрывает заявку, если:

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

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

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

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

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

Приложение А. Привилегии и роли MaxPatrol VM

При изменении роли коды добавленных и удаленных привилегий отображаются на странице **Журнал действий пользователя** в приложении Management and Configuration.

Таблица 8. Привилегии и роли MaxPatrol VM

Код привилегии	Привилегия	Администратор	Оператор	Наблюдатель
Assets	**Активы**			
Vulners	Уязвимости	+	+	-
Assets	Создание, просмотр, изменение, удаление	+	+	-
AssetsRead	Просмотр	-	-	+
Common	**Общее**			
AccessAdmin	Расширенные полномочия	+	-	-
DataCollect	**Сбор данных**			
DataCollectTasks	Задачи			
DataCollectTasks	Создание, просмотр, изменение, удаление	+	+	-
DataCollectTasksRead	Просмотр	-	-	+
DataCollectProfiles	Профили			
DataCollectProfiles	Создание, просмотр, изменение, удаление	+	+	-
DataCollectProfilesRead	Просмотр	-	-	+
DataCollectIdentity	Учетные записи			
DataCollectIdentity	Создание, просмотр, изменение, удаление	+	+	-
DataCollectIdentityRead	Просмотр	-	-	+
DataCollectReferences	Справочники			
DataCollectReferences	Создание, просмотр, изменение, удаление	+	+	-
DataCollectReferencesRead	Просмотр	-	-	+
DataCollectExclusions	Исключения			

Код привилегии	Привилегия	Администратор	Оператор	Наблюдатель
DataCollectExclusionsViewing	Просмотр	-	-	+
DataCollectExclusionsEditing	Создание, просмотр, изменение, удаление	+	+	-
Infrastructure	Инфраструктура	+	-	-
System	**Система**			
AccessRights	Права доступа	+	-	-
Triggers	Уведомления	+	+	-
SystemManagement	Управление системой	+	+	-
ChecksManagement	Управление контролями	+	+	-
Reports	Отчеты	+	+	-
Topology	**Топология**			
TopologyAnalyzer	Расчет достижимости	+	+	-
Topology	Топология	+	+	-

Приложение Б. Параметры конфигурации компонентов MaxPatrol VM на Linux

В этом разделе приведены описания параметров и их значения по умолчанию.

Таблица 9. Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
`CertificateVendorEmail`	Адрес электронной почты вендора. **Примечание.** Этот параметр может быть изменен только при первой установке продукта	`pt@ptsecurity.com`
`CertificateVendorLocality`	Город, где располагается главный офис вендора. **Примечание.** Этот параметр может быть изменен только при первой установке продукта	`Moscow`
`CertificateVendorName`	Название вендора. **Примечание.** Этот параметр может быть изменен только при первой установке продукта	`Positive Technologies`
`CustomDockerAddressPool`	Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию. Рекомендуется использовать подсеть с маской /21 или шире в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	—

Параметр	Описание	Значение по умолчанию
CustomDockerNetworkSize	Размер подсетей, которые будут выделяться из диапазона, указанного в параметре CustomDockerAddressPool. Рекомендуется использовать значение, не превышающее 25 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра CustomDockerAddressPool, как минимум на 4 бит	—
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	—
Network	Сетевое имя реестра Docker-образов	registry-network
NetworkDriver	Драйвер Docker-образов	bridge
RegistryPort	Номер порта для доступа к локальному реестру Docker-образов	5000

Таблица 10. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorAgentHttpPort	Порт доступа к коллектору OpenTelemetry для роли SqlStorage по протоколу HTTP	4319
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	Адрес и порт сервера MP 10 Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)	False

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
`Network`	Сетевое имя реестра Docker-образов	`storage-network.sqlstorage`
`NetworkDriver`	Драйвер Docker-образов	`bridge`
`PgAdminPort`	Порт для доступа к pgAdmin	`9001`
`PgAnalyzeScaleFactor`	Доля от числа кортежей в таблице, которая прибавляется к значению параметра `PgAnalyzeThreshold` при расчете порога срабатывания команды ANALYZE. Например, если значение `PgAnalyzeThreshold` равно 200 000, а значение параметра `PgAnalyzeScaleFactor` равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет 200 000 + 100 000 = 300 000 кортежей	`0.0`
`PgAnalyzeThreshold`	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	`200000`
`PgChecksums`	Включение контрольных сумм на страницах данных СУБД PostgreSQL. Возможные значения: `auto`, `on`, `off`. Если выбрано значение `auto`, контрольные суммы при первичной установке роли SqlStorage включаются, а при обновлении или переустановке роли — остаются без изменений. **Примечание.** При обновлении или изменении конфигурации роли SqlStorage подсчет контрольных сумм может занять длительное время. До завершения процесса база данных не будет запущена и продолжение работы будет невозможно	`auto`
`PgEffectiveCacheSize`	Эффективный размер дискового кэша, доступный для одного запроса	`6GB`

