MaxPatrol VM версия 2.8

Руководство по внедрению

Дата редакции документа: 10.06.2025

Содержание

1. Об этом документе ... 6
   - 1.1. Условные обозначения ... 6
   - 1.2. Другие источники информации о MaxPatrol VM ... 7
2. О MaxPatrol VM ... 8
   - 2.1. Архитектура MaxPatrol VM ... 9
     - 2.1.1. Компонент MaxPatrol 10 Core ... 9
     - 2.1.2. Компонент MaxPatrol 10 Collector ... 9
     - 2.1.3. Компонент PT Management and Configuration ... 10
     - 2.1.4. Компонент PT Update and Configuration Service ... 10
     - 2.1.5. Локальный сервер обновлений ... 10
   - 2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов ... 11
3. Развертывание MaxPatrol VM ... 13
   - 3.1. Программные и аппаратные требования ... 14
     - 3.1.1. Требования к программному обеспечению ... 14
     - 3.1.2. Требования к аппаратному обеспечению ... 14
     - 3.1.3. Рекомендации по развертыванию MaxPatrol VM в виртуальной среде ... 17
   - 3.2. Подготовка к развертыванию MaxPatrol VM ... 19
   - 3.3. Сценарий развертывания MaxPatrol VM ... 20
   - 3.4. Об установке компонентов на Linux с помощью ролей ... 21
   - 3.5. Автоматическое развертывание MaxPatrol VM ... 23
   - 3.6. Развертывание MaxPatrol VM вручную ... 25
     - 3.6.1. Установка роли Deployer ... 25
     - 3.6.2. Установка компонента PT MC на Linux ... 27
       - 3.6.2.1. Установка роли SqlStorage ... 27
       - 3.6.2.2. Установка роли LogConnector ... 29
       - 3.6.2.3. Установка роли Observability ... 30
       - 3.6.2.4. Установка роли Management and Configuration ... 32
     - 3.6.3. Установка компонента MP 10 Core на Linux ... 33
       - 3.6.3.1. Установка роли RMQ Message Bus на сервер MP 10 Core ... 34
       - 3.6.3.2. Установка роли Core ... 35
   - 3.7. Активация PT MC ... 36
   - 3.8. Активация лицензии MaxPatrol VM ... 38
   - 3.9. Установка компонента MP 10 Collector ... 40
     - 3.9.1. Установка модуля Salt Minion на сервер MP 10 Collector ... 40
     - 3.9.2. Установка роли Collector ... 41
     - 3.9.3. Установка компонента MP 10 Collector на Microsoft Windows ... 43
   - 3.10. Настройка подключения к Collector, расположенному в недоверенном сегменте ... 44
     - 3.10.1. Добавление сертификата роли Deployer из защищенного сегмента сети в доверенные сертификаты основной роли Deployer ... 45
     - 3.10.2. Настройка подключения MP 10 Core к Collector на Linux ... 46
     - 3.10.3. Настройка подключения MP 10 Core к Collector на Windows ... 51
   - 3.11. Установка компонента PT UCS ... 58
   - 3.12. Установка доверенного сертификата для сайта MaxPatrol VM ... 60

3.13. Установка пользовательского сертификата для роли SqlStorage ... 61
3.14. Установка пользовательского сертификата для RMQ Message Bus и компонентов MP 10 Core и MP 10 Collector ... 63
3.15. Настройка обновления экспертных данных ... 64
3.15.1. Изменение параметров обновления экспертных данных для роли Management and Configuration ... 66
3.15.2. Аппаратные и программные требования к локальному серверу обновлений ... 67
3.15.3. Установка локального сервера обновлений ... 68
3.15.4. Активация лицензии локального сервера обновлений ... 69
3.15.5. Настройка подключения локального сервера обновлений к прокси-серверу ... 70
3.15.6. Настройка автоматического переноса обновлений в закрытый сегмент сети ... 72
3.15.7. Ручной перенос обновлений MaxPatrol VM в закрытый сегмент сети ... 73
3.15.8. Проверка и изменение параметров локального сервера обновлений ... 74
3.16. Харденинг MaxPatrol VM: MP 10 Core установлен на Linux ... 76
4. Обновление MaxPatrol VM ... 80
4.1. Обновление с помощью дистрибутивов ... 80
4.1.1. Управление обновлением ролей и компонентов MaxPatrol VM с помощью манифеста ... 81
4.1.1.1. Обновление ролей и компонентов MaxPatrol VM с помощью манифеста ... 82
4.1.1.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей ... 83
4.1.2. Обновление роли Deployer ... 86
4.1.3. Обновление компонента PT MC на Linux ... 87
4.1.3.1. Обновление роли SqlStorage ... 88
4.1.3.2. Обновление роли LogConnector ... 89
4.1.3.3. Обновление роли Observability ... 91
4.1.3.4. Обновление роли Management and Configuration ... 92
4.1.4. Активация PT MC ... 94
4.1.5. Добавление лицензии в PT MC ... 95
4.1.6. Обновление компонента MP 10 Core на Linux ... 96
4.1.6.1. Обновление роли RMQ Message Bus на сервере MP 10 Core ... 96
4.1.6.2. Обновление роли Core ... 97
4.1.7. Обновление компонента MP 10 Collector на Linux ... 99
4.1.8. Обновление компонента MP 10 Collector на Microsoft Windows ... 101
4.1.9. Обновление компонента PT UCS ... 101
4.1.10. Обновление локального сервера обновлений ... 102
4.1.11. Привязка лицензии MaxPatrol VM к приложению в PT MC ... 103
5. Просмотр и изменение параметров конфигурации MaxPatrol VM ... 105
5.1. Просмотр конфигурации роли ... 105
5.2. Изменение конфигурации роли ... 106
5.3. Управление изменением конфигурации ролей с помощью манифеста ... 107
5.3.1. Изменение конфигурации ролей с помощью манифеста ... 108
5.3.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей ... 109
5.4. Настройка SMTP-сервера для отправки уведомлений по электронной почте ... 112
5.5. Настройка прокси-сервера для онлайн-активации PT MC ... 113

5.6. Включение AI-поиска по запросам ... 114
5.7. Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol VM ... 114
5.8. Изменение времени устаревания активов ... 114
6. О технической поддержке ... 115
Приложение. Параметры конфигурации компонентов MaxPatrol VM на Linux ... 119

1. Об этом документе

Руководство по внедрению содержит информацию для планирования и выполнения развертывания Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM) в инфраструктуре организации. В руководстве вы найдете типовые схемы развертывания MaxPatrol VM, а также инструкции по установке, первоначальной настройке и обновлению продукта.

Руководство адресовано руководителям и специалистам IT-подразделения организации, которые планируют и выполняют развертывание MaxPatrol VM.

Комплект документации MaxPatrol VM включает в себя следующие документы:

— Этот документ.

— Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.

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

— Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.

— Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.

— PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol VM.

— Руководство разработчика — содержит информацию о доступных в MaxPatrol VM функциях сервиса REST API.

В этом разделе

Условные обозначения (см. раздел 1.1)

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

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

Пример	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
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 **ОК**	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 6).

См. также

О технической поддержке (см. раздел 6)

2. О MaxPatrol VM

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

— управление активами;

— анализ защищенности активов ИБ;

— приоритизацию и проверку устранения уязвимостей на активах ИБ.

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

MaxPatrol VM позволяет:

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

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

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

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

— определять способы устранения уязвимостей и настраивать политики контроля;

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

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

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

В этом разделе

Архитектура MaxPatrol VM (см. раздел 2.1)

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

2.1. Архитектура MaxPatrol VM

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

В этом разделе

Компонент MaxPatrol 10 Core (см. раздел 2.1.1)

Компонент MaxPatrol 10 Collector (см. раздел 2.1.2)

Компонент PT Management and Configuration (см. раздел 2.1.3)

Компонент PT Update and Configuration Service (см. раздел 2.1.4)

Локальный сервер обновлений (см. раздел 2.1.5)

2.1.1. Компонент MaxPatrol 10 Core

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

— централизованное хранение конфигурации активов;

— централизованное управление всеми компонентами системы;

— автоматизацию процесса управления уязвимостями;

— поддержку веб-интерфейса системы.

2.1.2. Компонент MaxPatrol 10 Collector

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

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

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

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

2.1.3. Компонент PT Management and Configuration

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

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

2.1.4. Компонент PT Update and Configuration Service

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

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

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

2.1.5. Локальный сервер обновлений

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

2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol VM:

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

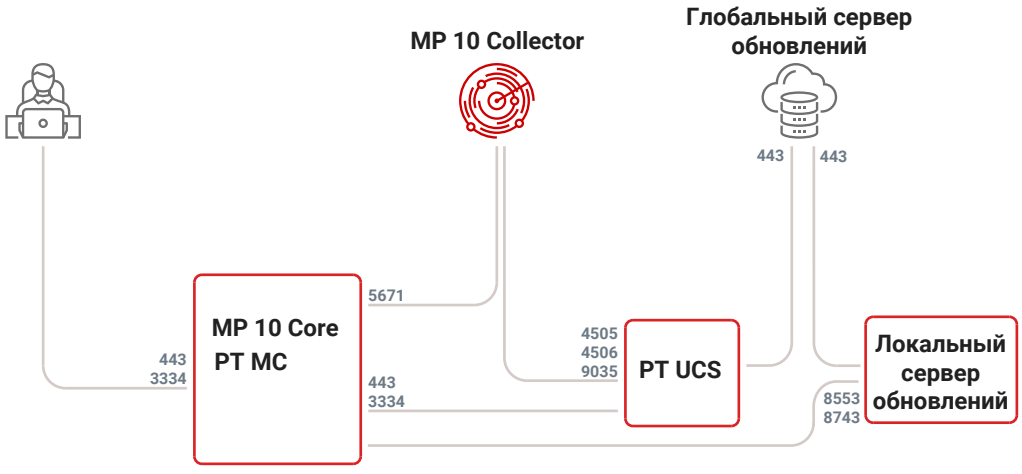

Рисунок 1. Взаимодействие компонентов MaxPatrol VM

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

Таблица 2. Компоненты и порты взаимодействия

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

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

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

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

3. Развертывание MaxPatrol VM

Для развертывания MaxPatrol VM вам потребуется один сервер. На него необходимо установить компоненты MP 10 Core, PT MC и MP 10 Collector.

Также вы можете установить компонент PT UCS на сервер MP 10 Core.

> **Примечание.** При отсутствии прямого доступа к интернету компонент PT UCS устанавливается на отдельный сервер.

Для обновления экспертных данных (см. раздел 3.15) при отсутствии прямого доступа к интернету вы можете установить локальный сервер обновлений на отдельный сервер.

Компоненты системы могут быть установлены в виртуальной среде.

В зависимости от физической или логической топологии IT-инфраструктуры организации может потребоваться сканировать узлы, расположенные в отдельных сетевых сегментах. В этом случае на каждый сегмент рекомендуется устанавливать отдельный MP 10 Collector. Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных MP 10 Collector.

Если вы планируете развертывать MaxPatrol VM на базе уже развернутой системы MaxPatrol SIEM, вам не требуется устанавливать компоненты. Для работы MaxPatrol VM необходимо активировать лицензию, перезапустить службы компонента MP 10 Core, а затем выйти из системы и заново войти в нее.

В этом разделе

Программные и аппаратные требования (см. раздел 3.1)

Подготовка к развертыванию MaxPatrol VM (см. раздел 3.2)

Сценарий развертывания MaxPatrol VM (см. раздел 3.3)

Об установке компонентов на Linux с помощью ролей (см. раздел 3.4)

Автоматическое развертывание MaxPatrol VM (см. раздел 3.5)

Развертывание MaxPatrol VM вручную (см. раздел 3.6)

Активация PT MC (см. раздел 3.7)

Активация лицензии MaxPatrol VM (см. раздел 3.8)

Установка компонента MP 10 Collector (см. раздел 3.9)

Настройка подключения к Collector, расположенному в недоверенном сегменте (см. раздел 3.10)

Установка компонента PT UCS (см. раздел 3.11)

Установка доверенного сертификата для сайта MaxPatrol VM (см. раздел 3.12)

Установка пользовательского сертификата для роли SqlStorage (см. раздел 3.13)

Установка пользовательского сертификата для RMQ Message Bus и компонентов MP 10 Core и MP 10 Collector (см. раздел 3.14)

Настройка обновления экспертных данных (см. раздел 3.15)

Харденинг MaxPatrol VM: MP 10 Core установлен на Linux (см. раздел 3.16)

3.1. Программные и аппаратные требования

В этом разделе приведены требования к программному и аппаратному обеспечению серверов MaxPatrol VM.

В этом разделе

Требования к программному обеспечению (см. раздел 3.1.1)

Требования к аппаратному обеспечению (см. раздел 3.1.2)

Рекомендации по развертыванию MaxPatrol VM в виртуальной среде (см. раздел 3.1.3)

3.1.1. Требования к программному обеспечению

Все компоненты MaxPatrol VM поддерживают установку на 64-разрядные ОС семейства Linux — Astra Linux Special Edition 1.7.5 (на базе ядра Linux версии 5.15) и 1.7.6 или Debian 10.3 и выше, Debian 11 и 12 (на базе ядра Linux версии 5.10 и выше). Кроме того, вы можете установить компонент MP 10 Collector на Microsoft Windows Server 2012, 2012 R2, 2016, 2019 и 2022.

Для работы в интерфейсе MaxPatrol VM рекомендуется использовать последние версии браузеров Google Chrome, Mozilla Firefox, Microsoft Edge или Яндекс Браузер.

3.1.2. Требования к аппаратному обеспечению

Компоненты системы необходимо устанавливать на серверы, удовлетворяющие приведенным ниже аппаратным требованиям.

Таблица 3. Аппаратные требования к серверам MP 10 Core, PT MC

Количество активов	Центральный процессор, ядра	Память (ОЗУ), ГБ	Свободное дисковое пространство		
			При сканировании 1 раз в неделю	При сканировании 1 раз в 2 недели	При сканировании 1 раз в месяц
До 1000	12	64 ГБ	450 ГБ	300 ГБ	250 ГБ
До 5000	14	64 ГБ	1,8 ТБ	1,1 ТБ	650 ГБ
До 10 000	18	64 ГБ	3 ТБ	1,7 ТБ	1,1 ТБ
До 20 000	24	80 ГБ	5,9 ТБ	3,3 ТБ	2 ТБ
До 50 000	24	90 ГБ	6,5 ТБ	4,1 ТБ	3 ТБ
До 100 000	32	100 ГБ	11,8 ТБ	7,5 ТБ	5,3 ТБ

Внимание! При количестве активов до 50 000 и выше рекомендуемый объему ОЗУ зависит от набора активов. Рекомендации в таблице получены для усредненного набора активов.

Рекомендуется использовать процессоры с технологией Hyper-Threading, например процессоры Intel Xeon Scalable второго поколения и выше (или их аналоги), с минимальной тактовой частотой 2,2 ГГц.

Рекомендуется использовать сетевой адаптер со скоростью не менее 1 Гбит/с.

Для хранения данных необходимо использовать твердотельные накопители (SSD) с производительностью не менее 30 000 IOPS, объединенные в отказоустойчивый массив RAID с файловой системой ext4 (размер блока 4096 байт).

Для работы ОС на дисковом пространстве рекомендуется создать раздел объемом 200 ГБ и смонтировать его как каталог `/`. Для хранения данных рекомендуется создать раздел объемом не менее указанного в таблице выше и смонтировать его как каталог `/var`.

> **Примечание.** Объем свободного дискового пространства рассчитан при условии хранения данных в течение двух лет.

Рекомендуется использовать область подкачки объемом не менее 10% от общего объема памяти (ОЗУ).

Таблица 4. Аппаратные требования к серверу MP 10 Collector, размещенному в отдельном сегменте сети (сканирование активов)

	Минимальные требования при сканировании активов модулями Audit и Pentest		
	До 4 потоков на коллектор	**До 10 потоков на коллектор**	**До 20 потоков на коллектор**
Количество логических ядер в системе виртуализации [2]	4	6	8
Память (ОЗУ)	4 ГБ	8 ГБ	12 ГБ
Жесткий диск (HDD) [1]	300 ГБ	300 ГБ	300 ГБ

Таблица 5. Аппаратные требования к серверу PT UCS

Компонент сервера	**Минимальное требование**
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 4 логических ядра
Память (ОЗУ)	4 ГБ
Сетевой адаптер	1 порт со скоростью 1 Гбит/с
Жесткие диски	300 ГБ

2 Соответствует количеству потоков в физических ядрах процессора с включенной технологией Hyper-Threading. Рекомендуется использовать процессоры Intel Xeon Scalable второго поколения и выше или их аналоги.

1 Рекомендуется объединить жесткие диски (HDD) со скоростью 7200 об./мин каждый в массив RAID 10, создать раздел с файловой системой ext4 (размер блока 4096 байт) объемом не менее указанного в таблице и смонтировать его как корневой каталог `/`.

Таблица 6. Аппаратные требования для MaxPatrol VM в мобильной комплектации

Количество активов	Центральный процессор, ядра	Память (ОЗУ), ГБ	Свободное дисковое пространство		
			При сканировании 1 раз в неделю	При сканировании 1 раз в 2 недели	При сканировании 1 раз в месяц
До 1000	12	64 ГБ	450 ГБ	300 ГБ	250 ГБ

3.1.3. Рекомендации по развертыванию MaxPatrol VM в виртуальной среде

Для развертывания MaxPatrol VM в виртуальной среде рекомендуется использовать системы виртуализации VMware vSphere или zVirt.

VMware vSphere

Рекомендуется использовать версию 11 виртуальной машины VMware vSphere и версию 6.0 гипервизора VMware ESXi с параметрами распределения ресурсов, приведенными в таблице ниже.

Таблица 7. Распределение ресурсов для VMware vSphere

Компонент	Рекомендуемые параметры
Гипервизор	Рекомендуется использовать технологию Storage I/O Control при обмене данными между гипервизором и хранилищами, содержащими виртуальные машины, на которых будут развернуты компоненты системы
Виртуальная машина	Для закрепления за виртуальной машиной выделенных для нее аппаратных ресурсов (например, логических ядер) рекомендуется в параметрах виртуальной машины **VM Options** → **Advanced** в раскрывающемся списке **Latency Sensitivity** выбрать **High**. Для каждой такой виртуальной машины нужно дополнительно оставлять два свободных логических ядра.

