MaxPatrol VM версия 2.0

Руководство по внедрению

Дата редакции документа: 06.10.2023

Содержание

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, обновлению и удалению 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

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 кнопку **OK**	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду `Stop-Service`	Текст командной строки, примеры кода, прочие данные, которые нужно ввести с клавиатуры, выделены специальным шрифтом. Также выделены специальным шрифтом имена файлов и пути к файлам и папкам
Ctrl+Alt+Delete	Комбинация клавиш. Чтобы использовать комбинацию, клавиши нужно нажимать одновременно
<Название программы>	Переменные заключены в угловые скобки

1.2. Другие источники информации о MaxPatrol VM

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

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

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

2.1. Архитектура MaxPatrol VM

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

В этом разделе

2.1.1. Компонент MaxPatrol 10 Core

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

— централизованное хранение конфигурации активов;

— централизованное управление всеми компонентами системы;

— оперативное реагирование на инциденты информационной безопасности;

— обеспечение взаимодействия подразделений организации при расследовании инцидентов;

— автоматизацию процесса управления уязвимостями;

— поддержку веб-интерфейса системы.

2.1.2. Компонент MaxPatrol 10 Collector

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

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

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

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

2.1.3. Компонент Knowledge Base

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

2.1.4. Компонент PT Management and Configuration

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

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

2.1.5. Компонент PT Update and Configuration Service

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

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

2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol VM:

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

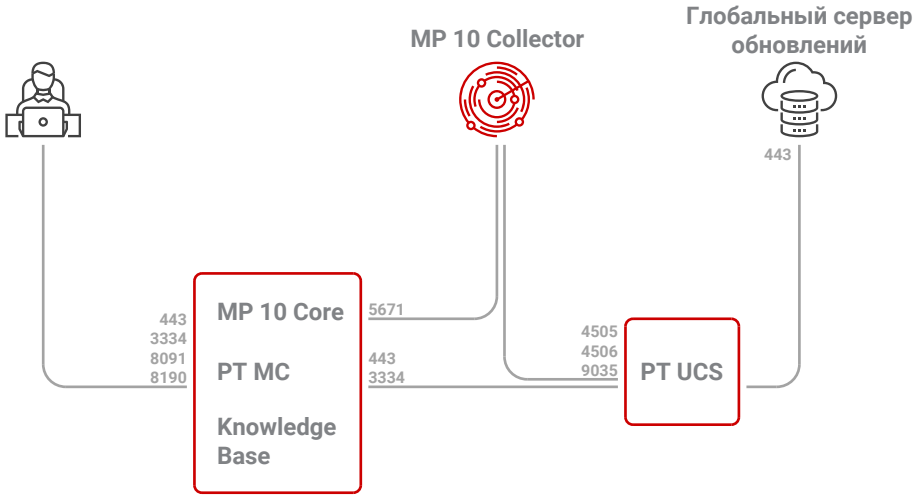

Рисунок 1. Взаимодействие компонентов MaxPatrol VM

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

Таблица 2. Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя	MP 10 Core	443
MP 10 Collector	MP 10 Core	5671
PT UCS	MP 10 Core	443, 3334
Рабочая станция пользователя	PT MC	3334
Рабочая станция пользователя	Knowledge Base	8091, 8190
MP 10 Core, MP 10 Collector	PT UCS	4505, 4506, 9035
PT UCS	Глобальный сервер обновлений	443

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

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

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

3. Развертывание MaxPatrol VM

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

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

Компоненты системы могут быть установлены в виртуальной среде (см. раздел 3.3).

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 коллектор. Количество серверов, требуемых для такой схемы развертывания, увеличивается на число дополнительных коллекторов.

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 (см. раздел 3.10), перезапустить службы компонентов MP 10 Core и Knowledge Base, а затем выйти из системы и заново войти в нее.

В этом разделе

3.1. Требования к программному обеспечению

Все компоненты MaxPatrol VM поддерживают установку на 64-разрядные ОС семейства Linux — Astra Linux Special Edition 1.7 (на базе ядра Linux версий 5.4, 5.10 или 5.15) или Debian 10.3—10.13. Кроме того, вы можете установить компонент MP 10 Collector на Microsoft Windows Server 2012, 2012 R2, 2016, 2019 и 2022.

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).

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.

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).

Поддерживаемые браузеры — Google Chrome версий 49 и выше, Mozilla Firefox версий 45 и выше, Яндекс.Браузер версий 22 и выше.

3.2. Требования к аппаратному обеспечению

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

Требования таблицы рассчитаны для одновременно обрабатываемых результатов сканирования узлов. В задаче на сканирование может быть указано несколько узлов. Количество результатов одной задачи равно количеству сканируемых в задаче узлов: один результат сканирования узла соответствует одному узлу.

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

Количество сканов[1]	**Процессор с тактовой частотой 2,4 ГГц**		**Оперативная память, ГБ**	**Свободное дисковое пространство**
	с использованием технологии Hyperthreading, количество логических ядер	**без использования технологии Hyperthreading, количество физических ядер**		
До 1 000	10	—	20	200 ГБ, HDD

1 Скан — результат успешного сканирования узла.

Количество сканов[1]	Процессор с тактовой частотой 2,4 ГГц		Оперативная память, ГБ	Свободное дисковое пространство
	с использованием технологии Hyperthreading, количество логических ядер	без использования технологии Hyperthreading, количество физических ядер		
До 5 000	20	10	40	300 ГБ, HDD
До 10 000	20	12	72	500 ГБ, HDD
			40	500 ГБ, SSD
До 20 000	20	12	40	900 ГБ, SSD
До 50 000	20	12	70	2,5 ТБ, SSD
До 100 000	20	16	70	4,5 ТБ, SSD

Для повышения производительности MaxPatrol VM рекомендуем использовать процессоры с технологией Hyperthreading.

Таблица 4. Аппаратные требования к серверам MP 10 Collector и PT UCS

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 32 логических ядра. Поддержка инструкций SSE4.2 и AVX
Память (ОЗУ)	64 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый
Жесткие диски	4 диска[2] емкостью 1200 ГБ и скоростью вращения 10 000 об./мин. каждый

Таблица 5. Аппаратные требования к серверу компонента MP 10 Collector, размещенному в отдельном сегменте сети

Компонент сервера	Минимальное требование
Центральный процессор	Тактовая частота 2,2 ГГц, суммарно 8 логических ядер
ОЗУ	32 ГБ
Сетевой адаптер	2 порта со скоростью 1 Гбит/с каждый

2 Рекомендуется объединить диски в массив RAID 10 и преобразовать файловую систему в NTFS (для Microsoft Windows) или ext4 (для Linux, размер блока 4096 байт). Для работы компонентов и баз данных рекомендуется выделить отдельный логический раздел требуемого объема (для каталога /var на Linux или диска D:\ на Microsoft Windows).

Компонент сервера	Минимальное требование
Жесткие диски	2 диска[3] емкостью 1200 ГБ и скоростью вращения 7200 об./мин. каждый

Таблица 6. 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

3.3. Рекомендации по развертыванию MaxPatrol VM в виртуальной среде

Внимание! Не используйте динамическую миграцию виртуальных машин для сервера MP 10 Core, например VMware vSphere vMotion, так как после каждой миграции необходимо повторно активировать лицензию на MaxPatrol VM.

