



MaxPatrol VM

версия 2.10

Руководство администратора

© Positive Technologies, 2026.

Настоящий документ является собственностью Positive Technologies и защищен законодательством Российской Федерации и международными соглашениями об авторских правах и интеллектуальной собственности.

Копирование документа либо его фрагментов в любой форме, распространение, в том числе в переводе, а также их передача третьим лицам возможны только с письменного разрешения Positive Technologies.

Документ может быть изменен без предварительного уведомления.

Товарные знаки, использованные в тексте, приведены исключительно в информационных целях, исключительные права на них принадлежат соответствующим правообладателям.

Дата редакции документа: 10.09.2026

Содержание

1.	Об этом документе.....	6
1.1.	Условные обозначения.....	6
1.2.	Другие источники информации о MaxPatrol VM.....	7
2.	О MaxPatrol VM.....	8
2.1.	Архитектура MaxPatrol VM.....	9
2.1.1.	Компонент MaxPatrol 10 Core.....	9
2.1.2.	Компонент MaxPatrol 10 Collector.....	9
2.1.3.	Компонент Positive Technologies Management and Configuration.....	10
2.1.4.	Компонент PT Update and Configuration Service.....	10
2.1.5.	Локальный сервер обновлений.....	10
2.2.	Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов.....	11
3.	Предоставление прав доступа.....	16
3.1.	О приложениях PT MC.....	17
3.2.	Предоставление доступа к активам и уязвимостям.....	17
3.3.	Предоставление доступа к задачам на сбор данных.....	18
4.	Управление политиками.....	19
4.1.	Создание правила для значимости активов.....	21
4.2.	Создание правила для сроков актуальности данных.....	21
4.3.	Создание правила для статусов уязвимостей.....	21
4.4.	Создание правила для отметки «важная».....	22
5.	Мониторинг состояния MaxPatrol VM.....	23
5.1.	Страницы раздела «Управление системой».....	23
5.2.	Удаление недоступного коллектора.....	25
5.3.	Настройка количества подзадач, одновременно выполняемых модулем.....	26
6.	Количество активов: условия и ограничения лицензионного контроля.....	27
7.	Сбор телеметрических данных.....	28
8.	Мониторинг ресурсов в Grafana.....	29
8.1.	Настройка дашбордов в Grafana на отдельном сервере.....	29
8.2.	Работа с дашбордом SqlStorage.....	33
9.	Удаление истории изменения активов.....	36
10.	Изменение сроков актуальности данных сканирования активов.....	39
11.	Ротация результатов сканирования, импорта и ручного ввода активов.....	40
12.	Максимальный размер собранных данных.....	41
13.	Тайм-аут для подзадач сбора данных.....	42
14.	Оптимизация выполнения PDQL-запросов для высоконагруженных систем.....	43
15.	Резервное копирование данных.....	47
15.1.	Особенности создания резервной копии поли SqlStorage.....	48
15.2.	Создание резервной копии данных.....	48
15.3.	Создание резервной копии пользовательских определений поли RMQ Message Bus.....	49
16.	Восстановление данных из резервной копии.....	50
16.1.	Восстановление данных компонентов MaxPatrol VM на Linux из резервной копии.....	50
16.2.	Восстановление пользовательских определений поли RMQ Message Bus.....	53
17.	Смена паролей служебных учетных записей.....	54

17.1.	Смена пароля служебной учетной записи в PostgreSQL	54
17.2.	Смена паролей служебных учетных записей в RabbitMQ	54
17.2.1.	RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Core на Linux	55
17.2.2.	RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Microsoft Windows.....	55
17.2.3.	RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Linux	56
17.3.	Смена пароля служебной учетной записи в Grafana	57
18.	Настройка журналирования работы MaxPatrol VM	58
18.1.	Настройка журналирования работы компонента MP 10 Core на Linux	58
18.2.	Настройка журналирования работы компонента MP 10 Collector	58
19.	Просмотр и изменение параметров конфигурации MaxPatrol VM.....	60
19.1.	Просмотр конфигурации роли.....	60
19.2.	Изменение конфигурации роли	61
19.3.	Управление изменением конфигурации ролей с помощью манифеста	63
19.3.1.	Изменение конфигурации ролей с помощью манифеста	63
19.3.2.	Создание манифеста для обновления компонентов или изменения конфигурации ролей	64
19.4.	Настройка прокси-сервера для онлайн-активации PT MC.....	67
19.5.	Включение AI-поиска по запросам	68
19.6.	Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol VM.....	68
19.7.	Изменение времени устаревания активов.....	68
19.8.	Отключение правил Declarative Detect.....	69
20.	Удаление экземпляра роли Collector.....	71
21.	Настройка очереди выпуска отчетов.....	72
22.	Пользовательские поля в модели актива	73
22.1.	Добавление пользовательских полей в модель актива.....	74
22.2.	Добавление описания пользовательских полей	79
22.3.	Изменение имен пользовательских полей.....	81
22.4.	Удаление пользовательских полей из модели актива.....	82
23.	Работа с инфраструктурами	84
23.1.	Создание инфраструктуры.....	84
23.2.	Изменение названия инфраструктуры	84
23.3.	Удаление инфраструктуры	85
24.	Изменение проверок по чек-листу	86
25.	Диагностика и решение проблем	87
25.1.	Вход в веб-интерфейс RabbitMQ	88
25.2.	Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога»	89
25.3.	Задача аудита не собирает сведения об активах.....	89
25.4.	Не приходят уведомления, отправляемые по электронной почте	90
25.5.	Настройка компонентов после изменения IP-адресов или FQDN их серверов.....	90
25.6.	Подсеть Docker-контейнера MaxPatrol VM совпадает с одной из подсетей предприятия	92
25.7.	Не удается получить обновления с сервера Positive Technologies	95
25.8.	Ошибка при установке, переконфигурации или обновлении компонентов в высоконагруженных системах.....	96

25.9.	Задача на сбор данных с коллектором на Windows завершается с ошибкой	96
25.10.	На коллекторах, установленных на Linux, задачи на сбор данных с профилем Microsoft Active Directory завершаются ошибкой.....	97
25.11.	Большое количество запросов к DNS-серверу от Docker-контейнеров сервера MP 10 Core	98
25.12.	Установка модуля Salt Minion завершается с ошибкой.....	99
25.13.	Ошибка при загрузке шаблона для экспорта записей в формате XLSX.....	99
25.14.	Результат сканирования отклонен. Объем данных превышает допустимый лимит.....	100
25.15.	Ошибка «There is no application package with following properties: WithHidden True Id <Идентификатор пакета приложения>» при обновлении MaxPatrol VM.....	104
25.16.	Ошибки, связанные с сертификатом MP 10 Collector на Microsoft Windows.....	105
25.17.	Ошибка «The repository <Ссылка на репозиторий> does not have a Release file»	106
25.18.	Справочная информация	107
25.18.1.	Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки.....	107
25.18.2.	Сбор информации о нагрузке на файловую систему и запущенных процессах.....	108
25.18.3.	Проверка доступности сетевого порта сервера	108
25.18.4.	Деактивация РТ МС	108
25.18.5.	Создание дампа памяти процесса	109
25.18.6.	Расположение файлов журналов.....	110
25.18.7.	Расположение временных файлов аудита	111
25.18.8.	Параметры мониторинга обработки активов.....	112
25.18.9.	Очистка записей об операциях	115
25.18.10.	Экспорт конфигурационных параметров ролей в файл	119
25.18.11.	Экспорт и импорт пользовательских профилей	120
25.18.12.	Настройка мандатного контроля целостности для Astra Linux.....	123
25.18.13.	Расположение пользовательских сертификатов.....	124
25.18.14.	Реорганизация данных в таблицах СУБД PostgreSQL.....	124
25.18.15.	Удаление неиспользуемых пакетов ролей.....	126
25.18.16.	Добавление исключений в Kaspersky Endpoint Security для БД PostgreSQL.....	126
25.18.17.	Установка сертификатов для компонента Collector на Microsoft Windows	127
26.	О технической поддержке.....	129
Приложение А.	Привилегии и роли MaxPatrol VM	133
Приложение Б.	Параметры конфигурации компонентов MaxPatrol VM на Linux	135
Приложение В.	Параметры проверок по чек-листу.....	154
Приложение Г.	О проверке серверов перед установкой ролей	159
Приложение Д.	Возможности привилегии «Расширенные полномочия»	161
Предметный указатель		162

1. Об этом документе

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

Руководство адресовано специалистам, администрирующим MaxPatrol VM.

Комплект документации MaxPatrol VM включает в себя следующие документы:

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

В этом разделе

[Условные обозначения \(см. раздел 1.1\)](#)

[Другие источники информации о MaxPatrol VM \(см. раздел 1.2\)](#)

1.1. Условные обозначения

В документе приняты условные обозначения.

Таблица 1. Условные обозначения

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

Пример	Описание
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом
► Чтобы открыть файл:	Начало инструкции выделено специальным значком
Нажмите OK	Названия элементов интерфейса (например, кнопок, полей, пунктов меню) выделены полужирным шрифтом
Выполните команду <i>Stop-Service</i>	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 справочном портале help.ptsecurity.com и на [Позитивном портале](#). Через Позитивный портал вы также можете обратиться [в техническую поддержку \(см. раздел 26\)](#).

2. О MaxPatrol VM

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

- управление активами;
- анализ защищенности активов ИБ;
- приоритизацию и проверку устранения уязвимостей на активах ИБ.

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

MaxPatrol VM позволяет:

- в любой момент предоставлять пользователю и другим системам актуальную информацию об IT-инфраструктуре, полученную путем активного и пассивного сбора данных;
- объединять активы в группы по различным критериям, чтобы упростить управление активами;
- оценивать степень влияния активов на информационную безопасность предприятия в целом;
- на основе постоянно обновляемой со стороны Positive Technologies базы знаний предоставлять пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных на активах, и отображать степень защищенности активов;
- определять способы устранения уязвимостей и настраивать политики контроля;
- выбирать среди уязвимостей те, которые необходимо устранять в первую очередь;
- контролировать степень защищенности IT-инфраструктуры и отслеживать информацию об уязвимостях на интерактивных дашбордах;
- выгружать данные для внешних систем и выпускать отчеты для различных подразделений и должностных лиц.

В этом разделе

[Архитектура MaxPatrol VM \(см. раздел 2.1\)](#)

[Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов \(см. раздел 2.2\)](#)

2.1. Архитектура MaxPatrol VM

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

В этом разделе

[Компонент MaxPatrol 10 Core \(см. раздел 2.1.1\)](#)

[Компонент MaxPatrol 10 Collector \(см. раздел 2.1.2\)](#)

[Компонент Positive Technologies Management and Configuration \(см. раздел 2.1.3\)](#)

[Компонент PT Update and Configuration Service \(см. раздел 2.1.4\)](#)

[Локальный сервер обновлений \(см. раздел 2.1.5\)](#)

2.1.1. Компонент MaxPatrol 10 Core

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

- централизованное хранение конфигурации активов;
- централизованное управление всеми компонентами системы;
- автоматизация процесса управления уязвимостями;
- поддержка 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 Positive Technologies Management and Configuration

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

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

2.1.4. Компонент PT Update and Configuration Service

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

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

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

2.1.5. Локальный сервер обновлений

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

2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol VM:

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

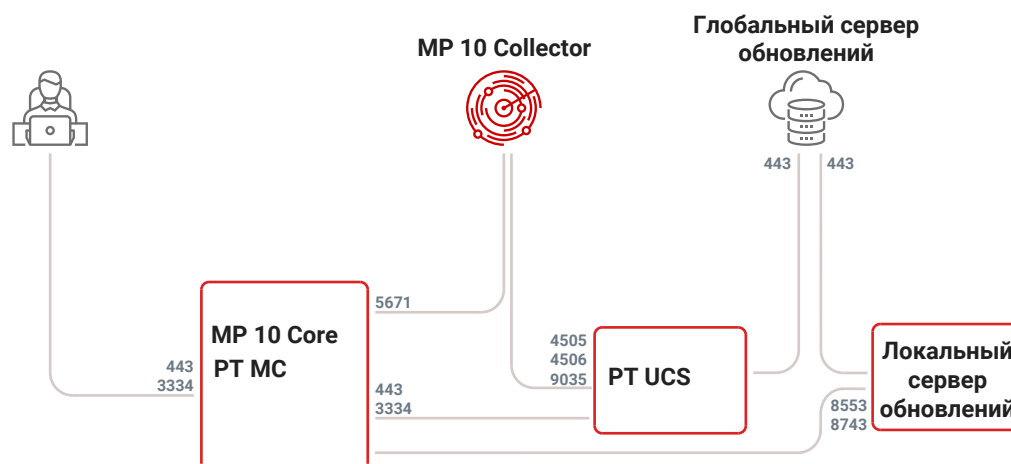


Рисунок 1. Взаимодействие компонентов MaxPatrol VM

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

Таблица 2. Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя	MP 10 Core	443
MP 10 Collector	MP 10 Core	5671
PT UCS	MP 10 Core	443, 3334
Рабочая станция пользователя	PT MC	3334
MP 10 Core, MP 10 Collector	PT UCS	4505, 4506, 9035
Docker Registry	Deployer	5000
PT UCS, локальный сервер обновлений	Глобальный сервер обновлений	443
PT MC	Локальный сервер обновлений	8553, 8743
Локальные агенты OTEL	Коллектор OTEL	4318

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

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

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

Если при развертывании MaxPatrol VM роли Core и SqlStorage устанавливаются на разные серверы, необходимо разрешить соединения:

- через порт 5432/TCP — от сервера Core к серверу SqlStorage;
- через порт 4318/TCP — от сервера SqlStorage к серверу Core.

Открытые порты, используемые службами MaxPatrol VM

Список открытых портов, используемых службами MaxPatrol VM, приведен в таблице ниже.

Таблица 3. Открытые порты служб

Служба	Порты
ai.assistant.proxy	8738
archivemanager	8737
assets.groups	8730
assets.identity	8721
assets.input	8731
assets.processing	8723
assets.projections	8799
assets.scans	8722
assets.temporalreadmodel	8782
assets.triggers	8733
collector-agent (Management and Configuration)	54528, 54529
collector-agent (Core)	4317–4320, 55679–55680
collector-server	4317, 4318
consul-server	8320-8322
contentservice	8727
core-groups	8787
core-triggers	8834

Служба	Порты
core-chromium	9232
core.analytics.reportsdelivery	8762
core.apigateway	8711
core.assets.compliance.control	8724
core.contentdeployer	8586
core.deployment.configuration	8740
core.events	8776
core.events.monitoring	8706
core.events.triggers	8707
core.healthmonitoring	8774
core.healthmonitoring.agent	8773
core.incidents	8781
core.incidents.triggers	8779
core.incidentsreadmodel	8777
core.pipeline.control.service	8729
core.portal	8712
core.scanning	8769
core.siem-querying	8050
core.siemmanager	8990
core.tables	8735
core.tenants	8703
core.topology	8775
core.topology.analyzer	8705
help-portal-maxpatrol (Core)	4211
help-portal-maxpatrol (Management and Configuration)	3336
mc-apigateway	8709
mc-consul	8511
mc-portal	8710
messagebus-rabbitmq	4369, 5671, 5672, 15671, 15672
observability.grafana	9002
platform-policies	8852

Служба	Порты
platform-branding (Management and Configuration)	3335
platform.branding (Core)	4210
storage-pgadmin	9001
storage-postgres	5432
storage-victorialogs	9428
storage-victoriametrics	8428
task-manager	10239
telemetry.adapter.victoriametrics	9339
ti-feeds	7869
ui.am-app	4204
ui.hcc-app	4212
ui.infosec-platform	3334
ui.infosec-platform-dashboards	4207
ui.infosec-platform-edr-adapter	4301
ui.infosec-platform-mp10	4202
ui.infosec-platform-navbar	4201
ui.infosec-platform-reports	3208
ui.infosec-platform-siem-api	4206
ui.infosec-platform-mc	4300
ui.platform-services	4209
ui.vm-app	4205
vulnerabilities-processing	8811

3. Предоставление прав доступа

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

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

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

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

Для обеспечения выполнения пользователем производственных задач необходимо:

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

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

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

В этом разделе

[О приложениях РТ МС \(см. раздел 3.1\)](#)

[Предоставление доступа к активам и уязвимостям \(см. раздел 3.2\)](#)

[Предоставление доступа к задачам на сбор данных \(см. раздел 3.3\)](#)

См. также

[Возможности привилегии «Расширенные полномочия» \(см. приложение Д\)](#)

3.1. О приложениях РТ МС

При развертывании MaxPatrol VM в РТ МС регистрируются следующие приложения:

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

3.2. Предоставление доступа к активам и уязвимостям

► Чтобы предоставить доступ к активам:

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

Откроется страница **Права доступа**.

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

3. В панели **«Название роли»** в блоке параметров **Доступ к активам** нажмите .
4. В открывшемся окне в раскрывающемся списке **Доступ** выберите необходимый тип доступа.
5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы активов, к которым необходимо предоставить доступ.

Примечание. Вы можете искать группы активов с помощью поля поиска и выбирать группы активов, устанавливая флажки напротив них.

6. Нажмите кнопку **Сохранить**.

Доступ к активам предоставлен.

3.3. Предоставление доступа к задачам на сбор данных

- Чтобы предоставить доступ к задачам на сбор данных:

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

Примечание. Вы можете искать группы задач с помощью поля поиска и выбирать группы задач, устанавливая флажки напротив них.

6. Нажмите кнопку **Сохранить**.

Доступ к задачам предоставлен.

4. Управление политиками

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

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

Порядок применения правил

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

Применение изменений в политиках

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

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

Типы политик

В MaxPatrol VM доступны следующие политики.

- **Значимость активов** — правила политики автоматически изменяют значимость активов. Определение значимости активов позволяет упорядочить работу с ними, выделить значимые активы, уязвимости на которых могут нанести больше всего вреда IT-инфраструктуре организации, и уделять им повышенное внимание. Необходимо стремиться к тому, чтобы для всех активов была указана значимость.
- **Сроки актуальности** — правила политики автоматически устанавливают сроки актуальности и устаревания данных об активах, полученных в результате сканирования IT-инфраструктуры методами аудита и пентеста. Опасные уязвимости на активах, данные о

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

- **Статусы уязвимостей** — правила политики автоматически изменяют статус экземпляров уязвимостей, определяют срок их устранения или откладывают их обработку на определенный срок. Перечень запланированных к устранению уязвимостей можно выпускать в виде отчета по расписанию и отправлять по электронной почте системному администратору.
- **Отметка «важная»** — правила политики автоматически отмечают отдельные экземпляры уязвимостей как важные. Например, в качестве важных могут быть отмечены наиболее опасные для IT-инфраструктуры уязвимости. Вы можете найти активы с важными уязвимостями с помощью PDQL-запроса.

Работа с правилами

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

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

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

В таблице в центральной панели отображаются состояния правил:

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

В этом разделе

[Создание правила для значимости активов \(см. раздел 4.1\)](#)

[Создание правила для сроков актуальности данных \(см. раздел 4.2\)](#)

[Создание правила для статусов уязвимостей \(см. раздел 4.3\)](#)

[Создание правила для отметки «важная» \(см. раздел 4.4\)](#)

4.1. Создание правила для значимости активов

► Чтобы создать правило:

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

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

6. Выберите значимость, которую правило будет назначать активам.
7. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только [после применения изменений в политике \(см. раздел 4\)](#).

4.2. Создание правила для сроков актуальности данных

► Чтобы создать правило:

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

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

5. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только [после применения изменений в политике \(см. раздел 4\)](#).

4.3. Создание правила для статусов уязвимостей

► Чтобы создать правило:

1. В главном меню выберите **Система** → **Политики**.
2. Выберите политику **Статусы уязвимостей**.
3. Нажмите **Создать правило**.

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

Пример:

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

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

6. Выберите действие, которое необходимо выполнять с экземплярами уязвимостей.
7. Если требуется исключать из мониторинга экземпляры уязвимостей, в раскрывающемся списке **Уточнение к статусу** выберите причину исключения.

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

8. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только [после применения изменений в политике \(см. раздел 4\)](#).

