Positive Technologies MaxPatrol VM

Версия 1.0

Руководство администратора

POSITIVE TECHNOLOGIES

Дата редакции документа: 11.11.2020

Версия документа: 3

Содержание

1. Об этом документе

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

Руководство адресовано специалистам, администрирующим MaxPatrol VM.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство оператора безопасности — 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.

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 текста с условным обозначением	Описание
Внимание! При выключении модуля снижается уровень защищенности сети	Предупреждения. Содержат информацию о действиях или событиях, которые могут иметь нежелательные последствия
Примечание. Вы можете создать дополнительные отчеты	Примечания. Содержат советы, описания важных частных случаев, дополнительную или справочную информацию, которая может быть полезна при работе с продуктом

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

1.2. Другие источники информации о MaxPatrol VM

Вы можете найти дополнительную информацию о MaxPatrol VM на сайте ptsecurity.com и на портале технической поддержки support.ptsecurity.com.

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Если вы не нашли нужную информацию или решение проблемы самостоятельно, обратитесь в службу технической поддержки (см. раздел 16).

2. О MaxPatrol VM

Positive Technologies MaxPatrol VM (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 "Позитив Текнолоджиз" базы знаний предоставлять пользователю и другим системам актуальную информацию об уязвимостях, обнаруженных на активах, и отображать степень защищенности активов;
- определять способы устранения уязвимостей и настраивать политики контроля;
- выбирать среди уязвимостей те, которые необходимо устранять в первую очередь;
- контролировать степень защищенности IT-инфраструктуры и отслеживать информацию об уязвимостях на интерактивных дашбордах;
- выгружать данные для внешних систем и выпускать отчеты для различных подразделений и должностных лиц.

В этом разделе

Архитектура MaxPatrol VM (см. раздел 2.1)

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

2.1. Архитектура MaxPatrol VM

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

В этом разделе

2.1.1. Компонент PT MaxPatrol 10 Core

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

- централизованное хранение конфигурации активов;
- централизованное управление всеми компонентами системы;
- оперативное реагирование на инциденты информационной безопасности;
- обеспечение взаимодействия подразделений организации при расследовании инцидентов;
- автоматизацию процесса управления уязвимостями;
- поддержку веб-интерфейса системы.

В состав компонента входят следующие службы:

- Core Application Registration;
- Core Assets Identification;
- Core Assets Premerger;
- Core Assets Processing;
- Core Assets Projections;
- Core Assets Scans;
- Core Assets Temporal Read Model;
- Core Assets Triggers;
- Core Authorization Decision Point;

- Core Deployment Configuration;
- Core Events;
- Core Events Sources Monitoring;
- Core Events Triggers;
- Core Groups;
- Core Health Monitoring;
- Core Incidents Management;
- Core Incidents Read Model;
- Core Licensing;
- Core Notifications Management;
- Core Policies;
- Core Printing;
- Core Query Aggregator;
- Core Reporting;
- Core Reporting Delivery;
- Core Scanning;
- Core Scopes;
- Core Tables;
- Core Telemetry Collector;
- Core Topology;
- Core Topology Analyzer;
- Core Triggers;
- Core Usage Monitoring;
- Core Users Settings;
- Core Watchdog;
- Core Widgets.

2.1.2. Компонент PT MaxPatrol 10 Agent

Компонент PT MaxPatrol 10 Agent (далее также — MP 10 Agent) 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 Agent 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.

В состав компонента входят следующие модули:

— Audit — сканирование актива методом белого ящика;

— Hostdiscovery — поиск узлов методами ICMP ping, TCP ping;

— MP8ScanImporter — импорт информации об активах, обнаруженных MP8;

— Pentest — сканирование актива методом черного ящика;

— Remote Executor — удаленное исполнение сценариев одновременно на нескольких узлах и сбор результатов их выполнения.

Примечание. Существует возможность подключения модулей, разработанных сторонними производителями.

Компонент MP 10 Agent 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 Agent. Это позволяет увеличивать производительность, учитывать при сканировании топологию сети и типы каналов связи (например, наличие межсетевых экранов или других средств защиты).

В состав компонента входит служба Core Agent.

2.1.3. Компонент PT Management and Configuration

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

— сервис единого входа в продукты "Позитив Текнолоджиз", развернутые в инфраструктуре организации;

— управление пользователями системы, включая создание учетных записей, назначение прав, блокирование и активацию учетных записей;

— журналирование действий пользователей.

В состав компонента входят следующие службы:

— MC Application Registration Management Service;

— MC Identity and Access Management Service;

— MC Notifications service;

— MC Tenant Manager Service;

— MC User Action Logging Service.