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

Настройка гипервизора

Рекомендуется использовать технологию Storage I/O Control при обмене данными между гипервизором и хранилищами, содержащими виртуальные машины, на которых будут развернуты компоненты системы.

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.

Настройка центрального процессора

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

3 Рекомендуется объединить диски в массив RAID 1 и преобразовать файловую систему в NTFS (для Microsoft Windows) или ext4 (для Linux, размер блока 4096 байт).

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.

Для повышения производительности виртуальной машины рекомендуется в блоке параметров **Hyperthreaded Core Sharing** выбрать режим **None**, в блоке параметров **Resource Allocation** передвинуть максимально вправо ползунок **Reservation** и установить флажок **Unlimited**.

Настройка 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.

Настройка оперативной памяти

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)**.

Настройка виртуальных жестких дисков

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**.

3.4. Сценарий развертывания MaxPatrol VM

Компоненты MP 10 Core, PT MC и Knowledge Base устанавливаются на Linux. При такой установке базовыми единицами развертывания являются роли (см. раздел 3.5).

При развертывании необходимо придерживаться следующего порядка действий:

1. Установка роли Deployer.
2. Установка компонента PT MC.

3. Установка компонента Knowledge Base.
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.

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.

3.5. 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, Knowledge Base 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, Observability и Management and Configuration;

— приложение Knowledge Base — только роль Knowledge Base;

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

Примечание. При развертывании системы можно создать несколько приложений одного типа (например, несколько приложений Knowledge Base), 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.

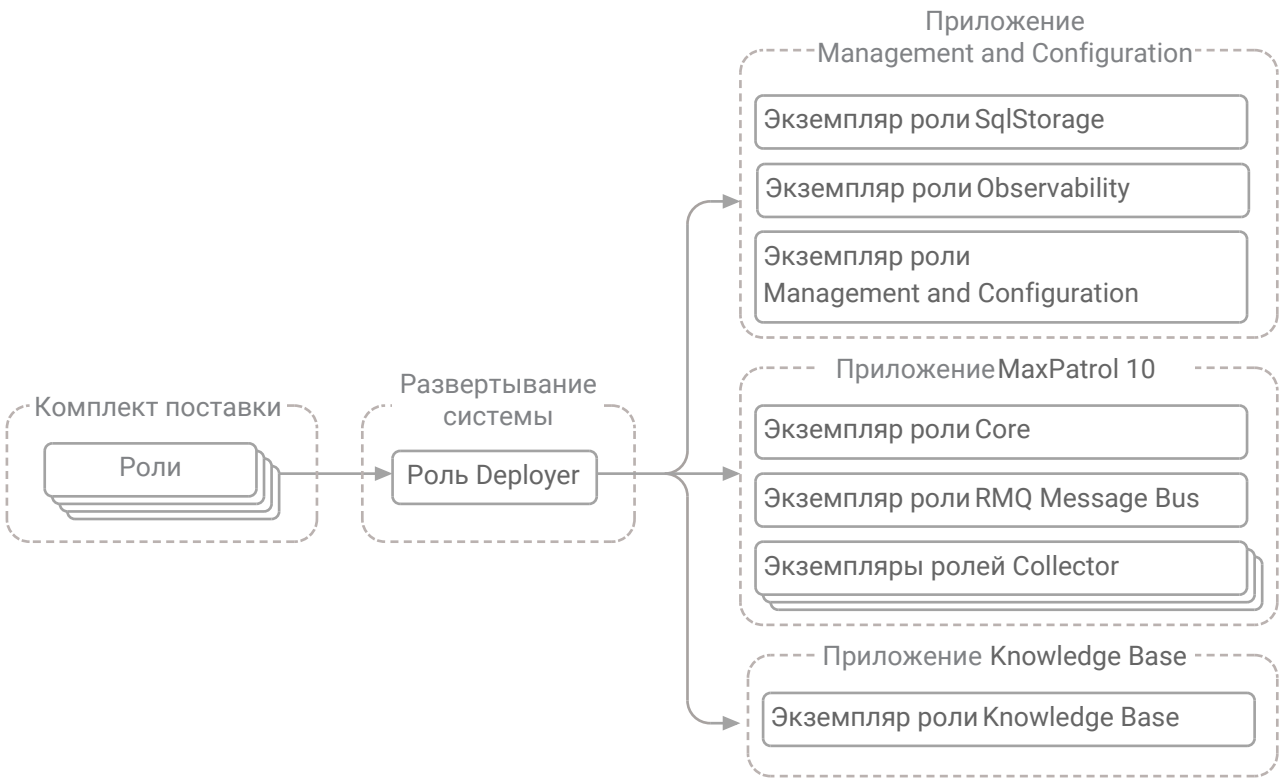

Рисунок 2. Развертывание системы с помощью ролей

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` необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

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.

