MaxPatrol VM версия 2.0

Руководство администратора

Дата редакции документа: 22.09.2023

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, обновлению и удалению 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

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 кнопку **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 16).

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

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;

— оперативное реагирование на инциденты информационной безопасности;

— обеспечение взаимодействия подразделений организации при расследовании инцидентов;

— 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 Knowledge Base

Компонент Knowledge Base — это единая база знаний для продуктов Positive Technologies. Knowledge Base содержит сведения об уязвимостях (об условиях их возникновения и способах устранения), бюллетенях безопасности и возможном ПО на активах.

2.1.4. 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.

2.1.5. Компонент PT Update and Configuration Service

Компонент PT Update and Configuration Service (далее также PT UCS) — это сервис онлайн-обновления компонентов MaxPatrol VM. PT UCS обеспечивает проверку наличия, загрузку и установку новых версий компонентов, а также обновление базы данных по уязвимостям.

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

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 Knowledge Base, 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 компонентов системы и базы знаний.

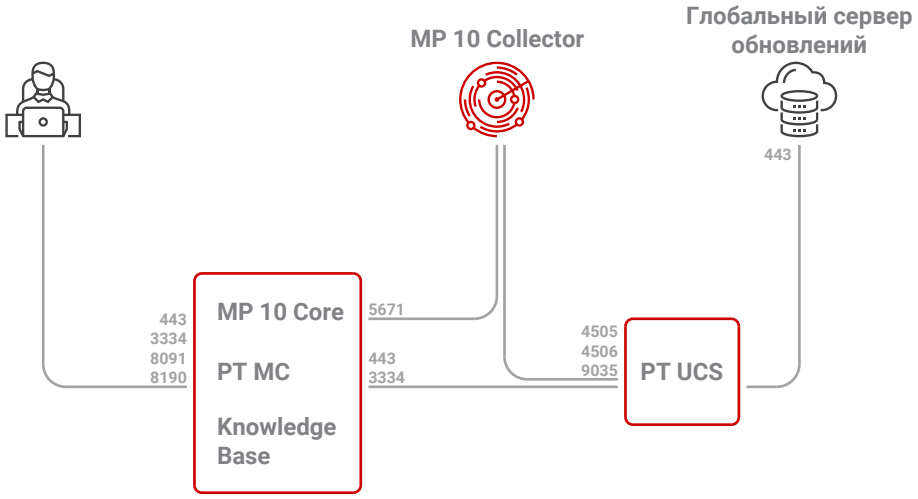

Рисунок 1. Взаимодействие компонентов MaxPatrol VM

Для получения обновлений межсетевой экран сервера компонента PT UCS не должен блокировать адрес глобального сервера обновлений Positive Technologies — 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
Рабочая станция пользователя	Knowledge Base	8091, 8190
MP 10 Core, MP 10 Collector	PT UCS	4505, 4506, 9035
PT UCS	Глобальный сервер обновлений	443

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

Для средненагруженных и высоконагруженных систем на серверах, на которые устанавливаются компоненты MP 10 Collector и MP 10 Core, порт 22/TCP должен быть открыт 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.

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 инциденты, 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 инцидентам в соответствии с производственными задачами пользователя.

В этом разделе приведена инструкция по предоставлению доступа к активам и связанным с ними уязвимостям и инцидентам. 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 B)

3.1. О приложениях PT MC

При развертывании MaxPatrol VM в PT MC регистрируются следующие приложения:

- **Management and Configuration.** Приложение предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления площадками и связями между ними. По умолчанию приложение содержит стандартные роли **Администратор** и **Пользователь**.
- **MaxPatrol 10.** Приложение предназначено для настройки сбора данных об IT-инфраструктуре предприятия и работы с активами, уязвимостями и инцидентами. По умолчанию приложение содержит стандартные роли **Администратор** и **Оператор**.