Параметр	Описание	Значение по умолчанию
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения — HDD или SSD)	HDD
PgInitArgs	Параметры инициализации кластера PostgreSQL	--locale='en_US.UTF8'
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения — panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgMasterPasswordRequired	Запрос мастер-пароля для СУБД PostgreSQL включен (флажок установлен) или выключен (флажок снят)	Флажок снят
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgServerMode	Режим сервера для экземпляра СУБД PostgreSQL	Флажок снят
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgTimeZone	Часовой пояс для экземпляра СУБД PostgreSQL	Europe/Moscow
PgUpgradeJobs	Количество одновременных процессов или потоков, используемых для pg_upgrade	4
PgUpgradeVerbose	Детализированное ведение журнала для pg_upgrade включено (флажок установлен) или выключено (флажок снят)	Флажок снят
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system

Параметр	Описание	Значение по умолчанию
PgVacuumNapTime	Минимальная задержка между двумя запусками автоочистки для отдельной базы данных	20min
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key

Таблица 11. Параметры конфигурации роли LogConnector

Параметр	Описание	Значение по умолчанию
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	—
TelemetryCollectCron	Время начала ежедневного сбора телеметрии. По умолчанию — 04:00 в текущей временной зоне	0 0 4 * * ? *
TelemetryConnectAuthority	FQDN сервера MaxPatrol VM с указанием порта	—
TelemetryCronScheduleEnabled	Данные телеметрии отправляются (True) или не отправляются (False) на сервер приема телеметрии	True
TelemetryExportDataPath	Путь к каталогу для экспорта данных телеметрии	/tmp/telemetry/files
TelemetryTrackerDataPath	Путь к каталогу для отправки данных телеметрии	./observability/telemetry/files
TelemetryType	Типы собираемых данных телеметрии	CFG, API, STATE, UAL

Таблица 12. Параметры конфигурации роли Observability

Параметр	Описание	Значение по умолчанию
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorServerHttpPort	Порт для доступа к серверу сбора журналов по протоколу HTTP	4318
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	Адрес и порт сервера компонента MP 10 Core
ExportEnabledFrom	Разрешенное начальное время отправки телеметрии	04:00:00
ExportEnabledTo	Разрешенное конечное время отправки телеметрии	05:00:00
FlusUri	Адрес сервера приема телеметрии	—
GrafanaAdminLogin	Логин служебной учетной записи для подключения к интерфейсу Grafana	admin
GrafanaAdminPassword	Пароль служебной учетной записи для подключения к интерфейсу Grafana	P@ssw0rd
GrafanaServerHttpPort	Порт для доступа к интерфейсу Grafana по протоколу HTTP	9002
GrafanaServerSubUri	Путь для подключения к серверу Grafana	grafana
HostAddress	IP-адрес или FQDN сервера с установленной ролью Observability	—
JobExecutingInterval	Интервал запуска работ внутри сервиса Telemetry.Tracker	00:05:00
MetricsHttpPort	Порт для доступа к метрическим данным	8428
MetricsPassword	Пароль для доступа к метрическим данным	P@ssw0rd
MetricsRetention	Время сохранения метрических данных в базе данных	90d

Параметр	Описание	Значение по умолчанию
MetricsUser	Логин для доступа к метрическим данным	admin
Network	Сетевое имя реестра Docker-образов	observability.network.observability
NetworkDriver	Драйвер Docker-образов	bridge
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	—
PostgrePassword	Пароль служебной учетной записи для доступа к серверу СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432
PostgreUserName	Логин служебной учетной записи для доступа к серверу СУБД PostgreSQL	pt_system
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	—
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	—
TelemetryFileSize	Максимальный размер файла телеметрии в мегабайтах	50
TelemetryPackSize	Максимальный размер архива в мегабайтах, который можно отправить на сервер приема телеметрии	35
TimeZone	Используемый часовой пояс	Europe/Moscow