3.6. 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! 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
   ```
5. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов. По завершении подготовки откроется окно с текстом лицензионного соглашения.
6. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

   Откроется окно для проверки и изменения параметров установки.
7. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.

8. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера, на который устанавливается роль Deployer.

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

9. Нажмите кнопку **OK**.

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

10. Нажмите кнопку **OK**.

11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.7. Установка компонента PT MC на Linux

Компонент PT MC устанавливается на одну операционную систему с компонентом MP 10 Core.

Установка компонента PT MC делится на следующие этапы:

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

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

В этом разделе

3.7.1. Установка роли SqlStorage

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

► Чтобы установить роль:

1. На сервере MP 10 Core 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. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Management and Configuration и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Core.
9. В открывшемся окне введите название экземпляра роли SqlStorage и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.

    Откроется страница со списком основных параметров.
11. 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.
12. Нажмите кнопку **OK**.

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

Роль установлена.

3.7.2. Установка роли Observability

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

► Чтобы установить роль:

1. На сервере MP 10 Core 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. В открывшемся окне нажмите кнопку **Yes**.
4. В открывшемся окне ознакомьтесь с соглашением о сборе телеметрических данных и нажмите **Accept**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
5. Выберите вариант с идентификатором приложения Management and Configuration.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Core.
9. В открывшемся окне введите название экземпляра роли Observability и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.

    Откроется страница со списком основных параметров.
11. В качестве значения параметра `PostgreHost` укажите IP-адрес или FQDN сервера PT MC.

    Внимание! Если в параметрах указать значение `localhost`, установка завершится с ошибкой. Для всех конфигураций систем необходимо указать IP-адрес или FQDN сервера.
12. Если вы хотите отключить отправку телеметрических данных, в окне параметров установки выберите вариант **Advanced configuration** и в качестве значения параметра `AllowToExportTelemetry` выберите `False`.
13. Нажмите кнопку **OK**.

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

14. Нажмите кнопку **OK**.
15. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.7.3. Установка роли Management and Configuration

Внимание! Если вы устанавливаете MaxPatrol VM в изолированном сегменте сети без прямого подключения к интернету, необходимо предварительно установить и настроить локальный сервер обновлений в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» (см. раздел 3.15).

Для установки роли вам потребуется архив `pt_ManagementAndConfiguration_<Номер версии>.tar.gz` из комплекта поставки и токен аутентификации, который хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

Примечание. Новые пользователи MaxPatrol VM получают файл `instance-access-token.key` вместе с лицензией на продукт, а существующие пользователи — вместе с дистрибутивом или через службу технической поддержки.

► Чтобы установить роль:

1. На сервере MP 10 Core 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. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Management and Configuration.
5. В окне **Instance selection** выберите вариант **Deploy New Instance**.
6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Core.
8. В открывшемся окне введите название экземпляра роли Management and Configuration и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.

9. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.

10. В качестве значения параметра `DefaultLocale` выберите язык веб-интерфейса приложения Management and Configuration.

11. 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.

12. 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`.

13. В качестве значения параметра `PackagesSourceUri` укажите:

    - Если вы устанавливаете MaxPatrol VM в сегменте сети с прямым подключением к интернету — адрес глобального сервера обновлений `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.

14. В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.

15. Нажмите кнопку **OK**.

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

16. Нажмите кнопку **OK**.

17. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

См. также

Настройка обновления экспертных данных (см. раздел 3.15)

3.8. Установка компонента Knowledge Base на Linux

Компонент Knowledge Base устанавливается с помощью роли Knowledge Base. Для установки роли вам потребуется архив `pt_KB_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы установить роль:

1. На сервере MP 10 Core распакуйте архив `pt_KB_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_KB_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_KB_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения Knowledge Base и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.
7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Core.
9. В открывшемся окне введите название экземпляра роли Knowledge Base и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.

    Откроется страница со списком основных параметров.
11. В качестве значения параметра `DefaultLocale` выберите желаемый язык интерфейса приложения Knowledge Base.
12. Укажите значения параметров:
    ```
    HostAddress: <IP-адрес или FQDN сервера MP 10 Core>
    PostgreHost: <IP-адрес или FQDN сервера MP 10 Core>
    MCAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:3334
    CoreAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:443
    ```

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

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

14. Нажмите кнопку **OK**.
15. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.9. 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

3.9.1. 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 MP 10 Core 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**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант **Create New Application**.
5. В открывшемся окне введите идентификатор приложения MaxPatrol 10 и нажмите кнопку **OK**.
6. В окне **Instance selection** выберите вариант **Deploy New Instance**.

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
8. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Core.
9. В открывшемся окне введите название экземпляра роли RMQ Message Bus и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
10. Выберите вариант **Basic configuration**.

    Откроется страница со списком основных параметров.
11. 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.
12. Нажмите кнопку **OK**.

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

Роль установлена.

3.9.2. Установка роли Core

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

► Чтобы установить роль:

1. На сервере MP 10 Core 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**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения MaxPatrol 10.
5. В окне **Instance selection** выберите вариант **Deploy New Instance**.

6. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.
7. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Core.
8. В открывшемся окне введите название экземпляра роли Core и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.
9. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.
10. В качестве значения параметра `DefaultLocale` выберите желаемый язык веб-интерфейса приложения MaxPatrol 10.
11. Укажите значения параметров:

    ```
    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.
12. Нажмите кнопку **OK**.

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

Роль установлена.

3.10. Активация лицензии MaxPatrol VM

Для активации лицензии вам потребуются следующие файлы из комплекта поставки:

— шаблон ключа `<Номер лицензии>.grdvd`;

— текстовый файл с серийным номером MaxPatrol VM `<Идентификатор ключа>.txt`;

— мастер активации лицензий `GuardantActivationWizard.exe` (только для офлайн-активации на серверах под управлением Microsoft Windows).

Активация лицензии выполняется на сервере компонента MP 10 Core.

Если активировать несколько лицензий, система будет использовать только одну из них — имеющую самую раннюю дату окончания. Поэтому в случае приобретения продукта, который может быть развернут на базе уже установленного MaxPatrol VM (например, приобретения

MaxPatrol SIEM) необходимо активировать объединенную лицензию на оба продукта (ее можно запросить в службе технической поддержки Positive Technologies). В противном случае после активации отдельной лицензии на второй продукт в системе будет доступен набор функций только одного продукта.

После изменения аппаратной конфигурации сервера MP 10 Core (например, по причине замены центрального процессора) необходимо повторно активировать лицензию. Количество таких повторных активаций ограничено — не более пяти раз. Дальнейшие попытки активации приведут к ошибке мастера активации «Количество активаций для введенного серийного номера исчерпано». Для получения нового шаблона ключа и нового серийного номера необходимо обратиться в службу технической поддержки (см. раздел 6).

Если вы повторно активировали лицензию (например, после переустановки ОС или компонента MP 10 Core) и при этом не изменяли аппаратную конфигурацию сервера, счетчик активаций не уменьшается (количество таких повторных активаций не ограничено).

Информация о лицензии доступна на странице **Система** → **Управление системой**.

В этом разделе

3.10.1. Активация лицензии на Linux при наличии доступа к интернету

► Чтобы активировать лицензию:

1. На сервер MP 10 Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` скопируйте шаблон ключа `<Номер лицензии>.grdvd` и текстовый файл с серийным номером `<Идентификатор ключа>.txt`.
2. Запустите активацию лицензии от имени суперпользователя (root):

   ```
   docker exec -it $(docker ps | awk '/licensing/ {print $NF}') /usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор ключа>.txt
   ```

   По завершении активации появится сообщение `License activation Succeeded`.

Лицензия активирована.

После активации лицензии необходимо перезапустить службы компонентов MP 10 Core и Knowledge Base с помощью команды `docker restart $(docker ps -q -a)`, а затем выйти из системы и заново войти.

3.10.2. Активация лицензии на Linux при отсутствии доступа к интернету

Для активации лицензии вам потребуются рабочая станция с доступом в интернет и файл `GuardantActivationWizard.exe` из комплекта поставки.

► Чтобы активировать лицензию:

1. На сервер MP 10 Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` скопируйте шаблон ключа `<Номер лицензии>.grdvd` и текстовый файл с серийным номером `<Идентификатор ключа>.txt`.
2. Выполните команду от имени суперпользователя (root):

   ```
   docker exec -it $(docker ps | awk '/licensing/ {print $NF}') /usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер лицензии>.grdvd /serialfile=/var/lib/microservice/<Идентификатор ключа>.txt /offline
   ```

   Мастер активации лицензий создаст в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing` файл `<Номер лицензии>.grdvd.toserver`.
3. На рабочей станции с доступом в интернет разместите в одной папке файлы `GuardantActivationWizard.exe` и `<Номер лицензии>.grdvd.toserver`.
4. Запустите файл `GuardantActivationWizard.exe`.

   Откроется окно мастера активации лицензий.
5. Нажмите кнопку **Указать файл лицензии**.
6. В открывшемся окне выберите файл `<Номер лицензии>.grdvd.toserver` и нажмите кнопку **Открыть**.
7. Нажмите кнопку **Далее**.

   Мастер активации лицензий создаст файл `<Номер лицензии>.grdvd.fromserver`. Папка с файлом откроется автоматически.
8. Нажмите кнопку **Готово**.
9. Скопируйте файл `<Номер лицензии>.grdvd.fromserver` на сервер MP 10 Core в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/data/licensing`.
10. Выполните команду:

    ```
    docker exec -it $(docker ps | awk '/licensing/ {print $NF}') /usr/local/bin/guardantutils/grdspactivation /var/lib/microservice/<Номер лицензии>.grdvd.fromserver
    ```

    По завершении активации появится сообщение `License activation Succeeded`.

Лицензия активирована.

После активации лицензии необходимо перезапустить службы компонентов MP 10 Core и Knowledge Base с помощью команды `docker restart $(docker ps -q -a)`, а затем выйти из системы и заново войти.

3.11. 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 проводить аудит активов с Microsoft Windows по протоколу SMBv1, собирать события с профилем CheckpointOpsecLog, собирать данные по протоколам SMB, DCE и RPC в режиме пентеста, а также использовать протокол Kerberos. Производительность работы MP 10 Collector, установленного на Linux, в режиме пентеста на 15—40% ниже, чем на Microsoft Windows.

Если компоненты MP 10 Core, PT MC и Knowledge Base установлены на Microsoft Windows, перед установкой компонента MP 10 Collector на Linux необходимо установить роль Deployer на сервер PT UCS.

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.

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

В этом разделе

См. также

Установка роли Deployer (см. раздел 3.6)

3.11.1. Установка модуля Salt Minion на сервер MP 10 Collector

> **Внимание!** Для средненагруженных и высоконагруженных систем на сервере, на который устанавливается модуль Salt Minion, порт 22/TCP должен быть открыт для входящих соединений.

► 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 кнопку **OK**.
9. Введите пароль учетной записи с правами суперпользователя (root) на сервере MP 10 Collector.

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

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

Модуль Salt Minion установлен.

3.11.2. Установка роли Collector

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

► Чтобы установить роль:

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

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

2. Запустите сценарий:

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

3. В открывшемся окне нажмите кнопку **Yes**.

   Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.

4. Выполните одно из следующих действий:

   - Если в открывшемся окне 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**, в открывшемся окне введите идентификатор приложения MaxPatrol 10 и нажмите кнопку **OK**.

6. В окне **Instance selection** выберите вариант **Deploy New Instance**.

7. В открывшемся окне ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

8. В открывшемся окне выберите вариант с доменным именем сервера MP 10 Collector.

9. В открывшемся окне введите название экземпляра роли Collector и нажмите кнопку **OK**.

   Откроется окно для проверки и изменения параметров установки.

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 кнопку **OK**.

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

15. Нажмите кнопку **OK**.
16. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль установлена.

3.11.3. Установка компонента MP 10 Collector на Microsoft Windows

Для установки компонента MP 10 Collector на Microsoft Windows вам потребуется файл `MPXAgentSetup_<Номер версии>.exe` из комплекта поставки.

► Чтобы установить компонент MP 10 Collector:

1. Запустите файл `MPXAgentSetup_<Номер версии>.exe`.

   Откроется окно мастера установки.
2. Ознакомьтесь по ссылке с текстом лицензионного соглашения.
3. Установите флажок **Я принимаю условия лицензионного соглашения** и нажмите кнопку **Продолжить**.
4. Укажите пути для установки.

   Примечание. Если вы хотите установить компоненты в папки по умолчанию, не изменяйте значения полей.
5. Нажмите кнопку **Продолжить**.
6. В поле **Имя коллектора** 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 кнопку **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 кнопку **Назад**, и указать корректные значения параметров.
9. Нажмите кнопку **Установить**.
10. По завершении установки нажмите кнопку **Закрыть**.

11. Если устанавливается первый компонент MP 10 Collector и компонент MP 10 Core установлен на Linux, на сервере с установленной ролью Deployer выполните команды:
```
cp /opt/deployer/pki/legacy_ca/windows-selfsigned-default.pem /opt/deployer/pki/trusted_ca/
dpkg-reconfigure deployer
/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId RmqMessageBus
```
12. Если устанавливается первый компонент MP 10 Collector и компонент MP 10 Core установлен на Linux, перезапустите службу core-agent.
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>
```