4.4. Создание правила для отметки «важная»

► Чтобы создать правило:

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

Пример:

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

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

6. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только [после применения изменений в политике \(см. раздел 4\)](#).

5. Мониторинг состояния MaxPatrol VM

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

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

В этом разделе

[Страницы раздела «Управление системой» \(см. раздел 5.1\)](#)

[Удаление недоступного коллектора \(см. раздел 5.2\)](#)

[Настройка количества подзадач, одновременно выполняемых модулем \(см. раздел 5.3\)](#)

5.1. Страницы раздела «Управление системой»

В разделе **Система** → **Управление системой** собраны страницы с информацией о состоянии компонентов MaxPatrol VM.

Страница «Коллекторы»

На странице **Коллекторы** вы можете просматривать информацию о MP 10 Collector, который обеспечивает поступление данных в систему. Для перехода на страницу необходимо в главном меню выбрать **Система** → **Управление системой** → **Коллекторы**.

Панель инструментов содержит следующие кнопки:

- **Обновить версию** — для обновления версии коллектора;
- **Удалить** — для удаления недоступного коллектора из списка.

В рабочей области страницы отображается таблица со списком коллекторов. Для каждого коллектора в таблице указаны статус, название, имя узла, версия, роли, а также семейство ОС сервера и IP-адреса сетевых интерфейсов сервера MP 10 Collector, которые доступны для внешнего подключения. Вы можете сортировать список, нажимая названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая  в правой верхней части

таблицы. Для поиска коллектора в списке вы можете нажать  и ввести в поле для поиска параметр коллектора. При выборе коллектора система отображает подробную информацию о нем, его модулях и их потоках в боковой панели с названием коллектора. Для модуля Pentest дополнительно отображаются его версия и дата обновления.

Внимание! Для проверки, получения и установки обновлений модуля Pentest с сервера Positive Technologies необходимо установить на сервере с ролью Deployer компонент PT UCS.

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

В колонке **Статус** отображается статус коллектора:

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

Страница «База уязвимостей»

На странице **База уязвимостей** вы можете просматривать информацию о пакетах экспертизы в подключенной базе уязвимостей. Для перехода на страницу необходимо в главном меню выбрать **Система** → **Управление системой** → **База уязвимостей**.

Панель инструментов содержит кнопку **Скачать в CSV** для скачивания таблицы с информацией о пакетах экспертизы в формате CSV.

В рабочей области страницы отображается таблица со списком пакетов экспертизы подключенной базы уязвимости. Для каждого пакета экспертизы в таблице указаны статус, название, версия, а также дата и время последнего обновления. Вы можете сортировать список, нажимая названия колонок таблицы. Вы можете обновить данные в таблице нажатием  и настроить период автоматического обновления данных в меню, открываемом при нажатии  (по умолчанию отключено). При выборе пакета экспертизы в таблице система отображает подробную информацию о нем в боковой панели с названием пакета экспертизы.

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

Страница «Обработка активов»

На странице **Обработка активов** вы можете просматривать информацию о работе служб MP 10 Core на различных этапах обработки данных об активах. Для перехода на страницу необходимо в главном меню выбрать **Система** → **Управление системой** → **Обработка активов**.

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

Страница «О системе»

На странице **О системе** отображается информация о версии компонента MP 10 Core, ссылка для перехода к управлению лицензиями в PT MC, а также информация об используемой базе данных GeoIP. Для перехода на страницу необходимо в главном меню выбрать **Система** → **Управление системой** → **О системе**.

5.2. Удаление недоступного коллектора

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

- если удаленный коллектор был выбран в задаче автоматически — использующие его подзадачи;
- если удаленный коллектор был выбран вручную — использующие его задачи.

► Чтобы удалить коллектор из списка:

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

Откроется страница **Управление системой**.

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

В рабочей области страницы отобразится таблица со списком коллекторов.

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

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

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

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

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

Коллектор удален из списка.

5.3. Настройка количества подзадач, одновременно выполняемых модулем

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

► Чтобы настроить количество одновременно выполняемых подзадач:

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

Откроется страница **Управление системой**.

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

В рабочей области страницы отобразится таблица со списком коллекторов.

3. Выберите коллектор.

4. В панели **Модули и потоки** выберите модуль.

5. По ссылке **Настроить** выберите вариант **Вручную** и укажите значение.

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

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

Количество одновременно выполняемых подзадач настроено.

6. Количество активов: условия и ограничения лицензионного контроля

Для каждой лицензии MaxPatrol VM действует ограничение на количество активов.

Лицензируемым считается актив, который был просканирован хотя бы одним из модулей: Audit, Pentest или WebEngine. Актив исключается из списка для лицензионного учета после того, как он пропадает из интерфейса системы.

Допустимое превышение — 10% количества активов, установленного для лицензии. Если ограничение будет превышено больше допустимого уровня, система сообщит об этом с помощью уведомлений. Ограничение функций системы при этом не применяется. Обратитесь к вашему менеджеру для обсуждения лицензионного контроля.

7. Сбор телеметрических данных

В MaxPatrol VM реализован сбор телеметрических данных о производительности микросервисов компонента MP 10 Core, об активах, их значимости и сроках актуальности данных, а также о действиях пользователя. Это необходимо для дальнейшего развития продукта и повышения качества экспертизы.

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

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

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

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

8. Мониторинг ресурсов в Grafana

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

Вы можете установить Grafana версии 7.5.17 под лицензией Apache 2.0 с помощью роли Grafana.

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

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

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

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

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

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

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

В этом разделе

[Настройка дашбордов в Grafana на отдельном сервере \(см. раздел 8.1\)](#)

[Работа с дашбордом SqlStorage \(см. раздел 8.2\)](#)

8.1. Настройка дашбордов в Grafana на отдельном сервере

Вы можете настроить отображение дашбордов MaxPatrol VM в Grafana, развернутой на отдельном сервере.

Внимание! Для настройки дашборда с журналами VictoriaLogs должна быть установлена Grafana версии 10.4.0 и выше.

Добавление дашборда с метриками VictoriaMetrics

► Чтобы добавить дашборд с метриками VictoriaMetrics:

1. В главном меню выберите **Connections** → **Data sources**.
2. Нажмите **Add data source**.
3. Выберите **Prometheus**.
4. В поле **Name** введите произвольное название источника данных, например, `VictoriaMetrics`.
5. В поле **Prometheus server URL** введите FQDN сервера с установленной ролью `Observability` с указанием порта из значения параметра `MetricsHttpPort` роли `Observability`.

Примечание. По умолчанию для доступа к VictoriaMetrics используется TCP-порт 8428. Вы можете посмотреть параметры роли с текущими значениями на сервере с установленной ролью `Observability` с помощью команды `deployer params get - <Идентификатор экземпляра роли Observability>`.

6. В поле **Authentication method** выберите вариант **Basic Authentication**.
7. В поле **User** укажите логин учетной записи для доступа к VictoriaMetrics из значения параметра `MetricsUser` роли `Observability`.

Значение по умолчанию: `admin`.

8. В поле **Password** укажите пароль из значения параметра `MetricsPassword` роли `Observability`.

Значение по умолчанию: `P@ssw0rd`.

9. В блоке **TLS settings** выполните одно из следующих действий:

- Если вы используете собственный сертификат или автоматически установленный сертификат из состава дистрибутива MaxPatrol VM, установите флажок **Add self-signed certificate** и в поле **CA Certificate** введите содержимое файла сертификата.

Примечание. Файл автоматически установленного сертификата `rootCA.crt` находится на сервере с ролью `Observability` в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Идентификатор экземпляра роли Observability>/certs`.

- Если политика информационной безопасности вашей организации позволяет не проверять подлинность сертификата, установите флажок **Skip TLS certificate validation**.

10. Нажмите **Save & test**.

Появится сообщение об успешном добавлении источника данных.

11. В главном меню выберите **Dashboards**.

12. Нажмите **Create Dashboard**.
13. Нажмите **Add visualization**.
14. Выберите источник данных VictoriaMetrics.
15. Настройте дашборд в соответствии с требованиями вашей организации.
16. Нажмите **Save dashboard**.

Дашборд с метриками VictoriaMetrics появится в списке дашбордов Grafana.

Добавление дашборда с журналом VictoriaLogs

► Чтобы добавить дашборд с журналом VictoriaLogs:

1. В главном меню выберите **Plugins and data** → **Plugins**.
2. Выберите **VictoriaLogs**.
3. Нажмите **Install**.
4. В главном меню выберите **Connections** → **Data sources**.
5. Нажмите **Add new data source**.
6. Выберите **VictoriaLogs**.
7. В поле **Name** введите произвольное название источника данных, например, `VictoriaLogs`.
8. В поле **URL** введите FQDN сервера с установленной ролью Observability с указанием порта.

Примечание. По умолчанию для доступа к VictoriaLogs используется TCP-порт 9428.

9. В блоке **Auth** включите **Basic Auth**.
10. Выполните одно из следующих действий:
 - Если вы используете доверенный сертификат для сайта MaxPatrol VM, включите **With CA Cert**.
 - Если политика информационной безопасности вашей организации позволяет не проверять подлинность сертификата, включите **Skip TLS Verify**.
11. В поле **User** укажите логин учетной записи для доступа к журналам VictoriaLogs.
Значение по умолчанию: `admin`.
12. В поле **Password** укажите пароль из значения параметра `LogsPassword` поли Observability.
Значение по умолчанию: `P@ssw0rd`.
13. Если вы используете доверенный сертификат для сайта MaxPatrol VM, в поле **CA Cert** введите содержимое файла доверенного сертификата.

Примечание. Файл доверенного сертификата `rootCA.crt` находится на сервере с установленной ролью `Observability` в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Идентификатор экземпляра роли Observability>/certs`.

14. Нажмите **Save & test**.

Появится сообщение об успешном добавлении источника данных.

15. В главном меню выберите **Dashboards**.

16. Нажмите **New** → **New dashboard**.

17. Нажмите **Add visualization**.

18. Выберите источник данных `VictoriaLogs`.

19. В правой части страницы выберите тип отображения данных **Logs**.

20. В правой части страницы в раскрывающемся блоке **Panel options** укажите имя и описание дашборда.

21. В правой части страницы в раскрывающемся блоке **Logs** включите **Show timestamps**.

22. В центральной части страницы нажмите **Add query**.

23. В поле **Quick start** выполните одно из следующих действий:

- Для вывода всех данных введите `*`.
- Для фильтрации данных введите запрос на языке LogQL.

24. Нажмите **Save dashboard**.

Дашборд с журналом `VictoriaLogs` появится в списке дашбордов Grafana.

Вы можете просмотреть метаданные записи журнала (например, имя и идентификатор сервера, от которого получено событие, или имя процесса, отправившего сообщение), нажав на запись в списке.

8.2. Работа с дашбордом SqlStorage

В MaxPatrol VM реализован сбор метрик производительности СУБД. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Дашборд содержит следующие виджеты:

- **Databases.** Виджет отображает общие данные о базах данных:
 - **count** — количество баз данных в СУБД;
 - **size** — общий размер всех баз данных;
 - **temp bytes** — объем временных файлов, создаваемых СУБД для обработки запросов.
- **Transaction rate.** Виджет отображает количество транзакций в секунду:
 - **commit** — количество успешных транзакций;
 - **rollback** — количество отмененных транзакций.
- **Checkpoint write time.** Виджет отображает время записи изменений из временного хранилища в основную базу данных. По умолчанию запись происходит каждые пять минут.
- **Checkpoint by request.** Виджет отображает время записи изменений из временного хранилища в основную базу данных вне очереди.
- **Checkpoint count.** Виджет отображает количество записей в основную базу данных с момента последнего перезапуска СУБД:
 - **timed** — записи по расписанию;
 - **req** — записи вне очереди.
- **Checksum fail.** Виджет отображает количество несовпадений контрольных сумм в табличных списках и в записанных на диск файлах.
- **No rollback.** Виджет отображает процент успешно проведенных транзакций в базах данных с момента перезапуска СУБД.
- **Cache hit.** Виджет отображает процент запросов, обработанных с помощью буферного кэша без обращения к памяти диска.
- **Deadlocks.** Виджет отображает количество взаимных блокировок между запросами к одним и тем же табличным спискам.
- **Checkpoint hit.** Виджет отображает соотношение записей в базы данных по расписанию и записей вне очереди.
- **Operation speed.** Виджет отображает количество операций определенного типа в секунду:
 - **return** — запрошенные у СУБД записи;
 - **fetch** — записи, возвращаемые СУБД в результате применения фильтров;
 - **insert** — вставленные записи;

- **delete** — удаленные записи;
 - **update** — измененные записи.
- **SqlStorage settings: size.** Виджет отображает заданные для роли SqlStorage параметры:
 - **effective_cache_size** — объем дискового кэша на узле, на котором развернута СУБД. Параметр влияет на работу планировщика запросов;
 - **shared_buffers** — объем буферного кэша, с помощью которого СУБД обрабатывает запросы;
 - **wal_buffers** — объем кэша, выделенного под журнал предзаписи;
 - **work_mem** — объем кэша, выделенного под запросы пользователя.
 - **SqlStorage settings: limits.** Виджет отображает заданные для роли SqlStorage лимиты:
 - **autovacuum_analyze_threshold** — количество изменений строк, после которого запускается операция `autovacuum_analyze`;
 - **max_connections** — максимальное количество установленных соединений;
 - **max_parallel_workers** — максимальное количество параллельных вычислений для выполнения одного запроса.
 - **SqlStorage settings: time.** Виджет отображает заданное для роли SqlStorage время:
 - **autovacuum_naptime** — интервал между операциями `autovacuum`. Параметр задает время, которое должно пройти между двумя операциями `autovacuum`, даже если лимит изменений строк превышен;
 - **checkpoint_timeout** — интервал между записями по расписанию.
 - **Database size.** Виджет отображает семь самых объемных баз данных:
 - **max** — наибольший размер базы данных с момента перезапуска СУБД;
 - **current** — текущий размер базы данных. Показатель может быть меньше максимального после выполнения операции `vacuum_full`.
 - **Database temporary file size.** Виджет отображает шесть баз данных с самыми объемными временными файлами.
 - **Sessions.** Виджет отображает количество сервисных соединений:
 - **idle** — установленные неактивные соединения;
 - **active** — установленные активные соединения;
 - **wait** — установленные активные соединения, ожидающие в очереди;
 - **total backends** — все установленные соединения.
 - **Query time.** Виджет отображает самый длинный исполняемый запрос на данный момент.
 - **Transaction idle time.** Виджет отображает время самой длинной незакрытой транзакции.
 - **Killed.** Виджет отображает количество принудительно отмененных транзакций.

- **Abandoned.** Виджет отображает количество транзакций, отмененных в результате потери соединения.
- **Query state.** Виджет отображает количество установленных соединений в разных статусах за время, прошедшее с перезапуска СУБД.
- **Session breaks.** Виджет отображает количество завершенных соединений за время, прошедшее с перезапуска СУБД.
- **Longest database query time.** Виджет отображает длинные запросы, выполненные с момента перезапуска СУБД, с разделением по базам данных.
- **Idle transactions.** Виджет отображает неактивные соединения с разделением по базам данных.

9. Удаление истории изменения активов

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

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

В ходе ротации удаляются:

- конфигурации активов и данные о состоянии активов до даты ротации;
- информация о вхождении активов в группы до даты ротации;
- данные о состоянии уязвимостей, найденных на активах до даты ротации.

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

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

Возможные последствия

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

- Сведения об активе могут заменяться значениями из версии, ближайшей к дате ротации.
- Данные об уязвимостях на активе будут соответствовать последнему актуальному состоянию. Например, открытая уязвимость может отображаться сразу в статусе **В работе**.
- Если актуальный статус уязвимости изменился в удаляемой версии актива, информация об уязвимости на дату обнаружения будет отсутствовать, но будет отображаться при выборе текущей даты.

- Данные о привязке актива к группе будут содержать только последнее актуальное состояние.
- Если перед датой ротации актив в последний раз изменялся вручную, а не по результатам аудита, в качестве даты последнего обновления в жизненном цикле на карточке актива будет отображаться дата последнего аудита актива, но состояние актива на эту дату отображаться не будет.

Настройка ротации истории изменения активов

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

Внимание! Исторические данные удаляются безвозвратно, поэтому перед включением ротации настоятельно рекомендуется создать резервную копию базы данных `assets_temporal_rm`. Инструкцию по созданию резервной копии вы можете найти на сайте [postgresql.org](https://www.postgresql.org).

► Чтобы включить и настроить ротацию истории изменения активов:

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

```
tar xzf pt_core_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_core_<Номер версии>/install.sh
```
3. Выберите вариант с идентификатором приложения роли.
4. Выберите вариант с идентификатором экземпляра роли.
 Откроется окно для выбора набора параметров.
5. Выберите вариант **Advanced configuration**.
 Откроется страница [со списком параметров \(см. приложение Б\)](#).
6. Установите флажок `HistoryRotationEnabled`.
7. В качестве значения параметра `HistoryRotationDepth` укажите глубину ротации — период истории изменения активов, данные за который необходимо удалять:

```
<Дни>.<Часы>:<Минуты>:<Секунды>
```

 Например:

```
110.00:00:00
```

Внимание! Минимально допустимое значение параметра `HistoryRotationDepth` — 14 дней (14.00:00:00).
8. В качестве значения параметра `HistoryRotationCronSchedule` укажите периодичность запуска ротации с помощью планировщика заданий cron:

```
<Минута> <Час> <Число> <Месяц> <День недели>
```

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

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

9. Нажмите кнопку **OK**.

10. Нажмите **Submit**.

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

11. Нажмите кнопку **OK**.

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

Ротация истории изменения активов включена и настроена.

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

10. Изменение сроков актуальности данных сканирования активов

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

11. Ротация результатов сканирования, импорта и ручного ввода активов

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

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

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

В ходе ротации устаревшие результаты удаляются пакетами указанного размера.

Внимание! Чтобы освободить дисковое пространство, после выполнения ротации необходимо [запустить утилиту pgcompactable](#) (см. [раздел 25.18.14](#)) для БД сервиса Assets.Scans.

Настройка ротации результатов сканирования, импорта и ручного ввода активов

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

- ▶ Чтобы настроить ротацию результатов сканирования, импорта и ручного ввода активов, измените конфигурацию роли MP 10 Core, указав значения следующих параметров:

`ScansRotationEnabled: True`

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

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

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

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

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

12. Максимальный размер собранных данных

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

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

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

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

Внимание! При выборе значения `MaxScanSizeKb` следует учитывать связанные с этим ограничения на размер Active Directory. Например, при значении `MaxScanSizeKb`, равном 600 000 КБ, поддерживается аудит служб каталогов Active Directory, включающих до 100 000 пользователей и 5000 групп.

Примечание. Чтобы снизить требования к размеру памяти при аудите Active Directory, вы можете ограничить количество собираемых активов. Подробности см. в разделе «Microsoft Active Directory в Windows Server 2003–2022: настройка MaxPatrol SIEM» Руководства по настройке источников.

Таблица 4. Максимальный размер собранных данных

Память (ОЗУ)	Рекомендуемое значение <code>MaxScanSizeKb</code> , КБ
80 ГБ	800 000
90 ГБ	900 000
100 ГБ	1 000 000

- ▶ Чтобы указать максимальный размер собранных данных, измените конфигурацию роли MP 10 Core, указав значение параметра `MaxScanSizeKb` в килобайтах.

13. Тайм-аут для подзадач сбора данных

Сбор данных о некоторых активах, например о файловых хранилищах и файлообменниках, занимает 20 минут и более. Аудит инфраструктуры крупной организации в таком случае может не уложиться в выбранный интервал сканирования.

По умолчанию тайм-аут для выполнения подзадач на сбор данных не установлен. Вы можете ограничить время выполнения подзадач для любого модуля в конфигурационном файле. Все подзадачи с этим модулем будут выполняться не более указанного времени. По истечении этого времени подзадачи перейдут в статус **Завершена** с ошибкой, результаты незавершенных подзадач не будут загружены в систему. Далее начнется сбор данных со следующего актива.