Таблица 13. Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
`ActionLogBatchSize`	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service единовременно отправляет службе MC User Action Logging Service	`100`
`ActionLogMillisecondsDelay`	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	`1000`
`ExpertDataUpdateMethod`	Метод получения обновлений экспертных данных. Возможные значения: `Online` или `Offline`	—
`PackageManagementPort`	Номер порта сервиса управления пакетами Package Management	`8585`
`PackagesSourceCredentialToken`	Токен для авторизации на сервере обновлений. Хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64	—
`PackagesSourceUri`	Адрес сервера обновлений	—
`UseProxy`	Использовать ли прокси-сервер для онлайн-активации	`false`
`ShowDiffObjectId`	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят

Таблица 14. Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
`AssetGridValidTimePeriodIndexFormat`	Режим оптимизации выполнения PDQL-запросов для высоконагруженных систем: `IdAndPeriod` (по умолчанию) —максимальное повышение производительности; `PeriodOnly` — среднее повышение производительности	`IdAndPeriod`
`AssetGridVersionRangeModeEnabled`	Режим оптимизации выполнения PDQL-запросов для высоконагруженных систем включен (флажок установлен) или выключен (флажок снят)	Флажок снят
`ConsiderEventsImportance`	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят)	Флажок установлен
`ContentDeployerPort`	Номер порта сервиса установки обновлений экспертизы Content Deployer	`8586`
`DefaultAssetTtl`	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	`90.00:00:00`
`DefaultLocale`	Интерфейс MaxPatrol VM отображается на русском (`ru-RU`) или английском (`en-US`) языке	`ru-RU`
`EmailNotificationRetryCount`	Максимальное количество попыток отправки сообщения на SMTP-сервер	`10`
`EmailNotificationRetryPeriodSeconds`	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	`60`
`HistoryRotationCronSchedule`	Периодичность запуска ротации с помощью планировщика заданий cron	`0 0 2 1 *`

Параметр	Описание	Значение по умолчанию
HistoryRotationDepth	Период истории изменения активов, данные за который необходимо удалять, в формате <Дни>.<Часы>:<Минуты>:<Секунды>. Минимально допустимое значение — 14 дней (14.00:00:00)	365.00:00:00
HistoryRotationEnabled	Автоматическая ротация истории изменения активов включена (флажок установлен) или выключена (флажок снят)	Флажок снят
HostAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
KBAddress	IP-адрес или FQDN сервера Knowledge Base	—
MaxScanSizeKb	Максимальный размер собранных данных по активам в килобайтах	716800
MCAddress	IP-адрес или FQDN сервера PT MC	—
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от MP 10 Core	—
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
PrintingQueueJobsLimit	Максимальное количество одновременно выпускаемых отчетов	5
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	—
PtkbUpdateCheckPeriod	Период проверки наличия обновления для базы знаний, используемой в MP 10 Core (<Часы>:<Минуты>:<Секунды>)	00:05:00
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost

Параметр	Описание	Значение по умолчанию
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
ScansRotationBatchDelay	Задержка между началом обработки пакетов в одной процедуре ротации результатов сканирования	00:00:30
ScansRotationBatchSize	Количество результатов сканирования в пакете в процедуре ротации результатов сканирования Допустимые значения — от 1 до 10 000	1000
ScansRotationDepth	Глубина хранения результатов сканирования	90.00:00:00
ScansRotationEnabled	Ротация результатов сканирования включена (True) или выключена (False)	True
ScansRotationRotationDelay	Задержка между процедурами ротации	01:00:00
SendAlertsToSiem	При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок установлен). Если флажок не установлен, события не регистрируются	Флажок не установлен
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpIgnoreCertificateValidation	MP 10 Core проверяет (False) или не проверяет (True) валидность сертификата при подключении к SMTP-серверу	True

Параметр	Описание	Значение по умолчанию
SmtpPassword	Пароль служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от MP 10 Core	25
SmtpSecureSocketOptions	Варианты шифрования при подключении к SMTP-серверу: — None — шифрование не используется; — Auto — почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется; — SslOnConnect — протоколы SSL или TLS используются при соединении; — StartTls — протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается; — StartTlsWhenAvailable — протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS	Auto
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpUser	Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—