Компонент MP 10 Collector установлен.

3.12. Установка компонента PT UCS

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

► Чтобы установить компонент PT UCS:

1. На сервере PT UCS распакуйте архив `ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar`:
```
tar -xf ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar -C <Путь к каталогу для распаковки архива>
```
2. Запустите сценарий:
```
<Путь к каталогу для распаковки архива>/siem-ucs-debian<Номер версии Debian>-<Номер версии MaxPatrol VM>/install.sh
```
   Откроется окно **UCS configuration**.
3. Выберите вариант **Skip** и подтвердите установку компонента.

   Запустится установка PT UCS. По завершении установки интерфейс терминала отобразит сообщение:
```
Done installing ucs-pt
```

Компонент PT UCS установлен, его настройка не требуется. Проверка наличия новых версий компонентов системы, их загрузка и установка будут происходить автоматически.

3.13. 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 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`;

— в расширении Subject Alternative Name (SAN) содержать запись об FQDN сервера компонента или его IP-адресе в зависимости от значения параметра `HostAddress` (оно может быть равно как FQDN, так и IP-адресу).

► 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, Management and Configuration и Knowledge Base.

2. На сервере MP 10 Core разместите файлы сертификатов центров сертификации всей цепочки в каталоге `/opt/deployer/pki/trusted_ca/`.

3. Выполните команду:
   ```
   dpkg-reconfigure deployer
   ```

4. Измените конфигурации (см. раздел 5.1.2) ролей Core, Management and Configuration и Knowledge Base:
   ```
   SSLCertificatePemFileName: <Имя файла сертификата>
   SSLKeyFileName: <Имя файла закрытого ключа>
   ```

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

Сертификат установлен.

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.

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;

— использовать отдельные файлы для хранения сертификата центра сертификации (ЦС), 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 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;

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

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

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

1. Разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей RMQ Message Bus, Core и Collector.

2. Измените конфигурацию роли RMQ Message Bus:

```
CACertFile: <Имя файла сертификата ЦС>
CertFile: <Имя файла пользовательского сертификата>
KeyFile: <Имя файла закрытого ключа>
```

3. Измените конфигурацию роли Core:

```
CACertificateFileName: <Имя файла сертификата ЦС>
RMQSslCertificateFileName: <Имя файла пользовательского сертификата>
RMQSslKeyFileName: <Имя файла закрытого ключа>
```

4. Измените конфигурацию роли Collector:

```
Agent_RMQ_SSL_CA_Certificate: <Полный путь к файлу сертификата ЦС>
Agent_RMQ_SSL_Certificate: <Полный путь к файлу пользовательского сертификата>
Agent_RMQ_SSL_Key: <Полный путь к файлу закрытого ключа>
```

Сертификат установлен.

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. Процесс миграции на новую модель хранения экспертных данных является обязательным и запускается после обновления MaxPatrol VM. Для осуществления миграции необходимо:

— Если обновление экспертных данных будет осуществляться напрямую с сервера обновлений Positive Technologies или через локальный сервер обновлений — настроить обновление одним из перечисленных ниже способов.

— Если обновление экспертных данных будет осуществляться вручную — после обновления роли Management and Configuration необходимо загрузить с сайта update.ptsecurity.com файл миграционного пакета данных с названием вида `migration.vm.s.1.0.v.<Версия пакета данных>.pkg` и разместить его на сервере с ролью Management and Configuration в каталоге `/var/lib/deployed-roles/mc-application/managementandconfiguration/data/resources/local-packages/`.

Перед настройкой подключения к серверу обновлений нужно получить токен для аутентификации. Новые пользователи MaxPatrol VM получают токен вместе с лицензией на продукт. Существующие пользователи MaxPatrol VM получают токен с дистрибутивом версии 2.0 или через службу технической поддержки. Токен хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64.