Компонент	Рекомендуемые параметры
	При использовании гипервизора VMware ESXi версии ниже 6.7 рекомендуется в аппаратных параметрах виртуальных машин **Virtual Hardware → CPU/MMU Virtualization** выбрать режим **Hardware CPU and MMU**, который позволит использовать аппаратные технологии поддержки виртуализации Intel VT-x/AMD-V и Intel EPT/AMD RVI. Для повышения производительности рекомендуется в параметрах виртуальной машины на вкладке **Resources** в блоке параметров процессора **Hyperthreaded Core Sharing** выбрать режим **None**, в блоке параметров **Resource Allocation** передвинуть максимально вправо ползунок **Reservation** и установить флажок **Unlimited**
Центральный процессор	В аппаратных требованиях к центральному процессору указано минимальное количество логических ядер. Если сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить вдвое меньше физических ядер. Если технология Hyperthreading не используется, количество выделенных физических ядер должно быть равно количеству логических. Например, если виртуальной машине требуется 56 логических ядер и сервер гипервизора использует технологию Hyperthreading, виртуальной машине достаточно выделить два процессора по 14 ядер каждый
BIOS	Для исключения задержек при выходе ядер процессора из спящего режима рекомендуется выбрать в параметрах BIOS производительный режим работы системы (профиль Performance в серверах компании Dell или аналогичные профили в серверах других производителей). Для повышения производительности ядер процессоров, поддерживающих технологию Intel Turbo Boost, рекомендуется включить в системных параметрах BIOS использование этой технологии
Оперативная память	Объем оперативной памяти, выделяемой каждой виртуальной машине, не должен быть меньше значения, указанного в аппаратных требованиях. Также необходимо учитывать, что часть оперативной памяти сервера (до 8% от общего объема) должна быть зарезервирована для работы гипервизора. Для работы виртуальной машины рекомендуется зарезервировать постоянный объем оперативной памяти, установив в блоке параметров **Resources Allocation** флажок **Reserve all guest memory (All locked)**
Виртуальные жесткие диски	Объем и производительность виртуальных жестких дисков не должны быть меньше значений, указанных в аппаратных требованиях. При создании виртуального жесткого диска на шаге **Create a Disk** в блоке параметров **Disk Provisioning** рекомендуется выбрать вариант **Thick Provision Eager Zeroed**, на шаге **Advanced Options** в блоке параметров **Mode** рекомендуется установить флажок **Independent**, а затем выбрать вариант **Persistent**

zVirt

Рекомендуется использовать систему zVirt версии 4.2.

3.2. Подготовка к развертыванию MaxPatrol VM

Если предполагается установка MaxPatrol VM на ядро Astra Linux типа hardened, то для корректной работы Docker-контейнеров перед установкой необходимо настроить ядра типа hardened на всех серверах с Astra Linux.

> **Внимание!** Перед развертыванием MaxPatrol VM на Astra Linux Special Edition 1.7 необходимо на серверах компонентов выполнить действия, указанные в бюллетенях производителя № 2021-1126SE17 и № 2022-0318SE17MD (подробнее см. в справочном центре Astra Linux).

Если MaxPatrol VM устанавливается на Astra Linux и включен мандатный контроль целостности (далее МКЦ), для учетной записи, которая используется при установке компонентов системы, необходим максимальный уровень целостности. Инструкция по настройке МКЦ приведена в разделе «Настройка мандатного контроля целостности для Astra Linux» Руководства администратора.

Для установки или обновления Debian необходимо использовать полный установочный образ. Он содержит необходимый набор пакетов и не требует подключения к интернету (подробнее см. на сайте debian.org).

Если в Debian 10.3—10.13 используется версия ядра ниже требуемой, перед установкой или обновлением MaxPatrol VM необходимо обновить его версию, установив метапакет ядра `linux-image-5.10-amd64`. При обновлении версии ядра не требуется обновление ОС.

При использовании NAT в IT-инфраструктуре организации рекомендуется использовать в качестве адресов компонентов MaxPatrol VM на узлах только FQDN.

Если в качестве адресов компонентов MaxPatrol VM на узлах используются FQDN, необходимо настроить и обеспечить доступность DNS для корректного разрешения имен узлов в IP-адреса.

> **Внимание!** Не рекомендуется вносить изменения в файл `/etc/hosts`. Этот файл не используется компонентами MaxPatrol VM.

При установке или обновлении операционной системы необходимо указать в качестве используемого формата размещения таблиц разделов на физическом жестком диске стандарт GPT.

> **Примечание.** При развертывании компонента MP 10 Collector устанавливается драйвер WinPcap 4.1.3. Не рекомендуется дополнительно устанавливать другие версии драйвера WinPcap, поскольку работа другой версии драйвера может привести к некорректной работе модуля hostdiscovery.

3.3. Сценарий развертывания MaxPatrol VM

Примечание. Вы можете выполнить автоматическое развертывание (см. раздел 3.5) MaxPatrol VM с помощью манифеста или установить все компоненты вручную по очереди, начиная с роли Deployer.

Компоненты MP 10 Core и PT MC устанавливаются на Linux. При такой установке базовыми единицами развертывания являются роли (см. раздел 3.4).

При развертывании необходимо придерживаться следующего порядка действий:

1. Установка роли Deployer.
2. Установка компонента PT MC.
3. Активация компонента PT MC.
4. Установка компонента MP 10 Core.
5. Активация лицензии.
6. Установка компонента MP 10 Collector.
7. Установка компонента PT UCS.
8. Настройка MaxPatrol VM для обеспечения его безопасной работы.

Сценарий развертывания MaxPatrol VM при установке ролей Core и SqlStorage на разных серверах

Установка ролей Core и SqlStorage на разные узлы может потребоваться в случае нехватки аппаратных ресурсов для установки всех ролей на одном сервере.

Примечание. Если СУБД PostgreSQL установлена отдельно от MaxPatrol VM, то обслуживание, обновление и резервирование данных, а также восстановление данных из резервных копий необходимо проводить самостоятельно.

При развертывании необходимо придерживаться следующего порядка действий:

1. Установка (см. раздел 3.6.1) роли Deployer на основном сервере.
2. Установка модуля Salt Minion на сервере с ролью Deployer. При установке модуля Salt Minion в качестве значения параметра `HostAddress` необходимо ввести IP-адрес или FQDN дополнительного сервера, на котором будет установлена роль SqlStorage.
3. Установка (см. раздел 3.6.2.1) роли SqlStorage на дополнительном сервере. При установке роли SqlStorage в качестве значения параметра `HostAddress` необходимо ввести IP-адрес или FQDN дополнительного сервера.
4. Установка роли Observability.
5. Установка роли Management and Configuration.
6. Активация компонента PT MC.

7. Установка компонента MP 10 Core.
8. Активация лицензии.
9. Установка компонента MP 10 Collector.
10. Установка компонента PT UCS.
11. Настройка MaxPatrol VM для обеспечения его безопасной работы.

Если на сервере компонента установлен Kaspersky Endpoint Security, необходимо приостановить его работу на время развертывания MaxPatrol VM. Во время развертывания операционная система сервера может быть перезагружена. После перезагрузки необходимо повторно приостановить работу Kaspersky Endpoint Security.

См. также

Об установке компонентов на Linux с помощью ролей (см. раздел 3.4)

3.4. Об установке компонентов на Linux с помощью ролей

Роль является базовой единицей развертывания на Linux и представляет собой совокупность служб, утилит и сценариев, обеспечивающих работу определенного набора функций системы. Каждая роль поставляется в виде отдельного архива, который может содержать Docker-образы или deb-пакеты.

При развертывании системы создаются экземпляры ролей, которые распределяются по приложениям определенного типа (Management and Configuration или MaxPatrol 10). Такая архитектура позволяет гибко и удобно развертывать систему, а также обновлять и настраивать ее в дальнейшем. Тип приложения определяется составом входящих в него экземпляров ролей:

— приложение Management and Configuration содержит только роли SqlStorage, LogConnector, Observability и Management and Configuration;

— приложение MaxPatrol 10 — только роли Core, RMQ Message Bus и Collector.

Примечание. При развертывании системы можно создать несколько приложений одного типа (например, несколько приложений Management and Configuration), однако такие конфигурации не поддерживаются производителем.

Управление развертыванием обеспечивается ролью Deployer, которая построена на базе системы управления конфигурациями SaltStack. Ее модуль Salt Master обеспечивает общее управление установкой (созданием экземпляров) ролей, модули Salt Minion — установку ролей на каждый сервер системы.

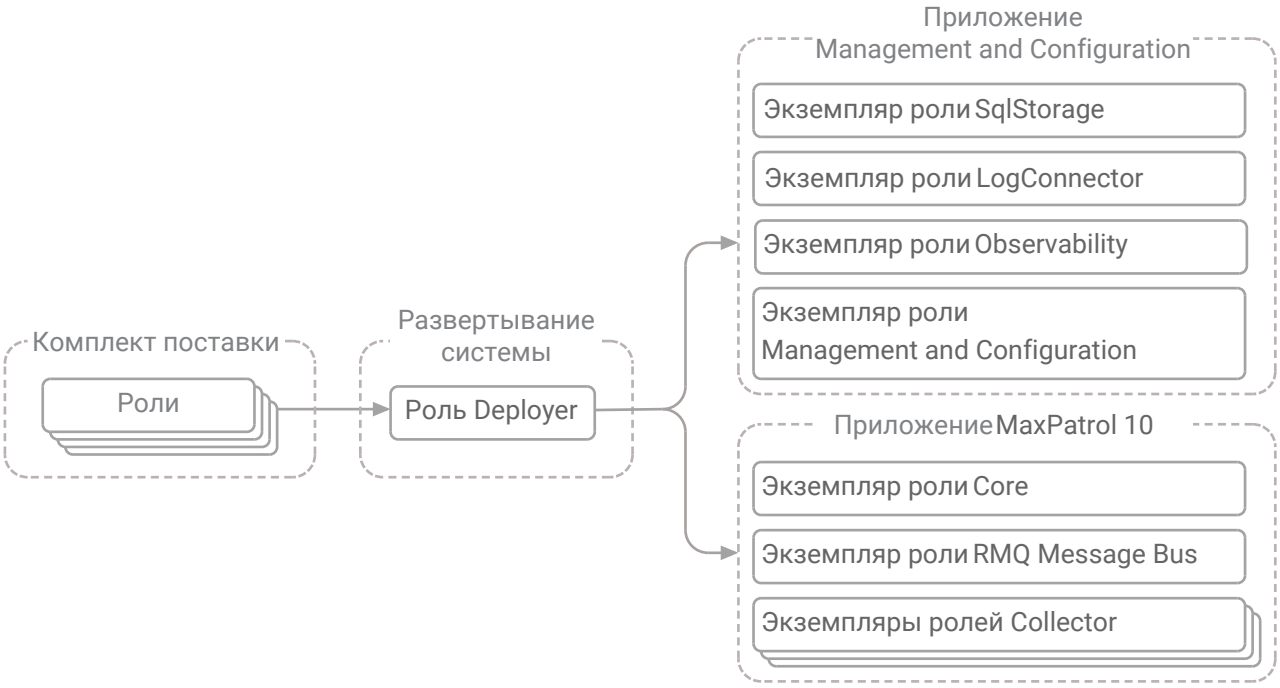

Рисунок 2. Развертывание системы с помощью ролей

Выбор режима развертывания

Для развертывания обязательных компонентов MaxPatrol VM вам потребуется один сервер. Есть два режима развертывания:

— Для автоматического развертывания вы можете использовать сценарий `install-aio.sh`. При авторазвертывании на сервер будут последовательно установлены компоненты: Deployer → PT MC (роли SqlStorage, LogConnector, Observability и Management and Configuration) → MP 10 Core (роли RMQ Message Bus и Core) → MP 10 Collector (версия для Linux).

  Подробности см. в инструкции по авторазвертыванию (см. раздел 3.5).

— При развертывании вручную необходимо последовательно установить все роли компонентов MaxPatrol VM.

  Подробности см. в инструкции по развертыванию вручную (см. раздел 3.6).

Порядок установки роли

Для установки компонента может потребоваться установка как одной, так и нескольких ролей. В общем случае установка роли делится на следующие этапы:

1. Распаковка архива и запуск сценария установки.

   Внимание! Сценарий установки `install.sh` или `install-aio.sh` необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

Внимание! Путь к каталогу, из которого будет запущен сценарий `install.sh` или `install-aio.sh`, а также имя самого каталога могут содержать только буквы латинского алфавита, цифры, знаки подчеркивания и точки.

2. Выбор приложения для установки роли. Вам потребуется или выбрать ранее созданное приложение необходимого типа, или создать новое, если приложение необходимого типа отсутствует. При создании приложения нужно ввести его идентификатор, который среди прочего будет использоваться в качестве имени каталога для размещения файлов всех экземпляров ролей, входящих в состав данного приложения.

   Примечание. Вы можете использовать идентификаторы, предлагаемые системой по умолчанию. Например, если для приложения Management and Configuration использовать предлагаемый по умолчанию идентификатор `mc-application`, файлы всех экземпляров ролей этого приложения будут размещены в каталоге `/var/lib/deployed-roles/mc-applicaton`.

3. Ввод названия экземпляра роли и выбор сервера для ее установки. Введенное название среди прочего будет использоваться в качестве имени каталога для размещения файлов создаваемого экземпляра роли (например, файлов журналов и файлов конфигурации).

   Примечание. Вы можете использовать названия, предлагаемые системой по умолчанию. Например, если для роли Collector использовать предлагаемое по умолчанию название `agent`, файлы этого экземпляра роли будут размещены в каталоге `/var/lib/deployed-roles/mc-applicaton/agent`.

4. Проверка и изменение параметров конфигурации.

5. Запуск установки.

См. также

Автоматическое развертывание MaxPatrol VM (см. раздел 3.5)

3.5. Автоматическое развертывание MaxPatrol VM

Для автоматического развертывания MaxPatrol VM на Linux вам понадобится сценарий установки `install-aio.sh` из комплекта поставки. Запускать сценарий в интерфейсе терминала необходимо с правами суперпользователя (root).

- Чтобы развернуть MaxPatrol VM:

  1. В каталоге `deploy_manifests` откройте на редактирование файл манифеста `VM-AIO.yaml` и в блок параметров `Instances` → `ManagementAndConfiguration` добавьте параметр `ExpertDataUpdateMethod` со значением `Online`, а также параметр `PackagesSourceUri`, в качестве значения которого укажите адрес сервера для получения экспертного контента:

     ```
     ManagementAndConfiguration:
       type: ManagementAndConfiguration
       host: local
       order: 3
     ```

```
params:
  ExpertDataUpdateMethod: Online
  PackagesSourceUri: <Адрес сервера для получения экспертного контента>
```

Внимание! Параметры и их значения в файле манифеста должны быть указаны с соблюдением синтаксиса языка YAML.

Примечание. Если вы устанавливаете MaxPatrol VM в сегменте сети с прямым подключением к интернету, в качестве значения параметра `PackagesSourceUri` необходимо указать один из адресов глобального сервера обновлений — `https://update.ptsecurity.ru/packman/v1/` или `https://update.ptsecurity.com/packman/v1/`; если в изолированном сегменте сети без прямого подключения к интернету — адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.

2. Если вы разворачиваете MaxPatrol VM на твердотельных накопителях, добавьте в блок параметров `Instances` → `SqlStorage` параметр `PgHardDiskType` со значением `SSD`:

   ```
   SqlStorage:
     type: SqlStorage
     host: local
     params:
       PgHardDiskType: SSD
     order: 1
   ```

3. Сохраните изменения и закройте файл.
4. Запустите сценарий установки `install-aio.sh` от имени суперпользователя (root).
5. Выберите манифест **VM-AIO** и нажмите **OK**.

   Начнется проверка сервера на соответствие программным и аппаратным требованиям.

   Если сервер не соответствует требованиям, отобразится сообщение `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

   Примечание. При авторазвертывании сообщения `Warning` автоматически игнорируются.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

   Начнется установка пакетов. По завершении установки появится сообщение `Application deploy manifest successfully applied`.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install-aio.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

После завершения установки MaxPatrol VM необходимо активировать (см. раздел 3.8) лицензию, приобретенную вашей организацией, а затем выполнить харденинг (см. раздел 3.16) MaxPatrol VM.

См. также

Установка локального сервера обновлений (см. раздел 3.15.3)

3.6. Развертывание MaxPatrol VM вручную

Чтобы развернуть MaxPatrol VM вручную, выполните на одном узле инструкции из следующих разделов:

— Установка роли Deployer (см. раздел 3.6.1);

— Установка компонента PT MC (см. раздел 3.6.2);

— Активация PT MC (см. раздел 3.7);

— Установка компонента MP 10 Core (см. раздел 3.6.3);

— Активация лицензии MaxPatrol 10 (см. раздел 3.8);

— Установка компонента MP 10 Collector (см. раздел 3.9).

В этом разделе

Установка роли Deployer (см. раздел 3.6.1)

Установка компонента PT MC на Linux (см. раздел 3.6.2)

Установка компонента MP 10 Core на Linux (см. раздел 3.6.3)

3.6.1. Установка роли Deployer

Для установки роли вам потребуется архив `pt_deployer_<Номер версии>.tar.gz` из комплекта поставки. Роль устанавливается вместе с компонентом PT UCS — либо на сервер с любым из компонентов MaxPatrol VM, либо на отдельный сервер.

> **Внимание!** Для любой конфигурации MaxPatrol VM необходимо установить только один экземпляр роли Deployer. Установка второго экземпляра роли Deployer на сервер любого компонента сделает работу MaxPatrol VM невозможной и потребует переустановки всей системы.
>
> **Внимание!** Для корректной работы MaxPatrol VM необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в вашей организации. По умолчанию система виртуализации Docker использует подсети в диапазонах 172.17.0.0—172.31.255.255 и 192.168.0.0—192.168.255.255. Если подсеть в таком диапазоне уже используется вашим оборудованием, вы можете изменить подсеть во время развертывания MaxPatrol VM при установке роли Deployer. Для этого в наборе конфигурационных параметров **Advanced configuration** необходимо указать в качестве

значения параметра `CustomDockerAddressPool` подсеть, отличную от используемых в вашей организации, а в качестве значения параметра `CustomDockerNetworkSize` — размер подсетей, которые будут использованы внутренними компонентами для работы. Вы также можете изменить подсеть Docker-контейнера по инструкции из раздела «Подсеть Docker-контейнера MaxPatrol VM совпадает с одной из подсетей предприятия» Руководства администратора.