Параметр	Описание	Значение по умолчанию
Text2PdqlEnabled	Доступен AI-поиск по PDQL-запросам для поиска активов и уязвимостей (флажок установлен)	Флажок не установлен
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsageMonitoringCheckingPeriod	Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)	00:15:00
UsePtbkServer	MP 10 Core проверяет (флажок установлен) или не проверяет (флажок снят) наличие обновления базы знаний об уязвимостях в Knowledge Base	Флажок установлен
UserIdleLogoutEnabled	Завершать ли сессию пользователя при его бездействии в системе	False
VulnerStateCheckInterval	Период проверки статусов экземпляров уязвимостей (<Дни>.<Часы>:<Минуты>:<Секунды>)	01.00:00:00
VulnerStateCheckPeriodEnabled	MP 10 Core проверяет (флажок установлен) или не проверяет (флажок снят) статусы экземпляров уязвимостей	Флажок установлен
VulnerStateCheckPeriodEnd	Время окончания суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	01:00:00
VulnerStateCheckPeriodOfRetry	Продолжительность паузы (<Часы>:<Минуты>:<Секунды>) перед повторным запуском проверки, если предыдущий запуск завершился с ошибкой	00:01:00
VulnerStateCheckPeriodStart	Время начала суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	00:00:00

Таблица 15. Параметры конфигурации роли Collector

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	—
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2	—

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentName	Имя коллектора в веб-интерфейсе MaxPatrol VM	FQDN сервера MP 10 Collector
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** Брокер RabbitMQ устанавливается на сервер MP 10 Core и обеспечивает обмен сообщениями между компонентами MaxPatrol VM	localhost
AgentRMQPassword	Пароль служебной учетной записи для подключения MP 10 Collector к RabbitMQ	P@ssw0rd
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от MP 10 Collector	5671
AgentRMQUser	Логин служебной учетной записи для подключения MP 10 Collector к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	RMQ_Server.crt

Параметр	Описание	Значение по умолчанию
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	MP 10 Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key

Таблица 16. Параметры конфигурации роли RMQ Message Bus

Параметр	Описание	Значение по умолчанию
CACertFile	Имя файла корневого сертификата	rootCA.crt
CertFile	Имя файла публичного сертификата	RMQ_Server.crt
HostAddress	IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus	—
KeyFile	Имя файла закрытого ключа сертификата	RMQ_Server.pem
MEMORY_HIGH_WATERMARK_GB	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10
RMQAdminPassword	Пароль служебной учетной записи администратора RabbitMQ	P@ssw0rd
RMQAdminUser	Логин служебной учетной записи администратора RabbitMQ	Administrator
RMQAgentPassword	Пароль служебной учетной записи для доступа коллекторов к RabbitMQ	P@ssw0rd

Параметр	Описание	Значение по умолчанию
RMQAgentUser	Логин служебной учетной записи для доступа коллекторов к RabbitMQ	agent
RMQHttpPort	Порт для доступа к RabbitMQ по протоколу HTTP	5672
RMQHttpsPort	Порт для доступа к RabbitMQ по протоколу HTTPS	5671
RMQLogRotateSize	Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, k для килобайтов)	50M
RMQPassword	Пароль служебной учетной записи для доступа MP 10 Core к RabbitMQ	P@ssw0rd
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для доступа MP 10 Core к RabbitMQ	core
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). **Примечание.** Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Таблица 17. Параметры конфигурации компонента PT UCS

Параметр	Описание	Значение по умолчанию
`AutoAcceptMinions`	Salt Master автоматически утверждает запрос на подключение от модулей Salt Minion (флажок установлен) или модули необходимо подключать вручную (флажок снят)	Флажок снят
`AutoDownloadProductsList`	PT UCS автоматически загружает с глобального сервера Positive Technologies обновления для следующих объектов: — `SIEM BINARY` — дистрибутивов компонентов на Windows; — `SIEM AGENT PENTEST` — модулей Pentest для коллекторов, установленных на Windows; — `SIEM AGENT PENTEST LINUX` — модулей Pentest для коллекторов, установленных на Linux	Установлены флажки `SIEM AGENT PENTEST` и `SIEM AGENT PENTEST LINUX`
`DeleteObsoleteProductVersions`	PT UCS загружает обновления только начиная с определенных версий объектов и удаляет из репозитория более старые версии (флажок установлен) или загружает все версии объектов (флажок снят)	Флажок установлен
`LogLevel`	Уровень журналирования для служб PT UCS	`info`
`ProxyAddress`	IP-адрес или FQDN прокси-сервера	`proxy.server.fqdn.or.ip`
`ProxyEnabled`	PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений Positive Technologies	Флажок снят
`ProxyPassword`	Пароль служебной учетной записи для подключения PT UCS к прокси-серверу	—
`ProxyPort`	Порт прокси-сервера для входящего подключения от PT UCS	`8080`