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 (см. раздел 3.7.3) или обновлении (см. раздел 4.1.3.2) роли Management and Configuration указать значения параметров

ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken. Если роль Management and Configuration уже установлена, укажите значения параметров в соответствии с инструкцией (см. раздел 3.15.1).

Получение обновлений через локальный сервер, установленный в демилитаризованной зоне

Если из изолированного сегмента сети организации есть доступ в интернет (напрямую 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. Установить (см. раздел 3.15.3) в демилитаризованной зоне локальный сервер обновлений.
2. Если требуется, настроить подключение (см. раздел 3.15.5) локального сервера обновлений к прокси-серверу.
3. Активировать лицензию (см. раздел 3.15.4) на локальном сервере обновлений.
4. При установке (см. раздел 3.7.3) или обновлении (см. раздел 4.1.3.2) роли Management and Configuration указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken. Если роль Management and Configuration уже установлена, укажите значения параметров в соответствии с инструкцией (см. раздел 3.15.1).

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. Установить (см. раздел 3.15.3) два локальных сервера обновлений: в закрытом сегменте сети и в демилитаризованной зоне.
2. Если планируется ручной перенос обновлений (см. раздел 3.15.7) между локальными серверами в закрытом сегменте сети и демилитаризованной зоне — активировать лицензию (см. раздел 3.15.4) на локальном сервере обновлений, установленном в демилитаризованной зоне.

3. Если планируется автоматический перенос обновлений (см. раздел 3.15.6) между локальными серверами в закрытом сегменте сети и демилитаризованной зоне — активировать лицензии (см. раздел 3.15.4) на обоих локальных серверах обновлений.
4. Если между локальными серверами обновлений есть сетевое взаимодействие и необходимо автоматизировать процесс обновления — настроить подключение (см. раздел 3.15.6) локального сервера обновлений в изолированном сегменте сети к локальному серверу в демилитаризованной зоне.
5. При установке (см. раздел 3.7.3) или обновлении (см. раздел 4.1.3.2) роли Management and Configuration указать значения параметров ExpertDataUpdateMethod, PackagesSourceUri и PackagesSourceCredentialToken. Если роль Management and Configuration уже установлена, укажите значения параметров в соответствии с инструкцией (см. раздел 3.15.1).

В этом разделе

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

Для выполнения инструкции вам потребуется токен аутентификации, который хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

> **Примечание.** Новые пользователи MaxPatrol VM получают файл `instance-access-token.key` вместе с лицензией на продукт, а существующие пользователи — вместе с дистрибутивом или через службу технической поддержки.

► Чтобы изменить параметры роли:

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

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

   Откроется страница со списком параметров (см. приложение).
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 — адрес глобального сервера обновлений `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. В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.
10. Нажмите кнопку **OK**.

    Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
11. 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 или 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, Ubuntu 18.04, Ubuntu 22.04, Debian 10 или Debian 11.

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 (см. раздел 3.15.8) 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 (см. раздел 3.15.2).

► 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 (см. раздел 3.15.4).

Если локальный сервер обновлений установлен в закрытом сегменте сети, активировать на нем лицензию необходимо только в случае, когда планируется автоматический перенос обновлений (см. раздел 3.15.6) между локальными серверами в закрытом сегменте сети и демилитаризованной зоне.

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.

Вы можете активировать лицензию с помощью ее серийного номера или токена лицензии (хранится в файле `license-access-token.key`), полученных на физическом носителе или в электронном письме на адрес, указанный при покупке.

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.

Активация лицензии с помощью серийного номера

► Чтобы активировать лицензию с помощью серийного номера:

1. Выполните команду:
   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --serial-number <Серийный номер лицензии>
   ```
2. Запустите процесс скачивания обновлений с помощью команды обновления репозитория:
   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
   ```

Лицензия активирована.

Активация лицензии с помощью токена лицензии

► Чтобы активировать лицензию с помощью токена лицензии:

1. Выполните команду:
   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror license activate --license-token <Путь к файлу license-access-token.key>
   ```
2. Запустите процесс скачивания обновлений с помощью команды обновления репозитория:
   ```
   sudo /opt/pt/pt-update-mirror/bin/pt-update-mirror repository update
   ```

Лицензия активирована.

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 (см. раздел 3.15.8) 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 (см. раздел 3.15.5).

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 (см. раздел 3.15.8) 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 (см. раздел 3.15.5).

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 порт подключения:

1. Откройте файл `pt-update-mirror.service`:
   `sudo nano etc/systemd/system/pt-update-mirror.service`
2. Выполните одно из следующих действий:

   Если для подключения локального сервера используется протокол HTTP, в блок параметров `Service` в конец строки с параметром `ExecStart` добавьте ключ `--http-port <Порт>`.

   Если для подключения локального сервера используется протокол HTTPS, в блок параметров `Service` в конец строки с параметром `ExecStart` добавьте ключ `--https-port <Порт>`.
3. Сохраните изменения в файле `pt-update-mirror.service`.
4. Примените изменения таймера:
   `sudo systemctl daemon-reload`
5. Перезапустите локальный сервер обновлений:
   `sudo systemctl restart pt-update-mirror`

Порт подключения изменен.

3.16. Настройка MaxPatrol VM для обеспечения его безопасной работы

В этом разделе приводятся инструкции по настройке развернутой конфигурации MaxPatrol VM для обеспечения его безопасной работы.

Компоненты системы рекомендуется разместить в доверенном сегменте сети. Доступ к ним из других сегментов рекомендуется ограничить с помощью межсетевого экрана.

В этом разделе

3.16.1. Настройка MaxPatrol VM для обеспечения его безопасной работы: 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 -F DOCKER-USER
   iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -m conntrack --ctstate
   ESTABLISHED,RELATED -j ACCEPT
   iptables -A DOCKER-USER -i <Название внешнего сетевого интерфейса> -s <IP-адреса рабочих
   станций пользователей> -p tcp -m multiport --dports 443,3334,8091,8190 -m conntrack --
   ctstate NEW -m comment --comment "Web user access" -j ACCEPT
   ```

3. 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>
   ```

4. 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
```

5. 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
```

6. 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
```

7. 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
```

8. 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.

9. Сохраните правила межсетевого экрана:

```
netfilter-persistent save
```

10. 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
```

11. 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`.

12. Если для сбора событий по стандарту syslog и протоколу Netflow коллекторы на Microsoft Windows не используют порты по умолчанию, на серверах коллекторов удалите правила для входящих соединений с этих портов:

```
for %P IN (514,1468) DO (netsh advfirewall firewall delete rule name=all protocol=tcp localport=%P)
for %P IN (514,2055) DO (netsh advfirewall firewall delete rule name=all protocol=udp localport=%P)
```

13. Разрешите входящие соединения для сбора событий по стандарту syslog и протоколу Netflow на серверах коллекторов на Linux для портов, указанных при создании задачи на сбор событий:

```
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p tcp -m tcp --dport 1468 -m conntrack --ctstate NEW -m comment --comment "Agent SysLog (TCP)" -j ACCEPT
iptables -A INPUT -i <Название внешнего сетевого интерфейса> -p udp -m udp --dport 514 -m conntrack --ctstate NEW -m comment --comment "Agent SysLog (UDP)" -j ACCEPT
```

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. Установите собственные доверенные сертификаты (см. раздел 3.13) для MP 10 Core, Knowledge Base, PT MC и RabbitMQ.