► Чтобы указать тайм-аут для выполнения подзадач сбора данных для модулей:

1. Перейдите в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра поли>/data/scanning/data/layer-updates/` на сервере с MP 10 Core.
2. Откройте файл `Sample_OverridenModuleTimeOuts.json`.
3. Укажите тайм-ауты для нужных модулей. Если требуется, добавьте в файл нужные модули в соответствии со структурой файла.

```
{
  "Modules": [
    {
      "ModuleName": "<Название модуля>",
      "Timeouts": {
        "ForceCompleteWithError": <Максимальная длительность выполнения подзадач в секундах>
      }
    }
  ]
}
```

4. Сохраните изменения.
5. Переименуйте файл в `OverridenModuleTimeOuts.json`.
6. Перезапустите контейнер:


```
docker restart $(docker ps -aqf name=scanning)
```

14. Оптимизация выполнения PDQL-запросов для высоконагруженных систем

Оптимизация выполнения PDQL-запросов в MaxPatrol VM влияет на производительность системы при построении виджетов, отчетов, списков активов и выполнении политик, так как PDQL используется во всех этих сценариях.

Режим работы оптимизации управляется следующими параметрами:

- `AssetGridVersionRangeModeEnabled` — определяет, включена оптимизация (значение `True`) или отключена (значение `False`).
- `AssetGridValidTimePeriodIndexFormat` — определяет режим оптимизации:
 - Максимальная оптимизация (значение `IdAndPeriod`). Режим обеспечивает максимальную производительность выполнения PDQL-запросов — скорость их обработки увеличивается в несколько десятков раз.
 - Средняя оптимизация (значение `PeriodOnly`). Режим снижает нагрузку на систему при работе с большими объемами данных. Скорость обработки PDQL-запросов увеличивается в несколько раз.

Примечание. По умолчанию в MaxPatrol VM версии 2.10 и выше включена оптимизация в максимальном режиме. В версиях ниже 2.10 рекомендуется включить оптимизацию вручную.

Таблица 5. Рекомендации по выбору режима оптимизации

Режим	Сценарии использования
<code>IdAndPeriod</code> (максимальная оптимизация)	Повседневная эксплуатация продукта (виджеты, отчеты, политики). Замедленная работа системы (долгое построение списков, отчетов, виджетов). Длительное выполнение PDQL-запросов. Ошибки <code>Out Of Memory</code> при выполнении запросов
<code>PeriodOnly</code> (средняя оптимизация)	Большой объем данных и активов. Выполнение запросов с большими выборками. Ограниченные аппаратные ресурсы. Нестабильность при использовании максимальной оптимизации

Режим	Сценарии использования
Оптимизация отключена	Выполнение миграции PDQL при зависаниях или длительном выполнении. Нестабильная инфраструктура (недостаток ресурсов, проблемы с дисковой подсистемой). Временная мера для повышения устойчивости служебных операций (после завершения рекомендуется включить оптимизацию обратно)

- Чтобы настроить оптимизацию выполнения PDQL-запросов, [измените конфигурацию \(см. раздел 19.2\)](#) роли Core, указав для параметра `AssetGridValidTimePeriodIndexFormat` одно из значений: `IdAndPeriod` или `PeriodOnly`.

Отключение и повторное включение оптимизации выполнения PDQL-запросов

Отключение оптимизации рекомендуется только в отдельных случаях:

- при выполнении миграции PDQL, если процесс зависает или выполняется длительное время;
- при нестабильной инфраструктуре (недостаток ресурсов, проблемы с дисковой подсистемой).

В этих случаях:

1. Отключите оптимизацию.
2. Перезапустите роли.
3. Выполните миграцию.
4. После завершения включите оптимизацию обратно (рекомендуется максимальный режим `IdAndPeriod`).

Внимание! При отключенной оптимизации PDQL-запросы выполняются значительно медленнее.

- Чтобы отключить оптимизацию, [измените конфигурацию \(см. раздел 19.2\)](#) роли Core, указав для параметра `AssetGridVersionRangeModeEnabled` значение `False`.

Если оптимизация уже была включена ранее, ее отключение не откатывает изменения, внесенные в БД сервиса TRM (`assets_temporal_rm`):

- созданные индексы не удаляются;
- структура БД не возвращается к базовому сценарию работы;
- ранее выполненные изменения в БД сохраняются.

Повторное включение оптимизации после ее отключения:

- не запускает повторную миграцию данных сервиса TRM;
- не приводит к повторному созданию индексов;
- не вызывает повторного увеличения размера БД, так как изменения уже были внесены ранее и не откатываются;
- только изменяет способ выполнения SQL-поиска в БД.

В отдельных случаях при повторном включении может измениться размер индекса, используемого для повышения производительности, но повторное применение миграции и повторное создание структуры индексов не выполняются.

► Чтобы определить размер базы данных сервиса TRM:

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

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

► Чтобы включить и настроить оптимизацию выполнения PDQL-запросов,

измените конфигурацию (см. раздел 19.2) роли Core, указав значения следующих параметров:

```
AssetGridVersionRangeModeEnabled: True
```

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

Миграция БД размером 100 ГБ может занимать более 10 часов в режиме `IdAndPeriod` и более часа в режиме `PeriodOnly`.

Дополнительные рекомендации

При проблемах с производительностью PDQL-запросов также рекомендуется:

- переводить виджеты в ручной режим обновления;
- уменьшать количество параллельных потоков;

- анализировать и оптимизировать политики;
- избегать использования ресурсоемких операторов (например, `like` с широкими шаблонами).

Комплексное применение этих мер совместно с корректной настройкой режима оптимизации позволяет повысить стабильность и производительность системы.

15. Резервное копирование данных

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

Внимание! Для стабильной работы системы необходимо использовать средства резервного копирования, описанные ниже. Использование сторонних средств может привести к потере данных или сбоям в работе продукта.

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

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

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

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

В этом разделе

[Особенности создания резервной копии роли SqlStorage \(см. раздел 15.1\)](#)

[Создание резервной копии данных \(см. раздел 15.2\)](#)

[Создание резервной копии пользовательских определений роли RMQ Message Bus \(см. раздел 15.3\)](#)

15.1. Особенности создания резервной копии роли SqlStorage

При создании резервной копии роли SqlStorage файлы резервной копии и метаданных сохраняются во временный каталог `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/tmp`, после чего из них формируется архив `backup_archive.tar`. Файл архива копируется в каталог, указанный пользователем при запуске сценария резервного копирования.

Внимание! Если в разделе диска с временным каталогом недостаточно места, резервное копирование не будет выполнено.

Вы можете указать в качестве временного каталог из раздела с достаточным объемом свободного места. Для этого необходимо запустить сценарий резервного копирования с ключом `--tmpdir`:

```
/var/lib/deployed-roles/mc-application/sqlstorage/backup.sh --tmpdir <Путь к временному каталогу> <Путь к каталогу для резервной копии>
```

Например:

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

15.2. Создание резервной копии данных

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

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

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

В ходе [восстановления данных из резервной копии](#) (см. [раздел 16.1](#)) необходимо добавить:

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

Чтобы избежать ошибок в ходе восстановления данных из резервной копии, при сохранении копий файлов пользовательских доверенных сертификатов их необходимо отличать от системных. Для этого вы можете воспользоваться [поиском пользовательских сертификатов \(см. раздел 25.18.13\)](#).

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

Внимание! Во время создания резервной копии SSH-соединение не должно прерываться. В случае завершения соединения сценарий завершится ошибкой.

- ▶ Чтобы создать резервную копию данных,

запустите сценарий резервного копирования:

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

Например:

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

По завершении сценария в консоли отобразится сообщение Done. Архив backup.tar с резервной копией будет сохранен в каталоге /<Путь к каталогу для резервной копии>/<Идентификатор приложения>/<Название экземпляра роли>/.

Например:

```
/home/mc-application/sqlstorage.
```

15.3. Создание резервной копии пользовательских определений роли RMQ Message Bus

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

- ▶ Чтобы создать резервную копию,

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

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

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

16. Восстановление данных из резервной копии

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

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

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

В этом разделе

[Восстановление данных компонентов MaxPatrol VM на Linux из резервной копии \(см. раздел 16.1\)](#)

[Восстановление пользовательских определений роли RMQ Message Bus \(см. раздел 16.2\)](#)

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

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

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

Примечание. Каталоги с резервными копиями должны иметь структуру вида `/<Имя каталога>/<Идентификатор приложения>/<Название экземпляра роли>/backup.tar`, полученную при резервном копировании, например `/backup/mc-application/sqlstorage/backup.tar`.

Примечание. Устанавливать роли в процессе восстановления данных необходимо в соответствии с инструкциями из раздела «Развертывание MaxPatrol VM» Руководства по внедрению. При установке всех ролей, кроме Deployer, необходимо выбирать идентификатор восстанавливаемого приложения и название экземпляра восстанавливаемой роли.

► Чтобы восстановить данные компонентов на Linux:

1. Установите пакеты ролей и экземпляр роли Deployer с помощью сценария `install_all_role_packages.sh`.
2. Восстановите данные роли Deployer:
`/var/lib/deployed-roles/<Идентификатор приложения Deployer>/<Название экземпляра роли Deployer>/restore.sh <Путь к архиву с файлами резервной копии>`
 Например:
`/var/lib/deployed-roles/Deployment-Application/Deployer/restore.sh /home/deploy-app/Deployer/backup.tar`
3. Запустите сценарий для обновления идентификаторов версий пакетов приложений:
`deployer maintenance fix -AppPackage`
 По завершении работы сценария отобразится сообщение `Finishing repair process for app package references`.
4. Если вы используете пользовательские сертификаты, добавьте файлы корневых и промежуточных пользовательских сертификатов центра сертификации для роли Deployer, сохраненные на этапе [резервного копирования](#) (см. [раздел 15.2](#)), в каталог `/opt/deployer/pki/trusted_ca/`.
5. Для каждой роли в каталоге `/var/lib/deployer/role_instances/<Название роли>` в файле `instance.yaml` в качестве значения параметра `HostId` укажите идентификатор Salt Minion.
6. Для каждой роли в каталоге `/var/lib/deployer/role_instances/<Название роли>` в файлах `params.yaml` и `params.default.yaml` в качестве значений параметров, содержащих FQDN, укажите FQDN серверов, на которые будут установлены соответствующие роли.

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

7. Если ранее были добавлены файлы корневых и промежуточных пользовательских сертификатов, выполните команду для их обработки:
`deployer instance reconfigure -type Deployer`
8. Создайте каталоги, в которых хранились файлы сертификатов.
`mkdir -p <Путь к каталогу сертификатов>`
 Например:
`mkdir -p /var/lib/deployed-roles/mp10-application/core-1/certs`
9. Скопируйте в эти каталоги файлы сертификатов, сохраненные при создании резервной копии:
`cp <Путь к каталогу резервной копии сертификатов>/* <Путь к каталогу сертификатов>`
 Например:
`cp backup/certs/core/certs/* /var/lib/deployed-roles/mp10-application/core-1/certs`

10. Установите роль SqlStorage.

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

В процессе установки система запросит реконфигурацию параметров ролей. Ее необходимо отклонить.

11. Восстановите данные роли SqlStorage:

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

Например:

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

12. Установите роль LogConnector:

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

В процессе установки система запросит реконфигурацию параметров ролей. Ее необходимо отклонить.

13. Установите роль Observability:

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

В процессе установки система запросит реконфигурацию параметров ролей. Ее необходимо отклонить.

14. Установите роль Management and Configuration.

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

В процессе установки система запросит реконфигурацию параметров ролей. Ее необходимо отклонить.

15. Установите роли RMQ Message Bus и Core.

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

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

В процессе установки система запросит реконфигурацию параметров ролей. Ее необходимо отклонить.

16. Восстановите данные роли Core:

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

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

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

- Если резервная копия была создана на том же сервере, на котором выполняется восстановление, добавьте файлы пользовательских сертификатов, сохраненные на этапе [резервного копирования \(см. раздел 15.2\)](#), в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.

- Если резервная копия была создана на одном сервере, а восстановление выполняется на другом, для доверенного сертификата в расширении Subject Alternative Name (SAN) должен быть указан IP-адрес или FQDN того сервера, на котором выполняется восстановление.

18. Выполните команду для восстановления экземпляров роли Collector:

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

19. Выполните реконфигурацию экземпляров ролей.

```
deployer instance reconfigure -diff -silent
```

20. Если ключ инсталляции PT MC уже использовался для активации PT MC на другом устройстве, [деактивируйте \(см. раздел 25.18.4\)](#) PT MC.

21. Если вы деактивировали PT MC, повторно активируйте систему по инструкции «Активация PT MC» Руководства по внедрению.

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

22. Если вы деактивировали PT MC, повторно активируйте MaxPatrol VM по инструкции «Активация лицензии MaxPatrol VM» Руководства по внедрению.

См. также

[Создание резервной копии данных \(см. раздел 15.2\)](#)

16.2. Восстановление пользовательских определений роли RMQ Message Bus

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

► Чтобы восстановить данные из резервной копии,

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

```
cat <Путь к каталогу с резервной копией данных роли на соответствующем сервере>/  
rmq_definitions.json | docker exec -i $(docker ps -aqf name=messagebus-rabbitmq) sh -c  
'cat > /tmp/rmq_definitions.json'
```

17. Смена паролей служебных учетных записей

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

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

В этом разделе

[Смена пароля служебной учетной записи в PostgreSQL \(см. раздел 17.1\)](#)

[Смена паролей служебных учетных записей в RabbitMQ \(см. раздел 17.2\)](#)

[Смена пароля служебной учетной записи в Grafana \(см. раздел 17.3\)](#)

17.1. Смена пароля служебной учетной записи в PostgreSQL

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

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

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

1. На сервере с установленной ролью Deployer выполните команду:
`deployer instance configure -type SqlStorage`
2. [Измените конфигурацию \(см. раздел 19.2\)](#) роли `SqlStorage`:
`PgPassword: <Новый пароль>`
3. [Измените конфигурации \(см. раздел 19.2\)](#) полей `LogConnector`, `Observability`, `Management and Configuration` и `Core`.

При изменении конфигурации зависимых ролей пароль, заданный в конфигурации роли `SqlStorage`, обновится автоматически.

17.2. Смена паролей служебных учетных записей в RabbitMQ

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

В этом разделе

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Core на Linux (см. раздел 17.2.1)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Microsoft Windows (см. раздел 17.2.2)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Linux (см. раздел 17.2.3)

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

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

Внимание! Не рекомендуется использовать в пароле служебных учетных записей следующие символы: `\ / ' " $`.

► Чтобы сменить пароль служебной учетной записи MP 10 Core:

1. На сервере MP 10 Core [измените конфигурации](#) (см. раздел 19.2) ролей Core и RMQ Message Bus:

```
RMQPassword: <Новый пароль>
```

2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

Пароль изменен.

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

По умолчанию при первой установке логин служебной учетной записи компонента MP 10 Collector на Microsoft Windows для доступа к RabbitMQ — `agent`, пароль — `P@ssw0rd`. При обновлении с версии 2.8 и ниже логин — `mpx_agent`.

Внимание! Не рекомендуется использовать в пароле служебных учетных записей следующие символы: `\ / ' " $`.

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

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

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

2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

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

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

Пароль изменен.

См. также

[Изменение конфигурации роли \(см. раздел 19.2\)](#)

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

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

Внимание! Не рекомендуется использовать в пароле служебных учетных записей следующие символы: \ / ' " \$.

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

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

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

2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

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

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

Пароль изменен.

См. также

[Изменение конфигурации роли \(см. раздел 19.2\)](#)

17.3. Смена пароля служебной учетной записи в Grafana

При развертывании роли Grafana в Grafana создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи — `admin`, пароль — `P@ssw0rd`.

Внимание! Не рекомендуется использовать в пароле служебных учетных записей следующие символы: `\ / ' " $`.

- ▶ Чтобы сменить пароль служебной учетной записи в Grafana, [измените конфигурацию \(см. раздел 19.2\)](#) роли Grafana, указав в качестве значения параметра `GrafanaAdminPassword` новый пароль учетной записи.

18. Настройка журналирования работы MaxPatrol VM

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

В этом разделе

[Настройка журналирования работы компонента MP 10 Core на Linux \(см. раздел 18.1\)](#)

[Настройка журналирования работы компонента MP 10 Collector \(см. раздел 18.2\)](#)

18.1. Настройка журналирования работы компонента MP 10 Core на Linux

Настройка выполняется отдельно для каждой службы компонента.

► Чтобы настроить журналирование:

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

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

2. Выполните команды:

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

Журналирование настроено.

18.2. Настройка журналирования работы компонента MP 10 Collector

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию в журнал записываются события уровня DEBUG. Размер каждого файла журнала ограничен 100 МБ, сохраняются последние 50 файлов.

Для настройки журналирования вам потребуется внести изменения в файл, расположенный на сервере MP 10 Collector:

- Если MP 10 Collector установлен на Microsoft Windows — `C:\Program Files (x86)\Positive Technologies\MP 10 Collector\agent.log.xml`;
- Если MP 10 Collector установлен на Linux — `/opt/core-agent/agent.log.xml`.

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

► Чтобы настроить журналирование:

1. В файле `agent.log.xml` измените значение атрибута `level` параметра `config` → `root`:
`<Название журналируемого компонента коллектора> level="<Уровень журналирования>"`

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

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

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

3. Перезапустите службу Core Agent.

Журналирование настроено.

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

19. Просмотр и изменение параметров конфигурации MaxPatrol VM

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

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

Внимание! Перед изменением конфигурации ролей компонентов MaxPatrol VM необходимо убедиться, что в файле `/etc/apt/sources.list` закомментированы все строки с источниками, так как в противном случае процедура завершится с ошибкой.

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

В этом разделе

[Просмотр конфигурации роли \(см. раздел 19.1\)](#)

[Изменение конфигурации роли \(см. раздел 19.2\)](#)

[Управление изменением конфигурации ролей с помощью манифеста \(см. раздел 19.3\)](#)

[Настройка прокси-сервера для онлайн-активации PT MC \(см. раздел 19.4\)](#)

[Включение AI-поиска по запросам \(см. раздел 19.5\)](#)

[Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol VM \(см. раздел 19.6\)](#)

[Изменение времени устаревания активов \(см. раздел 19.7\)](#)

[Отключение правил Declarative Detect \(см. раздел 19.8\)](#)

19.1. Просмотр конфигурации роли

► Чтобы просмотреть конфигурацию роли:

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

```
tar -xvf pt_<Название роли>_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_<Название роли>_<Номер версии>/install.sh
```
3. В открывшемся окне нажмите кнопку **Yes**.

4. Выберите вариант с идентификатором приложения роли.
5. Выберите вариант с идентификатором экземпляра роли.
Откроется окно для выбора набора параметров.
6. Выберите вариант **Advanced configuration**.
Откроется страница [со списком параметров \(см. приложение Б\)](#).
7. По завершении просмотра нажмите кнопку **Cancel**.
8. В окне для выбора набора параметров нажмите кнопку **Cancel**.

19.2. Изменение конфигурации роли

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

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

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

```
tar -xf pt_<Название роли>_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_<Название роли>_<Номер версии>/install.sh
```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Выберите вариант с идентификатором приложения роли.
5. Выберите вариант с идентификатором экземпляра роли.
Откроется окно для выбора набора параметров.
6. Выберите вариант **Advanced configuration**.
Откроется страница [со списком параметров \(см. приложение Б\)](#).
7. Измените значения параметров.
8. Нажмите кнопку **OK**.
9. Нажмите **Submit**.
Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
10. Нажмите кнопку **OK**.
11. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
Конфигурация роли изменена.

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

1. На сервере с установленной ролью `Deployer` выполните команду:

```
deployer instance configure -type <Тип роли>
```

2. Выберите вариант с идентификатором приложения роли.

3. Выберите вариант с идентификатором экземпляра роли.

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

Откроется окно для выбора набора параметров.

4. Выберите вариант **Advanced configuration**.

Откроется страница [со списком параметров](#) (см. приложение Б).

5. Измените значения параметров.

6. Нажмите **Submit**.

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

7. Нажмите кнопку **OK**.

8. Выполните команду:

```
deployer instance reconfigure -diff -silent
```

Конфигурация роли изменена.

Вы можете установить значение любого из параметров экземпляра роли с помощью команды `deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр>=<Значение>`.