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

- Чтобы установить роль:

1. Если роль устанавливается на сервере с Astra Linux, отключите на этом сервере обязательный ввод пароля для выполнения команды `sudo`:
   ```
   sudo astra-sudo-control disable
   ```
2. Если на сервере, на который устанавливается роль Deployer, есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
   ```
   rm /etc/salt/pki/minion/minion_master.pub
   ```
3. Распакуйте архив `pt_deployer_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_deployer_<Номер версии>.tar.gz
   ```
4. Запустите сценарий:
   ```
   pt_deployer_<Номер версии>/install.sh
   ```
   Начнется проверка сервера на соответствие программным и аппаратным требованиям.

   Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

   Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.
5. Нажмите **Yes**.

   Начнутся распаковка и подготовка пакетов.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль Deployer. Значение по умолчанию — FQDN локального сервера.

   Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
8. Нажмите **OK**.

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

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

Роль установлена.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.6.2. Установка компонента PT MC на Linux

Компонент PT MC необходимо установить на тот же сервер, на который впоследствии будет установлен компонент MP 10 Core.

Установка компонента PT MC делится на следующие этапы:

1. Установка роли SqlStorage.
2. Установка роли LogConnector.
3. Установка роли Observability.
4. Установка роли Management and Configuration.

Внимание! Роль Observability необходимо устанавливать до роли Management and Configuration.

В этом разделе

Установка роли SqlStorage (см. раздел 3.6.2.1)

Установка роли LogConnector (см. раздел 3.6.2.2)

Установка роли Observability (см. раздел 3.6.2.3)

Установка роли Management and Configuration (см. раздел 3.6.2.4)

3.6.2.1. Установка роли SqlStorage

Для установки роли вам потребуется архив `pt_sqlstorage_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_sqlstorage_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_sqlstorage_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_sqlstorage_<Номер версии>/install.sh
   ```
3. Нажмите **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки.
4. Выберите **Create New Application**.
5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MP 10 Core.
8. Введите название экземпляра роли SqlStorage и нажмите **OK**.

   Значение по умолчанию — `sqlstorage`.
9. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера MP 10 Core.

   Значение по умолчанию — FQDN локального сервера.

   Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
10. Нажмите **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.6.2.2. Установка роли LogConnector

Для установки роли вам потребуется архив `pt_logconnector_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы установить роль LogConnector:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_logconnector_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_logconnector_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_logconnector_<Номер версии>/install.sh
   ```
3. Нажмите **Yes**.

   Начнутся распаковка и подготовка пакетов.
4. Введите идентификатор приложения Management and Configuration и нажмите **OK**.

   Значение по умолчанию — `mc-application`.

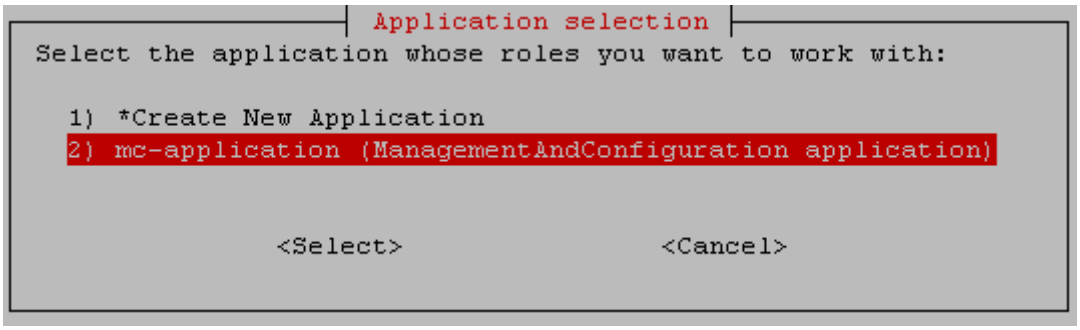

Рисунок 3. Выбор приложения

5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Введите название экземпляра роли и нажмите **OK**.

   Значение по умолчанию — `logconnector`.
8. Выберите **Basic configuration**, чтобы настроить основные параметры роли.
9. Для параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль LogConnector.

Значение по умолчанию — FQDN локального сервера.

Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.

10. Нажмите **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.6.2.3. Установка роли Observability

Для установки роли вам потребуется архив `pt_observability_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы установить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_observability_<Номер версии>.tar.gz`:

     ```
     tar -xf pt_observability_<Номер версии>.tar.gz
     ```

  2. Запустите сценарий:

     ```
     pt_observability_<Номер версии>/install.sh
     ```

  3. Нажмите **Yes**.
  4. Ознакомьтесь с соглашением о сборе телеметрических данных и нажмите **Accept**.
  5. Выберите вариант с идентификатором приложения Management and Configuration.

     Значение по умолчанию — `mc-application`.

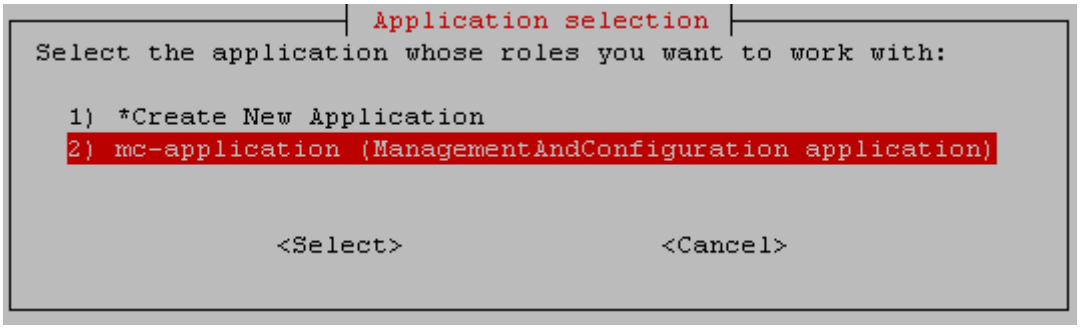

Рисунок 4. Выбор приложения

6. Выберите **Deploy New Instance**.
7. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. Выберите вариант с доменным именем сервера MP 10 Core.
9. Введите название экземпляра роли Observability и нажмите **OK**.

   Значение по умолчанию — `observability`.
10. Выберите **Advanced configuration**.
11. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера MP 10 Core.

    Значение по умолчанию — FQDN локального сервера.

    Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
12. Нажмите **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите **OK**.
14. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

После установки роли Observability вы можете просматривать ключевые показатели приложений и метрики серверов, на которых установлены компоненты MaxPatrol VM. Метрики отображаются на дашборде Grafana по адресу: `https://<IP-адрес или FQDN сервера компонента>:9002` (подробнее см. Руководство администратора).

Подробные инструкции по работе с Grafana приведены на сайте производителя.

3.6.2.4. Установка роли Management and Configuration

Внимание! Если вы устанавливаете MaxPatrol VM в изолированном сегменте сети без прямого подключения к интернету, до установки роли Management and Configuration необходимо установить локальный сервер обновлений, а после установки роли — настроить его в соответствии с инструкциями в разделе «Настройка обновления экспертных данных».

Для установки роли вам потребуется архив `pt_managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы установить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_managementandconfiguration_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_managementandconfiguration_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_managementandconfiguration_<Номер версии>/install.sh
     ```
  3. Нажмите **Yes**.
  4. Выберите вариант с идентификатором приложения Management and Configuration.
  5. Выберите **Deploy New Instance**.
  6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
  7. Выберите вариант с доменным именем сервера MP 10 Core.
  8. Введите название экземпляра роли Management and Configuration и нажмите **OK**.
  9. В качестве значения параметра `DefaultLocale` выберите язык веб-интерфейса приложения Management and Configuration.
  10. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера MP 10 Core.

      Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.

11. В качестве значения параметра `ExpertDataUpdateMethod` выберите:
    - Если обновление экспертных данных будет осуществляться напрямую с сервера обновлений Positive Technologies или с помощью локального сервера обновлений — `Online`.
    - Если вручную — `Offline`.
12. В качестве значения параметра `PackagesSourceUri` укажите:
    - Если вы устанавливаете MaxPatrol VM в сегменте сети с прямым подключением к интернету — один из адресов глобального сервера обновлений — `https://update.ptsecurity.ru/packman/v1/` или `https://update.ptsecurity.com/packman/v1/`.
    - Если в изолированном сегменте сети без прямого подключения к интернету — адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`.

      Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.
13. Нажмите **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
14. Нажмите **OK**.
15. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.6.3. Установка компонента MP 10 Core на Linux

Компонент MP 10 Core устанавливается с помощью ролей RMQ Message Bus и Core в следующем порядке: сначала устанавливается роль RMQ Message Bus, затем роль Core.

Внимание! Для установки компонента MP 10 Core необходимо, чтобы TCP-порт 80 был свободен. Если этот порт занят каким-либо веб-сервером, выключите этот веб-сервер, удалите его или перенесите на другой порт.

В этом разделе

Установка роли RMQ Message Bus на сервер MP 10 Core (см. раздел 3.6.3.1)

Установка роли Core (см. раздел 3.6.3.2)

3.6.3.1. Установка роли RMQ Message Bus на сервер MP 10 Core

Для установки роли вам потребуется архив `pt_rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_rmqmessagebus_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_rmqmessagebus_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_rmqmessagebus_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения MaxPatrol 10 и нажмите кнопку **OK**.
6. Выберите **Deploy New Instance**.
7. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. Выберите вариант с доменным именем сервера MP 10 Core.
9. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.
10. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера MP 10 Core.

    Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
11. Нажмите кнопку **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

Роль установлена.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.6.3.2. Установка роли Core

Для установки роли вам потребуется архив `pt_core_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_core_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_core_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Выберите вариант с идентификатором приложения MaxPatrol 10.
5. Выберите **Deploy New Instance**.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите вариант с доменным именем сервера MP 10 Core.
8. В открывшемся окне введите название экземпляра роли Core и нажмите кнопку **OK**.
9. В качестве значения параметра `DefaultLocale` выберите желаемый язык веб-интерфейса приложения MaxPatrol 10.

10. Укажите значения параметров:

    ```
    AssetGridVersionRangeModeEnabled: True
    HostAddress: <IP-адрес или FQDN сервера MP 10 Core>
    MCAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:3334
    KBAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:8091
    PostgreHost: <IP-адрес или FQDN сервера MP 10 Core>
    RMQHost: <IP-адрес или FQDN сервера MP 10 Core>
    ```

    Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.

11. Нажмите кнопку **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

12. Нажмите кнопку **OK**.

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

Роль установлена.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.7. Активация PT MC

Перед началом активации необходимо войти в PT MC по ссылке `https://<IP-адрес или FQDN сервера PT MC>:3334`. Для входа вам потребуются логин и пароль служебной учетной записи с ролью **Администратор**; также необходимо знать тип учетной записи (локальная или доменная).

При развертывании PT MC автоматически создается служебная учетная запись (логин — `Administrator`, пароль — `P@ssw0rd`) с ролью **Администратор** во всех приложениях и со всеми возможными привилегиями. Эту учетную запись невозможно заблокировать, также невозможно изменить ее логин. После входа в систему рекомендуется сменить пароль этой учетной записи на более сложный.

Для активации PT MC вам потребуется ZIP-файл ключа инсталляции из комплекта поставки.

> **Примечание.** Если ваш комплект не содержит ZIP-файла ключа инсталляции, вы можете запросить его в службе технической поддержки.

Онлайн-активация PT MC

- Чтобы активировать PT MC при наличии доступа к серверу обновлений update.ptsecurity.com:

  1. На странице **Активация платформы** выберите ZIP-файл ключа инсталляции.
  2. Нажмите **Активировать**.

  Примечание. Для онлайн-активации вы можете настроить прокси-сервер (см. раздел 5.5).

Офлайн-активация PT MC

- Чтобы активировать PT MC при отсутствии доступа к серверу обновлений update.ptsecurity.com:

  1. Внизу страницы **Активация платформы** нажмите **Перейти к офлайн-активации**.
  2. Выберите ZIP-файл ключа инсталляции.
  3. Нажмите **Далее**.
  4. Нажмите **Скачать файл**.

     Начнется скачивание файла фингерпринта.
  5. Отправьте файл фингерпринта сотруднику вашей компании, ответственному за работу с лицензиями.

     Ответственный сотрудник передаст файл фингерпринта менеджеру Positive Technologies, представителю компании-интегратора или в службу технической поддержки. После этого ответственный сотрудник передаст вам ZIP-файл с лицензиями, который необходимо использовать на следующем шаге активации.
  6. Нажмите **Далее**.
  7. Выберите ZIP-файл с лицензиями, полученный от ответственного сотрудника.
  8. Нажмите **Далее**.

Файлы для активации лицензии

Оба сценария активации лицензии в PT MC включают использование уникальных ZIP-файлов. В первом сценарии (для онлайн-активации) достаточно одного файла, который называется ZIP-файлом ключа инсталляции. Для офлайн-активации требуется и ZIP-файл ключа инсталляции, и ZIP-файл с лицензиями.

> **Примечание.** В случае онлайн-активации PT MC с последующей установкой локального сервера обновлений также потребуется ZIP-файл с лицензиями. Его необходимо скачать в приложении PT MC. Для этого потребуется перейти на страницу **Лицензии** и нажать **Скачать**.

Таблица 8. Характеристики файлов для лицензирования

	ZIP-файл ключа инсталляции	**ZIP-файл с лицензиями**
Имя по умолчанию	`installation_key.zip`	`license_keys.zip`
Обязательные компоненты	Ключ инсталляции: `installation_key.key`	Ключ инсталляции: `installation_key.key`; Локализация для сервиса лицензирования: `localization.json`
Необязательные компоненты		Один или несколько ключей лицензии, например `license_key_123.key`
Сценарий активации	Онлайн	Офлайн

Примечание. Если вы используете PT MC без привязанных продуктов, в файле с лицензиями может содержаться только ключ инсталляции и файл локализации для сервиса лицензирования.

См. также

Настройка прокси-сервера для онлайн-активации PT MC (см. раздел 5.5)

3.8. Активация лицензии MaxPatrol VM

Для работы MaxPatrol VM необходимо активировать лицензию.

Перед активацией лицензии MaxPatrol VM необходимо установить и активировать PT MC. Активация лицензии MaxPatrol VM выполняется в интерфейсе PT MC. Для активации необходима учетная запись с ролью администратора.

Активация лицензии MaxPatrol VM состоит из следующих этапов:

1. Добавление в PT MC лицензии продукта.

Примечание. При первой активации PT MC приобретенные лицензии добавляются автоматически. Если вы устанавливаете экземпляр MaxPatrol VM, который интегрирован с уже действующим компонентом PT MC, нужно добавить лицензию MaxPatrol VM по инструкции.

2. Привязка лицензии к приложению MaxPatrol VM.

Информация о лицензии доступна в интерфейсе PT MC на странице **Лицензии**.

Добавление лицензии

- Чтобы добавить лицензию при наличии доступа к интернету:

  1. В главном меню выберите **Лицензии**.
  2. Нажмите **Обновить список лицензий**.

Для добавления лицензии вручную вам потребуется ZIP-файл с лицензией из комплекта поставки.

Примечание. Если ваш комплект не содержит ZIP-файла с лицензией, вы можете запросить его в службе технической поддержки.

- Чтобы добавить лицензию вручную, без доступа к интернету:

  1. В главном меню выберите **Лицензии**.
  2. Нажмите **Добавить**.
  3. Выберите ZIP-файл с лицензией.

     Примечание. Файл может содержать как одну, так и несколько лицензий. В систему будут добавлены все корректные лицензии, которые содержатся в файле.
  4. Нажмите **Добавить**.

Теперь вы можете привязать лицензию к приложению.

Привязка лицензии

- Чтобы привязать лицензию к приложению:

  1. В главном меню выберите **Лицензии**.
  2. Выберите лицензию и нажмите **Привязать**.
  3. Выберите установленное приложение, к которому нужно привязать лицензию.
  4. Нажмите **Привязать**.

После привязки лицензии необходимо перезапустить службу компонента MP 10 Core с помощью команды `docker restart $(docker ps -q -a)`, а затем выйти из системы и заново войти.

Теперь вам доступны функции приложения, которые включены в лицензию.

3.9. Установка компонента MP 10 Collector

В этом разделе приведены инструкции по установке компонента MP 10 Collector на Linux и на Microsoft Windows.

> **Внимание!** Если MP 10 Collector установлен на Linux, MaxPatrol VM не сможет выполнять поиск файлов в режиме пентеста. Использование протокола Kerberos доступно с ограничениями и зависит от профиля для сбора данных. Производительность MP 10 Collector, установленного на Linux, в режиме пентеста в целом на 15—40% ниже, чем установленного на Microsoft Windows.
>
> **Внимание!** Если MP 10 Collector установлен на Microsoft Windows, MaxPatrol VM не сможет собирать события с профилем KafkaEventCollector.

Установка компонента на Linux выполняется с помощью роли Collector. Если MP 10 Collector устанавливается на отдельный сервер, перед установкой роли необходимо установить на этот сервер модуль Salt Minion.

Если MP 10 Collector устанавливается на Linux и на этом сервере уже установлен Kaspersky Endpoint Security, необходимо обновить антивирусные базы Kaspersky Endpoint Security и включить компонент Kaspersky Security Network (KSN).

> **Внимание!** Если на сервере, на котором развертывается компонент, уже установлена роль Deployer, установка модуля Salt Minion не требуется.

В этом разделе

Установка модуля Salt Minion на сервер MP 10 Collector (см. раздел 3.9.1)

Установка роли Collector (см. раздел 3.9.2)

Установка компонента MP 10 Collector на Microsoft Windows (см. раздел 3.9.3)

3.9.1. Установка модуля Salt Minion на сервер MP 10 Collector

Внимание! На сервере, на который устанавливается модуль Salt Minion, должен быть открыт доступ по SSH (например, через порт 22/TCP).

- Чтобы установить модуль Salt Minion:

  1. Если на сервере MP 10 Collector есть файл `/etc/salt/pki/minion/minion_master.pub`, удалите его:
     ```
     rm /etc/salt/pki/minion/minion_master.pub
     ```
  2. Если MP 10 Collector устанавливается на Astra Linux, на сервере MP 10 Collector отключите обязательный ввод пароля для выполнения команды `sudo`:
     ```
     sudo astra-sudo-control disable
     ```

3. Если MP 10 Collector устанавливается на Debian, на сервере компонента установите утилиту `sudo`, выполнив в интерфейсе терминала команду от имени суперпользователя (root):
   ```
   apt-get install sudo
   ```
4. Если MP 10 Collector устанавливается на Debian, на сервере компонента отключите обязательный ввод пароля для выполнения команды `sudo`, добавив в файл `etc/sudoers` строку:
   ```
   <Логин учетной записи, от имени которой устанавливается компонент> ALL=(ALL:ALL) NOPASSWD: ALL
   ```
5. На сервере с установленной ролью Deployer запустите сценарий:
   ```
   /var/lib/deployer/role_packages/Deployer_<Номер версии>/deploy_minion.sh
   ```
6. В открывшемся окне введите IP-адрес или FQDN сервера MP 10 Collector и нажмите кнопку **OK**.

   Внимание! Если в параметре `HostAddress` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
7. В открывшемся окне введите логин учетной записи, от имени которой устанавливается компонент, на сервере MP 10 Collector и нажмите кнопку **OK**.
8. В окне **Info** нажмите **OK**.
9. Введите пароль учетной записи с правами суперпользователя (root) на сервере MP 10 Collector.

   Запустится установка модуля Salt Minion.
10. Если требуется, введите FQDN сервера и нажмите **OK**.

    По завершении установки появится сообщение `Minion on '<IP-адрес или FQDN сервера>' successfully installed`.

3.9.2. Установка роли Collector

Для установки роли вам потребуется архив `pt_agent-linux_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_agent-linux_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_agent-linux_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_agent-linux_<Номер версии>/install.sh
   ```
3. Нажмите **Yes**.
4. Выполните одно из следующих действий:

- Если для выбора доступен вариант с идентификатором установленного ранее приложения MaxPatrol 10 — выберите этот вариант.
- Если вариант с идентификатором установленного ранее приложения MaxPatrol 10 отсутствует — выберите вариант **Create New Application**.