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

```
adduser <Логин администратора>
```

18. 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.

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

20. 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
```

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

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

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

23. Смените пароль учетной записи Administrator.

MaxPatrol VM настроен.

4. Обновление MaxPatrol VM

Вы можете обновлять компоненты MaxPatrol VM:

— с помощью дистрибутивов;

— MP 10 Collector на Microsoft Windows — через веб-интерфейс MaxPatrol VM.

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).

В версии 1.1 обновлены SSL-сертификаты, поставляемые в составе MaxPatrol VM. Во время обновления системы с версии 1.0 (после обновления MP 10 Core и до обновления коллекторов) будут недоступны как сами коллекторы, так и работа с задачами на сбор данных.

В этом разделе

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.

Начиная с версии 1.5 базовыми единицами установки и обновления компонентов Linux являются роли (см. раздел 3.5). Обновление компонентов на Linux необходимо выполнять в следующем порядке: PT UCS → роль Deployer → PT MC → Knowledge Base → MP 10 Core → MP 10 Collector.

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.

В этом разделе

4.1.1. Обновление компонента PT UCS

Для обновления вам потребуется архив `ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar` из комплекта поставки.

► Чтобы обновить компонент PT UCS:

1. На сервере PT UCS распакуйте архив `ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar`:

   ```
   tar -xf ucs-<Номер версии MaxPatrol VM>-debian<Номер версии Debian>.tar -C <Путь к каталогу для распаковки архива>
   ```

2. Запустите сценарий:

   ```
   <Путь к каталогу для распаковки архива>/siem-ucs-debian<Номер версии Debian>-<Номер версии MaxPatrol VM>/install.sh
   ```

   Откроется окно **UCS configuration**.

3. Выберите вариант **Skip** и подтвердите обновление компонента.

   Запустится обновление PT UCS. По завершении обновления интерфейс терминала отобразит сообщение:

   ```
   Done installing ucs-pt
   ```

Компонент PT UCS обновлен.

4.1.2. Обновление роли Deployer

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
   ```

3. В открывшемся окне нажмите кнопку **Yes**.

   Начнется распаковка и подготовка пакетов. По завершении подготовки откроется окно для проверки и изменения параметров обновления.

4. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.

5. Убедитесь, что в качестве значения параметра `HostAddress` указан IP-адрес или FQDN сервера, на который установлена роль Deployer.

6. Нажмите кнопку **OK**.

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

7. Нажмите кнопку **OK**.

8. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.1.3. Обновление компонента PT MC на Linux

Обновление компонента PT MC производится в следующем порядке:

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

В этом разделе

Обновление роли SqlStorage (см. раздел 4.1.3.1)

Обновление роли Management and Configuration (см. раздел 4.1.3.2)

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 MP 10 Core 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. В открывшемся окне нажмите кнопку **Yes**.

   Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.

4. Выберите вариант с идентификатором приложения Management and Configuration.

5. В открывшемся окне выберите вариант с названием экземпляра роли SqlStorage.

   Откроется окно для проверки и изменения параметров установки.

6. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.

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

8. Нажмите кнопку **OK**.

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

9. Нажмите кнопку **OK**.

10. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.1.3.2. Обновление роли Management and Configuration

Внимание! Если вы обновляете MaxPatrol VM в изолированном сегменте сети без прямого подключения к интернету, необходимо предварительно установить и настроить локальный сервер обновлений в соответствии с инструкциями в разделе «Настройка обновления экспертных данных» (см. раздел 3.15).

Для обновления роли вам потребуется архив `pt_ManagementAndConfiguration_<Номер версии>.tar.gz` из комплекта поставки и токен аутентификации, который хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64. Этот набор символов необходимо будет указать в качестве значения конфигурационного параметра `PackagesSourceCredentialToken` на одном из шагов инструкции.

Примечание. Новые пользователи MaxPatrol VM получают файл `instance-access-token.key` вместе с лицензией на продукт, а существующие пользователи — вместе с дистрибутивом или через службу технической поддержки.

► Чтобы обновить роль:

1. На сервере MP 10 Core 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. В открывшемся окне нажмите кнопку **Yes**.

Начнутся распаковка и подготовка пакетов, необходимых для установки. По завершении подготовки откроется окно для выбора приложения.

4. Выберите вариант с идентификатором приложения Management and Configuration.
5. В открывшемся окне выберите вариант с названием экземпляра роли Management and Configuration.

   Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.
7. В качестве значения параметров `HostAddress` и `PostgreHost` укажите IP-адрес или FQDN сервера MP 10 Core.
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 — адрес глобального сервера обновлений 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. В качестве значения параметра `PackagesSourceCredentialToken` укажите содержимое файла `instance-access-token.key`.
11. Нажмите кнопку **OK**.

    Начнется установка пакетов. По завершении установки появится сообщение `Deployment configuration successfully applied`.
12. Нажмите кнопку **OK**.
13. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

После обновления роли Management and Configuration необходимо загрузить с сайта update.ptsecurity.com файл миграционного пакета данных с названием вида `migration.vm.s.1.0.v.<Версия пакета данных>.pkg` и разместить его на сервере с ролью

Management and Configuration в каталоге `/var/lib/deployed-roles/mc-application/managementandconfiguration/data/resources/local-packages/`. Это необходимо для прохождения процесса миграции на новую модель хранения экспертных данных. Процесс миграции является обязательным и запускается после обновления MaxPatrol VM.

4.1.4. Обновление компонента Knowledge Base на Linux

Для обновления компонента необходимо обновить роль Knowledge Base. Для обновления роли вам потребуется архив `pt_KB_<Номер версии>.tar.gz` из комплекта поставки.

► Чтобы обновить роль:

1. На сервере MP 10 Core распакуйте архив `pt_KB_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_KB_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_KB_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения Knowledge Base.
5. В открывшемся окне выберите вариант с названием экземпляра роли Knowledge Base.

   Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.
7. Укажите значения параметров:
   ```
   HostAddress: <IP-адрес или FQDN сервера MP 10 Core>
   PostgreHost: <IP-адрес или FQDN сервера MP 10 Core>
   MCAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:3334
   CoreAddress: https://<IP-адрес или FQDN сервера MP 10 Core>:443
   ```
8. Нажмите кнопку **OK**.

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

Роль обновлена.

4.1.5. Обновление компонента MP 10 Core на Linux

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

В этом разделе

4.1.5.1. 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.

► Чтобы обновить роль:

1. На сервере MP 10 Core 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**.

   Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения MaxPatrol 10.
5. В открывшемся окне выберите вариант с названием экземпляра роли RMQ Message Bus, который установлен на сервер MP 10 Core.

   Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.
7. В качестве значения параметра `HostAddress` укажите IP-адрес или FQDN сервера MP 10 Core.
8. Нажмите кнопку **OK**.

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

9. Нажмите кнопку **OK**.
10. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Роль обновлена.

4.1.5.2. Обновление роли Core

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

► Чтобы обновить роль:

1. На сервере MP 10 Core 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**.

   Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения MaxPatrol 10.
5. В открывшемся окне выберите вариант с названием экземпляра роли Core.

   Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Basic configuration**.

   Откроется страница со списком основных параметров.
7. Укажите значения параметров:
   ```
   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>
   ```
8. Нажмите кнопку **OK**.

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

Роль обновлена.