Вы можете сбросить значение любого параметра до значения по умолчанию с помощью команды `deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр>=` (после символа `=` значение указывать не нужно).

В одной команде вы можете указать несколько параметров одновременно — установить значение одних и сбросить значение других: `deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр 1>=<Значение> <Параметр 2>=`.

Кроме того, с помощью команды `deployer instance clearparam -Id <Идентификатор экземпляра роли>` вы можете сбросить значения всех параметров экземпляра роли до значений по умолчанию.

Внимание! После внесения этих изменений необходимо изменить конфигурацию роли, выполнив команду `deployer instance reconfigure -type <Тип роли>`.

19.3. Управление изменением конфигурации ролей с помощью манифеста

Для оптимизации работы вы можете выбрать необходимые роли и внести изменения в их конфигурацию одновременно. Для этого необходимо [создать манифест \(см. раздел 19.3.2\)](#) — файл формата YAML, который задает параметры изменения конфигурации.

В этом разделе

[Изменение конфигурации ролей с помощью манифеста \(см. раздел 19.3.1\)](#)

[Создание манифеста для обновления компонентов или изменения конфигурации ролей \(см. раздел 19.3.2\)](#)

19.3.1. Изменение конфигурации ролей с помощью манифеста

► Чтобы изменить конфигурацию ролей с помощью манифеста:

1. Обновите роль Deployer.
2. [Создайте манифест \(см. раздел 19.3.2\)](#).
3. Если требуется, добавьте параметры в файл манифеста или измените значения существующих.

Структура файла манифеста и описание его параметров приведены в разделе «Авторазвертывание MaxPatrol VM с помощью манифеста» Руководства по внедрению.

4. Выполните команду для изменения конфигурации ролей:

```
deployer application deploy ./export_manifest.yaml
```
5. Ознакомьтесь с условиями лицензионного соглашения и нажмите **I Accept**, чтобы принять их.

В консоли появится информация о результатах изменения конфигурации:

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

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

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

19.3.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей

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

► Чтобы создать манифест,

на сервере с установленной ролью Deployer запустите сценарий:

```
deployer instance export -AppId "*"
```

В текущем каталоге появится файл `export_manifest.yaml` с информацией обо всех экземплярах ролей.

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

Таблица 6. Аргументы сценария

Аргумент	Описание	Пример использования
AppId	Добавление в манифест информации об идентификаторе приложения. Для добавления информации обо всех приложениях после аргумента необходимо добавить <code>"*"</code>	<code>deployer instance export -AppId "*"</code>
Id	Добавление в манифест информации об идентификаторе экземпляра роли. Для добавления информации обо всех ролях после аргумента необходимо добавить <code>"*"</code>	<code>deployer instance export -Id "*"</code>
Type	Добавление в манифест информации о типе экземпляра роли. Для добавления информации обо всех ролях после аргумента необходимо добавить <code>"*"</code>	<code>deployer instance export -Type "*"</code>
ExcludeType	Исключение из манифеста информации о типе экземпляра роли	<code>deployer instance export -AppId "*" -ExcludeType "agentlinux"</code>
ExcludeId	Исключение из манифеста информации об идентификаторе экземпляра роли	<code>deployer instance export -AppId "*" -ExcludeId "agentlinux-1"</code>

Аргумент	Описание	Пример использования
IncludeType	Добавление в манифест информации о типе экземпляра роли	<pre>deployer instance export -AppId "*" -IncludeType "agentlinux"</pre>
IncludeId	Добавление в манифест информации о идентификаторе экземпляра роли	<pre>deployer instance export -AppId "*" -IncludeId "agentlinux-1"</pre>
IncludeParam	Добавление в манифест информации о параметрах экземпляра роли	<pre>deployer instance export -AppId "*" -IncludeType "agentlinux" -IncludeParam "RmqPassword"</pre>
IncludeParamValue	Добавление в манифест определенных значений параметров экземпляра роли	<pre>deployer instance export -AppId "*" -IncludeType "agentlinux" -IncludeParamValue "P@ssw0rd"</pre>
NotExportParams	Исключение из манифеста параметров экземпляров ролей. Параметры, к которым применены аргументы IncludeParam или -IncludeParamValue, не будут исключены из манифеста	<pre>deployer instance export -AppId "*" -IncludeType "agentlinux" -NotExportParams "RmqPassword"</pre>
ExportVersion	Сохранение текущих версий экземпляров ролей и компонентов. Аргумент применяется, если необходимо изменить конфигурацию ролей без обновления их версий	<pre>deployer instance export -AppId "*" -ExportVersion</pre>

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

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

Добавление в манифест роли Grafana

С версии 27.6 для установки средства визуализации и мониторинга данных Grafana используется новая роль Grafana. Ее реализация связана с лицензионными ограничениями на использование средства. При создании манифеста для обновления MaxPatrol VM с версии 27.4 роль Grafana не будет добавлена в него автоматически. Если вы хотите использовать Grafana, необходимо вручную добавить роль Grafana в манифест после создания.

► Чтобы добавить в манифест роль Grafana:

1. Откройте на редактирование файл `export_manifest.yaml`.
2. Добавьте в блок `appId: mc-application appType: MC-Application instances:` следующие строки:

```
Grafana-1:
  type: Grafana
  host: <IP-адрес или FQDN сервера для установки MP 10 Core>
  order: 4
```

3. Если блок `params` для роли Observability содержит параметры, которые используются в роли Grafana, скопируйте блок с этими параметрами для роли Grafana.

Внимание! Для корректной работы MaxPatrol VM значения одноименных параметров ролей Observability и Grafana должны совпадать.

Примечание. Список параметров роли вы можете посмотреть в разделе «[Параметры конфигурации компонентов MaxPatrol VM на Linux \(см. приложение Б\)](#)».

4. Сохраните изменения и закройте файл.

Примеры сценариев создания манифеста

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

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

Манифест будет включать информацию обо всех экземплярах роли Collector.

— `deployer instance export -AppId "*" -IncludeType "agentlinux" -ExportVersion`

Манифест будет включать информацию обо всех экземплярах ролей Collector.

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

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

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

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

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

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

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

- `deployer instance export -Type "agentlinux"`

Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

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

- Чтобы настроить прокси-сервер,

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

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

19.5. Включение AI-поиска по запросам

- ▶ Чтобы включить AI-поиск по PDQL-запросам,

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

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

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

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

- ▶ Чтобы включить профиль безопасности в Docker-контейнерах ролей:

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

19.7. Изменение времени устаревания активов

Параметр `DefaultAssetTtl` определяет срок, по истечении которого актив будет автоматически скрыт из интерфейса системы, если о нем не поступает новая информация (например, результаты сканирования).

Значение по умолчанию — 90 дней.

Выбор значения параметра зависит от частоты сканирования инфраструктуры и требований к хранению данных.

Таблица 7. Рекомендации по выбору значения параметра `DefaultAssetTtl`

Частота или условия сканирования	Рекомендуемое время устаревания активов	Комментарий
Раз в неделю или чаще	30–45 дней	Позволяет быстро удалять неактуальные активы и снижает объем устаревших данных
Раз в месяц	90 дней (по умолчанию)	Обеспечивает баланс между актуальностью данных и стабильностью учета активов

Частота или условия сканирования	Рекомендуемое время устаревания активов	Комментарий
Раз в несколько месяцев	180–365 дней	Предотвращает преждевременное скрывание активов при редком получении данных
Повышенные требования к хранению (например, банки)	365 дней и более	Значение определяется внутренними регламентами и требованиями комплаенса

Практические замечания по настройке времени устаревания активов:

- Слишком большое значение (например, 90 дней и более при частом сканировании) может приводить к накоплению устаревших и дублирующихся активов, что усложняет работу с выборками и анализом данных.
- Уменьшение значения помогает снизить количество нерелевантных данных, особенно при интеграции с внешними источниками (например, антивирусами).
- Изменение параметра вступает в силу только после повторного обнаружения актива (например, при следующем сканировании).
- Удаление активов носит логический характер: они перестают отображаться в интерфейсе, но их данные сохраняются в базе и не освобождают физическое место хранения.

Примечание. Для освобождения дискового пространства необходимо [настроить ротацию данных \(см. раздел 9\)](#) сервиса Temporal Read Model.

- Чтобы изменить время устаревания активов,

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

19.8. Отключение правил Declarative Detect

Правила Declarative Detect используются в MaxPatrol VM для создания активов и для обогащения данных об активах. Список правил и особенности их работы смотрите в Руководстве оператора.

Выборочное отключение правил Declarative Detect

Некоторые правила (например, ARP Hosts и Routing tables) из-за особенностей своей работы могут создавать в системе лишние объекты. По умолчанию такие правила отключены.

- Чтобы изменить список отключенных правил Declarative Detect,

измените конфигурацию роли Core, указав для параметра `DeclarativeDetectDisabledRules` правила, которые вы хотите отключить, через точку с запятой.

Отключение всех правил Declarative Detect

Вы также можете отключить Declarative Detect (вместе со всеми правилами) в файле конфигурации.

Внимание! Отключение Declarative Detect может привести к потере данных.

► Чтобы отключить все правила:

1. Перейдите в каталог `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли>/images/core.assets.processing.extended/config/` на сервере с MP 10 Core.
2. В файл `custom.env` добавьте параметр `DeclarativeDetect_Disabled` и укажите значение `True`.
3. Сохраните изменения.
4. Удалите Docker-контейнер:

```
docker rm -f $(docker ps -aqf name=<Имя Docker-контейнера>)
```
5. Перезапустите Docker-контейнер службы `Assets.Processing`:

```
cd /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли>/images/core.assets.processing.extended/  
docker-compose up -d
```

20. Удаление экземпляра роли Collector

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

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

► Чтобы удалить экземпляр роли Collector:

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

Начнется процесс удаления экземпляра роли. После его завершения появится таблица со списком выбранных для удаления экземпляров и статусом их удаления.

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

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

21. Настройка очереди выпуска отчетов

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

► Чтобы настроить очередь выпуска отчетов:

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

```
tar xzf pt_core_<Номер версии>.tar.gz
```
2. Запустите сценарий:

```
pt_core_<Номер версии>/install.sh
```
3. Выберите вариант с идентификатором приложения роли.
4. Выберите вариант с идентификатором экземпляра роли.
5. Выберите вариант **Advanced configuration**.
6. В качестве значения параметра `PrintingQueueJobsLimit` укажите максимальное количество одновременно выпускаемых отчетов.

Примечание. Чем больше это количество, тем выше будет нагрузка на аппаратные ресурсы сервера MaxPatrol VM.

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

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

22. Пользовательские поля в модели актива

После развертывания системы в модели актива присутствуют только стандартные поля (например, «Полное имя узла», «Тип устройства», «Операционная система»). Вы можете добавлять в модель актива пользовательские поля (например, «Инвентаризационный номер актива в реестре», «Ответственный за актив») и их описание, изменять имена добавленных ранее полей или удалять их из модели актива. При любых действиях с моделью необходимо увеличивать ее версию. Система использует модель с наибольшим номером версии.

После добавления полей и ввода их значений пользователи системы смогут:

- просматривать значения добавленных полей в карточке и миникарточке актива;
- вводить поисковые запросы с учетом добавленных полей;
- осуществлять выборку, группировку и отбор по значениям добавленных полей (PDQL-запрос).

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

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

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

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

В этом разделе

[Добавление пользовательских полей в модель актива \(см. раздел 22.1\)](#)

[Добавление описания пользовательских полей \(см. раздел 22.2\)](#)

[Изменение имен пользовательских полей \(см. раздел 22.3\)](#)

[Удаление пользовательских полей из модели актива \(см. раздел 22.4\)](#)

22.1. Добавление пользовательских полей в модель актива

Версия пользовательской модели полей актива должна быть больше версии системной модели. Версии сравниваются по первым трем числам и по последнему. Например, если версия системной модели 19.0.20206.0, то минимальная версия пользовательской — 19.0.20206.1. Когда версия системной модели изменится на 19.0.20207.0, то версия пользовательской модели должна стать 19.0.20207.2.

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

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

Первичное добавление пользовательских полей в модель актива

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

► Чтобы впервые добавить пользовательские поля в модель актива:

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

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

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

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

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


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

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

Например:

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

6. Если требуется, [добавьте описание пользовательских полей \(см. раздел 22.2\)](#).
7. Перезапустите службы.

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

Повторное добавление пользовательских полей в модель актива

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

- Чтобы повторно добавить пользовательские поля в модель актива:

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

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

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

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

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

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

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

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

Например:

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="19.0.20206.2">
    <Dsl Version="19.0.20206.2">
      <Entities/>
      <Migrations>
        <Group Version="19.0.20206.1">
          <ChangeEntity Type="Core.Host">
            <AddProperty Property="UF_InformationSystem" PropertyType="String"/>
            <AddProperty Property="UF_Purpose" PropertyType="String"/>
            <AddProperty Property="UF_ProdTest" PropertyType="String"/>
            <AddProperty Property="UF_Segment" PropertyType="String"/>
            <AddProperty Property="UF_Tag" PropertyType="String"/>
          </ChangeEntity>
        </Group>
        <Group Version="19.0.20206.2">
          <ChangeEntity Type="Core.Host">
            <AddProperty Property="UF_ISOOwner" PropertyType="String"/>
            <AddProperty Property="UF_ISOOwnerLogin" PropertyType="String"/>
          </ChangeEntity>
        </Group>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="19.0.20206.2">
    <Entities>
    </Entities>
  </layer>
</model>
```

5. Если требуется, [добавьте описание пользовательских полей \(см. раздел 22.2\)](#).
6. Перезапустите службы.

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

Добавление пользовательских полей в модель актива после обновления системы

После обновления системы версия системной модели полей актива меняется. Версия пользовательской модели тоже должна измениться.

► Чтобы добавить поля в модель актива после обновления системы:

1. В файле `UserModel.xml` измените первые три цифры на такие же, как у системной модели; добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например,

version="20.0.20206.3") в качестве значения атрибута Version элементов layer id="UserModel", layer id="UserDescriptions" и значения атрибута Version элемента Dsl.

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="20.0.20206.3">
    <Dsl Version="20.0.20206.3">
      <Entities/>
      <Migrations>
        <Group Version="19.0.20206.2">
          <ChangeEntity Type="Core.Host">
            <AddProperty Property="UF_InformationSystem" PropertyType="String"/>
            <AddProperty Property="UF_Purpose" PropertyType="String"/>
            <AddProperty Property="UF_ProdTest" PropertyType="String"/>
            <AddProperty Property="UF_Segment" PropertyType="String"/>
            <AddProperty Property="UF_Tag" PropertyType="String"/>
          </ChangeEntity>
        </Group>
      </Migrations>
    </Dsl>
  </layer>
  <layer id="UserDescriptions" locale="ru-RU" version="20.0.20206.3">
    <Entities>
    </Entities>
  </layer>
</model>
```

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

```
<Group Version="20.0.20206.3">
</Group>
```

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

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

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

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

Например:

```
<model Version="0.0.0.0">
  <layer id="UserModel" version="20.0.20206.3">
```

```

<Dsl Version="20.0.20206.3">
  <Entities/>
  <Migrations>
    <Group Version="19.0.20206.2">
      <ChangeEntity Type="Core.Host">
        <AddProperty Property="UF_InformationSystem" PropertyType="String"/>
        <AddProperty Property="UF_Purpose" PropertyType="String"/>
        <AddProperty Property="UF_ProdTest" PropertyType="String"/>
        <AddProperty Property="UF_Segment" PropertyType="String"/>
        <AddProperty Property="UF_Tag" PropertyType="String"/>
      </ChangeEntity>
    </Group>
    <Group Version="20.0.20206.3">
      <ChangeEntity Type="Core.Host">
        <AddProperty Property="UF_IStenant" PropertyType="String"/>
        <AddProperty Property="UF_IStenantLogin" PropertyType="String"/>
      </ChangeEntity>
    </Group>
  </Migrations>
</Dsl>
</layer>
<layer id="UserDescriptions" locale="ru-RU" version="20.0.20206.3">
  <Entities>
  </Entities>
</layer>
</model>

```

5. Если требуется, [добавьте описание пользовательских полей](#) (см. раздел 22.2).

6. Перезапустите службы.

```

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

```

См. также

[Добавление описания пользовательских полей](#) (см. раздел 22.2)

22.2. Добавление описания пользовательских полей

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

► Чтобы добавить описание пользовательских полей:

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

Например, для активов на Windows необходимо указать:

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

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

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

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

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

4. Для элемента `Properties` добавьте дочерние элементы `Property` (по числу пользовательских полей с описанием) с атрибутом `Name`. В качестве значения атрибута `Name` укажите имя поля, например:

```
<Property Name="UF_AssetNumber">
</Property>
```

5. Для каждого элемента `Property` добавьте дочерний элемент `Title`. В качестве значения элемента `Title` укажите описание пользовательского поля.

Например:

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

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

Описание пользовательских полей добавлено.

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

22.3. Изменение имен пользовательских полей

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

► Чтобы изменить имена пользовательских полей:

1. В файле `UserModel.xml` в качестве значения атрибута `version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели. Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.3"`).
2. Для элемента `layer id="UserModel" → Dsl → Migrations` добавьте дочерний элемент `Group` с атрибутом `Version`. В качестве значения атрибута `Version` укажите версию пользовательской модели, например:


```
<Group Version="19.0.20206.3">
</Group>
```
3. Для элемента `Group` добавьте дочерний элемент `ChangeEntity` с атрибутом `Type`. В качестве значения атрибута `Type` укажите `Core.Host`:


```
<ChangeEntity Type="Core.Host">
</ChangeEntity>
```
4. Для элемента `ChangeEntity` добавьте дочерние элементы `RenameProperty` (по количеству изменяемых пользовательских полей) с атрибутами `Property` и `NewName`. В качестве значения атрибута `Property` укажите старое имя поля, значения атрибута `NewName` — новое имя поля.

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

Например:

```
<Group Version="19.0.20206.3">
  <ChangeEntity Type="Core.Host">
    <RenameProperty Property="UF_AssetNumber" NewName="UF_AssetNumber"/>
    <RenameProperty Property="UF_AssetOwner" NewName="UF_AssetOwner"/>
  </ChangeEntity>
</Group>
```

```
</ChangeEntity>
</Group>
```

5. Перезапустите службы:

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

Имена пользовательских полей изменены.

22.4. Удаление пользовательских полей из модели актива

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

► Чтобы удалить пользовательские поля из модели актива:

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


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


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

Например:

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

```
</ChangeEntity>  
</Group>
```

5. Перезапустите службы:

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

Пользовательские поля удалены из модели актива.

23. Работа с инфраструктурами

При сканировании IT-инфраструктуры предприятия важно правильно идентифицировать активы. Сканирование одним коллектором сетевых сегментов, активы в которых имеют одни и те же IP-адреса, может привести к неверной агрегации активов: вместо нескольких активов система может идентифицировать один актив. Также наличие в списке активов с одинаковым IP-адресом может затруднить оператору поиск необходимого актива.

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

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

В этом разделе

[Создание инфраструктуры \(см. раздел 23.1\)](#)

[Изменение названия инфраструктуры \(см. раздел 23.2\)](#)

[Удаление инфраструктуры \(см. раздел 23.3\)](#)

23.1. Создание инфраструктуры

► Чтобы создать инфраструктуру:

1. В главном меню в разделе **Сбор данных** выберите пункт **Инфраструктура**.
Откроется страница **Инфраструктура**.
2. В панели инструментов нажмите кнопку **Добавить инфраструктуру**.
Откроется страница **Создание инфраструктуры**.
3. Введите название инфраструктуры.
4. Нажмите кнопку **Создать**.
Инфраструктура создана.

23.2. Изменение названия инфраструктуры

► Чтобы изменить название инфраструктуры:

1. В главном меню в разделе **Сбор данных** выберите пункт **Инфраструктура**.
Откроется страница **Инфраструктура**.
2. В панели инструментов нажмите кнопку **Редактировать**.

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

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

Название инфраструктуры изменено.

23.3. Удаление инфраструктуры

► Чтобы удалить инфраструктуру:

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

Откроется страница **Инфраструктура**.

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

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

Инфраструктура удалена.