5. Если вы выбрали вариант **Create New Application**, введите идентификатор приложения MaxPatrol 10 и нажмите **OK**.
6. Выберите **Deploy New Instance**.
7. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. Выберите вариант с доменным именем сервера MP 10 Collector.
9. Введите название экземпляра роли Collector и нажмите **OK**.
10. Выберите вариант **Advanced configuration**.

    Откроется страница со списком параметров.
11. В качестве значения параметра `AgentName` введите название коллектора, которое будет отображаться в веб-интерфейсе приложения **MaxPatrol 10**.
12. В качестве значения параметра `AgentRMQHost` укажите IP-адрес или FQDN сервера MP 10 Core.

    Внимание! Если в параметре `AgentRMQHost` указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
13. В качестве значения параметра `AgentRMQVirtualHost` выберите **Core**.
14. Нажмите **OK**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу `Y`. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
15. Нажмите **OK**.
16. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.9.3. Установка компонента MP 10 Collector на Microsoft Windows

Для установки компонента MP 10 Collector на Microsoft Windows вам потребуется архив `pt_agent-windows_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы установить компонент MP 10 Collector:

  1. Запустите файл `MPXAgentSetup_<Номер версии>.exe`.
  2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
  3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите **Продолжить**.
  4. Укажите пути для установки.

     Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.
  5. Нажмите **Продолжить**.
  6. Введите имя коллектора, которое будет отображаться в интерфейсе MaxPatrol VM.
  7. В блоке параметров **Адрес обработчика данных** в раскрывающемся списке выберите значение **Core** и укажите в поле IP-адрес или полное доменное имя (FQDN) сервера MP 10 Core.

     Внимание! Если в поле указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
  8. Нажмите **Продолжить**.

     Мастер установки выполнит проверку указанных вами параметров и отобразит их после проверки.

     Примечание. По результатам проверки мастер может отображать сообщения о некорректных значениях указанных параметров. В этом случае вам необходимо вернуться, нажимая **Назад**, и указать корректные значения параметров.
  9. Нажмите **Установить**.
  10. По завершении установки нажмите **Закрыть**.
  11. Если компонент MP 10 Core установлен на Linux, на сервере с установленной ролью Deployer выполните команды:

      ```
      deployer cacert import /opt/deployer/pki/legacy_ca/windows-selfsigned-default.crt
      deployer instance reconfigure -RoleTypeId RmqMessageBus
      ```

Примечание. При последующей установке коллекторов на Windows реконфигурация ролей не требуется.

12. Если компонент MP 10 Core установлен на Linux, перезапустите службу Core Agent.

    Примечание. При последующей установке коллекторов на Windows перезапуск службы не требуется.

13. Для подключения модуля Salt Minion к модулю Salt Master выполните команду:

    ```
    saltcfg set -p SaltMasterHost <IP-адрес или FQDN сервера с модулем Salt Master>
    ```

3.10. Настройка подключения к Collector, расположенному в недоверенном сегменте

Внимание! Эту инструкцию рекомендуется выполнять только в инфраструктурах, где соединения инициируются из более доверенного сегмента в менее доверенный. В остальных случаях достаточно выполнить инструкции в общем разделе (см. раздел 3.9).

Для отправки данных от MP 10 Collector, расположенного в недоверенном сегменте, в MP 10 Core, расположенный в доверенном сегменте, необходимо настроить подключение так, чтобы соединение могло устанавливаться только со стороны MP 10 Core.

Для настройки подключения необходимо установить роли Deployer, Collector и RMQ Message Bus. Вы можете установить их на один сервер или на разные. В одном недоверенном сегменте вы можете развернуть несколько MP 10 Collector и подключить их к одному серверу с ролью Deployer.

Внимание! Если недоверенных сегментов несколько и взаимодействие между ними запрещено, роли Deployer, Collector и RMQ Message Bus необходимо развернуть в каждом недоверенном сегменте.

Порядок настройки подключения на серверах в недоверенном сегменте:

1. Установка второго экземпляра роли Deployer в соответствии с инструкцией «Установка роли Deployer» Руководства по внедрению.
2. Добавление сертификатов (см. раздел 3.10.1) для установленных экземпляров роли Deployer.
3. Установка роли Collector в соответствии с инструкцией «Установка роли Collector» Руководства по внедрению. Установить роль Collector можно как на сервере с установленной ролью Deployer, так и на отдельном сервере. При установке каждой роли Collector необходимо указать в качестве значения параметра `AgentRMQHost` IP-адрес или FQDN сервера с ролью RMQ Message Bus, установленной в недоверенном сегменте.

   Примечание. Если MP 10 Collector устанавливается на отдельный сервер, перед установкой роли необходимо установить на этот сервер модуль Salt Minion. Если на сервере, на котором устанавливается компонент MP 10 Collector, уже установлена роль Deployer, установка модуля Salt Minion не требуется. Подробное описание установки модуля см. в разделе «Установка модуля Salt Minion на сервер MP 10 Collector» Руководства по внедрению.

4. Установка роли RMQ Message Bus на серверах с установленными экземплярами роли Collector в соответствии с инструкцией «Установка роли RMQ Message Bus на сервер MP 10 Core» Руководства по внедрению.

   Примечание. Если в одном недоверенном сегменте находятся несколько серверов с установленной ролью Collector, необходимо обеспечить связь каждого их них с ролью RMQ Message Bus, установленной в недоверенном сегменте. Если недоверенных сегментов несколько, то необходимо установить в каждом из них один сервер с ролью Deployer и один сервер с ролью RMQ Message Bus.

5. Настройка подключения компонента MaxPatrol 10 Core к MP 10 Collector и RMQ Message Bus, установленным в недоверенном сегменте.

Если требуется обновить систему, сначала нужно обновить роли в основной инсталляции MaxPatrol VM, затем — на серверах в недоверенном сегменте.

Порядок обновления ролей на серверах в недоверенном сегменте:

1. Обновление роли Deployer в соответствии с инструкцией «Обновление роли Deployer» Руководства по внедрению.
2. Обновление роли RMQ Message Bus в соответствии с инструкцией «Обновление роли RMQ Message Bus на сервере MP 10 Core» Руководства по внедрению.
3. Обновление роли Collector в соответствии с инструкцией «Обновление компонента MP 10 Collector на Linux» Руководства по внедрению.

В этом разделе

Добавление сертификата роли Deployer из защищенного сегмента сети в доверенные сертификаты основной роли Deployer (см. раздел 3.10.1)

Настройка подключения MP 10 Core к Collector на Linux (см. раздел 3.10.2)

Настройка подключения MP 10 Core к Collector на Windows (см. раздел 3.10.3)

3.10.1. Добавление сертификата роли Deployer из защищенного сегмента сети в доверенные сертификаты основной роли Deployer

После установки дополнительных экземпляров роли Deployer необходимо добавить сертификаты этих экземпляров в доверенные сертификаты основного экземпляра роли Deployer.

- Чтобы добавить сертификат:

  1. Скопируйте сгенерированный при установке дополнительного экземпляра роли Deployer файл сертификата `rootCA.crt` из каталога `/opt/deployer/pki/` в рабочий каталог пользователя основного экземпляра роли Deployer.
  2. На сервере с основным экземпляром роли Deployer выполните команду:

     ```
     deployer cacert import <Путь к рабочему каталогу пользователя>/rootCA.crt
     deployer instance reconfigure -RoleTypeId RmqMessageBus
     ```

3.10.2. Настройка подключения MP 10 Core к Collector на Linux

После установки ролей Collector и RMQ Message Bus необходимо настроить подключение MP 10 Core к Collector. Для этого необходимо создать и настроить очередь RabbitMQ, а также настроить плагин Shovel для отправки сообщений из очереди.

Создание очереди RabbitMQ

- Чтобы создать очередь:

  1. Войдите в веб-интерфейс RabbitMQ MP 10 Core по адресу `http://<IP-адрес сервера MP 10 Core>:15672`.
  2. Выберите **Queues and Streams** → **Add a new queue**.
  3. Выберите **Virtual host** → **mpx**.
  4. Выберите **Type** → **Classic**.
  5. В поле **Name** введите `fwd_agentlinux.v2`.
  6. Нажмите **Add queue**.

     Примечание. Для каждого подключаемого коллектора необходимо создать отдельную очередь.

Настройка очереди RabbitMQ

Инструкцию необходимо выполнить шесть раз — для каждого ключа маршрутизации:

- `agent.<Идентификатор коллектора>.query_config`;
- `agent.<Идентификатор коллектора>.rmq.heartbeat`;
- `agent.<Идентификатор коллектора>.command_package`;
- `agent.<Идентификатор коллектора>.event_package_ack`;
- `agent.<Идентификатор коллектора>.reset`;
- `agent.<Идентификатор коллектора>.job.*.query_artifacts`.

- Чтобы настроить очередь:

  1. В таблице выберите созданную ранее очередь.

     Откроется страница с информацией об очереди.

  2. В блоке параметров **Bindings** → **Add binding to this queue** в поле **From exchange** введите `pt.mpx.agent.v2`.

  3. В поле **Routing key** введите ключ маршрутизации (например, `agent.e829c7ce-2e57-42be-bc43-6eb442c0992f.query_config`).

     Примечание. Идентификатор коллектора вы можете найти в его конфигурационном файле `/opt/core-agent/config.json`.

  4. Нажмите **Bind**.

Настройка плагина Shovel для отправки сообщений из очереди

- Чтобы настроить плагин:

  1. На узле, с которого производится настройка плагина, запустите терминальный клиент, поддерживающий сетевой протокол SSH.

  2. Подключитесь по протоколу SSH к серверу MP 10 Core.

  3. Выполните команду для настройки Shovel для отправки сообщений в MP 10 Collector от Core:

     ```
     sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
     -p mpx shovel fwdcoretoagent '{"src-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/
     usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/
     RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
     RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
     nal", "dest-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?cacertfile=/usr/local/share/
     rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/
     RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
     RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
     nal", "src-queue": "fwd_agentlinux.v2"}'
     ```

  4. Выполните команду для настройки Shovel для отправки сообщений в MP 10 Core от Collector:

     ```
     sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
     -p mpx shovel <--> '{"src-uri": "amqps:///<Уникальное имя правила Shovel>?cacertfile=/usr/
     local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local /share/rabbitmq/certs/
     RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.
     pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=external", "dest-
     uri": "amqps://<IP-адрес сервера RMQ Message Bus> /mpx?cacertfile=/usr/local/share/
     rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs /
     RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.
     pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=external", "src-
     exchange": "<Имя очереди обработки данных>", "src-exchange-key": "<Ключ маршрутизации>"}'
     ```

     Примечание. Имя очереди обработки данных и соответствующий ему ключ маршрутизации вы можете выбрать с помощью таблицы ниже.

Пример:

```
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.config '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.config"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.command_package_ack '{"src-uri": "amqps://<IP-адрес RMQ
Collector'a>/mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/
local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.command_package_ack"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.event_package '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.event_package"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.command_package_rejection '{"src-uri": "amqps://<IP-адрес RMQ
Collector'a>/mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/
local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.command_package_rejection"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.artifacts '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.job.*.artifacts"}'
```

```
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.progress '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.job.*.progress"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.progress '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.job.*.result.audit_check"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.progress '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.job.*.result.asset.event"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.result.model '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/
mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/
rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.job.*.result.model"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.savepoint '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.job.*.savepoint"}'
```

```
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.keepalive '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.keepalive"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel pt.mpx.incidents.events.v4 '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/
mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/
rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.incidents.events", "src-exchange-key":
"pt.mpx.incidents.events.v4"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel monitoring '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?cacertfile=/
usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.monitoring", "src-exchange-key": "monitoring"}'
```

Таблица 9. Имена очередей обработки данных и ключи маршрутизации

Имя очереди обработки данных	Ключ маршрутизации
pt.mpx.agent.v2	agent.*.config
pt.mpx.agent.v2	agent.*.command_package_ack
pt.mpx.agent.v2	agent.*.event_package
pt.mpx.agent.v2	agent.*.command_package_rejection
pt.mpx.agent.v2	agent.*.job.*.artifacts
pt.mpx.agent.v2	agent.*.job.*.progress
pt.mpx.agent.v2	agent.*.job.*.result.asset.event
pt.mpx.agent.v2	agent.*.job.*.result.asset.event
pt.mpx.agent.v2	agent.*.job.*.result.model
pt.mpx.agent.v2	agent.*.job.*.savepoint
pt.mpx.agent.v2	agent.*.keepalive

Имя очереди обработки данных	Ключ маршрутизации
`rpt.mpx.incidents.events`	`pt.mpx.incidents.events.v4`
`pt.mpx.monitoring`	`monitoring`

Вы можете проверить корректность настройки на вкладке **Admin** → **Shovel Status** в веб-интерфейсе RabbitMQ на сервере MP 10 Core. В таблице **Shovel Status** в столбце **State** все экземпляры Shovel должны иметь статус running.

Проверка подключения MP 10 Core к MP 10 Collector

- Чтобы проверить подключение:

  1. Войдите в веб-интерфейс MaxPatrol VM.
  2. На странице **Система** → **Управление системой** выберите **Коллекторы**.
  3. Если коллектор имеет статус **Недоступен**, перезапустите службу Core Agent.

     Примечание. Если после перезапуска службы проблема сохраняется, необходимо сохранить файлы журналов коллектора и отправить их в службу технической поддержки.
  4. Если коллектор имеет статус **Доступен**, создайте и запустите задачу на сбор данных с профилем HostDiscovery для проверки подключения к коллектору.

3.10.3. Настройка подключения MP 10 Core к Collector на Windows

После установки ролей Collector и RMQ Message Bus необходимо настроить подключение MP 10 Core к Collector. Для этого необходимо добавить сертификаты для RabbitMQ, создать и настроить очередь RabbitMQ, а также настроить плагин Shovel для отправки сообщений из очереди.

Добавление сертификатов для RabbitMQ

- Чтобы добавить сертификаты:

  1. На сервере с ролью Deployer создайте SLS-файл `/var/lib/deployer/role_packages/deployer/generate_custom_cert.sls`.

     Пример содержимого файла:

```
{%- macro generate_remote_signed_cert(common_name, cert, key, dns_subjects=['example.ru',
'localhost'], ip_subjects=['127.0.0.1', '10.10.248.163']) %}
{{ key }}:
 x509.private_key_managed:
  - bits: 2048
  - backup: True
{% set dns_subjects = (dns_subjects + [common_name, 'localhost'])|unique %}
```

```
{% set ip_subjects = (ip_subjects + ['127.0.0.1'])|unique %}
{% set subjects = [] %}
{% for name in dns_subjects %}{% do subjects.append('DNS:'~name) %}{%endfor%}
{% for ip in ip_subjects %}{% do subjects.append('IP:'~ip) %}{%endfor%}
Certificate {{ cert }}:
 x509.certificate_managed:
  - name: {{ cert }}
  - ca_server: {{pillar.deployer.pki.ca_server}}
  - signing_policy: {{pillar.deployer.pki.ssl_signing_policy}}
  - public_key: {{ key }}
  - private_key: {{ key }}
  - CN: {{ common_name }}
  - subjectAltName: {{subjects|join(', ')}}
  - keyUsage: "digitalSignature, dataEncipherment, keyEncipherment, keyAgreement"
  - extendedkeyUsage: "serverAuth, clientAuth"
  - C: RU
  - ST: None
  - L: Moscow
  - O: Company Name
  - OU: None
  - Mail: companyname@example.com
  - days_valid: 1825
  - days_remaining: 10
  - require:
   - x509: {{ key }}
  - backup: True
{%- endmacro %}
{{ generate_remote_signed_cert('Test', '/tmp/RMQ_Server.crt', '/tmp/RMQ_Server.pem',
dns_subjects= ['localhost', 'test.ru', 'example.ru'], ip_subjects=['127.0.0.1',
'10.10.248.163']) }}
```

Примечание. В качестве значений параметров `dns_subjects` и `ip_subjects` необходимо указать IP-адреса и FDQN серверов, на которых установлены коллекторы.

2. Для создания ключа и сертификата выполните команду:

   ```
   sudo salt-call state.apply deployer.generate_custom_cert
   ```

   Будут созданы ключ `RMQ_Server.pem` и сертификат `RMQ_Server.crt` внутри временного каталога `/tmp`.

3. Переместите файлы сертификатов с сервера с ролью Deployer на сервер с ролью Collector в соответствии с таблицей ниже.

4. На сервере с ролью Deployer выполните команды для генерации сертификатов `RMQ_Agent_Client.csr`, `RMQ_Agent_Client.crt`:

   ```
   openssl req -new -sha256 -nodes -newkey rsa:2048 -keyout RMQ_Agent_Client.key -subj '/
   CN=agent' -out RMQ_Agent_Client.csr
   openssl x509 -req -in RMQ_Agent_Client.csr -CA /opt/deployer/pki/rootCA.crt -CAkey /opt/
   deployer/pki/rootCA.key -days 356 -CAcreateserial -out RMQ_Agent_Client.crt
   ```

5. Замените существующие сертификаты `rootCA.crt`, `RMQ_Agent_Client.csr`, `RMQ_Agent_Client.crt` на сервере с ролью Collector (например, в папке `C:\Program Files (x86)\Positive Technologies\MP 10 Collector\.install\scripts\Certificates`) сертификатами, сгенерированными на сервере с ролью Deployer.
6. На сервере с ролью Collector перезапустите RabbitMQ с помощью команды:
   `rabbitmqcfg restart`

Таблица 10. Соответствие файлов сертификатов и путей к файлам

Имя файла на сервере с ролью Deployer	Путь к файлу на сервере с ролью Collector
`/tmp/RMQ_Server.crt`	`C:\ProgramData\RabbitMQ\tls\RMQ_Server.crt`
`/tmp/RMQ_Server.pem`	`C:\ProgramData\RabbitMQ\tls\RMQ_Server.pem`
`/var/lib/deployer/role_packages/deployer/rootCA.crt`	`C:\ProgramData\RabbitMQ\tls\rootCA.crt`

Создание очереди RabbitMQ

- Чтобы создать очередь:

1. Войдите в веб-интерфейс RabbitMQ MP 10 Core по адресу `http://<IP-адрес сервера MP 10 Core>:15672`.
2. Выберите **Queues and Streams** → **Add a new queue**.
3. Выберите **Virtual host** → **mpx**.
4. Выберите **Type** → **Classic**.
5. В поле **Name** введите `fwd_agentlinux.v2`.
6. Нажмите **Add queue**.