Параметр	Описание	Значение по умолчанию
`ProxyUser`	Логин служебной учетной записи для подключения PT UCS к прокси-серверу	—
`SaltMasterHost`	IP-адрес или FQDN сервера с модулем Salt Master	—
`SaltMinionLogLevel`	Уровень журналирования для модуля Salt Minion (возможные значения — `fatal`, `error`, `warn`, `info`, `debug` или `trace`)	`info`

Приложение В. Параметры проверок по чек-листу

В разделе приведены описания параметров и их значения по умолчанию. Для числовых параметров указаны допускаемые при проверке минимальные или максимальные значения.

Инструкция по изменению проверок приведена в разделе «Изменение проверок по чек-листу» (см. раздел 22).

Таблица 18. Параметры проверок по чек-листу

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
Выделены значимые активы	AM3-CriticalAssetsDefined	valued_assets_absolute_amount	Минимальное количество выделенных активов	10
		valued_assets_definition	В качестве значимых учитываются активы: — любого уровня значимости — all; — только среднего и высокого уровня — any; — только среднего — medium; — только высокого — high	high
Данные о значимых активах актуальны	AM8-CriticalAssetsActual	valued_assets_refresh_period	Максимальный период запуска задачи на сбор данных (в днях)	30
		valued_assets_definition	Задача собирает данные с активов: — любого уровня значимости — all; — только среднего и высокого уровня — any;	high

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
			— только среднего — `medium`; — только высокого — `high`	
		`actual_valued_assets_amount`	Максимальное количество неактуальных активов	`3`
Общий параметр для всех проверок	—	`check_period`	Период (в минутах) запуска проверок и обновления их результатов в веб-интерфейсе	`15`
Доля просроченных уязвимостей невелика (плановый процесс)	`VM2-OverdueVulnersRatio`	`overdue_vulners_percentage`	Порог допустимой доли просроченных уязвимостей при плановом устранении (в процентах)	`10`
Просроченные уязвимости устраняются быстро (плановый процесс)	`VM3-OverdueVulnersAutoLifeTime`	`evaluation_time`	Продолжительность непрерывного пребывания уязвимости в статусе «Просрочена» (в днях, не более 60 дней)	`7`
		`evaluation_criteria`	В качестве критерия оценки продолжительности непрерывного пребывания уязвимости в статусе «Просрочена» используется максимальное значение параметра `evaluation_time` (`max`) или его среднее значение (`average`) на момент выполнения запроса	`max`

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		valued_assets_definition	В качестве значимых учитываются активы: — любого установленного уровня значимости — all; — только высокого уровня — high; — только среднего уровня — medium; — только среднего и высокого уровня — any; — все активы в системе — nd.	any
		vulner_severity	Проверка распространяется на уязвимости следующих уровней опасности:	any
		vulner_isdanger	Проверка учитывает только уязвимости с меткой «важная» (IsDanger) или все уязвимости (any)	any
		vulner_metrics	Проверка учитывает наличие следующих метрик для уязвимостей:	any
Просроченные уязвимости устраняются быстро	VM4-OverdueVulnersManualLifeTime	evaluation_time	Продолжительность непрерывного пребывания уязвимости в статусе «Просрочена»	7
		evaluation_criteria	В качестве критерия оценки продолжительности непрерывного пребывания уязвимости в статусе «Просрочена» используется максимальное значение параметра evaluation_time (max) или его среднее значение (average) на момент выполнения запроса	max

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		valued_assets_definition	Определение значимых активов для сбора данных об уязвимостях на них:	any
		vulner_severity	Проверка распространяется на уязвимости следующих уровней опасности:	any
		vulner_isdanger	Проверка учитывает только уязвимости с меткой «важная» (IsDanger) или все уязвимости (any)	any
		vulner_metrics	Проверка учитывает наличие следующих метрик для уязвимостей:	any
Важные уязвимости устраняются достаточно быстро (плановый процесс)	VM6-ImportantVulnersMidLifetimeAuto	evaluation_time	Пороговое значение среднего времени устранения важных уязвимостей в плановом процессе	7
		valued_assets_definition	Определение значимых активов для сбора данных о важных уязвимостях на них:	all
Важные уязвимости устраняются достаточно быстро	VM7-ImportantVulnersMidLifetimeManual	evaluation_time	Пороговое значение среднего времени устранения важных уязвимостей вручную	7
		valued_assets_definition	Определение значимых активов для сбора данных о важных уязвимостях на них:	any
Важные уязвимости устраняются в срок (плановый процесс)	VM8-ImportantVulnersMaxLifetimeAuto	evaluation_time	Пороговое значение максимального времени устранения важных уязвимостей в плановом процессе	7