24. Изменение проверок по чек-листу

► Чтобы изменить параметры проверок:

1. На сервере PT MC в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Management and Configuration>/config/usagemonitoring` создайте копию файла `check_settings.default.yaml` — файл `check_settings.yaml`.
2. В файле `check_settings.yaml` измените необходимые параметры.
3. Перезапустите контейнер `core-usage-monitoring`:

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

См. также

[Параметры проверок по чек-листу \(см. приложение В\)](#)

25. Диагностика и решение проблем

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

Предусмотрены следующие цветовые индикаторы уведомлений:

- синий — информирует о каком-либо событии, не связанном с ошибками в работе системы (например, об остановке служб);
- желтый — предупреждает о проблеме в работе системы или ее компонента (например, о приближении к пороговому значению наблюдаемого параметра) или уведомляет об инициализации компонента;
- красный — сигнализирует об ошибке в работе системы или ее компонента (например, о том, что компонент недоступен).

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

В этом разделе

[Вход в веб-интерфейс RabbitMQ \(см. раздел 25.1\)](#)

[Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога» \(см. раздел 25.2\)](#)

[Задача аудита не собирает сведения об активах \(см. раздел 25.3\)](#)

[Не приходят уведомления, отправляемые по электронной почте \(см. раздел 25.4\)](#)

[Настройка компонентов после изменения IP-адресов или FQDN их серверов \(см. раздел 25.5\)](#)

[Подсеть Docker-контейнера MaxPatrol VM совпадает с одной из подсетей предприятия \(см. раздел 25.6\)](#)

[Не удается получить обновления с сервера Positive Technologies \(см. раздел 25.7\)](#)

[Ошибка при установке, переконфигурации или обновлении компонентов в высоконагруженных системах \(см. раздел 25.8\)](#)

[Задача на сбор данных с коллектором на Windows завершается с ошибкой \(см. раздел 25.9\)](#)

[На коллекторах, установленных на Linux, задачи на сбор данных с профилем Microsoft Active Directory завершаются ошибкой \(см. раздел 25.10\)](#)

[Большое количество запросов к DNS-серверу от Docker-контейнеров сервера MP 10 Core \(см. раздел 25.11\)](#)

[Установка модуля Salt Minion завершается с ошибкой \(см. раздел 25.12\)](#)

Ошибка при загрузке шаблона для экспорта записей в формате XLSX (см. раздел 25.13)

Результат сканирования отклонен. Объем данных превышает допустимый лимит (см. раздел 25.14)

Ошибка «There is no application package with following properties: WithHidden True Id <Идентификатор пакета приложения>» при обновлении MaxPatrol VM (см. раздел 25.15)

Ошибки, связанные с сертификатом MP 10 Collector на Microsoft Windows (см. раздел 25.16)

Ошибка «The repository <Ссылка на репозиторий> does not have a Release file» (см. раздел 25.17)

Справочная информация (см. раздел 25.18)

25.1. Вход в веб-интерфейс RabbitMQ

Для входа в веб-интерфейс RabbitMQ вы можете использовать порт 15671/TCP (для подключения по протоколу HTTPS) или порт 15672/TCP (по HTTP). Рекомендуется использовать подключение по протоколу HTTPS, так как оно обеспечивает шифрование трафика и защищает учетные данные.

Перед входом в веб-интерфейс необходимо убедиться, что правила межсетевого экрана разрешают соединение от рабочей станции администратора к серверу RabbitMQ через выбранный порт — 15671/TCP или 15672/TCP.

► Чтобы войти в веб-интерфейс RabbitMQ:

1. В адресной строке браузера введите:

<Протокол HTTP или HTTPS>://<IP-адрес или FQDN сервера RabbitMQ>:<Порт>

Например:

`https://example.org:15671`

2. Введите логин и пароль.

Примечание. По умолчанию для входа в веб-интерфейс RabbitMQ используются логин Administrator и пароль P@ssw0rd.

3. Нажмите кнопку **Login**.

Отобразится страница **Overview**.

Если веб-интерфейс недоступен, необходимо проверить статус контейнера, активность процесса RabbitMQ внутри контейнера и прослушивание используемого порта — 15671/TCP или 15672/TCP.

При успешной аутентификации в правом верхнем углу в выпадающем списке **Virtual host** будут доступны для выбора следующие варианты: **All**, ****, **mpx**, **siem**.

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

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

Возможные причины

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

Решение

► Чтобы решить проблему:

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

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

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

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

- файл журнала службы Core Health Monitoring;
- снимок экрана, отображающий свободное место на логическом диске.

25.3. Задача аудита не собирает сведения об активах

Возможные причины

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

Решение

► Чтобы решить проблему:

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

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

- файлы журналов задачи аудита, собранные с уровнем журналирования debug;
- название и версию источника;
- снимки экрана с данными о правах доступа и привилегиях учетной записи, используемой для аудита.

25.4. Не приходят уведомления, отправляемые по электронной почте

► Чтобы решить проблему:

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

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

Для взаимодействия между собой компоненты системы используют IP-адреса или FQDN серверов, на которых они установлены. Эти сетевые параметры указываются администратором при установке компонента и сохраняются в его конфигурации. Если во время работы системы IP-адрес или FQDN сервера изменился, взаимодействие между

компонентами нарушится, поскольку в конфигурации компонента будет храниться прежнее значение параметра. Для восстановления взаимодействия необходимо в качестве значений параметров компонентов указать актуальные IP-адреса или FQDN серверов.

Внимание! После указания новых IP-адресов или FQDN серверов в параметрах компонентов необходимо деактивировать PT MC [по инструкции \(см. раздел 25.18.4\)](#).

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

Настройка роли Deployer

Если был изменен IP-адрес или FQDN сервера, на котором установлена роль Deployer, необходимо выполнить следующие действия:

1. На сервере каждого Salt Minion в файле `/etc/salt/minion.d/deployer.conf` указать в качестве значения параметра `master` актуальный IP-адрес или FQDN сервера с ролью Deployer и выполнить команду `systemctl restart salt-minion`.

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

2. Изменить конфигурацию роли Deployer, указав актуальное значение параметра `HostAddress`.
3. Выполнить команду для изменения конфигурации роли `deployer instance reconfigure -type Deployer`.
4. Выполнить команду `openssl s_client -connect localhost:5000 -showcerts </dev/null 2>/dev/null | openssl x509 -noout -ext subjectAltName`. Результат должен содержать DNS-имена и IP-адреса, соответствующие текущим настройкам DNS, или измененный IP-адрес — в зависимости от настройки доступа к системе.

Настройка компонентов после изменения адреса сервера MP 10 Core и PT MC

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

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

См. также

[Изменение конфигурации роли \(см. раздел 19.2\)](#)

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

Решение

Необходимо изменить подсеть Docker-контейнера MaxPatrol VM.

Команды из инструкции необходимо выполнять в интерфейсе терминала Linux.

► Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol VM остановите Docker-контейнеры:
`docker stop $(docker ps -qa)`
2. На всех серверах с установленным MaxPatrol VM удалите Docker-контейнеры:
`docker rm $(docker ps -qa)`
3. На всех серверах с установленным MaxPatrol VM удалите действующие параметры сети Docker:
`docker network prune`
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz`:
`tar -xf pt_deployer_<Номер версии>.tar.gz`
5. На сервере с установленной ролью Deployer запустите сценарий:
6. В открывшемся окне нажмите кнопку **Yes**.
7. Выберите вариант с идентификатором приложения роли.
8. Выберите вариант с идентификатором экземпляра роли.
Откроется окно для выбора набора параметров.
9. Выберите вариант **Advanced configuration**.
Откроется страница [со списком параметров \(см. приложение Б\)](#).

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

Внимание! Значение параметра должно содержать адрес подсети с маской /20 или шире (например, /19, /18 или /17) в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Например: 10.1.32.0/19 или 172.19.64.0/19.

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

Примечание. Рекомендуется использовать значение, не превышающее 24 бита. Значение параметра также должно быть больше маски подсети, указанной в значении параметра CustomDockerAddressPool, минимум на 4 бита.

12. Нажмите кнопку **OK**.

13. Нажмите **Submit**.

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

14. Нажмите кнопку **OK**.

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

16. На сервере с установленной ролью Deployer запустите обновление конфигурации установленных компонентов MaxPatrol VM:

```
deployer instance reconfigure '*' -Verbose
```

Подсеть Docker-контейнера изменена.

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

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

Изменение подсети Docker-контейнера коллектора

Возможна ситуация, когда не удастся просканировать узлы из-за того, что подсеть предприятия совпадает с подсетью Docker-контейнера коллектора. В этом случае для изменения подсети Docker-контейнера необходимо воспользоваться инструкцией, приведенной выше. При этом все команды из инструкции необходимо выполнять на сервере, где развернут коллектор, и в конце перезапустить не все компоненты, а только роль коллектора, выполнив команду `deployer instance reconfigure -type AgentLinux`.

Изменение подсети Docker-контейнера при обновлении компонентов

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

► Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol VM остановите Docker-контейнеры:
`docker stop $(docker ps -qa)`
2. На всех серверах с установленным MaxPatrol VM удалите Docker-контейнеры:
`docker rm $(docker ps -qa)`

3. На всех серверах с установленным MaxPatrol VM удалите действующие параметры сети Docker:

```
docker network prune
```

4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz` с новой версией роли:

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

5. Запустите сценарий:

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

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

7. Выберите вариант **Advanced configuration**.

Откроется страница [со списком параметров \(см. приложение Б\)](#).

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

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

Внимание! Значение параметра должно содержать адрес подсети с маской /20 или шире (например, /19, /18 или /17) в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Например: 10.1.32.0/19 или 172.19.64.0/19.

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

Примечание. Рекомендуется использовать значение, не превышающее 24 бита. Значение параметра также должно быть больше маски подсети, указанной в значении параметра `CustomDockerAddressPool`, минимум на 4 бита.

11. Нажмите кнопку **OK**.

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

12. Нажмите кнопку **OK**.

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

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

Подсеть Docker-контейнера изменена.

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

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

25.7. Не удастся получить обновления с сервера Positive Technologies

Проблема

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

Возможные причины

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

Решение

► Чтобы добавить пакет обновлений в систему:

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

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

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

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

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

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

Проблема

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

Возможные причины

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

Решение

Вы можете увеличить тайм-аут выполнения сервисных операций.

► Чтобы изменить тайм-аут:

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

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

Журнал выбранной подзадачи содержит следующую информацию об ошибке:

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

Возможные причины

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

Решение

► Чтобы решить проблему,
восстановите файл из карантина.

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

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

Проблема

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

Возможные причины

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

Решение

Необходимо установить пакет `libkrb5-3` с библиотекой MIT Kerberos версии ниже 1.18 или пакет `libkrb5-26-heimdal` с библиотекой Heimdal Kerberos, которые вы можете скачать на сайте [debian.org](https://www.debian.org).

► Чтобы решить проблему:

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

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

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

- Если вы установили библиотеку MIT Kerberos:

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

- Если вы установили библиотеку Heimdal Kerberos:

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

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

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

Проблема

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

Решение

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

- Чтобы решить проблему:

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


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

Внимание! При редактировании файла необходимо соблюдать синтаксис языка YAML.

Например:

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

4. Запустите обновление конфигураций установленных компонентов MaxPatrol VM:


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

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

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

25.12. Установка модуля Salt Minion завершается с ошибкой

Решение

► Чтобы решить проблему:

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

По завершении работы утилиты в каталоге появится архив `minion_dist_<IP-адрес или FQDN сервера, на который необходимо установить модуль Salt Minion>_<Номер версии роли Deployer>.gz`.

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

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

Проблема

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

Возможные причины

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

Решение

- ▶ Чтобы решить проблему, проверьте поля шаблона: если поле содержит ненужную формулу, удалите ее.

25.14. Результат сканирования отклонен. Объем данных превышает допустимый лимит

Проблема

Задача сканирования активов завершается с ошибкой «Результат сканирования отклонен. Объем данных превышает допустимый лимит. Обратитесь в техническую поддержку».

Возможные причины

Количество обнаруженных элементов того или иного класса модели активов превысило лимит, установленный для этого класса в конфигурации сервиса сканирования Assets.Scans.

Пример разбора ошибки: как узнать, какой класс модели активов превысил лимит

Чтобы узнать какая именно коллекция данных превысила лимит, нужно просмотреть журнал сервиса Assets.Scans. Журнал находится в каталоге:

```
/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/log/assets.scans/
```

Например:

```
/var/lib/deployed-roles/mp10-application/core-1/log/assets.scans/
```

Ошибка в журнале выглядит следующим образом:

```
2025-09-05 15:47:29.526 +03:00 ERROR Some errors occurred while processing scan.
Collection limit has been exceeded. DeclaringType - 'OperatingSystem.UnixHost',
OwnerType - 'OperatingSystem.UNIX.Linux.Debian.DebianHost', PropertyName -
'FileObjects', ElementType - 'OperatingSystem.UNIX.FileObject', Size - '171645', Limit
- '100000'.
|||ScanId="510a13ff-fc53-407f-
a17c-2c514cae71b0";Source="audit";ScopeId="00000000-0000-0000-0000-000000000005";Scan
Time="2025-09-05T12:47:26.0319127Z";JobId="faac66cd-49c6-4fb4-94a1-
f5828a6644d2";@src="AddScanService";@pid=1;@thid=3;RequestId="39985b51-5dca-4e1a-91cc
-8165bbe4c6cf";
```

Информация о фактическом размере коллекции в скане и лимите коллекции содержится в записи:

```
DeclaringType - 'OperatingSystem.UnixHost', OwnerType -
'OperatingSystem.UNIX.Linux.Debian.DebianHost', PropertyName - 'FileObjects',
ElementType - 'OperatingSystem.UNIX.FileObject', Size - '171645', Limit - '100000'.
```

Таблица 8. Поля ошибки «Объем данных превышает допустимый лимит» (Collection limit has been exceeded)

Поле	Описание	Комментарий
DeclaringType	Класс модели активов, прописанный в конфигурационном файле, в котором содержится коллекция	OperatingSystem.UnixHost из примера выше
OwnerType	Класс модели активов из скана, в которой содержится коллекция	DebianHost из примера выше — это наследник UnixHost, поэтому к нему применился лимит, заданный для UnixHost
PropertyName	Имя атрибута-коллекции	FileObjects из примера выше — это атрибут сущности UnixHost Например, в PDQL к нему можно обратиться так: UnixHost.FileObjects
ElementType	Тип элемента коллекции. Может быть примитивом, структурой или классом	OperatingSystem.UNIX.FileObject из примера выше — полный тип элемента в модели активов, содержащийся в коллекции UnixHost.FileObjects Как определить полное имя класса модели активов

Поле	Описание	Комментарий
Size	Размер коллекции в скане	—
Limit	Лимит коллекции	—

В данном случае превышен лимит коллекции `DebianHost.FileObjects`. Сам лимит прописан для `UnixHost.FileObjects`, и применился к `DebianHost`, так как он является наследником `UnixHost`.

Также лимит может примениться к наследникам класса модели активов, содержащегося в коллекции. Например, `OperatingSystem.UNIX.Linux.LinuxFileObject` — наследник `OperatingSystem.UNIX.FileObject`, он также может содержаться в коллекции `UnixHost.FileObjects`, и к нему также применяется указанный лимит.

Решение

Возможно два варианта решения:

- исключить «проблемный» класс из задачи сбора данных;
- изменить лимит, установленный для этого класса в конфигурации сервиса сканирования `Assets.Scans`.

Как исключить сбор коллекции

Поле `ElementType` в ошибке указывает полное имя класса модели активов, который содержится в коллекции. Для исключения его из сбора достаточно указать это имя в поле **Имена пропускаемых классов** в [параметрах частичного сканирования](#).

Для примера выше это будет `OperatingSystem.UNIX.FileObject`. Также можно исключить сбор наследников этого класса, например `OperatingSystem.UNIX.Linux.LinuxFileObject`.

Как изменить лимит коллекции

Лимиты коллекций по умолчанию заданы в системном конфигурационном файле, который находится по пути `/usr/local/bin/microservice/config/scan_limits/ScanPropertyLimits.yaml` в контейнере сервиса `Assets.Scans`. Этот файл не подлежит изменению.

Пример содержимого системного файла:

```
DefaultLimits:
  PrimitiveCollectionLimit: 100000
  StructCollectionLimit: 100000
  ClassCollectionLimit: 100000
ModelTypeLimits:
  - ModelType: Core.Host
    PropertyLimits:
      - PropertyName: Endpoints
```

```

    Limit: 100000
  - ModelType: Core.Computer
    PropertyLimits:
      - PropertyName: Processes
        Limit: 100000
  - ModelType: OperatingSystem.UnixHost
    PropertyLimits:
      - PropertyName: FileObjects
        Limit: 100000
      - PropertyName: Packages
        Limit: 100000
  - ModelType: OperatingSystem.NetworkDevice.NetworkDeviceHost
    PropertyLimits:
      - PropertyName: MacAddressTable
        Limit: 100000
      - PropertyName: Vlans
        Limit: 100000
  - ModelType: DirectoryService.Domain
    PropertyLimits:
      - PropertyName: Users
        Limit: 100000
      - PropertyName: Groups
        Limit: 100000
      - PropertyName: Computers
        Limit: 100000
  - ModelType: Software.VMware.vSphere.Datacenter
    PropertyLimits:
      - PropertyName: VMs
        Limit: 100000

```

Установить собственные значения лимитов можно в пользовательском конфигурационном файле `UserScanPropertyLimits.yaml`. По умолчанию этот файл отсутствует, можно добавить его по пути:

```

/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/config/
user_scan_limits/UserScanPropertyLimits.yaml

```

Например:

```

/var/lib/deployed-roles/mp10-application/core-1/config/user_scan_limits/
UserScanPropertyLimits.yaml

```

Поля конфигурационного файла имеют следующие значения:

```

ModelTypeLimits:
  - ModelType: <Полное имя класса модели активов, в котором содержится коллекция>
    PropertyLimits:
      - PropertyName: <Имя атрибута-коллекции этого класса>
        Limit: <Максимальное количество элементов коллекции>
  - ModelType: <Полное имя модельного класса, в котором содержится коллекция>

```

```
PropertyLimits:
```

- PropertyName: <Имя атрибута-коллекции этого класса>
Limit: <Максимальное количество элементов коллекции>
- PropertyName: <Имя атрибута-коллекции этого класса>
Limit: <Максимальное количество элементов коллекции>

Пример пользовательского конфигурационного файла с лимитом на 200 000 элементов коллекции:

```
ModelTypeLimits:
```

- ModelType: OperatingSystem.UnixHost
- ```
PropertyLimits:
```
- PropertyName: FileObjects  
Limit: 200000

После создания пользовательского конфигурационного файла нужно перезапустить сервис сканирования, чтобы изменения вступили в силу:

```
docker restart $(docker ps | awk '/assets-scans/ {print $NF}')
```

## Другие варианты решения

Вы также можете ограничить область сбора данных с помощью параметра **Частичный сбор данных**.

## 25.15. Ошибка «There is no application package with following properties: WithHidden True Id <Идентификатор пакета приложения>» при обновлении MaxPatrol VM

Ошибка может возникнуть во время обновления MaxPatrol VM.

### Возможные причины

Пакет приложения MaxPatrol VM был удален из каталога `/var/lib/deployer/app_packages`, но в конфигурационном файле остались ссылки на идентификатор удаленного пакета.

### Решение

Если в каталоге `var/lib/deployer/app_packages` есть пакет того же типа приложения другой версии, указать в конфигурационном файле его идентификатор.

► Чтобы решить проблему:

1. Запустите сценарий:

```
deployer maintenance fix -AppPackage
```

Отобразятся сообщения:

```
Locating replacement package for <Шаблон имени пакета>_* in <Тип приложения>
Wildcard match found: <Идентификатор доступного пакета> instead of <Идентификатор удаленного пакета> for app <Тип приложения>. Replacing.
```

По завершении работы сценария отобразится сообщение `Finishing repair process for app package references`.

2. Запустите обновление заново.

## 25.16. Ошибки, связанные с сертификатом MP 10 Collector на Microsoft Windows

Если после установки сертификатов для MP 10 Collector на Microsoft Windows сервис недоступен, необходимо проанализировать журналы компонента. Файлы журналов хранятся в папке `<Диск установки>:\ProgramData\Positive Technologies\MaxPatrol 10 Agent\log`.