   Примечание. Для каждого подключаемого коллектора необходимо создать отдельную очередь.

Настройка очереди RabbitMQ

Инструкцию необходимо выполнить шесть раз — для каждого ключа маршрутизации:

— `agent.<Идентификатор коллектора>.query_config`;

— `agent.<Идентификатор коллектора>.rmq.heartbeat`;

- `agent.<Идентификатор коллектора>.command_package`;
- `agent.<Идентификатор коллектора>.event_package_ack`;
- `agent.<Идентификатор коллектора>.reset`;
- `agent.<Идентификатор коллектора>.job.*.query_artifacts`.

► Чтобы настроить очередь:

1. В таблице выберите созданную ранее очередь.
2. В блоке параметров **Bindings** → **Add binding to this queue** в поле **From exchange** введите `pt.mpx.agent.v2`.
3. В поле **Routing key** введите ключ маршрутизации (например, `agent.e829c7ce-2e57-42be-bc43-6eb442c0992f.query_config`).

   Примечание. Идентификатор коллектора вы можете найти в его конфигурационном файле `/opt/core-agent/config.json`.
4. Нажмите **Bind**.

Настройка плагина Shovel для отправки сообщений из очереди

► Чтобы настроить плагин:

1. На узле, с которого производится настройка плагина, запустите терминальный клиент, поддерживающий сетевой протокол SSH.
2. Подключитесь по протоколу SSH к серверу MP 10 Core.
3. Выполните команду для настройки Shovel для отправки сообщений в MP 10 Collector от Core:

   ```
   sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
   -p mpx shovel fwdcoretoagent '{"src-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/
   usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/
   RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
   RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
   nal", "dest-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?cacertfile=/usr/local/share/
   rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/
   RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
   RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
   nal", "src-queue": "fwd_agentlinux.v2"}'
   ```
4. Выполните команду для настройки Shovel для отправки сообщений в MP 10 Core от Collector:

   ```
   sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
   -p mpx shovel <--> '{"src-uri": "amqps:///<Уникальное имя правила Shovel>?cacertfile=/usr/
   local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local /share/rabbitmq/certs/
   RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.
   pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=external", "dest-
   uri": "amqps://<IP-адрес сервера RMQ Message Bus> /mpx?cacertfile=/usr/local/share/
   rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs /
   ```

```
RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.
pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=external", "src-
exchange": "<Имя очереди обработки данных>", "src-exchange-key": "<Ключ маршрутизации>"}'
```

Примечание. Имя очереди обработки данных и соответствующий ему ключ маршрутизации вы можете выбрать с помощью таблицы ниже.

Пример:

```
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.config '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.config"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.command_package_ack '{"src-uri": "amqps://<IP-адрес RMQ
Collector'a>/mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/
local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.command_package_ack"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.event_package '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.event_package"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.command_package_rejection '{"src-uri": "amqps://<IP-адрес RMQ
Collector'a>/mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/
local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.command_package_rejection"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.artifacts '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
```

```
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.job.*.artifacts"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.progress '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.job.*.progress"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.progress '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.job.*.result.audit_check"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.progress '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.job.*.result.asset.event"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.result.model '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/
mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/
rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key":
"agent.*.job.*.result.model"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.job.savepoint '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
```

```
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.job.*.savepoint"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel agent.01.keepalive '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?
cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/
certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.agent.v2", "src-exchange-key": "agent.*.keepalive"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel pt.mpx.incidents.events.v4 '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/
mpx?cacertfile=/usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/
rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.incidents.events", "src-exchange-key":
"pt.mpx.incidents.events.v4"}'
sudo docker exec -ti $(sudo docker ps -q --filter name=rabbitmq) rabbitmqctl set_parameter
-p mpx shovel monitoring '{"src-uri": "amqps://<IP-адрес RMQ Collector'a>/mpx?cacertfile=/
usr/local/share/rabbitmq/certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.crt&keyfile=/usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "dest-uri": "amqps://<IP-адрес RMQ Core>/mpx?cacertfile=/usr/local/share/rabbitmq/
certs/rootCA.crt&certfile=/usr/local/share/rabbitmq/certs/RMQ_SIEM_Client.crt&keyfile=/
usr/local/share/rabbitmq/certs/
RMQ_SIEM_Client.pem&verify=verify_peer&server_name_indication=disable&auth_mechanism=exter
nal", "src-exchange": "pt.mpx.monitoring", "src-exchange-key": "monitoring"}'
```

Таблица 11. Имена очередей обработки данных и ключи маршрутизации

Имя очереди обработки данных	Ключ маршрутизации
pt.mpx.agent.v2	agent.*.config
pt.mpx.agent.v2	agent.*.command_package_ack
pt.mpx.agent.v2	agent.*.event_package
pt.mpx.agent.v2	agent.*.command_package_rejection
pt.mpx.agent.v2	agent.*.job.*.artifacts
pt.mpx.agent.v2	agent.*.job.*.progress
pt.mpx.agent.v2	agent.*.job.*.result.asset.event
pt.mpx.agent.v2	agent.*.job.*.result.asset.event

Имя очереди обработки данных	Ключ маршрутизации
pt.mpx.agent.v2	agent.*.job.*.result.model
pt.mpx.agent.v2	agent.*.job.*.savepoint
pt.mpx.agent.v2	agent.*.keepalive
rpt.mpx.incidents.events	pt.mpx.incidents.events.v4
pt.mpx.monitoring	monitoring

Вы можете проверить корректность настройки на вкладке **Admin** → **Shovel Status** в веб-интерфейсе RabbitMQ на сервере MP 10 Core. В таблице **Shovel Status** в столбце **State** все экземпляры Shovel должны иметь статус running.

Проверка подключения MP 10 Core к MP 10 Collector

- Чтобы проверить подключение:

  1. Войдите в веб-интерфейс MaxPatrol VM.
  2. На странице **Система** → **Управление системой** выберите **Коллекторы**.
  3. Если коллектор имеет статус **Недоступен**, перезапустите службу Core Agent.

     Примечание. Если после перезапуска службы проблема сохраняется, необходимо сохранить файлы журналов коллектора и отправить их в службу технической поддержки.
  4. Если коллектор имеет статус **Доступен**, создайте и запустите задачу на сбор данных с профилем HostDiscovery для проверки подключения к коллектору.

3.11. Установка компонента PT UCS

Внимание! Компонент PT UCS и роль Deployer необходимо устанавливать на один сервер.

Если MaxPatrol VM установлен в закрытом сегменте сети, в PT UCS необходимо настроить загрузку новых версий компонентов с локального сервера обновлений. Для этого необходимо до установки PT UCS создать файл `/etc/salt/master.d/ucs_user.conf` со следующим содержимым:

```
updater:
 frontend_update_server:
  host: <Адрес локального сервера обновлений>:<Порт для подключения по протоколу HTTPS>
```

По умолчанию локальный сервер обновлений использует для подключения по протоколу HTTPS порт 8743.

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL. Для корректной работы сертификата необходимо назвать файл сертификата `cert.crt`, а файл его ключа `cert.key` — и поместить эти файлы в каталог `/etc/pt-update-mirror/https_certs/` на локальном сервере обновлений. Затем необходимо перезапустить сервис с помощью команды `sudo systemctl restart pt-update-mirror.service`.

- Чтобы установить компонент PT UCS:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_ucs_<Номер версии MaxPatrol VM>.tar.gz`:

     ```
     tar -xf pt_ucs_<Номер версии MaxPatrol VM>.tar.gz -C <Путь к каталогу для распаковки архива>
     ```

  2. Запустите сценарий:

     ```
     <Путь к каталогу для распаковки архива>/pt_ucs_<Номер версии MaxPatrol VM>/install.sh
     ```

  3. Нажмите **Да**.
  4. Выберите вариант с идентификатором приложения MaxPatrol 10.
  5. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
  6. Выберите вариант с доменным именем сервера роли Deployer.
  7. Введите название экземпляра роли UCS и нажмите **OK**.
  8. Выберите **Skip configuration**.
  9. Нажмите **OK**.

     Начнется проверка сервера на соответствие программным и аппаратным требованиям.

     Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

     Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

По завершении установки компонент PT UCS готов к работе, его настройка не требуется. Проверка наличия новых версий модуля Pentest для коллекторов, а также их загрузка и установка будут происходить автоматически.

В результате установки роли (в том числе и неуспешной), в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `installReports` с отчетами об установке. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

3.12. Установка доверенного сертификата для сайта MaxPatrol VM

При развертывании MaxPatrol VM для его сайта автоматически устанавливается самоподписанный сертификат, поставляемый в составе дистрибутива. Поэтому при попытке подключения к сайту вы получите предупреждение о том, что создаваемое подключение не защищено.

Вы можете установить собственный доверенный сертификат, который должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM, синтаксис PKCS #1, длиной не менее 2048 бит с заголовком `BEGIN RSA PRIVATE KEY` без дополнительных заголовков;

  Примечание. Чтобы расшифровать зашифрованный с помощью алгоритма RSA ключ, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.
- включать область применения сертификата Digital Signature или Key Encipherment;
- в расширении Extended Key Usage (EKU) содержать записи `serverAuth` и `clientAuth`;
- иметь расширение .crt;
- в расширении Subject Alternative Name (SAN) содержать запись об FQDN сервера компонента или его IP-адресе в зависимости от значения параметра `HostAddress` (оно может содержать как FQDN, так и IP-адрес).

Во время выполнения команды импорта пользовательские корневые сертификаты автоматически проверяются на соответствие требованиям безопасности. Выявленные несоответствия отображаются в терминале. Автоматизация проверки позволяет исключить риск установки потенциально небезопасных сертификатов.

Внимание! Если в сертификате указан URL-адрес списка отозванных сертификатов, необходимо обеспечить к нему доступ из контейнеров приложений, иначе система не сможет считать сертификат доверенным. Для проверки доступа вы можете перейти к указанному адресу в Docker-контейнере каждого приложения.

- Чтобы установить доверенный сертификат на Linux:

  1. На сервере MP 10 Core разместите файлы сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для каждой роли Core, Observability и Management and Configuration.
  2. Разместите файлы пользовательских корневых сертификатов в рабочем каталоге пользователя на сервере с установленной ролью Deployer.

     Примечание. Каждый сертификат должен находиться в отдельном файле с расширением .crt.
  3. Выполните команду:

     ```
     deployer cacert import <Путь к корневому сертификату> <Путь к промежуточному сертификату 1> … <Путь к промежуточному сертификату N> -verbose
     ```

     Внимание! Путь к корневому сертификату необходимо указать первым. Пути к промежуточным сертификатам можно указать в любом порядке.
  4. Измените конфигурации (см. раздел 5.2) ролей Core, Observability и Management and Configuration:

     ```
     SSLCertificatePemFileName: <Имя файла сертификата>
     SSLKeyFileName: <Имя файла закрытого ключа>
     ```

     Например:

     ```
     SSLCertificatePemFileName: website.crt
     SSLKeyFileName: website.key
     ```

В рамках установки доверенного сертификата для роли Observability также будут установлены сертификаты для всех служб роли (Grafana, OpenTelemetry Collector, VictoriaMetrics, TelemetryTracker).

Внимание! Имена файлов сертификата и ключа не должны совпадать с именами файлов, которые уже находятся в папке сертификатов: замена содержимого стандартных файлов приведет к некорректной работе системы.

См. также

Изменение конфигурации роли (см. раздел 5.2)

3.13. Установка пользовательского сертификата для роли SqlStorage

Для роли SqlStorage вы можете установить пользовательский сертификат безопасности. Он используется для защиты сетевых подключений между службами MaxPatrol VM и СУБД PostgreSQL.

Пользовательский сертификат безопасности должен отвечать следующим требованиям:

- использовать алгоритм подписи SHA-256;
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- использовать отдельные файлы для хранения сертификата центра сертификации, пользовательского сертификата и закрытого ключа;
- иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком `BEGIN RSA PRIVATE KEY` без дополнительных заголовков;

  Примечание. Чтобы расшифровать ключ, зашифрованный с помощью алгоритма RSA, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.
- включать область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Extended Key Usage записи аутентификации сервера `serverAuth` и аутентификации клиента `clientAuth`;
- содержать в расширении Subject Alternative Name запись типа `DNS:<FQDN узла компонента, для которого предназначен сертификат>`;
- содержать в поле `Common Name` FQDN узла компонента, для которого предназначен сертификат.

Владельцем всех файлов должен являться пользователь dockerns (UID 9009, GID 9009).

Во время выполнения команды импорта пользовательские корневые сертификаты автоматически проверяются на соответствие требованиям безопасности. Выявленные несоответствия отображаются в терминале. Автоматизация проверки позволяет исключить риск установки потенциально небезопасных сертификатов.

- Чтобы установить пользовательский сертификат для роли SqlStorage:

  1. Разместите файл пользовательского корневого сертификата в рабочем каталоге пользователя на сервере с установленной ролью Deployer.

     Примечание. Каждый сертификат должен находиться в отдельном файле с расширением .crt.

  2. Выполните команду:

     ```
     deployer cacert import <Путь к корневому сертификату> <Путь к промежуточному сертификату 1> … <Путь к промежуточному сертификату N> -verbose
     ```

     Внимание! Путь к корневому сертификату необходимо указать первым. Пути к промежуточным сертификатам можно указать в любом порядке.

3. Разместите файл сертификата и файл приватного ключа сертификата для роли SqlStorage в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Идентификатор экземпляра роли>/certs` на сервере с установленной ролью SqlStorage.
4. Измените конфигурацию роли SqlStorage:

   ```
   SSLCertificatePemFileName: <Имя файла сертификата>
   SSLKeyFileName: <Имя файла закрытого ключа>
   ```

3.14. Установка пользовательского сертификата для RMQ Message Bus и компонентов MP 10 Core и MP 10 Collector

Для RMQ Message Bus и компонентов MP 10 Core и MP 10 Collector вы можете установить пользовательский сертификат безопасности, который должен отвечать следующим требованиям:

— использовать алгоритм подписи SHA-256;

— использовать алгоритм шифрования ключей RSA;

— соответствовать формату PEM;

— иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;

— содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит с заголовком `BEGIN RSA PRIVATE KEY` без дополнительных заголовков;

Примечание. Чтобы расшифровать ключ, зашифрованный с помощью алгоритма RSA, необходимо выполнить команду `openssl rsa -in encrypted.key -out decrypted.key`.

— включать область применения сертификата Digital Signature или Key Encipherment;

— содержать в расширении Extended Key Usage записи аутентификации сервера `serverAuth` и аутентификации клиента `clientAuth`;

— содержать в расширении Subject Alternative Name запись типа `DNS:<FQDN узла компонента, для которого предназначен сертификат>`;

— содержать в поле `Common Name` значения `core` или `agent` для компонентов MP 10 Core и MP 10 Collector соответственно;

— каждый сертификат должен находиться в отдельном файле с расширением .crt;

— каждый закрытый ключ сертификата должен находиться в отдельном файле с расширением .key.

Во время выполнения команды импорта пользовательские корневые сертификаты автоматически проверяются на соответствие требованиям безопасности. Выявленные несоответствия отображаются в терминале. Автоматизация проверки позволяет исключить риск установки потенциально небезопасных сертификатов.

Сертификат центра сертификации должен отвечать следующим требованиям:

- использовать алгоритмы подписи семейства SHA-2 (SHA-256, SHA-384, SHA-512);
- использовать алгоритм шифрования ключей RSA;
- соответствовать формату PEM;
- использовать ключи RSA длиной не менее 2048 бит;
- каждый сертификат должен находиться в отдельном файле с расширением .crt.

Внимание! Перед установкой пользовательских сертификатов безопасности необходимо установить доверенные сертификаты (см. раздел 3.12) для сайта MaxPatrol VM.

- Чтобы установить пользовательский сертификат RMQ Message Bus и компонентов MP 10 Core и MP 10 Collector на Linux:

  ```
  deployer cert import -certpath <Путь к файлу пользовательского сертификата> -keypath <Путь к файлу закрытого ключа> -Id <Идентификатор экземпляра роли>
  ```

  Например:

  ```
  deployer cert import -certpath ./user-rmq.crt -keypath ./user-rmq.key
  -type rmqmessagebus-1
  ```

  Примечание. Если необходимо импортировать файлы для всех экземпляров одного типа роли, вы можете использовать команду `deployer cert import -certpath <Путь к файлу пользовательского сертификата> -keypath <Путь к файлу закрытого ключа> -type <Тип роли>`.

  Примечание. Вы можете получить список экземпляров и типов ролей компонентов с помощью команды `deployer instance list`.

  ```
  deployer instance setparam -Id <Идентификатор экземпляра роли> CertFile=<Имя файла пользовательского сертификата> KeyFile=<Имя файла закрытого ключа>
  ```

  Например:

  ```
  deployer instance setparam -Id rmqmessagebus-1 CertFile=user-rmq.crt KeyFile=user-rmq.key
  deployer instance reconfigure --diff
  ```

  Нажмите **Confirm**.

3.15. Настройка обновления экспертных данных

Автоматическое обновление экспертных данных в MaxPatrol VM осуществляется с помощью сервиса Package Management, который входит в состав компонента PT MC. Сервис получает пакеты обновлений с сервера Positive Technologies и устанавливает их в продукты с соответствующими лицензиями. Такой способ обновления стал возможен благодаря переходу на новую модель хранения экспертных данных.

Порядок настройки подключения к серверу обновлений зависит от размещения MaxPatrol VM в инфраструктуре компании.

Получение обновлений напрямую с сервера обновлений

Используется, когда для MaxPatrol VM доступно прямое подключение к интернету. Для получения обновлений необходимо при установке или обновлении роли Management and Configuration указать значения параметров `ExpertDataUpdateMethod` и `PackagesSourceUri`. Если роль Management and Configuration уже установлена, укажите значения параметров в соответствии с инструкцией. Если MaxPatrol VM устанавливается в первый раз, необходимо также активировать PT MC и активировать лицензию MaxPatrol VM.

Получение обновлений через локальный сервер, установленный в демилитаризованной зоне

Если из изолированного сегмента сети организации есть доступ в интернет (напрямую или через прокси-сервер), вы можете развернуть и настроить в демилитаризованной зоне локальный сервер обновлений. Он будет загружать обновления с глобального сервера обновлений Positive Technologies и передавать их в изолированный сегмент сети.