4.1.6. 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 Collector и установить роль Collector из комплекта поставки в соответствии с инструкцией (см. раздел 3.11.2).

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

► Чтобы обновить роль:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_AgentLinux_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_AgentLinux_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_AgentLinux_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.

   Начнется распаковка и подготовка пакетов, необходимых для обновления. По завершении подготовки откроется окно для выбора приложения.
4. Выберите вариант с идентификатором приложения MaxPatrol 10.
5. В открывшемся окне выберите вариант с названием экземпляра роли Collector.

   Откроется окно для проверки и изменения параметров установки.
6. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров.
7. В качестве значения параметра `AgentRMQHost` укажите IP-адрес или FQDN сервера MP 10 Core.
8. В качестве значения параметра `AgentRMQVirtualHost` выберите `Core.`
9. Нажмите кнопку **OK**.

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

Роль обновлена.

4.1.7. 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 файл `MPXAgentSetup_<Номер версии>.exe` из комплекта поставки.

► Чтобы обновить компонент MP 10 Collector:

1. 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 кнопку **Обновить**.
4. По завершении обновления нажмите кнопку **Закрыть**.
5. В командной строке Microsoft Windows выполните команду от имени администратора:
   ```
   coreagentcfg set -p AgentRMQVirtualHost mpx
   ```

Компонент MP 10 Collector обновлен.

4.2. Обновление компонента MP 10 Collector через веб-интерфейс

Перед обновлением необходимо:

— убедиться, что установлен и настроен компонент PT UCS;

— если версии компонента MP 10 Core ниже версии, на которую вы хотите обновить MP 10 Collector, — сначала обновить MP 10 Core.

► Чтобы обновить компонент MP 10 Collector:

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

   Откроется страница **Управление системой**.

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

   В рабочей области страницы отобразится таблица со списком коллекторов.

3. В списке выберите коллектор.

Если обновление для коллектора доступно, в правой панели отобразится информация о версии обновления и в панели управления станет активной кнопка **Обновить версию**.

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

4. Если обновление для коллектора доступно, нажмите кнопку **Обновить версию**.

   Статус коллектора изменится с **Доступен** на **Обновляется**.

По завершении обновления центральная панель отобразит новую версию коллектора. Компонент MP 10 Collector обновлен.

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.

В этом разделе

5.1. Просмотр и изменение конфигурации компонентов MaxPatrol VM на Linux

Конфигурация компонента включает в себя параметры конфигураций ролей, с помощью которых компонент был установлен. Для 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

См. также

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

5.1.1. Просмотр конфигурации роли

► Чтобы просмотреть конфигурацию роли:

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

   Откроется окно для выбора набора параметров.

5. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение).

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

5.1.2. Изменение конфигурации роли

► Чтобы изменить конфигурацию роли:

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

   Откроется окно для выбора набора параметров.

6. Выберите вариант **Advanced configuration**.

   Откроется страница со списком параметров (см. приложение).

7. Измените значения параметров.
8. Нажмите кнопку **OK**.
9. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

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

10. Нажмите кнопку **OK**.
11. Если требуется, подтвердите изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажав кнопку **Confirm** в открывшемся окне.

Конфигурация роли изменена.

5.1.3. 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, собираемых событиях и параметрах потока событий, а также о выявляемых инцидентах ИБ 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 MP 10 Core 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. В открывшемся окне выберите вариант с идентификатором приложения роли.
5. В открывшемся окне выберите вариант с названием экземпляра роли.

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

   Откроется страница со списком параметров (см. приложение).
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. Если необходима проверка 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. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

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

SMTP-сервер настроен.

6. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту);
- консультацию по использованию функциональных возможностей продукта.

Вы можете получать техническую поддержку на портале.

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

В этом разделе

6.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

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

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

Техническая поддержка на портале предоставляется на русском и английском языках.

6.2. Время работы службы технической поддержки

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

6.3. Как служба технической поддержки работает с запросами

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

В этом разделе

6.3.1. Предоставление информации для технической поддержки

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

— номер лицензии на использование продукта;

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

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

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

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

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

6.3.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

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

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

Устранение дефектов продукта

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

6.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 7).

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

Таблица 7. Время реакции на запрос и время его обработки

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

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

6.3.4. Выполнение работ по запросу

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

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

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

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

Работы по запросу считаются выполненными, если:

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

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

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

— проблема классифицирована как неподдерживаемая.

Приложение. Параметры конфигурации компонентов MaxPatrol VM на Linux

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

Таблица 8. Параметры конфигурации роли Deployer

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

Таблица 9. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
`PgAdminPort`	Порт для доступа к pgAdmin	`9001`
`PgAnalyzeScaleFactor`	Процент от размера таблицы, который будет добавляться к параметру autovacuum_analyze_threshold при выборе порога срабатывания команды ANALYZE	`0.0`
`PgAnalyzeThreshold`	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	`200000`
`PgEffectiveCacheSize`	Эффективный размер дискового кэша, доступный для одного запроса	`6GB`
`PgEmail`	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	`email@email.com`

Параметр	Описание	Значение по умолчанию
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения — HDD или SSD)	HDD
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения — panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5	warning
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который сервер баз данных будет использовать для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
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

Таблица 10. Параметры конфигурации роли Observability

Параметр	Описание	Значение по умолчанию
AllowToExportTelemetry	Данные телеметрии отправляются (True) или не отправляются (False) на сервер приема телеметрии	True
CollectorServerHttpPort	Порт для доступа к серверу сбора журналов по протоколу HTTP	4318

Параметр	Описание	Значение по умолчанию
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента MP 10 Core
ExportEnabledFrom	Разрешенное начальное время отправки телеметрии	00:00:00
ExportEnabledTo	Разрешенное конечное время отправки телеметрии	23:59:59
FlusUri	Адрес сервера приема телеметрии	—
InstanceAccessToken	Токен авторизации на сервере приема телеметрии	—
JobExecutingInterval	Интервал запуска работ внутри сервиса Telemetry.Tracker	00:01:00
MetricsHttpPort	Порт для доступа к метрическим данным	8428
MetricsRetention	Время сохранения метрических данных в базе данных	30d
Network	Сетевое имя реестра Docker-образов	observability.network.observability
NetworkDriver	Драйвер Docker-образов	bridge
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	—
PostgrePassword	Пароль служебной учетной записи для доступа к серверу СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432
PostgreUserName	Логин служебной учетной записи для доступа к серверу СУБД PostgreSQL	pt_system
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	—
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	—

Параметр	Описание	Значение по умолчанию
`TelemetryFileSize`	Максимальный размер файла телеметрии в мегабайтах	`50`
`TelemetryPackSize`	Максимальный размер архива в мегабайтах, который можно отправить на сервер приема телеметрии	`35`

Таблица 11. Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
`ActionLogBatchSize`	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service единовременно отправляет службе MC User Action Logging Service	`100`
`ActionLogMillisecondsDelay`	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	`1000`
`DefaultLocale`	Интерфейс PT MC отображается на русском (`ru-RU`) или английском (`en-US`) языке	`ru-Ru`
`ExpertDataUpdateMethod`	Метод получения обновлений экспертных данных. Возможные значения: Online или Offline	—
`HostAddress`	IP-адрес или FQDN сервера PT MC	—
`IamCookieLifetime`	Время жизни неактивной сессии в MaxPatrol VM (в часах)	`168`
`LdapTimeout`	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	`60000`
`LogCleanLimit`	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	`1000000`