3.2. Предоставление доступа к активам, уязвимостям и инцидентам

После получения доступа к активам также будут доступны связанные с активами уязвимости и инциденты.

► 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>** по ссылке **Редактировать** откройте окно **Доступ к активам, инцидентам и источникам**.
4. 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.

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).

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.

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.

В MaxPatrol VM доступны следующие политики.

Для значимости 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.

Для сроков актуальности данных

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.

Для статусов 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.

Для отметки «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.

Для работы с политиками предназначена страница **Система** → **Политики**.

В этом разделе

4.1. Страница «Политики»

Страница предназначена для работы с политиками. В панели инструментов находятся следующие кнопки:

— **Создать правило** — для создания правила;

— **Редактировать** — для изменения параметров правила (см. раздел 4.6);

— **Копировать** — для создания правила на основе имеющегося правила (см. раздел 4.7);

— **Удалить** — для удаления правила (см. раздел 4.9);

— **Включить** — для включения правила в работу (см. раздел 4.8);

— **Отключить** — для приостановки работы правила (см. раздел 4.8).

В рабочей области страницы расположены:

— Панель **Список политик**. Содержит список политик и предназначена для выбора политики, применения изменений (см. раздел 4.10), а также отмены непримененных изменений (см. раздел 4.11). При выборе политики составляющие ее правила отобразятся в центральной панели. Если политика имеет непримененные изменения, на левой границе строки с названием политики отобразится желтая полоска, в правой части строки — кнопка ⋮ для отмены изменений, а в нижней части панели — кнопка **Применить изменения**. Если выполняется применение изменений, слева от названия политики отобразится значок ◯.

— Центральная панель. Содержит таблицу с правилами и предназначена для выбора правила и изменения порядка применения правил. При выборе правила сведения о нем отобразятся в правой части страницы в панели **<Название правила>**. В таблице отображаются следующие 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.

— Панель **<Название правила>**. Содержит сведения о правиле, а также отображает сообщения о его работе.

4.2. Создание правила для значимости активов

► Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику для значимости активов.

3. Нажмите кнопку **Создать правило**.

   Откроется страница **Создание правила**.

4. Введите название правила.

5. В раскрывающемся списке выберите группы активов, для которых необходимо указывать значимость.

   Примечание. Вы можете отфильтровать активы с помощью PDQL-запроса.

6. В раскрывающемся списке выберите значимость актива.
7. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.3. Создание правила для сроков актуальности данных

► Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для сроков актуальности данных.
3. Нажмите кнопку **Создать правило**.

   Откроется страница **Создание правила**.
4. Введите название правила.
5. В раскрывающемся списке выберите группы активов, для которых необходимо указывать сроки актуальности данных.

   Примечание. Вы можете отфильтровать активы с помощью PDQL-запроса.
6. Если требуется, измените значения по умолчанию для сроков актуальности данных.
7. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.4. Создание правила для статусов уязвимостей

► Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.
2. В панели **Список политик** выберите политику для статусов уязвимостей.
3. Нажмите кнопку **Создать правило**.

   Откроется страница **Создание правила**.
4. Введите название правила.

5. В поле **Фильтр уязвимостей** введите запрос на языке PDQL для поиска тех экземпляров уязвимостей, статусы которых необходимо изменять.

   Примечание. Для уточнения результатов поиска вы можете указать группы активов, а также отфильтровать активы с помощью условия на языке PDQL.

6. В раскрывающемся списке 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 кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.5. Создание правила для отметки «важная»

► Чтобы создать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику для отметки «важная».

3. Нажмите кнопку **Создать правило**.

   Откроется страница **Создание правила**.

4. Введите название правила.

5. В поле **Фильтр уязвимостей** введите запрос на языке PDQL для поиска экземпляров уязвимостей, которые необходимо отмечать как важные.

   Примечание. Для уточнения результатов поиска вы можете указать группы активов, а также отфильтровать активы с помощью условия на языке PDQL.

6. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.6. Изменение правила

Вы можете изменять только пользовательские правила, стандартные правила недоступны для изменения.

► Чтобы изменить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется окно **Редактирование правила <Название правила>**.

5. Внесите изменения.
6. Нажмите кнопку **Сохранить**.

Правило изменено.

Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.7. Копирование правила

► Чтобы скопировать правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Копировать**.

   Откроется окно **Создание правила**.

5. Если требуется, внесите изменения.
6. Нажмите кнопку **Сохранить**.

Правило скопировано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.8. Включение и отключение правила

► Чтобы включить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Включить**.

Правило включено. Система начнет использовать правило только после применения изменений в политике (см. раздел 4.10).

► Чтобы отключить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Отключить**.

Правило отключено. Система перестанет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.9. Удаление правила

Вы можете удалять только пользовательские правила, стандартное правило удалить невозможно.

► Чтобы удалить правило:

1. В главном меню в разделе **Система** выберите пункт **Политики**.

   Откроется страница **Политики**.

2. В панели **Список политик** выберите политику.
3. Выберите правило.
4. В панели инструментов нажмите кнопку **Удалить**.

Правило удалено.

Система перестанет использовать правило только после применения изменений в политике (см. раздел 4.10).

4.10. Применение изменений в политиках

Приведенная инструкция описывает применение изменений, внесенных в несколько политик. Если изменения внесены только в одну политику, для их применения необходимо в панели **Список политик** нажать кнопку **Применить изменения**.

► Чтобы применить изменения, внесенные в несколько политик:

1. В панели **Список политик** нажмите кнопку **Применить изменения**.

   Откроется окно **Применение изменений**.

2. Установите флажки с названиями политик, изменения в которых необходимо применить.
3. Нажмите кнопку **Применить**.

Изменения применены.

4.11. Отмена изменений в черновике политики

► Чтобы отменить изменения:

1. В панели **Список политик** наведите курсор на строку с названием политики и нажмите ⋮ .
2. В открывшемся меню выберите пункт **Сбросить изменения**.

Изменения отменены.

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 — предупреждает о неполадке или сигнализирует об ошибке в работе системы или ее компонента (например, о том, что компонент недоступен);

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

— зеленый — информирует о том, что система работает корректно;

— синий — информирует 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 просмотра состояния лицензии, 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 лицензии, версиях системы и компонента MP 10 Core. На странице доступна информация об истечении срока действия лицензии, отсутствии лицензии или валидного ключа. Также система уведомляет о том, что срок действия лицензии заканчивается, за 14 дней до ее окончания.

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.

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.

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 формате JSON.

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.

> **Внимание!** Вы можете отключить отправку телеметрических данных. Для этого при установке или обновлении роли Observability установите для параметра `AllowToExportTelemetry` значение `False`. Если отправка телеметрических данных в системе отключена, при необходимости вы можете вручную передать архивы файлов с телеметрическими данными в рамках запроса в техническую поддержку.

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. Резервное копирование данных

Вы можете создавать резервные копии данных компонентов MP 10 Core, PT MC и Knowledge Base 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 → Knowledge Base → 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).

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

В этом разделе

7.1. Создание резервной копии данных роли на Linux

► Чтобы создать резервную копию данных,

запустите сценарий резервного копирования данных:

```
/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/backup.sh
<Путь к каталогу для размещения архива с резервной копией данных>
```

Например:

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

Архив `backup.tar` с резервной копией данных будет сохранен в каталоге `/home/mc-application/sqlstorage`.

7.2. Создание резервной копии данных хранилища LogSpace

Резервное копирование данных из хранилища LogSpace осуществляется с помощью утилиты backup_tool. Утилита входит в состав пакета dbtools и устанавливается вместе с ролью Event Storage.

Внимание! Утилита поддерживает только полное резервное копирование данных. Инкрементальное резервное копирование невозможно.