Для получения обновлений необходимо:

1. При установке или обновлении роли Management and Configuration указать значения параметров `ExpertDataUpdateMethod` и `PackagesSourceUri`. Если роль Management and Configuration уже установлена, необходимо указать значения параметров в соответствии с инструкцией.
2. Если MaxPatrol VM устанавливается в первый раз — активировать (см. раздел 3.7) PT MC и активировать лицензию (см. раздел 3.8) MaxPatrol VM.
3. Установить в демилитаризованной зоне локальный сервер обновлений.
4. Если требуется, настроить подключение локального сервера обновлений к прокси-серверу.
5. Активировать лицензию локального сервера обновлений.

Получение обновлений через локальные серверы обновлений, установленные в закрытом сегменте сети и в демилитаризованной зоне

Если MaxPatrol VM установлен в изолированном от интернета сегменте сети, вы можете использовать схему обновления с двумя локальными серверами обновлений: один в изолированном сегменте сети, где установлен MaxPatrol VM, другой — в демилитаризованной зоне. Локальный сервер в демилитаризованной зоне будет загружать обновления с глобального сервера обновлений Positive Technologies. Для передачи обновлений в закрытый сегмент сети вы можете либо вручную копировать их при помощи внешнего носителя, либо настроить автоматическую передачу — если между локальными серверами обновлений есть сетевое взаимодействие.

Для получения обновлений необходимо:

1. При установке или обновлении роли Management and Configuration указать значения параметров `ExpertDataUpdateMethod` и `PackagesSourceUri`. Если роль Management and Configuration уже установлена, необходимо указать значения параметров в соответствии с инструкцией.
2. Если MaxPatrol VM устанавливается в первый раз — активировать (см. раздел 3.7) PT MC и активировать лицензию (см. раздел 3.8) MaxPatrol VM.
3. Установить два локальных сервера обновлений: в закрытом сегменте сети и в демилитаризованной зоне.
4. Если планируется ручной перенос обновлений между локальными серверами в закрытом сегменте сети и демилитаризованной зоне — активировать лицензию на локальном сервере обновлений, установленном в демилитаризованной зоне.
5. Если планируется автоматический перенос обновлений между локальными серверами в закрытом сегменте сети и демилитаризованной зоне — активировать лицензии обоих локальных серверов обновлений.
6. Если между локальными серверами обновлений есть сетевое взаимодействие и необходимо автоматизировать процесс обновления — настроить подключение локального сервера обновлений в изолированном сегменте сети к локальному серверу в демилитаризованной зоне.

В этом разделе

Изменение параметров обновления экспертных данных для роли Management and Configuration (см. раздел 3.15.1)

Аппаратные и программные требования к локальному серверу обновлений (см. раздел 3.15.2)

Установка локального сервера обновлений (см. раздел 3.15.3)

Активация лицензии локального сервера обновлений (см. раздел 3.15.4)

Настройка подключения локального сервера обновлений к прокси-серверу (см. раздел 3.15.5)

Настройка автоматического переноса обновлений в закрытый сегмент сети (см. раздел 3.15.6)

Ручной перенос обновлений MaxPatrol VM в закрытый сегмент сети (см. раздел 3.15.7)

Проверка и изменение параметров локального сервера обновлений (см. раздел 3.15.8)

3.15.1. Изменение параметров обновления экспертных данных для роли Management and Configuration

- Чтобы изменить параметры роли:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки:

```
-xf tar pt_managementandconfiguration_<Номер версии>.tar.gz
```

2. Запустите сценарий:
   ```
   pt_managementandconfiguration_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Выберите вариант с идентификатором приложения роли.
5. Выберите вариант с идентификатором экземпляра роли.

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

   Откроется страница со списком параметров (см. приложение).
7. В качестве значения параметра `ExpertDataUpdateMethod` выберите:
   - Если обновление экспертных данных будет осуществляться напрямую с сервера обновлений Positive Technologies или с помощью локального сервера обновлений — `Online`.
   - Если вручную — `Offline`.
8. В качестве значения параметра `PackagesSourceUri` укажите:
   - Если MaxPatrol VM установлен в сегменте сети с прямым подключением к интернету — один из адресов глобального сервера обновлений — `https://update.ptsecurity.ru/packman/v1/` или `https://update.ptsecurity.com/packman/v1/`.
   - Если в изолированном сегменте сети без прямого подключения к интернету — адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`.

     Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.
9. Нажмите кнопку **OK**.

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

Параметры роли изменены.

3.15.2. Аппаратные и программные требования к локальному серверу обновлений

Локальный сервер обновлений может быть установлен как на физическом сервере, так и в виртуальной среде.

Примечание. Вы можете установить локальный сервер обновлений на один сервер с ролью Deployer и компонентом PT UCS.

Аппаратные требования

Для работы сервера требуются следующие минимальные аппаратные ресурсы:

— 1 ядро процессора;

— 2 ГБ оперативной памяти;

— 100 ГБ свободного места на диске.

Программные требования

Локальный сервер обновлений поддерживает установку на операционные системы семейства Linux — Astra Linux Special Edition 1.7, Debian 10—12, Ubuntu 18.04 или Ubuntu 22.04.

3.15.3. Установка локального сервера обновлений

В разделе приводится инструкция по установке локального сервера обновлений в закрытом сегменте сети или в демилитаризованной зоне.

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

Перед выполнением инструкции нужно убедиться, что физический сервер или виртуальная машина, на которые вы планируете устанавливать локальный сервер обновлений, удовлетворяет аппаратным и программным требованиям.

► Чтобы установить локальный сервер обновлений:

1. Скопируйте архив с дистрибутивом локального сервера обновлений в любой каталог на сервере или виртуальной машине, на которые планируете устанавливать локальный сервер обновлений.

   Примечание. Архив имеет название `pt-update-mirror-<Версия локального сервера обновлений>.tar.gz` и содержит установочный пакет `pt-update-mirror-<Версия локального сервера обновлений>.deb`, исполняемый файл `pt-update-mirror`, конфигурационный файл `config.json` и информационный файл `README.md`.

2. Перейдите в каталог со скопированным архивом:

   ```
   cd <Путь к каталогу с архивом>
   ```

3. Распакуйте скопированный архив:
   `tar -xf pt-update-mirror-<Версия локального сервера обновлений>.tar.gz`
4. Запустите установку локального сервера обновлений:
   `dpkg -i pt-update-mirror-<Версия локального сервера обновлений>.deb`

Локальный сервер обновлений установлен.

При установке локального сервера обновлений создается пользователь pt-update-mirror, который используется при выполнении сервером различных операций.

Если локальный сервер обновлений установлен в демилитаризованной зоне, необходимо активировать на нем лицензию в соответствии с инструкцией.

Если локальный сервер обновлений установлен в закрытом сегменте сети, активировать на нем лицензию необходимо только в случае, когда планируется автоматический перенос обновлений между локальными серверами в закрытом сегменте сети и демилитаризованной зоне.

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL. Для корректной работы сертификата необходимо назвать файл сертификата `cert.crt`, а файл его ключа `cert.key` — и поместить эти файлы в каталог `/etc/pt-update-mirror/https_certs/` на локальном сервере обновлений. Затем необходимо перезапустить сервис с помощью команды `sudo systemctl restart pt-update-mirror.service`.

3.15.4. Активация лицензии локального сервера обновлений

После установки локального сервера обновлений нужно активировать его лицензию. Это необходимо для аутентификации локального сервера на глобальном сервере обновлений Positive Technologies.

> **Примечание.** Если перенос обновлений на локальный сервер будет осуществляться вручную, активировать его лицензию не нужно.

> **Примечание.** При наличии нескольких лицензий вы можете активировать их по очереди.

Если локальный сервер обновлений должен подключаться к интернету через прокси-сервер, перед активацией лицензии нужно настроить подключение к этому прокси-серверу.

Для активации лицензии локального сервера обновлений вам потребуется ZIP-файл с лицензиями, полученный от ответственного сотрудника при офлайн-активации PT MC.

Активация лицензии с помощью ZIP-файла с лицензиями

- Чтобы активировать лицензию,

  выполните одно из действий:

- Если требуется, чтобы локальный сервер обновлений получал данные от сервера обновлений через интернет, выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --offline-pack <Путь к ZIP-файлу с лицензиями> --update-server https://update.ptsecurity.ru
  ```

- Если требуется, чтобы локальный сервер обновлений, установленный в закрытом сегменте сети, автоматически получал данные от локального сервера, установленного в демилитаризованной зоне, выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --offline-pack <Путь к ZIP-файлу с лицензиями>
  ```

  Примечание. Дальнейшую настройку автоматического переноса обновлений в закрытый сегмент сети нужно выполнять по инструкции (см. раздел 3.15.6).

3.15.5. Настройка подключения локального сервера обновлений к прокси-серверу

Для подключения локального сервера обновлений к интернету через прокси-сервер необходимо указать параметры этого подключения в конфигурационном файле локального сервера.

Локальный сервер обновлений поддерживает подключение к прокси-серверу по протоколам HTTP и HTTPS.

Подключение к прокси-серверу по протоколу HTTP

► Чтобы настроить подключение локального сервера обновлений к прокси-серверу:

1. На локальном сервере обновлений откройте конфигурационный файл `config.json`:

   ```
   sudo nano /etc/pt-update-mirror/config.json
   ```

2. В качестве значения параметра `proxy` укажите IP-адрес (и при необходимости порт) используемого прокси-сервера:

   ```
   "proxy":"http://<IP-адрес прокси-сервера>:<Порт>"
   ```

3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения:

   ```
   "proxy-user": "<Логин>",
   "proxy-password": "<Пароль>"
   ```

4. Сохраните изменения в файле `config.json`.

5. Перезапустите локальный сервер обновлений:

   ```
   sudo systemctl restart pt-update-mirror.service
   ```

Подключение настроено.

Подключение к прокси-серверу по протоколу HTTPS

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL, который должен:

- соответствовать формату PEM;
- использовать подпись с применением алгоритма шифрования SHA-256;
- использовать алгоритм шифрования ключей RSA;
- содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит;
- включать в себя область применения сертификата Digital Signature или Key Encipherment;
- содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;
- если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты — включать в себя всю цепочку сертификатов.

Для корректной работы необходимо добавить выпущенный сертификат в список доверенных.

► Чтобы добавить сертификат в список доверенных:

1. Скопируйте файлы сертификата в каталог `/usr/local/share/ca-certificates/` на узле, на который установлен локальный сервер обновлений.
2. Обновите список доверенных сертификатов:
   ```
   sudo update-ca-certificates
   ```

Сертификат добавлен в список доверенных.

► Чтобы настроить подключение локального сервера обновлений к прокси-серверу:

1. На локальном сервере обновлений откройте конфигурационный файл `config.json`:
   ```
   sudo nano /etc/pt-update-mirror/config.json
   ```
2. В качестве значения параметра `proxy` укажите IP-адрес (и при необходимости порт) используемого прокси-сервера:
   ```
   "proxy":"https://<IP-адрес прокси-сервера>:<Порт>"
   ```
3. Если прокси-сервер требует аутентификации, укажите логин и пароль для подключения:
   ```
   "proxy-user": "<Логин>",
   "proxy-password": "<Пароль>"
   ```
4. Сохраните изменения в файле `config.json`.
5. Перезапустите локальный сервер обновлений:
   ```
   sudo systemctl restart pt-update-mirror.service
   ```

Подключение настроено.

3.15.6. Настройка автоматического переноса обновлений в закрытый сегмент сети

Если между локальными серверами обновлений есть сетевое взаимодействие, вы можете настроить их подключение друг к другу. Это позволит автоматически переносить обновления с глобального сервера обновлений Positive Technologies в MaxPatrol VM в закрытом сегменте сети через цепочку локальных серверов обновлений.

Вы можете настроить автоматический перенос обновлений как по протоколу HTTP, так и по протоколу HTTPS.

Подключение по протоколу HTTP

Для подключения по протоколу HTTP вместо порта по умолчанию 80 используется порт 8553. Если требуется, вы можете изменить порт для подключения.

- Чтобы настроить автоматический перенос обновлений:

  1. На локальном сервере обновлений в изолированном сегменте откройте конфигурационный файл `config.json`:
     ```
     sudo nano /etc/pt-update-mirror/config.json
     ```
  2. В качестве значения параметра `update-server` укажите адрес локального сервера обновлений в демилитаризованной зоне:
     ```
     "update-server": "http://<Адрес локального сервера обновлений>:<Порт>"
     ```
     Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений.
  3. В качестве значения параметра `verify_ssl` укажите `false`.
  4. Если подключение к локальному серверу в демилитаризованной зоне выполняется через прокси-сервер, настройте параметры подключения к прокси-серверу.
  5. Сохраните изменения в файле `config.json`.
  6. Перезапустите сервис обновлений в закрытом сегменте сети:
     ```
     sudo systemctl restart pt-update-mirror.service
     ```

  Перенос обновлений настроен.

Подключение по протоколу HTTPS

Для подключения по протоколу HTTPS вместо порта по умолчанию 443 используется порт 8743. Если требуется, вы можете изменить порт для подключения.

Для проверки подлинности при передаче данных по протоколу HTTPS необходимо выпустить сертификат SSL, который должен:

— соответствовать формату PEM;

— использовать подпись с применением алгоритма шифрования SHA-256;

— использовать алгоритм шифрования ключей RSA;

— содержать закрытый незашифрованный ключ в формате PEM длиной не менее 2048 бит;

— включать в себя область применения сертификата Digital Signature или Key Encipherment;

— содержать в расширении Subject Alternative Name (SAN) запись о доменном имени или IP-адресе сервера с установленным веб-интерфейсом продукта;

— если в цепочке между корневым сертификатом и сертификатами компонентов и систем есть промежуточные сертификаты — включать в себя всю цепочку сертификатов.

Для корректной работы необходимо назвать файлы сертификата и его ключа `cert.crt` и `cert.key` соответственно и поместить их в каталог `/etc/pt-update-mirror/https_certs/` на локальном сервере обновлений.

► Чтобы настроить автоматический перенос обновлений:

1. На локальном сервере обновлений в изолированном сегменте откройте конфигурационный файл `config.json`:
   ```
   sudo nano /etc/pt-update-mirror/config.json
   ```
2. В качестве значения параметра `update-server` укажите адрес локального сервера обновлений в демилитаризованной зоне:
   ```
   "update-server": "https://<Адрес локального сервера обновлений>:<Порт>"
   ```
   Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений.
3. Если подключение к локальному серверу в демилитаризованной зоне выполняется через прокси-сервер, настройте параметры подключения к прокси-серверу.
4. Сохраните изменения в файле `config.json`.
5. Перезапустите сервис обновлений в закрытом сегменте сети:
   ```
   sudo systemctl restart pt-update-mirror.service
   ```

Перенос обновлений настроен.

3.15.7. Ручной перенос обновлений MaxPatrol VM в закрытый сегмент сети

Если между локальными серверами обновлений отсутствует сетевое взаимодействие, вам нужно вручную перенести обновления в закрытый сегмент сети для последующего обновления MaxPatrol VM.

- Чтобы вручную перенести обновления в закрытый сегмент сети:

  1. На локальном сервере обновлений в демилитаризованной зоне запустите получение обновлений с глобального сервера обновлений Positive Technologies:
     ```
     sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
     ```
  2. Запустите экспорт репозитория с обновлениями в файл:
     ```
     sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository export --repo vm-expertise
     <Название файла>.tgz
     ```

     Примечание. Выполнение команды экспорта без ключа `--repo <Название репозитория>` позволяет экспортировать все репозитории базы обновлений в указанный архив. Вы можете просмотреть список репозиториев в базе обновлений локального сервера с помощью команды `sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository view`.
  3. Скопируйте с помощью внешнего носителя полученный файл архива в каталог, принадлежащий пользователю pt-update-mirror, на локальном сервере обновлений в закрытом сегменте сети.
  4. На локальном сервере обновлений в закрытом сегменте сети импортируйте обновления из скопированного файла архива:
     ```
     sudo opt/pt/pt-update-mirror/bin/pt-update-mirror repository import <Путь к архиву>/
     <Название архива>.tgz
     ```

  Обновления MaxPatrol VM перенесены.

3.15.8. Проверка и изменение параметров локального сервера обновлений

Проверка состояния сервера

- Чтобы проверить состояние локального сервера обновлений,

  на локальном сервере выполните команду:
  ```
  sudo systemctl status pt-update-mirror
  ```

  На экране отобразится информация о параметрах загрузки и состоянии локального сервера.

Проверка состояния таймера получения обновлений

- Чтобы проверить состояние таймера получения обновлений,

  на локальном сервере выполните команду:
  ```
  sudo systemctl status pt-update-mirror-update.timer
  ```

  На экране отобразится информация о параметрах загрузки и состоянии таймера получения обновлений.

Проверка состояния сервиса получения обновлений

- Чтобы проверить состояние сервиса получения обновлений,

  на локальном сервере выполните команду:

  ```
  sudo systemctl status pt-update-mirror-update
  ```

  На экране отобразится информация о параметрах загрузки и состоянии сервиса получения обновлений.

Просмотр журналов событий сервиса получения обновлений

- Чтобы просмотреть журнал событий сервиса получения обновлений,

  на локальном сервере выполните команду:

  ```
  journalctl -u pt-update-mirror.service
  ```

  На экране отобразится список событий сервиса получения обновлений.

Изменение времени получения обновлений

По умолчанию обновление запускается в 13, 27, 42 и 58 минут каждого часа. Вы можете изменить эти значения в параметрах таймера получения обновлений.

- Чтобы изменить время получения обновлений:

  1. Откройте файл `pt-update-mirror-update.timer`:
     ```
     sudo nano etc/systemd/system/pt-update-mirror-update.timer
     ```
  2. В блоке параметров `Timer` в качестве значения параметра `OnCalendar` укажите нужное время получения обновлений (в формате systemd.timer).
  3. Сохраните изменения в файле `pt-update-mirror-update.timer`.
  4. Примените изменения таймера:
     ```
     sudo systemctl daemon-reload
     ```
  5. Перезапустите таймер получения обновлений:
     ```
     sudo systemctl restart pt-update-mirror-update.timer
     ```

  Время получения обновлений изменено.

Изменение порта подключения по протоколам HTTP и HTTPS

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

- Чтобы изменить порты подключения:

  1. Откройте файл `config.json`:
     ```
     sudo nano /etc/pt-update-mirror/config.json
     ```
  2. Укажите в качестве значений параметров `http_port` и `https_port` порты, которые нужно использовать для подключения.
  3. Если требуется принудительно отключить использование протокола HTTP, присвойте параметру `http_disabled` значение `true`.
  4. Сохраните изменения в файле `config.json`.
  5. Перезапустите локальный сервер обновлений:
     ```
     sudo systemctl restart pt-update-mirror
     ```

  Порты подключения изменены.

3.16. Харденинг MaxPatrol VM: MP 10 Core установлен на Linux

- Чтобы настроить MaxPatrol VM:

  1. На серверах под управлением Linux разрешите удаленный доступ по протоколу SSH только с рабочих станций администраторов:
     ```
     iptables -A INPUT -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
     iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m tcp --dport 22 -m conntrack --ctstate NEW -m comment --comment "SSH admin access" -j ACCEPT
     ```

     Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, `-s 198.51.100.0,198.51.100.1,192.0.2.0/24`.
  2. На сервере MP 10 Core разрешите доступ к веб-интерфейсу системы с рабочих станций пользователей:
     ```
     iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m conntrack --ctstate NEW --ctorigdstport 80 -m comment --comment "Web user access" -j ACCEPT
     iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m conntrack --ctstate NEW --ctorigdstport 443 -m comment --comment "Web user access" -j ACCEPT
     iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp --dport 3334 -m conntrack --ctstate NEW -m comment --comment "Web user access" -j ACCEPT
     ```