### Ошибка доступа к сертификату и ключу

Вид сообщения об ошибке: `librmq: Failed to connect to broker [:5671/siem [SSL ON]]`. Description: `cert path check FAILED`.

#### Возможные причины

Не были указаны полные пути к файлам сертификата и закрытого ключа. Также возможно, что файлы сертификата и закрытого ключа находятся в папке, к которой нет доступа у пользователя Network Service.

#### Решение

► Чтобы решить проблему:

1. Проверьте правильность путей к файлам сертификата и закрытого ключа.
2. Убедитесь, что у пользователя Network Service есть доступ к папке с файлами сертификата и закрытого ключа.
3. Установите параметры сертификата повторно:

```
coreagentcfg set -p RMQ_SSL_CA_CERTIFICATE <Путь к файлу сертификата ЦС>
RMQ_SSL_CERTIFICATE <Путь к файлу сертификата Collector> RMQ_SSL_KEY <Путь к файлу
закрытого ключа Collector>
```

### Указан неверный файл сертификата

Вид сообщения об ошибке: `librmq: Error connect to amqp server: amqp_ssl_socket_set_key FAILED`.

#### Возможные причины

В качестве файла ключа `RMQ_SSL_KEY` указан неподходящий файл.

## Решение

- ▶ Чтобы исправить проблему,

Проверьте соответствие путей параметрам.

- `RMQ_SSL_CA_CERTIFICATE` — Путь к файлу сертификата ЦС;
- `RMQ_SSL_CERTIFICATE` — Путь к файлу сертификата MP 10 Collector;
- `RMQ_SSL_KEY` — Путь к файлу закрытого ключа MP 10 Collector.

## 25.17. Ошибка «The repository <Ссылка на репозиторий> does not have a Release file»

Ошибка может возникнуть во время установки, обновления или изменения конфигурации роли с помощью сценария `install.sh`. Для роли `Deployer` запись с ошибкой отображается в журнале установки роли `<Название_экземпляра_роли_версия>.log`. Для других ролей — в журнале соответствующего модуля Salt Minion `<Идентификатор модуля>.log`. Оба журнала создаются в каталоге, из которого был запущен сценарий `install.sh`.

Идентификатор модуля Salt Minion вы можете определить по сообщению `Failed to wait for the <Идентификатор модуля Salt Minion> minion to update in the given time`, которое отобразится в журнале установки роли `<Название_экземпляра_роли_версия>.log` в том же каталоге.

## Возможные причины

Во время проверки источников пакетов в файле `/etc/apt/sources.list` были обнаружены недоступные репозитории.

## Решение

- ▶ Чтобы решить проблему:

1. Откройте на редактирование файл `/etc/apt/sources.list`:
  - если ошибка возникла при установке, обновлении или изменении конфигурации роли `Deployer` — на сервере, где был запущен сценарий `install.sh`;
  - если ошибка возникла при установке, обновлении или изменении конфигурации другой роли — на сервере, соответствующем модулю Salt Minion.
2. Закомментируйте все строки, содержащие источники пакетов.
3. Сохраните изменения в файле.
4. Запустите процедуру установки, обновления или изменения конфигурации роли заново.

## 25.18. Справочная информация

В разделе приведены рекомендации по выполнению шагов инструкций.

### В этом разделе

[Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки \(см. раздел 25.18.1\)](#)

[Сбор информации о нагрузке на файловую систему и запущенных процессах \(см. раздел 25.18.2\)](#)

[Проверка доступности сетевого порта сервера \(см. раздел 25.18.3\)](#)

[Деактивация PT MC \(см. раздел 25.18.4\)](#)

[Создание дампа памяти процесса \(см. раздел 25.18.5\)](#)

[Расположение файлов журналов \(см. раздел 25.18.6\)](#)

[Расположение временных файлов аудита \(см. раздел 25.18.7\)](#)

[Параметры мониторинга обработки активов \(см. раздел 25.18.8\)](#)

[Очистка записей об операциях \(см. раздел 25.18.9\)](#)

[Экспорт конфигурационных параметров ролей в файл \(см. раздел 25.18.10\)](#)

[Экспорт и импорт пользовательских профилей \(см. раздел 25.18.11\)](#)

[Настройка мандатного контроля целостности для Astra Linux \(см. раздел 25.18.12\)](#)

[Расположение пользовательских сертификатов \(см. раздел 25.18.13\)](#)

[Реорганизация данных в таблицах СУБД PostgreSQL \(см. раздел 25.18.14\)](#)

[Удаление неиспользуемых пакетов ролей \(см. раздел 25.18.15\)](#)

[Добавление исключений в Kaspersky Endpoint Security для БД PostgreSQL \(см. раздел 25.18.16\)](#)

[Установка сертификатов для компонента Collector на Microsoft Windows \(см. раздел 25.18.17\)](#)

### 25.18.1. Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки

► Чтобы просмотреть данные о распределении памяти ОЗУ,

выполните команду:

```
free -h
```

Интерфейс терминала отобразит информацию об объеме используемой и неиспользуемой памяти ОЗУ, а также информацию об объеме раздела подкачки.

Если объем раздела подкачки не равен нулю, необходимо его отключить.

- ▶ Чтобы отключить раздел подкачки,

выполните команду:

```
swapoff -a
```

## 25.18.2. Сбор информации о нагрузке на файловую систему и запущенных процессах

- ▶ Чтобы собрать информацию о нагрузке на файловую систему,

выполните команду:

```
iostat -xt 10 10 > iostat.txt
```

Информация о нагрузке на файловую систему сохранится в файле `/root/iostat.txt`.

**Примечание.** Если утилита `iostat` отсутствует в ОС, необходимо установить ее, выполнив команду `apt-get install -f sysstat`.

- ▶ Чтобы собрать информацию о запущенных в системе процессах,

выполните команду:

```
top -b -d 10 -n 10 -o %MEM > top.txt
```

Информация о запущенных в системе процессах сохранится в файле `/root/top.txt`.

## 25.18.3. Проверка доступности сетевого порта сервера

- ▶ Чтобы проверить доступность сетевого порта сервера,

выполните команду:

```
telnet <IP-адрес или FQDN сервера> <Номер порта>
```

Если порт доступен, интерфейс терминала отобразит `Connected to <IP-адрес или FQDN сервера>`.

## 25.18.4. Деактивация РТ МС

Вы можете деактивировать РТ МС через веб-интерфейс.

**Внимание!** После деактивации РТ МС лицензии будут автоматически отвязаны от приложений. После повторной активации лицензии необходимо привязать.

При восстановлении данных из резервной копии вам потребуется деактивировать РТ МС, если ключ инсталляции уже использовался для активации РТ МС на другом устройстве.

- ▶ Чтобы деактивировать РТ МС через веб-интерфейс:

1. В главном меню выберите **Лицензии**.
2. Выберите лицензию.

3. В панели инструментов нажмите  → **Деактивировать платформу**.
4. Установите флажок **Я понимаю, что могу потерять доступ к приложениям и их данным**.
5. Нажмите **Деактивировать**.

## 25.18.5. Создание дампа памяти процесса

► Чтобы создать дамп памяти процесса на Linux:

1. Определите идентификатор процесса:

```
pgrep <Название процесса>
```

Интерфейс терминала отобразит идентификатор процесса.

2. Создайте файл дампа:

```
kill -12 <Идентификатор процесса>
```

DMP-файл дампа сохранится в том же каталоге, где расположен исполняемый файл процесса.

Дамп памяти процесса создан.

## 25.18.6. Расположение файлов журналов

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

Таблица 9. Расположение файлов журналов компонентов на Linux

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

## 25.18.7. Расположение временных файлов аудита

Во время аудита на активе создаются временные файлы. На активах с ОС Windows эти файлы хранятся в папке `C:\Windows\Temp\MPTRL`, с Unix-подобными ОС — в папках `/tmp/MPTRL` и `/tmp/.Agent-unix`.

Эти папки можно добавить в исключения, например, чтобы антивирусное ПО не останавливало сканирование.

## 25.18.8. Параметры мониторинга обработки активов

Основными показателями обработки активов являются длина очереди, время ожидания в очереди и средняя скорость обработки активов. Для тонкой настройки мониторинга обработки вы можете изменять пороговые значения длины очереди и времени ожидания, а также период вычисления средней скорости обработки активов для каждой стадии обработки. Эти параметры находятся в файлах `/var/lib/deployed-roles/mp10-application/core-*/images/<Название службы>/config/custom.env` и приведены в таблице. Для реконфигурации всех ролей необходимо выполнить команду `deployer instance reconfigure -type Core`.

**Примечание.** В файле `/var/lib/deployed-roles/mp10-application/core-*/images/core.tables.extended/config/custom.env` нет значений по умолчанию. Вы можете добавить их самостоятельно.

Таблица 10. Параметры мониторинга обработки активов

| Стадия обработки     | Служба                | Длина очереди                                                   |                                                                  | Время ожидания                                                  |                                                                  | Период вычисления средней скорости обработки                         |
|----------------------|-----------------------|-----------------------------------------------------------------|------------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------|
|                      |                       | Допустимое значение                                             | Критическое значение                                             | Допустимое значение                                             | Критическое значение                                             |                                                                      |
| Идентификация актива | Assets Identification | Statistics_QueueLengthAllowedThreshold                          | Statistics_QueueLengthCriticalThreshold                          | Statistics_WaitingTimeAllowedThreshold                          | Statistics_WaitingTimeCriticalThreshold                          | Statistics_ProcessingSpeedCalculationPeriod                          |
| Буферизация          | Assets Processing     | Statistics_IdentityCommandsBufferingQueueLengthAllowedThreshold | Statistics_IdentityCommandsBufferingQueueLengthCriticalThreshold | Statistics_IdentityCommandsBufferingWaitingTimeAllowedThreshold | Statistics_IdentityCommandsBufferingWaitingTimeCriticalThreshold | Statistics_IdentityCommandsBufferingProcessingSpeedCalculationPeriod |

| Стадия обработки                         | Служба                     | Длина очереди                                                  |                                                                 | Время ожидания                                                 |                                                                 | Период вычисления средней скорости обработки                        |
|------------------------------------------|----------------------------|----------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|-----------------------------------------------------------------|---------------------------------------------------------------------|
|                                          |                            | Допустимое значение                                            | Критическое значение                                            | Допустимое значение                                            | Критическое значение                                            |                                                                     |
| Слияние данных об активах                | Assets Processing          | Statistics_AssetsMergingQueueLengthAllowedThreshold            | Statistics_AssetsMergingQueueLengthCriticalThreshold            | Statistics_AssetsMergingWaitingTimeAllowedThreshold            | Statistics_AssetsMergingWaitingTimeCriticalThreshold            | Statistics_AssetsMergingProcessingSpeedCalculationPeriod            |
| Расчет содержимого динамических групп    | Assets Groups              | Statistics_DynamicGroupsCalculationQueueLengthAllowedThreshold | Statistics_DynamicGroupsCalculationQueueLengthCriticalThreshold | Statistics_DynamicGroupsCalculationWaitingTimeAllowedThreshold | Statistics_DynamicGroupsCalculationWaitingTimeCriticalThreshold | Statistics_DynamicGroupsCalculationProcessingSpeedCalculationPeriod |
| Расчет данных об уязвимостях             | Vulnerabilities Processing | Statistics_VulnerabilityCalculationQueueLengthAllowedThreshold | Statistics_VulnerabilityCalculationQueueLengthCriticalThreshold | Statistics_VulnerabilityCalculationWaitingTimeAllowedThreshold | Statistics_VulnerabilityCalculationWaitingTimeCriticalThreshold | Statistics_VulnerabilityCalculationProcessingSpeedCalculationPeriod |
| Расчет соответствия активов требованиям  | Host Compliance Control    | Statistics_AssetsQueueLengthAllowedThreshold                   | Statistics_AssetsQueueLengthCriticalThreshold                   | Statistics_AssetsWaitingTimeAllowedThreshold                   | Statistics_AssetsWaitingTimeCriticalThreshold                   | Statistics_AssetsProcessingSpeedCalculationPeriod                   |
| Обновление отображаемых данных об активе | Assets Temporal Read Model | Statistics_QueueLengthAllowedThreshold                         | Statistics_QueueLengthCriticalThreshold                         | Statistics_WaitingTimeAllowedThreshold                         | Statistics_WaitingTimeCriticalThreshold                         | Statistics_ProcessingSpeedCalculationPeriod                         |

| Стадия обработки                              | Служба                     | Длина очереди                          |                                         | Время ожидания                         |                                         | Период вычисления средней скорости обработки |
|-----------------------------------------------|----------------------------|----------------------------------------|-----------------------------------------|----------------------------------------|-----------------------------------------|----------------------------------------------|
|                                               |                            | Допустимое значение                    | Критическое значение                    | Допустимое значение                    | Критическое значение                    |                                              |
| Обновление отображаемых данных о требованиях  | Assets Temporal Read Model | Statistics_QueueLengthAllowedThreshold | Statistics_QueueLengthCriticalThreshold | Statistics_WaitingTimeAllowedThreshold | Statistics_WaitingTimeCriticalThreshold | Statistics_ProcessingSpeedCalculationPeriod  |
| Обновление отображаемых данных об уязвимостях | Assets Temporal Read Model | Statistics_QueueLengthAllowedThreshold | Statistics_QueueLengthCriticalThreshold | Statistics_WaitingTimeAllowedThreshold | Statistics_WaitingTimeCriticalThreshold | Statistics_ProcessingSpeedCalculationPeriod  |
| Обновление табличных списков                  | Tables                     | Statistics_QueueLengthAllowedThreshold | Statistics_QueueLengthCriticalThreshold | Statistics_WaitingTimeAllowedThreshold | Statistics_WaitingTimeCriticalThreshold | Statistics_ProcessingSpeedCalculationPeriod  |

## 25.18.9. Очистка записей об операциях

Механизм очистки предназначен для удаления устаревших записей об операциях (в первую очередь связанных с политиками), что позволяет контролировать рост базы данных.

Настройка параметров очистки рекомендуется в следующих случаях:

- наблюдается быстрый рост базы данных;
- активно используются политики и часто изменяются данные;
- увеличивается объем записей об операциях, влияющий на производительность системы.

Как правило, необходимость настройки становится очевидной в процессе эксплуатации системы.

### Параметры очистки записей об операциях

Таблица 11. Параметры очистки записей об операциях

| Параметр                                                | Описание                                                                                                                                                                              | Значение по умолчанию   |
|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <code>StreamCleanup_SearchToCleanupJobPeriod</code>     | Периодичность запуска задания поиска записей об операциях, подлежащих очистке. Определяет, как часто система анализирует таблицу на наличие устаревших данных, связанных с политиками | <code>'02:00:00'</code> |
| <code>StreamCleanup_SearchToCleanupJobDisabled</code>   | Флаг отключения задания поиска записей для очистки. При значении <code>true</code> поиск не выполняется                                                                               | <code>false</code>      |
| <code>StreamCleanup_SearchToCleanupJobStartDelay</code> | Задержка перед первым запуском задания поиска записей после старта системы в формате чч:мм:сс. Используется для завершения инициализации системы перед началом обработки              | <code>'00:05:00'</code> |
| <code>StreamCleanup_CleanupJobPeriod</code>             | Периодичность запуска задания физической очистки (удаления) устаревших записей об операциях в формате                                                                                 | <code>'00:01:00'</code> |

| Параметр                                      | Описание                                                                                                                                                                                                                                                                                                                                                                | Значение по умолчанию |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                               | чч:мм:сс. Влияет на скорость освобождения места в базе данных                                                                                                                                                                                                                                                                                                           |                       |
| StreamCleanup_CleanupJob Disabled             | Флаг отключения задания физической очистки. При значении true удаление данных не выполняется                                                                                                                                                                                                                                                                            | false                 |
| StreamCleanup_CleanupJob StartDelay           | Задержка перед первым запуском задания физической очистки после старта системы в формате чч:мм:сс. Позволяет снизить начальную нагрузку и синхронизировать выполнение с другими заданиями                                                                                                                                                                               | '00:05:00'            |
| StreamCleanup_VulnerOperationsSearchBatchSize | Количество записей (размер пакета), обрабатываемых за одну итерацию при поиске устаревших данных, связанных с уязвимостями. Влияет на нагрузку на базу данных во время сканирования                                                                                                                                                                                     | 3                     |
| StreamCleanup_CleanupBatchSize                | Количество записей (размер пакета), удаляемых за одну транзакцию. Обычно не требует изменения. Корректировка может потребоваться, если за один запуск задания по параметру StreamCleanup_CleanupJob Period не удаляется достаточный объем устаревших записей. Увеличение значения позволяет удалять больше данных за одну итерацию, но повышает нагрузку на базу данных | 1000                  |

## Настройка параметров очистки

Общие рекомендации по настройке параметров очистки записей об операциях:

- Чем больше количество политик и выше частота изменений данных, тем чаще следует выполнять очистку.
- При наличии достаточного дискового пространства рекомендуется использовать значения по умолчанию.
- Не рекомендуется без необходимости использовать агрессивные значения параметров очистки, так как это приводит к увеличению нагрузки на базу данных и вычислительные ресурсы (CPU).

Вы можете использовать следующие значения параметров для ускоренной очистки и уменьшения размера баз данных `maxpatrol_assets_processing` и `core_vulnerabilities_processing`:

- `StreamCleanup_SearchToCleanupJobPeriod='00:05:00'` — увеличивает частоту поиска устаревших записей об операциях;
- `StreamCleanup_CleanupJobPeriod='00:00:00.1'` — ускоряет выполнение физической очистки;
- `StreamCleanup_VulnerabilityOperationsSearchBatchSize=10000` — увеличивает размер обрабатываемых пакетов.

**Внимание!** Увеличение частоты поиска и размера пакетов повышает нагрузку на систему.

► Чтобы изменить параметры очистки:

1. Откройте файл `custom.env`, расположенный в каталоге соответствующего сервиса:
  - для базы `maxpatrol_assets_processing` — `/var/lib/deployed-roles <Идентификатор приложения MaxPatrol VM>/<Название экземпляра роли Core>/images/core.assets.processing.extended/config/`
  - для базы `core_vulnerabilities_processing` — `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol VM>/<Название экземпляра роли Core>/images/core.vulnerabilities.processing.extended/config/`

2. Добавьте необходимые параметры в файл `custom.env`.

**Внимание!** Необходимо указывать только изменяемые параметры (не копировать все содержимое файла `default.env`).

**Внимание!** Необходимо соблюдать корректность синтаксиса (формат `параметр=значение`), в противном случае это может привести к удалению контейнеров.

3. Перезапустите Docker-контейнер:

```
docker-compose -p $(docker inspect --format '{{ index .Config.Labels "com.docker.compose.project" }}' $(docker ps -qf name=<Название сервиса>)) up -d --force-recreate
```

После изменения параметров рекомендуется подождать не менее 30 минут и оценить прогресс очистки с помощью SQL-запросов.

## Контроль выполнения очистки

► Чтобы оценить прогресс очистки записей об операциях:

1. Если сервер MP 10 Core установлен на Unix, в браузере перейдите по адресу `http://<IP-адрес сервера>:9001`.
2. В списке баз данных выберите `maxpatrol_assets_processing`, нажмите правой кнопкой мыши и выберите **Query Tool**.
3. Для анализа распределения типов записей об операциях выполните запрос:
 

```
select s.streamtype,
 sum(pg_column_size(s.payload)) as size,
 count(s.fingerprint),
 count(s.fingerprint) / (select count(*) from commits)::numeric * 100 as pct
from commits s
group by s.streamtype
order by pct desc;
```
4. Для оценки процента очищенных данных выполните запрос:
 

```
SELECT EmptyPayloadCount, TotalCount, to_char(EmptyPayloadCount*100.0/TotalCount, '999D9')
as Percent
FROM
(
SELECT
(
SELECT count(1)
FROM public.commits
WHERE streamtype IN ('VulnerabilityOperationAssetsPack',
'VulnerabilityOperationProcessManager')
AND length(payload) = 0) as EmptyPayloadCount,
(
SELECT count(1)
FROM public.commits
WHERE streamtype IN ('VulnerabilityOperationAssetsPack',
'VulnerabilityOperationProcessManager')
) as TotalCount
) as t;
```
5. После выполнения каждого запроса нажмите F8 или выберите опцию **Save As** и сохраните результаты в формате CSV или TXT для последующего анализа.