► Чтобы создать резервную копию данных,

на сервере с ролью Event Storage выполните команду:

```
/opt/dbtools/bin/backup_tool --cmd full_backup --repopath /<Каталог для резервной копии данных>
```

Например:

```
/opt/dbtools/bin/backup_tool --cmd full_backup --repopath /backup_dir
```

Резервная копия данных будет сохранена в каталоге `/backup_dir`.

Примечание. При выполнении команды `full_backup` без ключа `--repopath` резервная копия данных будет сохранена в каталоге `/db_backup`.

8. Восстановление данных из резервной копии

Вы можете восстанавливать данные компонентов MP 10 Core, PT MC и Knowledge Base 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 → Knowledge Base → 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

8.1. 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.

► Чтобы восстановить данные компонентов на Linux:

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

   ```
   cd /opt/deployer/bin
   ./Install-RolePackage.ps1 -ManifestPath <Путь к файлам дистрибутива роли>/package.yaml
   ```

   Например:

   ```
   ./Install-RolePackage.ps1 -ManifestPath /home/Roles/SqlStorage_1.0.3218/package.yaml
   ```

3. Восстановите данные роли Deployer:

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

   Например:

   ```
   /var/lib/deployed-roles/Deployment-Application/Deployer/restore.sh /backup
   ```

4. 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.

5. 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>/' {} \;`

6. Установите роль SqlStorage.

7. 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 /backup
   ```

8. Установите роли Management and Configuration и Knowledge Base.

9. Восстановите данные роли Knowledge Base:

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

10. Установите роли RMQ Message Bus и Core.

11. Восстановите данные роли Core:

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

Данные компонентов восстановлены.

8.2. Восстановление данных хранилища LogSpace из резервной копии

Восстановление данных хранилища LogSpace из резервной копии осуществляется с помощью утилиты backup_tool. Утилита входит в состав пакета dbtools и устанавливается вместе с ролью Event Storage.

► Чтобы восстановить данные из резервной копии:

1. Удалите таблицы events, counters и cp из базы данных, в которую планируете восстанавливать данные:

```
logspace-client --query 'drop table siem.events'
logspace-client --query 'drop table siem.counters'
logspace-client --query 'drop table siem.cp'
```

2. На сервере с ролью Event Storage выполните команду:

```
/opt/dbtools/bin/backup_tool --cmd full_restore -db <Название базы данных> --arc <Название резервной копии > --repopath /<Каталог с резервной копией данных>
```

Например:

```
/opt/dbtools/bin/backup_tool --cmd full_restore -db logspace_db --arc siem.*.20220512.000001 --repopath /backup_dir
```

Примечание. При выполнении команды `full_restore` без ключа `-db` для базы данных будет использовано название siem. При выполнении команды `full_restore` без ключа `--arc` утилита восстановит данные из самой актуальной резервной копии.

Данные из резервной копии восстановлены.

9. 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

9.1. 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. На сервере с установленной ролью SqlStorage выполните команду:
   ```
   docker exec -it $(docker ps | awk '/storage-postgres/ {print $NF}') psql -U pt_system -d postgres -c "ALTER USER pt_system WITH PASSWORD '<Новый пароль>'"
   ```
2. Измените конфигурацию роли SqlStorage:
   ```
   PgPassword: <Новый пароль>
   ```
3. Измените конфигурации ролей Management and Configuration, Knowledge Base и Core:
   ```
   PostgrePassword: <Новый пароль>
   ```

Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 11.1.2)

9.2. Смена паролей служебных учетных записей в RabbitMQ

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

В этом разделе

9.2.1. 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 11.1.2) 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.

9.2.2. 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 роли RMQ Message Bus, установленной 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 11.1.2)

9.2.3. 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 роли RMQ Message Bus, установленной 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 11.1.2)

10. Настройка журналирования работы MaxPatrol VM

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

В этом разделе

10.1. 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.

10.2. 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).

11. 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.

В этом разделе

11.1. Просмотр и изменение конфигурации компонентов MaxPatrol VM на Linux

Конфигурация компонента включает в себя параметры конфигураций ролей, с помощью которых компонент был установлен. Для просмотра и изменения конфигурации компонента необходимо просмотреть и 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

См. также

Параметры конфигурации компонентов MaxPatrol VM на Linux (см. приложение A)

11.1.1. Просмотр конфигурации роли

► Чтобы просмотреть конфигурацию роли:

1. На сервере с установленной ролью Deployer запустите сценарий:
   `/var/lib/deployer/role_packages/<Название роли>/install.sh`
2. В открывшемся окне нажмите кнопку **Yes**.
3. В открывшемся окне выберите вариант с идентификатором приложения роли.
4. В открывшемся окне выберите вариант с названием экземпляра роли.

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

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

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

11.1.2. Изменение конфигурации роли

► Чтобы изменить конфигурацию роли:

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

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

   Откроется страница со списком параметров (см. приложение А).
7. Измените значения параметров.
8. Нажмите кнопку **OK**.
9. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

   Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Конфигурация роли изменена.

12. 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

12.1. 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`.

► Чтобы добавить пользовательские поля в модель 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.

   - Если вы добавляете пользовательские поля впервые, в файле `ModelMigrations.xml` скопируйте значение атрибута `Version` элемента `Dsl`, добавьте единицу к последней цифре скопированного значения и укажите полученное значение в файле `UserModel.xml` в качестве версии пользовательской модели (например, `version="19.0.20206.1"`).
   - Если вы добавляете пользовательские поля повторно, добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.2"`).

   Например:

   ```
   <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>
   ```

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="19.0.20206.1">
   </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:

```
<Group Version="19.0.20206.1">
    <ChangeEntity Type="Core.Host">
        <AddProperty Property="UF_AssetNumber" PropertyType="Int"/>
        <AddProperty Property="UF_AssetOwner" PropertyType="String"/>
        <AddProperty Property="UF_AssetRevisionDate" PropertyType="DateTime"/>
    </ChangeEntity>
</Group>
```

5. Если необходимо, добавьте описание пользовательских полей (см. раздел 12.2).

6. Перезапустите службы.

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

Пользовательские поля добавлены в модель актива.

12.2. 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`. В качестве значения атрибута `Name` укажите алиас типа актива.

   Например, для активов на ОС Microsoft Windows укажите:

```
<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`.

2. Для элемента `Entity` добавьте дочерний элемент `Properties`:

```
<Properties>
</Properties>
```

3. 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>
```

4. 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_AssetRevisionDate">
            <Title>Дата последней ревизии актива</Title>
        </Property>
    </Properties>
</Entity>
```

Описание пользовательских полей добавлено.

12.3. 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-identity|assets-projections|assets-scans|core.scanning|core-tables|core-topology|core-topology-analyzer/ {print $NF}')
```

Имена пользовательских полей изменены.

12.4. 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-identity|assets-projections|assets-scans|core.scanning|core-tables|core-topology|core-topology-analyzer/ {print $NF}')
```

Пользовательские поля удалены из модели актива.

13. 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

13.1. 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.

13.2. 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.

13.3. 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.

14. 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 Б).
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 Б)

15. Диагностика и решение проблем

В этом разделе приводятся инструкции по диагностике и решению проблем, 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, выполнять следующие за ним шаги не нужно.

В этом разделе

15.1. Уведомления о состоянии системы

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:

🔵 — информирует о каком-либо событии, не связанном с ошибками в работе системы (например, сообщает об инициализации компонента);

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

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

15.2. 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 выполнение указанных выше шагов не решило проблему, 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.

15.3. 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 выполнение указанных выше шагов не решило проблему, 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.

15.4. 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` утилиты `corecfg.exe` 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.

15.5. Расположение файлов журналов

Для анализа проблемы и выработки путей ее решения службе технической поддержки могут потребоваться файлы журналов. Система может использовать эти файлы во время их сбора, поэтому для сбора файлов необходимо их скопировать, создать из скопированных файлов архив (со сжатием) и отправить его в службу технической поддержки.