```
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m conntrack --ctstate NEW --ctorigdstport 8091 -m comment --comment "Web user access" -j ACCEPT
iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций пользователей> -p tcp -m conntrack --ctstate NEW --ctorigdstport 8190 -m comment --comment "Web user access" -j ACCEPT
```

3. На серверах под управлением Linux разрешите удаленный доступ к веб-интерфейсу Grafana:

   ```
   iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 9002 -m comment --comment "Grafana access" -j ACCEPT
   ```

4. На сервере с установленной ролью Deployer разрешите входящие соединения от коллекторов:

   ```
   iptables -A INPUT -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера MP 10 Collector> -p tcp -m multiport --dports 4505,4506,9035 -m conntrack --ctstate NEW -m comment --comment "From MP 10 Collector to Deployer" -j ACCEPT
   ```

5. В файл `custom.env`, расположенный в каталоге `/var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли SqlStorage>/images/storage-pgadmin/config/`, добавьте параметры:

   ```
   PGADMIN_CONFIG_MASTER_PASSWORD_REQUIRED=True
   PGADMIN_DEFAULT_PASSWORD=<Пароль PGAdmin>
   ```

6. Пересоберите службу pgAdmin:

   ```
   cd /var/lib/deployed-roles/<Идентификатор приложения Management and Configuration>/<Название экземпляра роли SqlStorage>/images/storage-pgadmin
   docker-compose down
   docker-compose up -d
   ```

7. Разрешите доступ к панели управления pgAdmin с рабочих станций администраторов:

   ```
   iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих станций администраторов> -p tcp -m conntrack --ctstate NEW --ctorigdstport 9001 -m comment --comment "pgAdmin access" -j ACCEPT
   ```

8. Разрешите входящие соединения от коллекторов:

   ```
   iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера MP 10 Collector> -p tcp -m tcp --dport 5671 -m conntrack --ctstate NEW -m comment --comment "From MP 10 Collector to MP 10 Core" -j ACCEPT
   ```

9. На серверах под управлением Linux заблокируйте все входящие соединения, кроме разрешенных:

   ```
   iptables -A INPUT -i <Название внешнего сетевого интерфейса> -j DROP
   iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -j REJECT
   ```

10. Для сохранения созданных правил на серверах под управлением Debian установите пакет iptables-persistent:

    ```
    apt-get install iptables-persistent
    ```

    Примечание. Порядок сохранения правил на серверах под управлением Astra Linux описан в справочном центре производителя операционной системы.

11. Сохраните правила межсетевого экрана:

    ```
    netfilter-persistent save
    ```

12. На серверах коллекторов под управлением Microsoft Windows удалите все правила удаленного доступа по протоколу RDP:

    ```
    netsh advfirewall firewall delete rule name=all protocol=tcp localport=3389
    netsh advfirewall firewall delete rule name=all protocol=udp localport=3389
    ```

13. Разрешите удаленный доступ по протоколу RDP только с рабочих станций администраторов:

    ```
    netsh advfirewall firewall add rule name="Allow RDP TCP in" dir=in action=allow
    protocol=tcp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>
    netsh advfirewall firewall add rule name="Allow RDP UDP in" dir=in action=allow
    protocol=udp localport=3389 remoteip=<IP-адреса рабочих станций администраторов>
    ```

    Примечание. IP-адреса рабочих станций необходимо перечислять через запятую. Также вы можете указать маску подсети, где находятся рабочие станции, в формате CIDR. Например, `remoteip=198.51.100.0,198.51.100.1,192.0.2.0/24`.

14. Смените пароли служебных учетных записей в MaxPatrol VM (подробнее см. Руководство администратора).

15. На серверах под управлением Microsoft Windows убедитесь, что пароли для входа в операционную систему соответствуют требованиям к сложности, установленным в организации.

16. На серверах под управлением Linux для каждого администратора MaxPatrol VM создайте отдельную учетную запись:

    ```
    adduser <Логин администратора>
    ```

17. На рабочих станциях администраторов MaxPatrol VM сгенерируйте ключевую пару.

    Примечание. Для генерации ключевой пары на Linux вы можете использовать утилиту ssh-keygen, на Microsoft Windows — PuTTygen.

18. На серверах под управлением Linux добавьте открытый ключ в файл `/home/<Логин администратора>/.ssh/authorized_keys`.

19. В файле `/etc/ssh/sshd_config` раскомментируйте и измените значения параметров (разрешите вход только с помощью SSH-ключей):

    ```
    PubkeyAuthentication yes
    RhostsRSAAuthentication no
    HostbasedAuthentication no
    PermitEmptyPasswords no
    PasswordAuthentication no
    ```

20. В файле `/etc/sudoers` измените значение параметра:

    ```
    <Логин администратора> ALL=(ALL) ALL
    ```

21. Для каждого пользователя MaxPatrol VM создайте отдельную учетную запись.

22. Смените пароль учетной записи Administrator.

Подключение к локальному серверу обновлений

Если локальный сервер обновлений установлен на сервере, отличном от сервера PT MC, на локальном сервере обновлений необходимо разрешить входящие соединения от PT MC.

- Чтобы настроить подключение к локальному серверу обновлений,

  на локальном сервере обновлений выполните команду:

  ```
  iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адрес сервера PT MC> -p tcp -m multiport --dports 8553,8743 -m conntrack --ctstate NEW -m comment --comment "From PT MC to LUS" -j ACCEPT
  ```

4. Обновление MaxPatrol VM

Вы можете обновлять компоненты MaxPatrol VM с помощью дистрибутивов.

> **Внимание!** Если требуется обновить MaxPatrol VM вместе с ОС, сначала нужно выполнить подготовку к обновлению MaxPatrol VM, описанную в этом разделе, затем обновить ОС и после этого — обновить компоненты MaxPatrol VM. Если обновления MaxPatrol VM не требуется, после обновления ОС необходимо обновить роль Deployer. При обновлении ОС не рекомендуется выполнять вычистку удаленных пакетов.

> **Внимание!** Перед началом обновления создайте резервную копию данных компонентов.

Прежде чем приступать к обновлению MaxPatrol VM, рекомендуется остановить все задачи по сбору данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.

Перед началом обновления необходимо убедиться в отсутствии ошибок в работе системы (индикатор состояния системы не красный).

При обновлении роли RMQ Message Bus до версии 27.0 или выше все хранящиеся в RabbitMQ данные, а также пользовательские модификации определений (например, созданные вручную сущности queue, exchange или shovel) будут удалены. Для сохранения пользовательских модификаций определений необходимо перед обновлением роли создать их резервные копии и восстановить данные после обновления.

В этом разделе

Обновление с помощью дистрибутивов (см. раздел 4.1)

4.1. Обновление с помощью дистрибутивов

Для обновления MaxPatrol VM необходимо обратиться в Positive Technologies и получить дистрибутивы с новыми версиями компонентов. Перед началом обновления рекомендуется создать резервную копию данных.

> **Внимание!** Перед началом обновления до версии 2.5 необходимо обратиться в Positive Technologies и получить ключ инсталляции PT MC нового формата. Ключи и лицензии из комплекта поставки предыдущих версий продукта несовместимы с новым механизмом лицензирования.

Начиная с версии 1.5 базовыми единицами установки и обновления компонентов Linux являются роли (см. раздел 3.4). Обновление компонентов на Linux необходимо выполнять в следующем порядке:

1. Обновление роли Deployer.
2. Обновление компонента PT MC.
3. Активация компонента PT MC.

4. Добавление лицензии MaxPatrol VM в PT MC.
5. Обновление компонента MP 10 Core.
6. Обновление компонента MP 10 Collector.
7. Обновление компонента PT UCS.
8. Обновление локального сервера обновлений.
9. Привязка лицензии MaxPatrol VM к приложению в PT MC.

   Внимание! Путь к каталогу, из которого будет запущен сценарий `install.sh`, а также имя самого каталога могут содержать только буквы латинского алфавита, цифры, знаки подчеркивания и точки.

Если на сервере компонента установлен Kaspersky Endpoint Security, необходимо приостановить его работу на время обновления MaxPatrol VM.

В этом разделе

Управление обновлением ролей и компонентов MaxPatrol VM с помощью манифеста (см. раздел 4.1.1)

Обновление роли Deployer (см. раздел 4.1.2)

Обновление компонента PT MC на Linux (см. раздел 4.1.3)

Активация PT MC (см. раздел 4.1.4)

Добавление лицензии в PT MC (см. раздел 4.1.5)

Обновление компонента MP 10 Core на Linux (см. раздел 4.1.6)

Обновление компонента MP 10 Collector на Linux (см. раздел 4.1.7)

Обновление компонента MP 10 Collector на Microsoft Windows (см. раздел 4.1.8)

Обновление компонента PT UCS (см. раздел 4.1.9)

Обновление локального сервера обновлений (см. раздел 4.1.10)

Привязка лицензии MaxPatrol VM к приложению в PT MC (см. раздел 4.1.11)

4.1.1. Управление обновлением ролей и компонентов MaxPatrol VM с помощью манифеста

Начиная с версии 2.8 для оптимизации работы вы можете выбрать необходимые роли, а затем одновременно обновить их. Для этого необходимо создать манифест (см. раздел 4.1.1.2) — файл формата YAML, который задает параметры изменения конфигурации. Структура файла манифеста и описание его параметров приведены в разделе «Авторазвертывание MaxPatrol VM с помощью манифеста».

Обновление ролей с помощью манифеста доступно сразу после обновления роли Deployer до версии из комплекта поставки 2.8.

В этом разделе

Обновление ролей и компонентов MaxPatrol VM с помощью манифеста (см. раздел 4.1.1.1)

Создание манифеста для обновления компонентов или изменения конфигурации ролей (см. раздел 4.1.1.2)

4.1.1.1. Обновление ролей и компонентов MaxPatrol VM с помощью манифеста

- Чтобы обновить роли и компоненты MaxPatrol 10 с помощью манифеста:

  1. Распакуйте архив `pt_<Идентификатор приложения>_distro_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_<Идентификатор приложения>_distro_<Номер версии>.tar.gz
     ```
  2. Выполните команду для установки роли Deployer и загрузки пакетов всех ролей в хранилище Deployer:
     ```
     ./install_all_role_packages.sh –silent
     ```
  3. Создайте манифест (см. раздел 4.1.1.2).
  4. Выполните команду для обновления ролей и компонентов:
     ```
     deployer application deploy ./export_manifest.yaml --accepteula
     ```

В консоли появится информация о результатах обновления:

— Если экземпляр роли был обновлен успешно, рядом с его идентификатором будет добавлен комментарий `Instance installation is successful`.

— Если экземпляр роли не был обновлен, рядом с его идентификатором будет добавлен комментарий с причиной неудачи.

— Если экземпляр роли не был обновлен из-за отсутствия соединения с модулем Salt Minion, появится сообщение об ошибке `There are no SCM hosts available`.

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

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

См. также

Создание манифеста для обновления компонентов или изменения конфигурации ролей (см. раздел 4.1.1.2)

4.1.1.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей

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

- Чтобы создать манифест:

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

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

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

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

Таблица 12. Аргументы сценария

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

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

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

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

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

Примеры сценариев создания манифеста

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

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

  Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

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

— `deployer instance export -Type "agentlinux"`

  Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

4.1.2. Обновление роли Deployer

Внимание! Для корректной работы MaxPatrol VM необходимо, чтобы подсеть его Docker-контейнеров не совпадала с подсетями, используемыми в вашей организации. По умолчанию система виртуализации Docker использует подсети в диапазонах 172.17.0.0—172.31.255.255 и 192.168.0.0—192.168.255.255. Вы можете изменить подсеть по инструкции из раздела «Подсеть Docker-контейнера MaxPatrol VM совпадает с одной из подсетей предприятия» Руководства администратора.

Для обновления роли вам потребуется архив `pt_deployer_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы обновить роль:

1. Распакуйте архив `pt_deployer_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_deployer_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_deployer_<Номер версии>/install.sh
   ```

   Начнется проверка сервера на соответствие программным и аппаратным требованиям.

Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

3. Нажмите **Yes**.

   Начнутся распаковка и подготовка пакетов.

4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

   Значение по умолчанию — FQDN локального сервера.

5. Нажмите **OK**.

6. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

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

7. Нажмите **OK**.

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

9. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

   Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.3. Обновление компонента PT MC на Linux

Обновление компонента PT MC производится в следующем порядке:

1. Обновление роли SqlStorage.
2. Обновление роли LogConnector.
3. Обновление роли Observability.
4. Обновление роли Management and Configuration.

В этом разделе

Обновление роли SqlStorage (см. раздел 4.1.3.1)

Обновление роли LogConnector (см. раздел 4.1.3.2)

Обновление роли Observability (см. раздел 4.1.3.3)

Обновление роли Management and Configuration (см. раздел 4.1.3.4)

4.1.3.1. Обновление роли SqlStorage

Для обновления роли вам потребуется архив `pt_sqlstorage_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_sqlstorage_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_sqlstorage_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_sqlstorage_<Номер версии>/install.sh
     ```
  3. Нажмите **Yes**.

     Начнутся распаковка и подготовка пакетов, необходимых для обновления.
  4. Выберите вариант с идентификатором приложения Management and Configuration.

     Значение по умолчанию — `mc-application`.
  5. Выберите вариант с названием экземпляра роли SqlStorage.

     Название по умолчанию — `sqlstorage`.
  6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
  7. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера MP 10 Core.

     Значение по умолчанию — FQDN локального сервера.
  8. Если требуется включить контрольные суммы для страниц СУБД PostgreSQL, в качестве значения параметра `PgChecksums` укажите `on`.

     Внимание! Если в базе PostgreSQL хранится большой объем данных, расчет контрольных сумм займет длительное время (более часа при объеме данных 100 ГБ). Работа базы данных будет остановлена до конца этого процесса.

     Примечание. Рекомендуется включить контрольные суммы. Вы можете отслеживать прогресс расчета контрольных сумм в журнале `pg_checksums.log` в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/log`.

9. Нажмите **OK**.
10. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
11. Нажмите **OK**.
12. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
13. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

    Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.3.2. Обновление роли LogConnector

Внимание! При обновлении версии MaxPatrol VM ниже 2.8 роль LogConnector необходимо установить.

Для обновления роли вам потребуется архив `pt_logconnector_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_logconnector_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_logconnector_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_logconnector_<Номер версии>/install.sh
     ```

3. Нажмите **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для обновления.

4. Выберите вариант с идентификатором приложения Management and Configuration.

   Значение по умолчанию — `mc-application`.

5. Выберите вариант с названием экземпляра роли LogConnector.

   Название по умолчанию — `logconnector`.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

   Значение по умолчанию — FQDN локального сервера.

7. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера MP 10 Core.

8. Нажмите **OK**.

9. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

   Начнется проверка сервера на соответствие программным и аппаратным требованиям.

   Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

   Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

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

11. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

    Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.3.3. Обновление роли Observability