2.1.4. Компонент Knowledge Base

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

В состав компонента входят следующие службы:

- KB ApiGateway service;
- KB Candidates Service;
- KB Platform Registration Service;
- KB Portal service;
- KnowledgeBase service.

2.1.5. Компонент PT Update and Configuration Service

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

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

2.2. Алгоритм работы MaxPatrol VM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol VM:

1. Модули компонента MP 10 Agent сканируют IT-инфраструктуру предприятия и собирают сведения о сетевых узлах. Собранные данные агенты 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 прочих свойствах и связях между ними. Компонент сохраняет параметры заданий сбора данных, профили сканирования, справочники и другие параметры. MP 10 Core осуществляет контроль доступа к данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов.
3. Компонент Knowledge Base содержит базу знаний, необходимых MP 10 Core для структурирования сведений об активах и обнаружения уязвимостей.
4. Используя данные Knowledge Base, компонент MP 10 Core рассчитывает уязвимости активов.

5. Компонент PT MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
6. Компонент PT UCS обеспечивает обновление компонентов системы и базы знаний.

Взаимодействие компонентов MaxPatrol VM отражено на схеме.

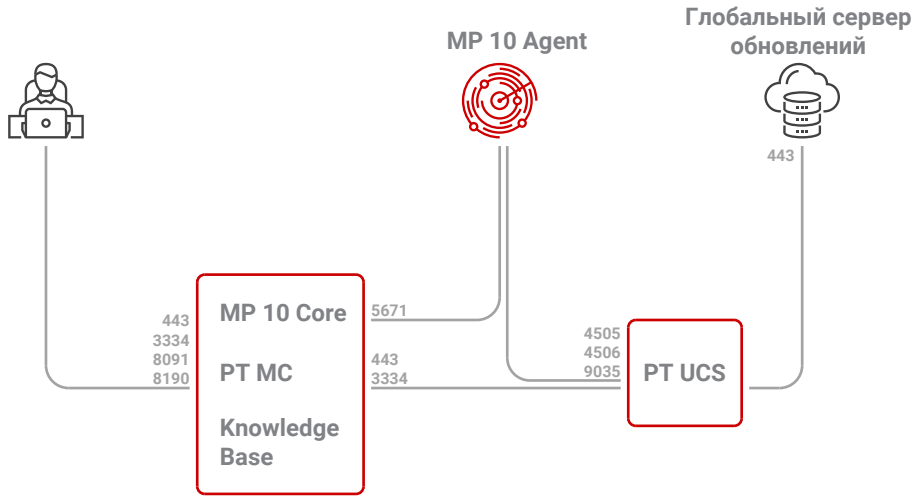

Рисунок 1. Схема взаимодействия компонентов MaxPatrol VM

Для получения обновлений межсетевой экран сервера компонента PT UCS не должен блокировать адрес глобального сервера обновлений "Позитив Текнолоджиз" — 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 Agent	MP 10 Core	5671
PT UCS	MP 10 Core	443, 3334
Рабочая станция пользователя	PT MC	3334
Рабочая станция пользователя	Knowledge Base	8091, 8190
MP 10 Core, MP 10 Agent	PT UCS	4505, 4506, 9035
PT UCS	Глобальный сервер обновлений	443

Для исходящих соединений нет необходимости 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 Debian.

3. Пользователи и права 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 и инциденты, доступ к которым получат пользователи с этой ролью.

При развертывании системы ее компоненты передают службе MC Identity and Access Management Service 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. По умолчанию система содержит приложения Management and Configuration и MaxPatrol 10.

Приложение Management and Configuration предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления иерархией площадок. По умолчанию приложение содержит стандартные роли "Администратор" и "Пользователь".

Приложение MaxPatrol 10 предназначено для настройки сбора данных об IT-инфраструктуре предприятия и работы с активами и инцидентами. По умолчанию приложение содержит стандартные роли "Администратор" и "Оператор".

Служба MC Identity and Access Management Service обеспечивает механизм единого входа (технология single sign-on), поэтому другие продукты "Позитив Текнолоджиз" в случае их интеграции с MaxPatrol VM также могут быть зарегистрированы службой, а их роли и привилегии будут доступны для назначения пользователям.

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

Для обеспечения выполнения пользователем производственных задач необходимо:

1. Создать для пользователя учетную запись.
2. Если набор привилегий стандартных ролей не подходит для выполнения производственных задач — создать пользовательские роли с нужным набором привилегий.
3. Назначить пользователю необходимые роли.
4. Настроить для ролей доступ к активам и инцидентам в соответствии с производственными задачами пользователя.