## Освобождение дискового пространства после очистки записей об операциях

После достижения высокого процента очищенных данных в базе `maxpatrol_assets_processing` рекомендуется выполнить команду `VACUUM FULL` для фактического освобождения места.

Перед выполнением команды необходимо выполнить следующие условия:

- остановить сервис `maxpatrol_assets_processing`;
- заранее выделить технологическое окно;
- убедиться в наличии свободного места на диске, достаточного для создания компактной копии таблиц. Рекомендуется обеспечить не менее 80% от текущего размера базы данных. Минимально допустимое значение — около 50% от размера базы данных, если ожидается высокий уровень фрагментации и большое количество удалённых записей.

**Примечание.** Операция `VACUUM FULL` может быть ресурсоемкой и занимать продолжительное время.

При недостатке свободного места рекомендуется выполнять очистку по таблицам или обратиться в техническую поддержку за дополнительными рекомендациями.

## 25.18.10. Экспорт конфигурационных параметров ролей в файл

Вы можете экспортировать конфигурационные параметры ролей MaxPatrol VM в файл манифеста с помощью утилиты `Export-Configuration`, поставляемой с ролью `Deployer`. Полученный в результате экспорта манифест вы можете использовать при развертывании MaxPatrol VM на другом сервере.

► Чтобы экспортировать конфигурационные параметры ролей в файл:

1. Запустите утилиту `Export-Configuration`:  
`/opt/deployer/bin/Export-Configuration.ps1`
2. В открывшемся окне выберите варианты с идентификаторами приложений.
3. В открывшемся окне выберите экземпляры ролей, для которых необходимо экспортировать конфигурационные параметры.

Начнется экспорт параметров выбранных экземпляров ролей. В каталоге с утилитой появится файл `export_manifest.yaml`.

**Примечание.** Если в каталоге уже существует файл с именем `export_manifest.yaml`, в конец его имени будут добавлены дата и время создания нового файла: `export_manifest.yaml.<yyyyMMddHHmmss>`. Новый файл будет сохранен с именем `export_manifest.yaml`.

Параметры роли экспортированы.

При запуске утилиты вы можете также использовать специальные ключи:

- для указания приложения — ключ `AppInstanceId` <Идентификатор приложения>. Например: `/opt/deployer/bin/Export-Configuration.ps1 -AppInstanceId mc-application`

**Примечание.** После запуска утилиты с этим ключом в файл манифеста будут экспортированы конфигурационные параметры всех ролей приложения, указанного в ключе.

- для указания роли — ключ `RoleInstanceId` <Идентификатор экземпляра роли>. Например: `/opt/deployer/bin/Export-Configuration.ps1 -RoleInstanceId managementandconfiguration`

Для каждого ключа можно указать только один идентификатор.

## 25.18.11. Экспорт и импорт пользовательских профилей

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

Для запуска скрипта необходимы следующие конфигурационные файлы:

- `enabled_profiles.yaml` — содержит список профилей, которые необходимо экспортировать (импортировать);
- `hosts` — содержит параметры подключения к узлу, с которого необходимо экспортировать (или на который импортировать) профили.

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

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

### Экспорт профилей

► Чтобы экспортировать пользовательские профили:

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

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

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

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

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

3. Перейдите в каталог `core.unitmigrator`:

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

4. Запустите скрипт с помощью команды:

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

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

JSON-файл с результатами экспорта содержит следующие объекты:

- `hash` — хеш-сумма файла без учета пробелов;
- `microservice_version` — версия микросервиса, из которого экспортировались профили;
- `scanning_api_version` — версия API (ресурса), из которого экспортировались профили;
- `dictionaries_api_version` — версия API (ресурса), из которого экспортировались справочники;
- `credentials_api_version` — версия API (ресурса), из которого экспортировались учетные записи;
- `profiles` — список экспортируемых профилей;
- `dictionaries` — список пользовательских справочников, которые относятся к экспортируемым профилям;
- `credentials` — список учетных записей, которые относятся к экспортируемым профилям.

## Импорт профилей

- Чтобы импортировать пользовательские профили:

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

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

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

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

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

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

4. Перейдите в каталог `core.unitmigrator`:

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

## 5. Запустите скрипт с помощью команды с параметрами импорта:

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

Например:

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

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

Профили импортированы.

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

Таблица 12. Параметры запуска скрипта при импорте профилей

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

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

## 25.18.12. Настройка мандатного контроля целостности для Astra Linux

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

► Чтобы изменить уровень целостности,

выполните команды:

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

После установки MaxPatrol VM рекомендуется установить прежнее значение уровня целостности.

## 25.18.13. Расположение пользовательских сертификатов

При резервном копировании и восстановлении данных вам могут потребоваться файлы пользовательских сертификатов. Вы можете найти их в списке параметров всех установленных ролей.

► Чтобы отобразить параметры ролей,

на сервере с установленной ролью `Deployer` выполните команду:

```
deployer params get
```

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

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

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

Путь к найденным файлам сертификатов указан в подразделе `InstanceDefined` в значении параметра `CertificatesDir` каждой роли, для которой был добавлен сертификат: `CertificatesDir=/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.

## 25.18.14. Реорганизация данных в таблицах СУБД PostgreSQL

При работе с СУБД PostgreSQL данные таблиц БД могут фрагментироваться, что приводит к ухудшению производительности работы системы и нерациональному использованию дискового пространства. Чтобы безопасно реорганизовать фрагментированные данные таблиц, восстановить индексы и вернуть дисковое пространство без влияния на производительность БД, можно использовать утилиту `pgcompactable`, которая поставляется с ролью `SqlStorage`.

Утилита `pgcompactable` является альтернативой команды `VACUUM FULL`, но, в отличие от `VACUUM FULL`, не требует большого количества свободного места на диске и не блокирует таблицы на время своей работы. В ходе работы утилиты таблицы обрабатываются с адаптивными задержками для предотвращения перегрузки ввода и вывода данных и задержек репликации.

**Внимание!** Не запускайте утилиту `pgcompactable` и команду `VACUUM FULL` одновременно.

Для работы утилиты pgcompacttable необходимо свободное место, равное размеру самого большого индекса в БД. Перед запуском утилиты для каждой БД, где планируется использовать утилиту, необходимо создать расширение pgstattuple с помощью команды `docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}') psql -U pt_system -d <Имя БД PostgreSQL> -c "CREATE EXTENSION IF NOT EXISTS pgstattuple;"`.

Узнать размер БД для сравнения результатов до и после работы утилиты вы можете с помощью команды `docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}') psql -c "SELECT datname AS Database_Name, pg_size_pretty(pg_database_size(datname)) AS Size FROM pg_database ORDER BY pg_database_size(datname) DESC LIMIT 15;" -d postgres -U pt_system`.

Продолжительность работы утилиты зависит от размера БД PostgreSQL, объема фрагментированных данных, а также от аппаратного обеспечения сервера и нагрузки на него, и в некоторых случаях может занимать до нескольких часов. Чтобы работа утилиты не прерывалась из-за разрыва соединения, рекомендуется выполнять запуск в одном из терминальных мультиплексоров, например в `screen`.

► Чтобы запустить утилиту,

на сервере с установленной ролью `SqlStorage` выполните команду:

```
docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}')
pgcompacttable --verbose -U pt_system -d <Имя БД PostgreSQL> >> /var/tmp/
pgcompacttable.log
```

Журнал работы утилиты будет сохранен в файл `/var/tmp/pgcompacttable.log`.

При запуске утилиты вы можете использовать специальные ключи:

— `-a` и `--all`

Запуск утилиты на всех БД кластера.

— `-t TABLE` и `--table TABLE`

Запуск утилиты для конкретной таблицы.

— `-T TABLE` и `--exclude-table TABLE`

Исключение таблицы из обработки.

— `-n SCHEMA` и `--schema SCHEMA`

Обработка таблиц и индексов в конкретной схеме.

— `-N SCHEMA` и `--exclude-schema SCHEMA`

Исключение схемы из обработки.

— `-f` и `--force`

Принудительный запуск обработки.

**Примечание.** Без использования этого ключа таблицы и индексы с избыточностью данных менее 20% по умолчанию не обрабатываются.

— --man

Просмотр списка всех доступных ключей и информации о них.

Пример запуска утилиты на всех БД кластера:

```
docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}')
pgcompacttable --all --verbose -U pt_system >> /var/tmp/pgcompacttable.log
```

## 25.18.15. Удаление неиспользуемых пакетов ролей

Вы можете удалить неиспользуемые пакеты ролей компонентов MaxPatrol VM с помощью утилиты `deployer`, которая поставляется с ролью `Deployer`. Запускать утилиту в интерфейсе терминала необходимо с правами суперпользователя (`root`) на сервере с установленной ролью `Deployer`.

**Примечание.** Утилита запускается автоматически после установки или обновления роли, а в низконагруженных системах — после автоматического развертывания конфигурации. Если в хранилище есть неиспользуемые пакеты, вам будет предложено подтвердить их удаление.

Вы можете удалить неиспользуемые пакеты всех ролей сразу или пакеты одной роли.

► Чтобы удалить неиспользуемые пакеты всех ролей:

1. Выполните команду:  
`deployer package clean`
2. Выберите пакеты для удаления и нажмите **Confirm**.

► Чтобы удалить неиспользуемые пакеты одной роли:

1. Выполните команду:  
`deployer package clean -type <Тип роли>`  
Например:  
`deployer package clean -type SqlStorage`
2. Выберите пакеты для удаления и нажмите **Confirm**.

## 25.18.16. Добавление исключений в Kaspersky Endpoint Security для БД PostgreSQL

В процессе проверки на вирусы Kaspersky Endpoint Security может ошибочно помещать в карантин нужные файлы БД PostgreSQL. Вы можете исключить такие файлы из проверки. Для этого необходимо определить путь расположения файлов и добавить его в список исключений Kaspersky Endpoint Security.

- Чтобы определить путь расположения файлов,

выполните одно из следующих действий:

- если PostgreSQL установлена в Docker-контейнере, выполните команду:  

```
docker inspect -f 'Name: {{println .Name}}{{range .Mounts }}Mount: {{println .Source}}
{{end}}' $(docker ps -aqf name=postgres)
```

На экране появится имя контейнера и пути расположения файлов и журналов.

Например:

```
Name: /storage-postgres.mc-application.sqlstorage-1
Mount: /var/lib/deployed-roles/mc-application/sqlstorage-1/data
Mount: /var/lib/deployed-roles/mc-application/sqlstorage-1/log
```

**Примечание.** По умолчанию файлы БД PostgreSQL расположены в каталоге /data.

- если PostgreSQL установлена как служба, выполните команду:

```
ps -auxw | grep -Eo "postgres\s+?-D\s+[^s]+\s"
```

На экране появится путь расположения файлов:

```
postgres -D <Путь расположения файлов>
```

**Примечание.** Если служба работает под управлением Patroni, по умолчанию файлы расположены в каталоге /data/patroni.

После определения пути расположения файлов PostgreSQL его необходимо добавить в списки исключений (подробнее см. на сайте [support.kaspersky.ru](https://support.kaspersky.ru)).

## 25.18.17. Установка сертификатов для компонента Collector на Microsoft Windows

### Выпуск сертификатов

- Чтобы установить сертификаты:

1. На сервере с установленной ролью Deployer разместите [утилиту для генерации сертификатов](#).

2. Создайте сертификат и закрытый ключ для компонента Collector:

```
./generate_remote_signed_cert.sh --common-name agent --cert ~/RmqClientAgent.crt --key ~/RmqClientAgent.key
```

Внутри указанных каталогов будут созданы файлы сертификата и закрытого ключа.

### Установка сертификатов на сервер Microsoft Windows

**Примечание.** Вы можете воспользоваться этой инструкцией, чтобы перенести на сервер пользовательские сертификаты.

- ▶ Чтобы перенести сертификаты и закрытые ключи для компонента MP 10 Collector на Microsoft Windows:

1. Разместите файлы сертификата ЦС (расположен на сервере с ролью Deployer в файле /opt/deployer/pki/rootCA.crt), пользовательского сертификата и закрытого ключа на сервере Microsoft Windows в постоянной папке, к которой есть доступ у пользователя Network Service.

2. Откройте командную строку от имени администратора.

3. Установите сертификат для MP 10 Collector, выполнив следующую команду:

```
coreagentcfg set -p RMQ_SSL_CA_CERTIFICATE <Полный путь к файлу сертификата ЦС>
RMQ_SSL_CERTIFICATE <Полный путь к файлу пользовательского сертификата> RMQ_SSL_KEY
<Полный путь к файлу закрытого ключа>
```

Например:

```
coreagentcfg set -p RMQ_SSL_CA_CERTIFICATE "C:\ProgramData\Positive Technologies\MaxPatrol
10 Agent\cert\rootCA.crt" RMQ_SSL_CERTIFICATE "C:\ProgramData\Positive
Technologies\MaxPatrol 10 Agent\cert\RmqClientAgent.crt" RMQ_SSL_KEY "C:
\ProgramData\Positive Technologies\MaxPatrol 10 Agent\cert\RmqClientAgent.key"
```

4. Проверьте установку сертификатов:

```
coreagentcfg get
```

Значения параметров RMQ\_SSL\_CA\_CERTIFICATE, RMQ\_SSL\_CERTIFICATE и RMQ\_SSL\_KEY должны содержать пути к установленным сертификатам и закрытому ключу.

Если при установке сертификатов возникли проблемы, вы можете ознакомиться с [часто возникающими ошибками \(см. раздел 25.16\)](#).

## 26. О технической поддержке

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

### Предоставление доступа к обновленным версиям продукта

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

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

### Восстановление работоспособности продукта

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

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

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

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

### Рассмотрение предложений по доработке продукта

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

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются [на портале технической поддержки](#).

## Портал технической поддержки

[На портале технической поддержки](#) вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

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

Поддержка на портале предоставляется на русском и английском языках.

## Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку [на портале технической поддержки](#) и предоставить следующие данные:

- номер лицензии на использование продукта;
- файлы журналов и наборы диагностических данных, которые требуются для анализа;
- снимки экрана.

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

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

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

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

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

## Время реакции и приоритизация заявок

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

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

Таблица 13. Время реакции на заявку

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

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

## Обработка и закрытие заявок

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

- о ходе диагностики по заявленной проблеме и ее результатах;
- планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

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

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

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

## Приложение А. Привилегии и роли MaxPatrol VM

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

Таблица 14. Привилегии и роли MaxPatrol VM

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

| Код привилегии               | Привилегия                              | Администратор | Оператор | Наблюдатель |
|------------------------------|-----------------------------------------|---------------|----------|-------------|
| DataCollectExclusionsViewing | Просмотр                                | -             | -        | +           |
| DataCollectExclusionsEditing | Создание, просмотр, изменение, удаление | +             | +        | -           |
| <b>Infrastructure</b>        | <b>Инфраструктура</b>                   | +             | -        | -           |
| <b>System</b>                | <b>Система</b>                          |               |          |             |
| AccessRights                 | Права доступа                           | +             | -        | -           |
| Triggers                     | Уведомления                             | +             | +        | -           |
| SystemManagement             | Управление системой                     | +             | +        | -           |
| ChecksManagement             | Управление контролями                   | +             | +        | -           |
| Reports                      | Отчеты                                  | +             | +        | -           |
| <b>AI.Assistant</b>          | <b>AI-помощник</b>                      |               |          |             |
| AI.Assistant                 | Использование AI-помощника              | +             | +        | -           |
| <b>Topology</b>              | <b>Топология</b>                        |               |          |             |
| TopologyAnalyzer             | Расчет достижимости                     | +             | +        | -           |
| Topology                     | Топология                               | +             | +        | -           |

## Приложение Б. Параметры конфигурации компонентов MaxPatrol VM на Linux

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

Таблица 15. Параметры конфигурации роли Deployer

| Параметр                  | Описание                                                                                                                                                                                                                           | Значение по умолчанию |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| CertificateVendorEmail    | Адрес электронной почты вендора.<br><b>Примечание.</b> Этот параметр может быть изменен только при первой установке продукта                                                                                                       | pt@ptsecurity.com     |
| CertificateVendorLocality | Город, где располагается главный офис вендора.<br><b>Примечание.</b> Этот параметр может быть изменен только при первой установке продукта                                                                                         | Moscow                |
| CertificateVendorName     | Название вендора.<br><b>Примечание.</b> Этот параметр может быть изменен только при первой установке продукта                                                                                                                      | Positive Technologies |
| CustomDockerAddressPool   | Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию. Рекомендуется использовать подсеть с маской /20 или шире в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 | —                     |

| Параметр                | Описание                                                                                                                                                                                                                                                                                                    | Значение по умолчанию |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| CustomDockerNetworkSize | Размер подсетей, которые будут выделяться из диапазона, указанного в параметре CustomDockerAddressPool. Рекомендуется использовать значение, не превышающее 24 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра CustomDockerAddressPool, как минимум на 4 бит | —                     |
| DockerBindHost          | IP-адрес или FQDN сервера с локальным реестром Docker-образов                                                                                                                                                                                                                                               | 0.0.0.0               |
| HostAddress             | IP-адрес или FQDN сервера с установленной ролью Deployer                                                                                                                                                                                                                                                    | —                     |
| Network                 | Сетевое имя реестра Docker-образов                                                                                                                                                                                                                                                                          | registry-network      |
| NetworkDriver           | Драйвер Docker-образов                                                                                                                                                                                                                                                                                      | bridge                |
| RegistryPort            | Номер порта для доступа к локальному реестру Docker-образов                                                                                                                                                                                                                                                 | 5000                  |

Таблица 16. Параметры конфигурации роли SqlStorage

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

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

| Параметр                 | Описание                                                                                                                                                                                            | Значение по умолчанию |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| PgEmail                  | Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL                                                                                                                            | email@email.com       |
| PgHardDiskType           | Тип используемого оборудования для хранилища (возможные значения — HDD или SSD)                                                                                                                     | HDD                   |
| PgInitArgs               | Параметры инициализации кластера PostgreSQL                                                                                                                                                         | --locale='en_US.UTF8' |
| PgLogLevel               | Уровень журналирования работы СУБД PostgreSQL (возможные значения — panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)                                     | warning               |
| PgMasterPasswordRequired | Запрос мастер-пароля для СУБД PostgreSQL включен (флажок установлен) или выключен (флажок снят)                                                                                                     | Флажок снят           |
| PgPassword               | Пароль служебной учетной записи для доступа к СУБД PostgreSQL.<br><b>Внимание!</b> Не рекомендуется использовать в паролях служебных учетных записей в PostgreSQL следующие символы: # \ / ' " ; \$ | P@ssw0rdP@ssw0rd      |
| PgPort                   | Порт для доступа к СУБД PostgreSQL                                                                                                                                                                  | 5432                  |
| PgServerMode             | Режим сервера для экземпляра СУБД PostgreSQL                                                                                                                                                        | Флажок снят           |
| PgSharedBufferSize       | Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти                                                                                                         | 4GB                   |
| PgTimeZone               | Часовой пояс для экземпляра СУБД PostgreSQL                                                                                                                                                         | Europe/Moscow         |
| PgUpgradeJobs            | Количество одновременных процессов или потоков, используемых для pg_upgrade                                                                                                                         | 4                     |

| Параметр                  | Описание                                                                                                                                            | Значение по умолчанию |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| PgUpgradeVerbose          | Детализированное ведение журнала для pg_upgrade включено (флажок установлен) или выключено (флажок снят)                                            | Флажок снят           |
| PgUser                    | Логин служебной учетной записи для доступа к СУБД PostgreSQL                                                                                        | pt_system             |
| PgVacuumNapTime           | Минимальная задержка между двумя запусками автоочистки для отдельной базы данных                                                                    | 20min                 |
| PgWorkMem                 | Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске | 200MB                 |
| SSLCertificatePemFileName | Имя файла сертификата SSL в формате PEM                                                                                                             | Portal.crt            |
| SSLKeyFileName            | Имя файла закрытого ключа SSL-сертификата                                                                                                           | Portal.key            |