Для обновления роли вам потребуется архив `pt_observability_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_observability_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_observability_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_observability_<Номер версии>/install.sh
   ```
3. Нажмите **Yes**.
4. Ознакомьтесь с соглашением о сборе телеметрических данных и нажмите **Accept**.

   Начнутся распаковка и подготовка пакетов, необходимых для обновления.
5. Выберите вариант с идентификатором приложения Management and Configuration.

   Значение по умолчанию — `mc-application`.
6. Выберите вариант с названием экземпляра роли Observability.

   Название по умолчанию — `observability`.
7. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. Выберите **Advanced configuration**.
9. В качестве значения параметра `PostgreHost` укажите IP-адрес или FQDN сервера PT MC.

   Значение по умолчанию — FQDN локального сервера.
10. Нажмите **OK**.
11. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

12. Нажмите **OK**.
13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
14. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

    Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.3.4. Обновление роли Management and Configuration

Внимание! Для получения обновлений экспертных данных MaxPatrol VM в изолированном сегменте сети без прямого подключения к интернету необходим локальный сервер обновлений, установленный и настроенный в соответствии с инструкциями в разделе «Настройка обновления экспертных данных».

Примечание. После обновления роли Management and Configuration происходит завершение сессий для всех пользователей. При переходе с версий MaxPatrol VM ниже 2.5 потребуется заново активировать PT MC и привязать лицензии приложений.

Для обновления роли вам потребуется архив `pt_managementandconfiguration_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_managementandconfiguration_<Номер версии>.tar.gz`:

     ```
     tar -xf pt_managementandconfiguration_<Номер версии>.tar.gz
     ```

  2. Запустите сценарий:

     ```
     pt_managementandconfiguration_<Номер версии>/install.sh
     ```

  3. Нажмите **Yes**.

     Начнутся распаковка и подготовка пакетов, необходимых для обновления.

  4. Выберите вариант с идентификатором приложения Management and Configuration.

     Значение по умолчанию — `mc-application`.

  5. Выберите вариант с названием экземпляра роли Management and Configuration.

Название по умолчанию — `managementandconfiguration`.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера MP 10 Core.

   Значение по умолчанию — FQDN локального сервера.
8. В качестве значения параметра `ExpertDataUpdateMethod` выберите:
   - Если обновление экспертных данных будет осуществляться напрямую с сервера обновлений Positive Technologies или с помощью локального сервера обновлений — `Online`.
   - Если вручную — `Offline`.
9. В качестве значения параметра `PackagesSourceUri` укажите:
   - Если вы обновляете MaxPatrol VM в сегменте сети с прямым подключением к интернету — один из адресов глобального сервера обновлений — `https://update.ptsecurity.ru/packman/v1/` или `https://update.ptsecurity.com/packman/v1/`.
   - Если в изолированном сегменте сети без прямого подключения к интернету — адрес локального сервера обновлений в формате `http://<Адрес сервера>:<Порт>/packman/v1/`.

   Примечание. Указанный в параметре порт локального сервера обновлений должен быть открыт для входящих соединений. Для подключения по протоколам HTTP и HTTPS по умолчанию используются порты 8553 и 8743 соответственно.
10. Нажмите **OK**.
11. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
12. Нажмите **OK**.

13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
14. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

    Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.4. Активация PT MC

Активация выполняется в интерфейсе PT MC. Перед началом активации необходимо войти в PT MC по ссылке `https://<IP-адрес или FQDN сервера PT MC>:3334`. Для входа вам потребуются логин и пароль служебной учетной записи с ролью **Администратор**; также необходимо знать тип учетной записи (локальная или доменная).

Для активации PT MC вам потребуется ZIP-файл ключа инсталляции.

Онлайн-активация PT MC

- Чтобы активировать PT MC при наличии доступа к серверу обновлений update.ptsecurity.com:

  1. На странице **Активация платформы** выберите ZIP-файл ключа инсталляции.
  2. Нажмите кнопку **Активировать**.

     Откроется страница **Лицензии**.

  Активация завершена.

Офлайн-активация PT MC

- Чтобы активировать PT MC при отсутствии доступа к серверу обновлений update.ptsecurity.com:

  1. Внизу страницы **Активация платформы** нажмите **Перейти к офлайн-активации**.
  2. На странице **Загрузка ключа инсталляции** выберите ZIP-файл ключа инсталляции.
  3. Нажмите кнопку **Далее**.

     Откроется страница **Скачивание и передача файла**.
  4. Нажмите кнопку **Скачать файл**.

Начнется скачивание файла фингерпринта.

5. Отправьте файл фингерпринта сотруднику вашей компании, ответственному за работу с лицензиями.

   Ответственный сотрудник передаст файл фингерпринта менеджеру Positive Technologies, представителю компании-интегратора или в службу технической поддержки. После этого ответственный сотрудник передаст вам ZIP-файл с лицензиями, который необходимо использовать на следующем шаге активации.

6. Нажмите кнопку **Далее**.

   Откроется страница **Активация платформы**.

7. Выберите ZIP-файл с лицензиями, полученный от ответственного сотрудника.

8. Нажмите кнопку **Далее**.

   Откроется страница **Лицензии**.

Активация завершена.

4.1.5. Добавление лицензии в PT MC

Если после активации PT MC лицензия MaxPatrol VM не добавилась в PT MC автоматически, необходимо выполнить одну из инструкций ниже.

Добавление лицензии выполняется в интерфейсе PT MC. Сначала необходимо войти в PT MC по ссылке `https://<IP-адрес или FQDN сервера PT MC>:3334`. Для входа вам потребуются логин и пароль учетной записи с ролью **Администратор**, также необходимо знать тип учетной записи (локальная или доменная).

Для добавления лицензии вручную вам потребуется ZIP-файл с лицензией.

- Чтобы добавить лицензию без доступа к интернету:

  1. В главном меню выберите раздел **Лицензии**.
  2. В панели инструментов нажмите **Добавить**.
  3. Выберите ZIP-файл с лицензией.

     Примечание. Файл может содержать как одну, так и несколько лицензий. В систему будут добавлены все корректные лицензии, которые в нем содержатся.

  4. Нажмите **Добавить**.

  Лицензия добавлена.

- Чтобы добавить лицензию при наличии доступа к интернету:

  1. В главном меню выберите раздел **Лицензии**.
  2. В панели инструментов нажмите **Обновить список лицензий**.

  Лицензия добавлена.

4.1.6. Обновление компонента MP 10 Core на Linux

Компонент необходимо обновлять в следующем порядке: сначала обновить роль RMQ Message Bus, затем — роль Core.

> **Примечание.** Версия MaxPatrol VM 2.8 поддерживает обновление с версий 2.0 и выше.

В этом разделе

Обновление роли RMQ Message Bus на сервере MP 10 Core (см. раздел 4.1.6.1)

Обновление роли Core (см. раздел 4.1.6.2)

4.1.6.1. Обновление роли RMQ Message Bus на сервере MP 10 Core

Для обновления роли вам потребуется архив `pt_rmqmessagebus_<Номер версии>.tar.gz` из комплекта поставки.

> **Примечание.** Если роль RMQ Message Bus имеет пользовательские модификации определений (например, созданные вручную сущности queue, exchange или shovel), необходимо до обновления роли создать резервные копии таких определений и восстановить данные после обновления.

Перед обновлением роли необходимо убедиться, что очереди RabbitMQ не содержат необработанных сообщений (количество сообщений должно быть равно нулю).

- Чтобы обновить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_rmqmessagebus_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_rmqmessagebus_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_rmqmessagebus_<Номер версии>/install.sh
     ```
  3. Нажмите **Yes**.

     Начнутся распаковка и подготовка пакетов, необходимых для обновления.
  4. Выберите вариант с идентификатором приложения MaxPatrol 10.

5. Выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер MP 10 Core.

   Название по умолчанию — `rmqmessagebus-2`.

6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

7. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера MP 10 Core.

8. Нажмите **OK**.

9. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

   Начнется проверка сервера на соответствие программным и аппаратным требованиям.

   Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

   Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

10. Нажмите **OK**.

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

12. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

    Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.6.2. Обновление роли Core

Для обновления роли вам потребуется архив `pt_core_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_core_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_core_<Номер версии>/install.sh
     ```
  3. Нажмите **Yes**.

     Начнутся распаковка и подготовка пакетов, необходимых для обновления.
  4. Выберите вариант с идентификатором приложения MaxPatrol 10.
  5. Выберите вариант с названием экземпляра роли Core.

     Название по умолчанию — `core`.
  6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
  7. Выберите **Advanced configuration**.
  8. Укажите значения параметров:
     ```
     AssetGridVersionRangeModeEnabled: True
     HostAddress: <IP-адрес или FQDN сервера MP 10 Core>
     MCAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:3334
     KBAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:8091
     PostgreHost: <IP-адрес или FQDN сервера MP 10 Core>
     RMQHost: <IP-адрес или FQDN сервера MP 10 Core>
     ```
  9. Выберите значение параметра `AssetGridValidTimePeriodIndexFormat`.

     Внимание! При первом включении параметра `AssetGridVersionRangeModeEnabled` выполняется миграция данных. Если для параметра `AssetGridValidTimePeriodIndexFormat` выбрано значение по умолчанию (`IdAndPeriod`), миграция данных может занять более 10 часов для базы данных размером 100 ГБ.

     Внимание! Перед выполнением миграции необходимо убедиться, что свободного места на диске достаточно. В ходе миграции создаются новые индексы, что приводит к увеличению размера БД сервиса TRM (`maxpatrol_assets_temporal_rm`). Увеличение может составить до 100%. Определить размер БД можно, выполнив на сервере PT MC команду `docker exec -it $(docker ps -q --filter name=postgres) psql -U pt_system -t -d postgres -c "SELECT pg_size_pretty(pg_database_size('maxpatrol_assets_temporal_rm')) AS size;"`.

     Подробности см. в разделе «Оптимизация выполнения PDQL-запросов для высоконагруженных систем» Руководства администратора.
  10. Если установлен компонент PT UCS, укажите значение параметра `SaltMasterHost`:
      ```
      SaltMasterHost: <IP-адрес или FQDN сервера PT UCS>
      ```

11. Нажмите **OK**.
12. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

    Начнется проверка сервера на соответствие программным и аппаратным требованиям.

    Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

    Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
13. Нажмите **OK**.
14. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
15. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

    Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.7. Обновление компонента MP 10 Collector на Linux

Внимание! Для обновления компонента с версии 24.0 или 24.1 до версии 25.0 или выше необходимо удалить существующую роль Agent и установить роль Collector из комплекта поставки в соответствии с инструкцией.

Для обновления компонента необходимо обновить роль Collector. Для обновления роли вам потребуется архив `pt_agent-linux_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить роль:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_agent-linux_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_agent-linux_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_agent-linux_<Номер версии>/install.sh
     ```
  3. Нажмите **Yes**.

     Начнутся распаковка и подготовка пакетов, необходимых для обновления.
  4. Выберите вариант с идентификатором приложения MaxPatrol 10.
  5. Выберите вариант с названием экземпляра роли Collector.

     Название по умолчанию — `agentlinux`.
  6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
  7. Выберите **Advanced configuration**.
  8. В качестве значения параметра `AgentRMQHost` укажите IP-адрес или FQDN сервера MP 10 Core.
  9. В качестве значения параметра `AgentRMQVirtualHost` выберите `Core.`
  10. Нажмите **OK**.
  11. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

      Начнется проверка сервера на соответствие программным и аппаратным требованиям.

      Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

      Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

      Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
  12. Нажмите **OK**.
  13. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
  14. Если требуется подтвердить удаление неиспользуемых пакетов предыдущей версии роли, выберите пакеты для удаления и нажмите **Confirm**.

Например, при обновлении роли с версии 2.7 до версии 2.8 система предложит удалить пакеты роли версии 2.6 при их наличии.

В результате обновления роли (в том числе и неуспешного) в каталоге, из которого был запущен сценарий `install.sh`, формируется каталог `/installReports` с отчетами об обновлении. Отчеты сохраняются в HTML-файлах и содержат информацию о системе и журналы установки. Вы можете передавать отчеты в рамках запроса в техническую поддержку для анализа проблем.

4.1.8. Обновление компонента MP 10 Collector на Microsoft Windows

Внимание! В результате обновления компонентов установленные ранее пользовательские сертификаты безопасности будут заменены сертификатами из комплекта поставки. Если для работы компонентов использовались сертификаты безопасности, отличные от стандартных, необходимо снова настроить их после обновления.

Для обновления вам потребуется архив `pt_agent-windows_<Номер версии>.tar.gz` из комплекта поставки.

- Чтобы обновить компонент MP 10 Collector:

  1. На сервере с установленной ролью Collector запустите файл `MPXAgentSetup_<Номер версии>.exe`.

     Откроется окно мастера обновления.
  2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
  3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите **Обновить**.
  4. По завершении обновления нажмите **Закрыть**.
  5. В командной строке Microsoft Windows выполните команду от имени администратора:
     ```
     coreagentcfg set -p AgentRMQVirtualHost mpx
     ```

4.1.9. Обновление компонента PT UCS

- Чтобы обновить компонент PT UCS:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_ucs_<Номер версии MaxPatrol VM>.tar.gz`:
     ```
     tar -xf pt_ucs_<Номер версии MaxPatrol VM>.tar.gz -C <Путь к каталогу для распаковки архива>
     ```
  2. Запустите сценарий:
     ```
     <Путь к каталогу для распаковки архива>/pt_ucs_<Номер версии MaxPatrol VM>/install.sh
     ```
  3. Нажмите **Yes**.

Начнутся распаковка и подготовка пакетов, необходимых для обновления.

4. Выберите вариант с идентификатором приложения MaxPatrol 10.
5. Выберите вариант с названием экземпляра роли UCS.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. Выберите **Skip configuration**.
8. Нажмите **OK**.
9. Если требуется подтвердить добавление или изменение имеющихся параметров, нажмите **Submit**.

   Начнется проверка сервера на соответствие программным и аппаратным требованиям.

   Если сервер не соответствует требованиям, отобразится сообщение `Warning` или `Error`. Описание параметров и ошибок приведено в разделе «Параметры соответствия сервера программным и аппаратным требованиям» Руководства администратора.

   Примечание. Если в результате проверки отобразилось сообщение `Warning`, вы все равно можете продолжить установку, нажав клавишу Y. Чтобы включить режим установки, при котором сообщения `Warning` будут автоматически игнорироваться, необходимо использовать ключ `--silent` при запуске сценария `install.sh`.

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

4.1.10. Обновление локального сервера обновлений

- Чтобы обновить локальный сервер обновлений:

1. Если вы обновляете MaxPatrol VM с версии 2.0 или 2.1, на локальном сервере обновлений выполните команду:

   ```
   /opt/pt/pt-update-mirror/bin/pt-update-mirror license deactivate --license-token <Путь к файлу license-access-token.key>
   ```
2. Скопируйте архив `pt-update-mirror-<Версия локального сервера обновлений>.tar.gz` с новым дистрибутивом локального сервера обновлений в любой каталог на сервере или виртуальной машине, на которых планируете обновлять локальный сервер обновлений.
3. Перейдите в каталог со скопированным архивом:

   ```
   cd <Путь к каталогу с архивом>
   ```

4. Распакуйте скопированный архив:

   ```
   tar -xf pt-update-mirror-<Версия локального сервера обновлений>.tar.gz
   ```

5. Выполните команду:

   ```
   dpkg -i pt-update-mirror-<Версия локального сервера обновлений>.deb
   ```

Локальный сервер обновлен.

Активация лицензии локального сервера обновлений с помощью ZIP-файла с лицензиями

Внимание! Активацию лицензии локального сервера обновлений необходимо выполнять только при обновлении MaxPatrol VM с версии 2.0 или 2.1.

Для активации лицензии локального сервера обновлений вам потребуется ZIP-файл с лицензиями, полученный от ответственного сотрудника при офлайн-активации PT MC.

► Чтобы активировать лицензию,

Выполните одно из действий:

- Если требуется, чтобы локальный сервер обновлений получал данные от сервера обновлений через интернет, выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --offline-pack <Путь к ZIP-файлу с лицензиями> --update-server https://update.ptsecurity.ru
  ```

- Если требуется, чтобы локальный сервер обновлений, установленный в закрытом сегменте сети, автоматически получал данные от локального сервера, установленного в демилитаризованной зоне, выполните команду:

  ```
  sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --offline-pack <Путь к ZIP-файлу с лицензиями>
  ```

4.1.11. Привязка лицензии MaxPatrol VM к приложению в PT MC

Примечание. Привязку лицензии к приложению необходимо выполнять после завершения установки или обновления MaxPatrol VM.

Привязка выполняется в интерфейсе PT MC. Перед началом привязки необходимо войти в PT MC по ссылке. Для входа вам потребуются логин и пароль учетной записи, также необходимо знать тип учетной записи (локальная или доменная).

► Чтобы привязать лицензию к приложению:

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

   Откроется страница **Лицензии**.

2. Выберите лицензию и нажмите **Привязать**.

   Откроется окно **Привязка лицензии <№> к приложению**.

3. Выберите установленное приложение, к которому нужно привязать лицензию.
4. Нажмите кнопку **Привязать**.

Лицензия привязана.

После привязки лицензии необходимо перезапустить службу компонента MP 10 Core с помощью команды `docker restart $(docker ps -q -a)`, а затем выйти из системы и заново войти.

5. Просмотр и изменение параметров конфигурации MaxPatrol VM

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

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

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

В этом разделе

Просмотр конфигурации роли (см. раздел 5.1)

Изменение конфигурации роли (см. раздел 5.2)

Управление изменением конфигурации ролей с помощью манифеста (см. раздел 5.3)

Настройка SMTP-сервера для отправки уведомлений по электронной почте (см. раздел 5.4)

Настройка прокси-сервера для онлайн-активации PT MC (см. раздел 5.5)

Включение AI-поиска по запросам (см. раздел 5.6)

Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol VM (см. раздел 5.7)

Изменение времени устаревания активов (см. раздел 5.8)

5.1. Просмотр конфигурации роли

- Чтобы просмотреть конфигурацию роли:

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

     Откроется окно для выбора набора параметров.

6. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение).

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

5.2. Изменение конфигурации роли

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

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

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

     Откроется окно для выбора набора параметров.

  6. Выберите вариант **Advanced configuration**.

     Откроется страница со списком параметров (см. приложение).

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

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

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

  Конфигурация роли изменена.

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

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

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

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

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

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

Конфигурация роли изменена.

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

5.3. Управление изменением конфигурации ролей с помощью манифеста

Начиная с версии 2.8 для оптимизации работы вы можете выбрать необходимые роли и внести изменения в их конфигурацию одновременно. Для этого необходимо создать манифест (см. раздел 5.3.2) — файл формата YAML, который задает параметры изменения конфигурации.

В этом разделе

Изменение конфигурации ролей с помощью манифеста (см. раздел 5.3.1)

Создание манифеста для обновления компонентов или изменения конфигурации ролей (см. раздел 5.3.2)

5.3.1. Изменение конфигурации ролей с помощью манифеста

- Чтобы изменить конфигурацию ролей с помощью манифеста:

  1. Обновите (см. раздел 4.1.2) роль Deployer.
  2. Создайте манифест (см. раздел 5.3.2).
  3. Если требуется, добавьте параметры в файл манифеста или измените значения существующих.

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

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

В консоли появится информация о результатах изменения конфигурации:

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

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

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

См. также

Создание манифеста для обновления компонентов или изменения конфигурации ролей (см. раздел 5.3.2)

5.3.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей

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

- Чтобы создать манифест:

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

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

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

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

Таблица 13. Аргументы сценария

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

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

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

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

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

Примеры сценариев создания манифеста

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

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

  Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

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

— `deployer instance export -Type "agentlinux"`

  Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

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

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

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

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

Откроется окно для выбора набора параметров.

6. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение).

7. Укажите значения параметров:

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

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

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

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

10. Нажмите кнопку **OK**.

11. Нажмите **Submit**.

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

12. Нажмите кнопку **OK**.

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

SMTP-сервер настроен.

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

- Чтобы настроить прокси-сервер,

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

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

5.6. Включение AI-поиска по запросам

- Чтобы включить AI-поиск по PDQL-запросам,

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

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

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

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

- Чтобы включить профиль безопасности в Docker-контейнерах ролей:

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

5.8. Изменение времени устаревания активов

По умолчанию время устаревания активов — 90 дней.

- Чтобы установить другое время,

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

6. О технической поддержке

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

Предоставление доступа к обновленным версиям продукта

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

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

Восстановление работоспособности продукта

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

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

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

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

Рассмотрение предложений по доработке продукта

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

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

Портал технической поддержки

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

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

Техническая поддержка на портале предоставляется на русском и английском языках.

Условия предоставления технической поддержки

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

— номер лицензии на использование продукта;

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

— снимки экрана.

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

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

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

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

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

Время реакции и приоритизация заявок

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

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

Таблица 14. Время реакции на заявку

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

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

Обработка и закрытие заявок

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

— о ходе диагностики по заявленной проблеме и ее результатах;

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

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

Специалист закрывает заявку, если:

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

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

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

— заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

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

Приложение. Параметры конфигурации компонентов MaxPatrol VM на Linux

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

Таблица 15. Параметры конфигурации роли Deployer

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

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

Таблица 16. Параметры конфигурации роли SqlStorage

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

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

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

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

Таблица 17. Параметры конфигурации роли LogConnector

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

Таблица 18. Параметры конфигурации роли Observability

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

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

Таблица 19. Параметры конфигурации роли Management and Configuration

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

Таблица 20. Параметры конфигурации роли Core

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

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

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

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

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

Таблица 21. 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 22. Параметры конфигурации роли RMQ Message Bus

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

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

Таблица 23. Параметры конфигурации компонента PT UCS

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

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

positive
technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют около 3000 организаций по всему миру. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.