Таблица 3. Расположение файлов журналов компонентов на Linux

Компонент	Путь к файлам
MP 10 Core , PT MC , Knowledge Base , MP 10 Collector	Файлы журналов MP 10 Core , PT MC и Knowledge Base 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`

15.6. 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.

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

— `RMQHost` компонента MP 10 Collector, установленного для отдельного сегмента сети.

15.7. Не удается сканировать узлы из подсети предприятия

Проблема

Ошибка при попытке сканировать узлы, расположенные в определенной подсети организации.

Возможные причины

Совпадение подсети, в которой находятся узлы, с подсетью Docker-контейнера, в котором находится MaxPatrol VM.

Решение

Необходимо изменить подсеть докер-контейнера, в которой находится MaxPatrol VM.

Команды из инструкции необходимо выполнять в интерфейсе терминала Linux.

► Чтобы изменить подсеть докер-контейнера:

1. Создайте резервную копию файла конфигурации `daemon.json.j2`:
```
cp /var/lib/deployer/role_packages/common/docker/daemon.json.j2 /var/lib/deployer/
role_packages/common/docker/daemon.json.j2.bak
```
2. Откройте конфигурационный файл `daemon.json.j2`:
```
sudo nano /var/lib/deployer/role_packages/common/docker/daemon.json.j2
```
3. Добавьте в конец файла перед закрывающей фигурной скобкой строки:
```
"bip": "<IP-адрес bridge-интерфейса Docker>/<Префикс сети>",
"default-address-pools": [
  {
```

```
    "base": "<Сеть>/<Префикс сети>",
    "size": "<Префикс создаваемых сетей Docker>"
  }
]
```

Внимание! Параметр `bip` задает IP-адрес bridge-интерфейса Docker и не должен пересекаться со значением параметра `base`, который задает диапазон IP-адресов для создания сетей Docker. Значение параметра `bip` должно относиться к одной из поддерживаемых подсетей: 10.0.0.0/8, 172.16.0.0/12 или 192.168.0.0/16. Параметр `size` задает префикс создаваемых сетей Docker и не может иметь значение меньше 8 и больше 26.

Пример конфигурационного файла с параметрами подсетей:

```
{
  "log-driver": "json-file",
  "log-opts": {
    "max-size": "100m",
    "max-file": "2",
    "compress": "true"
  },
  "dns-opts": ["ndots:1"],
  "bip": "10.10.0.1/24",
  "default-address-pools": [
    {
      "base": "10.0.0.0/20",
      "size": "24"
    }
  ]
}
```

4. Сохраните изменения в файле `daemon.json.j2`.
5. Остановите все докер-контейнеры:
   ```
   docker stop $(docker ps -qa)
   ```
6. Удалите все докер-контейнеры:
   ```
   docker rm $(docker ps -qa)
   ```
7. Удалите действующие параметры сети Docker:
   ```
   docker network prune
   ```
8. На сервере с установленной ролью Deployer запустите обновление конфигурации установленных компонентов MaxPatrol VM:
   ```
   /opt/deployer/bin/Restart-Configuration.ps1 '*' -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
```

16. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

— решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;

— диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;

— разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;

— устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

16.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

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

Техническая поддержка на портале предоставляется на русском и английском языках.