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		valued_assets_definition	Определение значимых активов для сбора данных о важных уязвимостях на них:	all
Важные уязвимости устраняются в срок	VM9-ImportantVulnersMaxLifetimeManual	evaluation_time	Пороговое значение максимального времени устранения важных уязвимостей вручную	7
		valued_assets_definition	Определение значимых активов для сбора данных о важных уязвимостях на них:	all
Трендовые уязвимости устраняются в срок	VM10-TrendVulnersMaxLifetime	evaluation_time	Пороговое значение максимального времени устранения трендовых уязвимостей	7
		valued_assets_definition	Определение значимых активов для сбора данных о трендовых уязвимостях на них:	all

Приложение Г. О проверке серверов перед установкой ролей

При установке и обновлении ролей серверы компонентов автоматически проверяются на наличие факторов, которые могут помешать корректной установке или обновлению MaxPatrol VM. Также серверы проверяются на соответствие программным и аппаратным требованиям (подробнее см. в разделе «Программные и аппаратные требования» Руководства по внедрению). Проверка выполняется для всех ролей как на локальных, так и на удаленных серверах. Описание параметров, по которым проводится проверка, а также возможные ошибки приведены в таблице ниже.

В результате проверки появится одно из сообщений:

— `OK` — проверка пройдена успешно;

— `Warning` — рекомендуется устранить несоответствия, но установка может быть продолжена;

— `Error` — проверка не пройдена, установка будет прервана.

Таблица 19. Параметры соответствия сервера программным и аппаратным требованиям

Параметр	Ошибка	Описание ошибки и рекомендации по ее устранению
`check_os_version`	`Error`	Версия ОС не соответствует требуемой. Используйте ОС той версии, которая указана в разделе «Программные и аппаратные требования» Руководства по внедрению
`check_kernel_version`	`Warning`	Версия ядра ОС для Debian и Astra Linux не соответствует требуемой. Рекомендуется использовать версию ядра, указанную в разделе «Программные и аппаратные требования» Руководства по внедрению
`check_os_arch`	`Error`	Архитектура процессора отличается от x86-64. Для корректной установки MaxPatrol 10 необходимо использовать процессор x86-64
`check_apt_sources`	`Error`	Обнаружен некорректный репозиторий системного менеджера пакетов APT.

Параметр	Ошибка	Описание ошибки и рекомендации по ее устранению
		Необходимо удалить некорректный репозиторий или закомментировать содержащую его строку и перезапустить установку. Путь к репозиторию указан в тексте ошибки
`check_disk_space`	`Error` или `Warning`	Недостаточно свободного места на жестком диске (HDD) или твердотельном накопителе (SSD). Меньше 20 ГБ — `Error`, от 20 до 40 ГБ — `Warning`. Необходимо освободить место на диске или накопителе
`check_breaking_packages`	`Error`	Обнаружен пакет, несовместимый с ролью Deployer, например `golang-docker-credential-helpers`. Необходимо удалить пакет из системы. Название пакета указано в тексте ошибки

Приложение Д. Возможности привилегии «Расширенные полномочия»

Раздел содержит описание возможностей привилегии «Расширенные полномочия».

Таблица 20. Возможности привилегии «Расширенные полномочия»

Ресурс или сервис	**Действия**
База уязвимостей	Обновление
Инфраструктура	Создание, изменение, удаление
Коллектор	Обновление, удаление
Мониторинг источников	Настройка, включение и отключение предупреждения, удаление источника
Политики	Создание, изменение, удаление, применение, просмотр правил политик
Правила корреляции	Запуск, остановка (разделы «Правила корреляции», «Табличные списки»)
Правила обогащения	Запуск, остановка (разделы «Правила обогащения», «Табличные списки»)
Табличные списки	Редактирование, очищение, импорт
Отчеты	Создание, редактирование и удаление шаблонов отчетов (в том числе удаление шаблонов, созданных другими пользователями)
Все объекты в системе	Просмотр

Предметный указатель

positive
technologies

Positive Technologies — один из лидеров в области 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 около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.