Таблица 17. Параметры конфигурации роли LogConnector

| Параметр        | Описание                                                              | Значение по умолчанию |
|-----------------|-----------------------------------------------------------------------|-----------------------|
| DockerBindHost  | IP-адрес или FQDN сервера с локальным реестром Docker-образов         | 0.0.0.0               |
| HostAddress     | IP-адрес или FQDN сервера с установленной ролью Deployer              | —                     |
| PostgreHost     | IP-адрес или FQDN сервера СУБД PostgreSQL                             | localhost             |
| 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             |

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

Таблица 18. Параметры конфигурации роли 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                  |
| PackageManagementPort        | Номер порта сервиса управления пакетами Package Management                                                                                                            | 8585                  |
| PackagesSourceUri            | Адрес сервера обновлений                                                                                                                                              | —                     |
| Policy_RecalculationInterval | Тип значения: интервал времени в формате hh:mm:ss.                                                                                                                    | 00:07:30              |

| Параметр | Описание                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | Значение по умолчанию |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|          | <p>Определяет интервал между пересчетами политик и применением их действия. Влияет на все политики MaxPatrol VM.</p> <p>При слишком большом интервале (например, раз в сутки) возможна значительная задержка реакции политик: новая критичная или трендовая уязвимость будет обработана только при следующем пересчете. Слишком маленький интервал может увеличивать нагрузку системе при обработке большого количества активов и уязвимостей.</p> <p>Рекомендации:</p> <ul style="list-style-type: none"> <li>— Для обработки уязвимостей в соответствии с регламентами используйте значения в диапазоне нескольких минут, например, 15.</li> <li>— Не рекомендуется использовать длительные интервалы, например, сутки.</li> <li>— При необходимости быстрой реакции на критические уязвимости допускается сокращение интервала пересчета. Предварительно нужно оценить объем данных для обработки и текущую производительность экземпляра приложения MaxPatrol VM</li> </ul> |                       |
| UseProxy | Использовать ли прокси-сервер для онлайн-активации                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | false                 |

Таблица 19. Параметры конфигурации роли Core

| Параметр                            | Описание                                    | Значение по умолчанию |
|-------------------------------------|---------------------------------------------|-----------------------|
| AssetGridValidTimePeriodIndexFormat | Режим оптимизации выполнения PDQL-запросов: | IdAndPeriod           |

| Параметр                                         | Описание                                                                                                                                                          | Значение по умолчанию |
|--------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                                  | <p><code>IdAndPeriod</code> (по умолчанию) — максимальное повышение производительности;</p> <p><code>PeriodOnly</code> — среднее повышение производительности</p> |                       |
| <code>AssetGridVersionRangeModeEnabled</code>    | Режим оптимизации выполнения PDQL-запросов включен (флажок установлен) или выключен (флажок снят)                                                                 | Флажок установлен     |
| <code>ConsiderEventsImportance</code>            | В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят)                                  | Флажок установлен     |
| <code>ContentDeployerPort</code>                 | Номер порта сервиса установки обновлений экспертизы Content Deployer                                                                                              | 8586                  |
| <code>DefaultAssetTtl</code>                     | Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)                                                                                                       | 90.00:00:00           |
| <code>DefaultLocale</code>                       | Интерфейс MaxPatrol VM отображается на русском (ru-RU) или английском (en-US) языке                                                                               | ru-RU                 |
| <code>EmailNotificationRetryCount</code>         | Максимальное количество попыток отправки сообщения на SMTP-сервер                                                                                                 | 10                    |
| <code>EmailNotificationRetryPeriodSeconds</code> | Период между попытками отправки сообщения на SMTP-сервер (в секундах)                                                                                             | 60                    |
| <code>GroupsSchedulerRecalculationTimeout</code> | Таймер пересчета динамических групп активов (в минутах)                                                                                                           | 5                     |
| <code>HistoryRotationCronSchedule</code>         | Периодичность запуска ротации с помощью планировщика заданий cron                                                                                                 | 0 0 2 1 *             |

| Параметр               | Описание                                                                                                                                                                  | Значение по умолчанию |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| HistoryRotationDepth   | Период истории изменения активов, данные за который необходимо удалять, в формате <Дни>.<Часы>:<Минуты>:<Секунды>. Минимально допустимое значение — 14 дней (14.00:00:00) | 365.00:00:00          |
| HistoryRotationEnabled | Автоматическая ротация истории изменения активов включена (флажок установлен) или выключена (флажок снят)                                                                 | Флажок снят           |
| HostAddress            | IP-адрес или FQDN сервера MP 10 Core                                                                                                                                      | localhost             |
| KBAddress              | IP-адрес или FQDN сервера Knowledge Base                                                                                                                                  | —                     |
| MaxScanSizeKb          | Максимальный размер собранных данных по активам в килобайтах                                                                                                              | 716800                |
| MCAddress              | IP-адрес или FQDN сервера PT MC                                                                                                                                           | —                     |
| PostgreHost            | IP-адрес или FQDN сервера СУБД PostgreSQL                                                                                                                                 | localhost             |
| PostgrePassword        | Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL                                                                                              | P@ssw0rdP@ssw0rd      |
| PostgrePort            | Порт сервера СУБД PostgreSQL для входящих подключений от MP 10 Core                                                                                                       | —                     |
| PostgreUserName        | Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL                                                                                               | pt_system             |
| PrintingQueueJobsLimit | Максимальное количество одновременно выпускаемых отчетов                                                                                                                  | 5                     |
| ProcessingWorkerCount  | Количество потоков обработки событий идентификации активов в сервисе Assets.Processing                                                                                    | 2                     |
| PtkbDbName             | Имя базы знаний, из которой импортируются данные об уязвимостях                                                                                                           | —                     |

| Параметр                   | Описание                                                                                                                          | Значение по умолчанию |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 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              |
| RMQSslCertificateFileName  | Имя файла сертификата SSL                                                                                                         | RMQ_Core_Client.crt   |
| RMQSslKeyFileName          | Имя файла закрытого ключа сертификата SSL                                                                                         | RMQ_Core_Client.key   |
| RMQSslServerName           | IP-адрес или FQDN SSL-сервера RabbitMQ                                                                                            | localhost             |
| RMQUser                    | Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ                                                              | mpx_core              |
| RMQVirtualHost             | Имя виртуального узла RabbitMQ                                                                                                    | mpx                   |
| ScansRotationBatchDelay    | Задержка между началом обработки пакетов в одной процедуре ротации результатов сканирования                                       | 00:00:30              |
| ScansRotationBatchSize     | Количество результатов сканирования в пакете в процедуре ротации результатов сканирования<br>Допустимые значения — от 1 до 10 000 | 1000                  |
| ScansRotationDepth         | Глубина хранения результатов сканирования                                                                                         | 90.00:00:00           |
| ScansRotationEnabled       | Ротация результатов сканирования включена (True) или выключена (False)                                                            | True                  |
| ScansRotationRotationDelay | Задержка между процедурами ротации                                                                                                | 01:00:00              |

| 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         | <p>Варианты шифрования при подключении к SMTP-серверу:</p> <ul style="list-style-type: none"> <li>— None — шифрование не используется;</li> <li>— Auto — почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется;</li> <li>— SslOnConnect — протоколы SSL или TLS используются при соединении;</li> <li>— StartTls — протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается;</li> <li>— StartTlsWhenAvailable — протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS</li> </ul> | Auto                  |

| Параметр                      | Описание                                                                                                                               | Значение по умолчанию                                  |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| SmtpSender                    | Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте                                                           | Notification System<br><NoReply@SiemNotifications.com> |
| SmtpUser                      | Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу                                                               | —                                                      |
| TableListsWorkersCount        | Количество потоков, которые используются для одновременного перерасчета табличных списков                                              | 1                                                      |
| Text2PdqlEnabled              | Доступен AI-поиск по PDQL-запросам для поиска активов и уязвимостей (флажок установлен)                                                | Флажок не установлен                                   |
| TtlCheckPeriod                | Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)                                             | 01.00:00:00                                            |
| UsageMonitoringCheckingPeriod | Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)                                                                       | 00:15:00                                               |
| UsePtbkServer                 | MP 10 Core проверяет (флажок установлен) или не проверяет (флажок снят) наличие обновления базы знаний об уязвимостях в Knowledge Base | Флажок установлен                                      |
| UserIdleLogoutEnabled         | Завершать ли сессию пользователя при его бездействии в системе                                                                         | False                                                  |
| VulnerStateCheckInterval      | Период проверки статусов экземпляров уязвимостей (<Дни>.<Часы>:<Минуты>:<Секунды>)                                                     | 01.00:00:00                                            |
| VulnerStateCheckPeriodEnabled | MP 10 Core проверяет (флажок установлен) или не проверяет (флажок снят) статусы экземпляров уязвимостей                                | Флажок установлен                                      |

| Параметр                      | Описание                                                                                                                           | Значение по умолчанию |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 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 20. 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 | —                     |

| Параметр                        | Описание                                                                                                                                                                            | Значение по умолчанию        |
|---------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
| 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              | —                            |
| 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.<br><br><b>Примечание.</b> Брокер RabbitMQ устанавливается на сервер MP 10 Core и обеспечивает обмен сообщениями между компонентами MaxPatrol VM | localhost                    |

| Параметр                     | Описание                                                                                                               | Значение по умолчанию |
|------------------------------|------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 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. Выбирается при установке роли из возможных значений: SIEM или Core                     | SIEM                  |
| Agent_RMQ_SSL_CA_Certificate | Путь к файлу корневого SSL-сертификата                                                                                 | RMQ_Server.crt        |
| 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 21. Параметры конфигурации роли RMQ Message Bus

| Параметр              | Описание                                                        | Значение по умолчанию |
|-----------------------|-----------------------------------------------------------------|-----------------------|
| CACertFile            | Имя файла корневого сертификата                                 | rootCA.crt            |
| CACertificateFileName | Имя файла корневого сертификата для веб-интерфейса RabbitMQ     | rootCA.crt            |
| CertFile              | Имя файла публичного сертификата                                | RMQ_Server.crt        |
| HostAddress           | IP-адрес или FQDN сервера с установленной ролью RMQ Message Bus | —                     |

| Параметр                 | Описание                                                                                                                                                                                                                                      | Значение по умолчанию |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| KeyFile                  | Имя файла закрытого ключа сертификата                                                                                                                                                                                                         | RMQ_Server.pem        |
| MEMORY_HIGH_WATERMARK_GB | <p>Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах).</p> <p><b>Примечание.</b> Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений</p> | 10                    |
| RMQAdminPassword         | Пароль служебной учетной записи администратора RabbitMQ                                                                                                                                                                                       | P@ssw0rd              |
| RMQAdminUser             | Логин служебной учетной записи администратора RabbitMQ                                                                                                                                                                                        | Administrator         |
| RMQAgentPassword         | Пароль служебной учетной записи для доступа коллекторов к RabbitMQ                                                                                                                                                                            | P@ssw0rd              |
| RMQAgentUser             | Логин служебной учетной записи для доступа коллекторов к RabbitMQ                                                                                                                                                                             | agent                 |
| RMQHttpPort              | Порт для доступа к RabbitMQ по протоколу HTTP                                                                                                                                                                                                 | 5672                  |
| RMQHttpsPort             | Порт для доступа к RabbitMQ по протоколу HTTPS                                                                                                                                                                                                | 5671                  |
| RMQLogRotateSize         | Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, k для килобайтов)                                                                                                                                        | 50M                   |
| RMQPassword              | Пароль служебной учетной записи для доступа MP 10 Core к RabbitMQ                                                                                                                                                                             | P@ssw0rd              |
| RMQQueueVersion          | Версия формата хранения метаданных очередей RabbitMQ                                                                                                                                                                                          | 2                     |
| RMQSiemPassword          | Пароль служебной учетной записи для доступа MP SIEM Server к RabbitMQ                                                                                                                                                                         | P@ssw0rd              |

| Параметр                  | Описание                                                                                                                                                                                                                                                                                       | Значение по умолчанию |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| 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                  |
| RMQVirtualHost            | Имя виртуального узла RabbitMQ                                                                                                                                                                                                                                                                 | mpx                   |
| RMQ_DISK_FREE_LIMIT       | <p>Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах).</p> <p><b>Примечание.</b> Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений</p>                                              | 20                    |
| SSLCertificatePemFileName | Имя файла публичного сертификата для веб-интерфейса RabbitMQ                                                                                                                                                                                                                                   | Portal.crt            |
| SSLKeyFileName            | Имя файла закрытого ключа сертификата для веб-интерфейса RabbitMQ                                                                                                                                                                                                                              | Portal.key            |
| WATERMARK_PAGING_RATIO    | <p>Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK).</p> <p><b>Примечание.</b> Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск</p> | 0.5                   |

Таблица 22. 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: <ul style="list-style-type: none"> <li>— SIEM BINARY — дистрибутивов компонентов на Windows;</li> <li>— SIEM AGENT PENTEST — модулей Pentest для коллекторов, установленных на Windows;</li> <li>— SIEM AGENT PENTEST LINUX — модулей Pentest для коллекторов, установленных на Linux</li> </ul> | Установлены флажки SIEM AGENT PENTEST и SIEM AGENT PENTEST LINUX |
| DeleteObsoleteProductVersions | PT UCS загружает обновления только начиная с определенных версий объектов и удаляет из репозитория более старые версии (флажок установлен) или загружает все версии объектов (флажок снят)                                                                                                                                                                                                                     | Флажок установлен                                                |
| LogLevel                      | Уровень журналирования для служб PT UCS                                                                                                                                                                                                                                                                                                                                                                        | info                                                             |
| ProxyAddress                  | IP-адрес или FQDN прокси-сервера                                                                                                                                                                                                                                                                                                                                                                               | proxy.server.fqdn.or.ip                                          |
| ProxyEnabled                  | PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений Positive Technologies                                                                                                                                                                                                                                                     | Флажок снят                                                      |
| ProxyPassword                 | Пароль служебной учетной записи для подключения PT UCS к прокси-серверу                                                                                                                                                                                                                                                                                                                                        | —                                                                |
| ProxyPort                     | Порт прокси-сервера для входящего подключения от PT UCS                                                                                                                                                                                                                                                                                                                                                        | 8080                                                             |

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

## Приложение В. Параметры проверок по чек-листу

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

Инструкция по изменению проверок приведена в разделе «[Изменение проверок по чек-листу](#)» (см. раздел 24).

Таблица 23. Параметры проверок по чек-листу

| Проверка                            | Блок параметров           | Параметр                      | Описание                                                                                                                                                                                                                                                                                           | Значение по умолчанию |
|-------------------------------------|---------------------------|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| Выделены значимые активы            | AM3-CriticalAssetsDefined | valued_assets_absolute_amount | Минимальное количество выделенных активов                                                                                                                                                                                                                                                          | 10                    |
|                                     |                           | valued_assets_definition      | В качестве значимых учитываются активы: <ul style="list-style-type: none"> <li>любого уровня значимости — <code>all</code>;</li> <li>только среднего и высокого уровня — <code>any</code>;</li> <li>только среднего — <code>medium</code>;</li> <li>только высокого — <code>high</code></li> </ul> | high                  |
| Данные о значимых активах актуальны | AM8-CriticalAssetsActual  | valued_assets_refresh_period  | Максимальный период запуска задачи на сбор данных (в днях)                                                                                                                                                                                                                                         | 30                    |
|                                     |                           | valued_assets_definition      | Задача собирает данные с активов: <ul style="list-style-type: none"> <li>любого уровня значимости — <code>all</code>;</li> <li>только среднего и высокого уровня — <code>any</code>;</li> </ul>                                                                                                    | high                  |

| Проверка                                                      | Блок параметров                    | Параметр                                 | Описание                                                                                                                                                                                                                                                                             | Значение по умолчанию |
|---------------------------------------------------------------|------------------------------------|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                                               |                                    |                                          | <ul style="list-style-type: none"> <li>— только среднего — <code>medium</code>;</li> <li>— только высокого — <code>high</code></li> </ul>                                                                                                                                            |                       |
|                                                               |                                    | <code>actual_valued_assets_amount</code> | Максимальное количество неактуальных активов                                                                                                                                                                                                                                         | 3                     |
| Общий параметр для всех проверок                              | —                                  | <code>check_period</code>                | Период (в минутах) запуска проверок и обновления их результатов в веб-интерфейсе                                                                                                                                                                                                     | 15                    |
| Доля просроченных уязвимостей невелика (плановый процесс)     | VM2-<br>OverdueVulnersRatio        | <code>overdue_vulners_percentage</code>  | Порог допустимой доли просроченных уязвимостей при плановом устранении (в процентах)                                                                                                                                                                                                 | 10                    |
| Просроченные уязвимости устраняются быстро (плановый процесс) | VM3-<br>OverdueVulnersAutoLifeTime | <code>evaluation_time</code>             | Продолжительность непрерывного пребывания уязвимости в статусе «Просрочена» (в днях, не более 60 дней)                                                                                                                                                                               | 7                     |
|                                                               |                                    | <code>evaluation_criteria</code>         | В качестве критерия оценки продолжительности непрерывного пребывания уязвимости в статусе «Просрочена» используется максимальное значение параметра <code>evaluation_time</code> ( <code>max</code> ) или его среднее значение ( <code>average</code> ) на момент выполнения запроса | <code>max</code>      |

| Проверка                                   | Блок параметров                  | Параметр                 | Описание                                                                                                                                                                                                                                                                                                                                                                         | Значение по умолчанию |
|--------------------------------------------|----------------------------------|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
|                                            |                                  | valued_assets_definition | В качестве значимых учитываются активы: <ul style="list-style-type: none"> <li>любого установленного уровня значимости — <code>all</code>;</li> <li>только высокого уровня — <code>high</code>;</li> <li>только среднего уровня — <code>medium</code>;</li> <li>только среднего и высокого уровня — <code>any</code>;</li> <li>все активы в системе — <code>nd</code></li> </ul> | <code>any</code>      |
|                                            |                                  | vulner_severity          | Проверка распространяется на уязвимости следующих уровней опасности:                                                                                                                                                                                                                                                                                                             | <code>any</code>      |
|                                            |                                  | vulner_isdanger          | Проверка учитывает только уязвимости с меткой «важная» ( <code>IsDanger</code> ) или все уязвимости ( <code>any</code> )                                                                                                                                                                                                                                                         | <code>any</code>      |
|                                            |                                  | vulner_metrics           | Проверка учитывает наличие следующих метрик для уязвимостей:                                                                                                                                                                                                                                                                                                                     | <code>any</code>      |
| Просроченные уязвимости устраняются быстро | VM4-OverdueVulnersManualLifeTime | evaluation_time          | Продолжительность непрерывного пребывания уязвимости в статусе «Просрочена»                                                                                                                                                                                                                                                                                                      | 7                     |
|                                            |                                  | evaluation_criteria      | В качестве критерия оценки продолжительности непрерывного пребывания уязвимости в статусе «Просрочена» используется максимальное значение параметра <code>evaluation_time</code> ( <code>max</code> ) или его среднее значение ( <code>average</code> ) на момент выполнения запроса                                                                                             | <code>max</code>      |

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

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

## Приложение Г. О проверке серверов перед установкой ролей

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

В результате проверки появится одно из сообщений:

- **OK** — проверка пройдена успешно;
- **Warning** — рекомендуется устранить несоответствия, но установка может быть продолжена;
- **Error** — проверка не пройдена, установка будет прервана.

Таблица 24. Параметры соответствия сервера программным и аппаратным требованиям

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

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

## Приложение Д. Возможности привилегии «Расширенные полномочия»

Раздел содержит описание возможностей привилегии «Расширенные полномочия».

Таблица 25. Возможности привилегии «Расширенные полномочия»

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

# Предметный указатель

## В

---

восстановление данных из копии 50

учетная запись служебная

смена пароля

54

## Д

---

доступ

к активам 17

## И

---

инфраструктуры 84

## К

---

компоненты системы

алгоритм взаимодействия 11

описание 9

## П

---

пользовательские поля 73

добавление 79

изменение 81

удаление 82

## Р

---

резервное копирование 47

## У

---

уведомления

о состоянии системы 87



Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.