16.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

16.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

16.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

16.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

16.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 4).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 4. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

16.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

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

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

Приложение А. Параметры конфигурации компонентов MaxPatrol VM на Linux

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

Таблица 5. Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью Deployer	—
`RegistryPort`	Номер порта для доступа к локальному реестру Docker-образов	`5000`

Таблица 6. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
`PgAdminPort`	Порт для доступа к pgAdmin	`9001`
`PgEffectiveCacheSize`	Эффективный размер дискового кэша, доступный для одного запроса	`6GB`
`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`
`PgLogLevel`	Уровень журналирования работы СУБД PostgreSQL (возможные значения — `panic`, `fatal`, `log`, `error`, `warning`, `notice`, `info`, `debug1`, `debug2`, `debug3`, `debug4` или `debug5`	`warning`

Параметр	Описание	Значение по умолчанию
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который сервер баз данных будет использовать для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB

Таблица 7. Параметры конфигурации роли Observability

Параметр	Описание	Значение по умолчанию
AllowToExportTelemetry	Данные телеметрии отправляются (True) или не отправляются (False) на сервер приема телеметрии	True
CollectorServerHttpPort	Порт для доступа к серверу сбора журналов по протоколу HTTP	4318
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента MP 10 Core
ExportEnabledFrom	Разрешенное начальное время отправки телеметрии	00:00:00
ExportEnabledTo	Разрешенное конечное время отправки телеметрии	23:59:59
FlusUri	Адрес сервера приема телеметрии	—
InstanceAccessToken	Токен авторизации на сервере приема телеметрии	—

Параметр	Описание	Значение по умолчанию
JobExecutingInterval	Интервал запуска работ внутри сервиса Telemetry.Tracker	00:01:00
MetricsHttpPort	Порт для доступа к метрическим данным	8428
MetricsRetention	Время сохранения метрических данных в базе данных	30d
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

Таблица 8. 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`
`DefaultLocale`	Интерфейс PT MC отображается на русском (`ru-RU`) или английском (`en-US`) языке	`ru-Ru`
`ExpertDataUpdateMethod`	Метод получения обновлений экспертных данных. Возможные значения: Online или Offline	—
`HostAddress`	IP-адрес или FQDN сервера PT MC	—
`IamCookieLifetime`	Время жизни неактивной сессии в MaxPatrol VM (в часах)	`168`
`LdapTimeout`	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	`60000`
`LogCleanLimit`	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	`1000000`
`MasterRedirectEnabled`	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
`PackageManagementPort`	Номер порта сервиса управления пакетами Package Management	`8585`

Параметр	Описание	Значение по умолчанию
`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	–
`PostgreHost`	IP-адрес или FQDN сервера с установленной ролью SqlStorage	–
`PostgrePassword`	Пароль служебной учетной записи для доступа PT MC к СУБД PostgreSQL	`P@ssw0rdP@ssw0rd`
`PostgrePort`	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	`5432`
`PostgreUserName`	Логин служебной учетной записи для доступа PT MC к СУБД PostgreSQL	`pt_system`
`TmSiteAlias`	Псевдоним площадки	`SITE`
`TmSiteId`	Идентификатор площадки	—
`TmTenantManagerId`	Идентификатор службы MC Tenant Manager Service	—

Таблица 9. Параметры конфигурации роли Knowledge Base

Параметр	Описание	Значение по умолчанию
`ClientId`	Идентификатор для регистрации приложения Knowledge Base в PT MC	`ptkb`
`ClientSecret`	Ключ для регистрации приложения Knowledge Base в PT MC	`secret`
`CoreAddress`	IP-адрес или FQDN сервера MP 10 Core	`localhost`

Параметр	Описание	Значение по умолчанию
DefaultLocale	Интерфейс Knowledge Base отображается на русском (ru-RU) или английском (en-US) языке	—
DeploymentType	Тип развертывания Knowledge Base	—
DisplayName	Название приложения Knowledge Base в PT MC	Knowledge Base
EditableOrigins	Поставщик, атрибуты объектов которого можно изменять	Local
HostAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
OriginNameENG	Полное название поставщика для объектов Knowledge Base на английском языке	Local system
OriginNameRUS	Полное название поставщика для объектов Knowledge Base на русском языке	Локальная система
OriginNickName	Псевдоним поставщика для объектов Knowledge Base	LOC
OriginSystemName	Поставщик объектов Knowledge Base	Local
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR

Параметр	Описание	Значение по умолчанию
`ShowDiffObjectId`	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят
`SmtpHost`	IP-адрес или FQDN SMTP-сервера	`localhost`
`SmtpPassword`	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
`SmtpPort`	Порт SMTP-сервера для входящих подключений от Knowledge Base	`25`
`SmtpSender`	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	`Knowledge Base Notification System <NoReply@knowledgebase.com>`
`SmtpUseDefaultCredentials`	Режим аутентификации SMTP-сервера: флажок установлен — для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров `SmtpUser` и `SmtpPassword`); флажок снят — для аутентификации используются логин и пароль, указанные в параметрах `SmtpUser` и `SmtpPassword`	Флажок установлен
`SmtpUser`	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
`StartPage`	Стартовая страница при входе в веб-интерфейс Knowledge Base	`statistics`

Таблица 10. Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
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
HostAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
IncidentAggregationTimeout	Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>)	00:01:00
IncidentIdenticalNotificationLimit	Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент	100
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost

Параметр	Описание	Значение по умолчанию
PostgrePassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
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
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O
RMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	RMQ_Core_Client.p12
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
SaltMasterHost	IP-адрес или FQDN сервера с модулем Salt Master	—
SaltMasterPort	Порт сервера с модулем Salt Master для входящих подключений от MP 10 Core	9035
SendAlertsToSiem	При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок установлен). Если флажок не установлен, события не регистрируются	Флажок не установлен

Параметр	Описание	Значение по умолчанию
`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`
`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 использования 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`

Параметр	Описание	Значение по умолчанию
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	—
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
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 11. 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 12. Параметры конфигурации роли RMQ Message Bus

Параметр	Описание	Значение по умолчанию
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
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	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

Параметр	Описание	Значение по умолчанию
RMQAgentPassword	Пароль служебной учетной записи для доступа коллекторов к RabbitMQ	P@ssw0rd
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
RMQPassword	Пароль служебной учетной записи для доступа MP 10 Core к RabbitMQ	P@ssw0rd
RMQSiemPassword	Пароль служебной учетной записи для доступа MP SIEM Server к RabbitMQ	P@ssw0rd
RMQSiemUser	Логин служебной учетной записи для доступа MP SIEM Server к RabbitMQ	siem
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).	0.5

Параметр	Описание	Значение по умолчанию
	Примечание. Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	

Таблица 13. 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: — `KB VM DATA` — уязвимостей, условий их возникновения и закрытия, бюллетеней, возможного ПО на активах; — `KB BINARY` — дистрибутивов Knowledge Base; — `SIEM BINARY` — дистрибутивов компонентов на Microsoft Windows	Установлены флажки `KB VM DATA` и `KB BINARY`
`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	—

Параметр	Описание	Значение по умолчанию
`ProxyPort`	Порт прокси-сервера для входящего подключения от PT UCS	`8080`
`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`
`TelemetrySendPeriod`	Расписание отправки в Positive Technologies собранных данных о работе системы (в формате планировщика заданий cron)	`30 0 * * *`

Приложение Б. 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 14).

Таблица 14. 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 В. Возможности привилегии «Расширенные полномочия»

Раздел содержит описание возможностей привилегии «Расширенные полномочия».

Таблица 15. Возможности привилегии «Расширенные полномочия»

Ресурс или сервис	Действия
Инциденты	Удаление
Инфраструктура	Создание, изменение, удаление
Табличные списки	Редактирование, очищение, импорт
Правила корреляции	Запуск, остановка (разделы «Правила корреляции», «Табличные списки»)
Правила обогащения	Запуск, остановка (разделы «Правила обогащения», «Табличные списки»)
Мониторинг источников	Настройка, включение и отключение предупреждения, удаление источника
Коллектор	Обновление, удаление
База уязвимостей	Обновление
Политики	Создание, изменение, удаление, применение, просмотр правил политик

Предметный указатель

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.