Параметр	Описание	Значение по умолчанию
`MasterRedirectEnabled`	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
`PackageManagementPort`	Номер порта сервиса управления пакетами Package Management	`8585`
`PackagesSourceCredentialToken`	Токен для авторизации на сервере обновлений. Хранится в файле `instance-access-token.key` и представляет собой набор символов, закодированных с использованием стандарта Base64	–
`PackagesSourceUri`	Адрес сервера обновлений	–
`PostgreHost`	IP-адрес или FQDN сервера с установленной ролью SqlStorage	–
`PostgrePassword`	Пароль служебной учетной записи для доступа PT MC к СУБД PostgreSQL	`P@ssw0rdP@ssw0rd`
`PostgrePort`	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	`5432`
`PostgreUserName`	Логин служебной учетной записи для доступа PT MC к СУБД PostgreSQL	`pt_system`
`TmSiteAlias`	Псевдоним площадки	`SITE`
`TmSiteId`	Идентификатор площадки	—
`TmTenantManagerId`	Идентификатор службы MC Tenant Manager Service	—

Таблица 12. Параметры конфигурации роли Knowledge Base

Параметр	Описание	Значение по умолчанию
`ClientId`	Идентификатор для регистрации приложения Knowledge Base в PT MC	`ptkb`
`ClientSecret`	Ключ для регистрации приложения Knowledge Base в PT MC	`secret`
`CoreAddress`	IP-адрес или FQDN сервера MP 10 Core	`localhost`
`DefaultLocale`	Интерфейс Knowledge Base отображается на русском (`ru-RU`) или английском (`en-US`) языке	—
`DeploymentType`	Тип развертывания Knowledge Base	—
`DisplayName`	Название приложения Knowledge Base в PT MC	`Knowledge Base`
`EditableOrigins`	Поставщик, атрибуты объектов которого можно изменять	`Local`
`HostAddress`	IP-адрес или FQDN сервера Knowledge Base	`localhost`
`OriginNameENG`	Полное название поставщика для объектов Knowledge Base на английском языке	`Local system`
`OriginNameRUS`	Полное название поставщика для объектов Knowledge Base на русском языке	`Локальная система`
`OriginNickName`	Псевдоним поставщика для объектов Knowledge Base	`LOC`
`OriginSystemName`	Поставщик объектов Knowledge Base	`Local`
`PostgreHost`	IP-адрес или FQDN сервера БД PostgreSQL	`localhost`
`PostgrePassword`	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	`P@ssw0rdP@ssw0rd`

Параметр	Описание	Значение по умолчанию
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
ShowDiffObjectId	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>
SmtpUseDefaultCredentials	Режим аутентификации SMTP-сервера: флажок установлен — для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtpUser и SmtpPassword); флажок снят — для аутентификации используются логин и пароль, указанные в параметрах SmtpUser и SmtpPassword	Флажок установлен
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—

Параметр	Описание	Значение по умолчанию
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics

Таблица 13. Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
ConsiderEventsImportance	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят)	Флажок установлен
ContentDeployerPort	Номер порта сервиса установки обновлений экспертизы Content Deployer	8586
DefaultAssetTtl	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	90.00:00:00
DefaultLocale	Интерфейс MaxPatrol VM отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
EmailNotificationRetryCount	Максимальное количество попыток отправки сообщения на SMTP-сервер	10
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
IncidentAggregationTimeout	Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>)	00:01:00

Параметр	Описание	Значение по умолчанию
IncidentIdenticalNotificationLimit	Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент	100
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
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	—
PtkbUpdateCheckPeriod	Период проверки наличия обновления для базы знаний, используемой в MP 10 Core (<Часы>:<Минуты>:<Секунды>)	00:05:00
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O
RMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	RMQ_Core_Client.p12
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
SaltMasterHost	IP-адрес или FQDN сервера с модулем Salt Master	—
SaltMasterPort	Порт сервера с модулем Salt Master для входящих подключений от MP 10 Core	9035

Параметр	Описание	Значение по умолчанию
`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`
`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`

Параметр	Описание	Значение по умолчанию
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpUser	Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsageMonitoringCheckingPeriod	Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)	00:15:00
UsePtbkServer	MP 10 Core проверяет (флажок установлен) или не проверяет (флажок снят) наличие обновления базы знаний об уязвимостях в Knowledge Base	Флажок установлен
VulnerStateCheckInterval	Период проверки статусов экземпляров уязвимостей (<Дни>.<Часы>:<Минуты>:<Секунды>)	01.00:00:00
VulnerStateCheckPeriodEnabled	MP 10 Core проверяет (флажок установлен) или не проверяет (флажок снят) статусы экземпляров уязвимостей	Флажок установлен
VulnerStateCheckPeriodEnd	Время окончания суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	01:00:00
VulnerStateCheckPeriodOfRetry	Продолжительность паузы (<Часы>:<Минуты>:<Секунды>) перед повторным запуском проверки, если предыдущий запуск завершился с ошибкой	00:01:00
VulnerStateCheckPeriodStart	Время начала суточного периода, в котором может запускаться проверка (от 00:00:00 до 23:59:59)	00:00:00

Таблица 14. 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 15. Параметры конфигурации роли RMQ Message Bus

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

Параметр	Описание	Значение по умолчанию
RMQAgentPassword	Пароль служебной учетной записи для доступа коллекторов к RabbitMQ	P@ssw0rd
RMQAgentUser	Логин служебной учетной записи для доступа коллекторов к RabbitMQ	agent
RMQHttpPort	Порт для доступа к RabbitMQ по протоколу HTTP	5672
RMQHttpsPort	Порт для доступа к RabbitMQ по протоколу HTTPS	5671
RMQPassword	Пароль служебной учетной записи для доступа MP 10 Core к RabbitMQ	P@ssw0rd
RMQSiemPassword	Пароль служебной учетной записи для доступа MP SIEM Server к RabbitMQ	P@ssw0rd
RMQSiemUser	Логин служебной учетной записи для доступа MP SIEM Server к RabbitMQ	siem
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для доступа MP 10 Core к RabbitMQ	core
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). **Примечание.** Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK).	0.5

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

Таблица 16. Параметры конфигурации компонента PT UCS

Параметр	Описание	Значение по умолчанию
`AutoAcceptMinions`	Salt Master автоматически утверждает запрос на подключение от модулей Salt Minion (флажок установлен) или модули необходимо подключать вручную (флажок снят)	Флажок снят
`AutoDownloadProductsList`	PT UCS автоматически загружает с глобального сервера Positive Technologies обновления для следующих объектов: — `KB BINARY` — дистрибутивов Knowledge Base; — `SIEM BINARY` — дистрибутивов компонентов на Microsoft Windows	Установлен флажок `KB BINARY`
`LogLevel`	Уровень журналирования для служб PT UCS	`info`
`ProxyAddress`	IP-адрес или FQDN прокси-сервера	`proxy.server.fqdn.or.ip`
`ProxyEnabled`	PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений Positive Technologies	Флажок снят
`ProxyPassword`	Пароль служебной учетной записи для подключения PT UCS к прокси-серверу	—
`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`
`TelemetrySendPeriod`	Расписание отправки в Positive Technologies собранных данных о работе системы (в формате планировщика заданий cron)	`30 0 * * *`

positive technologies

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