В этом разделе

Страница Журнал действий пользователей (см. раздел 3.4)

Просмотр записей о действиях пользователей (см. раздел 3.5)

Смена пароля учетной записи Administrator с помощью командной строки Microsoft Windows (см. раздел 3.6)

3.1. Управление учетными записями

Управление учетными записями различается в зависимости от типа аутентификации пользователей.

В случае локальной аутентификации необходимо вручную создавать учетные записи (см. раздел 3.1.3), аутентификация пользователей выполняется в PT MC. Администратор указывает в приложении Management and Configuration логин, пароль, статус пользователя, персональную и организационную информацию, а также роли пользователя. Эти параметры доступны для изменения и хранятся только в PT MC.

Для использования LDAP-аутентификации необходимо настроить LDAP-подключение (см. раздел 3.1.7) перед созданием учетных записей (см. раздел 3.1.3). Администратор указывает в приложении Management and Configuration логин, статус и роли пользователя. Пароль учетной записи хранится в Microsoft Active Directory и не может быть изменен в приложении Management and Configuration. Персональная и организационная информация по умолчанию загружается из Microsoft Active Directory, но может быть указана и изменена в приложении.

Учетная запись может автоматически создаваться в PT MC при первом входе пользователя. Для этого необходимо настроить LDAP-подключение (см. раздел 3.1.7) и синхронизацию с Microsoft Active Directory (см. раздел 3.1.8). Логин, пароль, а также группы пользователя, соответствующие его ролям, хранятся в Microsoft Active Directory и не могут быть изменены в приложении Management and Configuration. Персональная и организационная информация также по умолчанию загружается из Microsoft Active Directory, но может быть указана и изменена в приложении.

Система может содержать учетные записи пользователей с разными типами аутентификации. Вы можете сменить пользователю тип аутентификации в системе.

В случае иерархической инсталляции в приложении Management and Configuration будут отображаться учетные записи пользователей других площадок. Вы можете сменить статус таких учетных записей на локальной площадке, а также, если эти учетные записи не синхронизируются с Microsoft Active Directory, назначить пользователям роли.

Список пользователей и назначенных им ролей приведен на странице **Пользователи**, список LDAP-подключений — на странице **Настройка LDAP-подключений**.

В этом разделе

Страница Пользователи (см. раздел 3.1.1)

Страница Настройка LDAP-подключений (см. раздел 3.1.2)

Создание учетной записи (см. раздел 3.1.3)

3.1.1. Страница Пользователи

Страница **Пользователи** предназначена для работы с учетными записями пользователей. В панели инструментов страницы находятся следующие кнопки:

- **Добавить пользователя** — для создания учетной записи пользователя (см. раздел 3.1.3);
- **Изменить данные** — для изменения персональных данных пользователя и организационной информации (см. раздел 3.1.4);
- **Роли в приложениях** — для назначения пользователям ролей в приложениях (см. раздел 3.3.2);
- **Заблокировать** — для блокирования учетной записи пользователя (см. раздел 3.1.5);
- **Разблокировать** — для разблокирования учетной записи пользователя (см. раздел 3.1.5);
- **Экспорт** — для экспорта данных о пользователях (см. раздел 3.1.6) в текстовый файл.

В рабочей области страницы расположены:

- Панель **Пользователи по приложениям**. Содержит список фильтров по приложениям и фильтр **Все пользователи**. При выборе приложения в панели **Пользователи <Название приложения>** отобразятся учетные записи пользователей, которым назначены роли в выбранном приложении, при выборе фильтра **Все пользователи** — все учетные записи, созданные в системе.
- Панель **Пользователи <Название приложения>**. Содержит таблицу с учетными записями и кнопки  и  . В таблице доступны выбор учетных записей, а также их сортировка по нажатию на название колонки. При нажатии  в верхней части панели открывается поле для быстрого поиска учетной записи, при нажатии  открывается панель для настройки фильтра учетных записей.
- Панель **<Логин пользователя>@<Домен> (Псевдоним площадки)**. Содержит данные о выбранной учетной записи пользователя, ссылки для просмотра его ролей и привилегий.

3.1.2. Страница Настройка LDAP-подключений

Страница **Настройка LDAP-подключений** предназначена для настройки подключения к LDAP-серверам. В панели инструментов страницы находятся следующие кнопки:

- **Добавить подключение** — для создания подключения (см. раздел 3.1.7);
- **Изменить параметры** — для изменения параметров подключения (см. раздел 3.1.10);
- **Удалить** — для удаления подключения (см. раздел 3.1.12);
- **Запустить синхронизацию** — для запуска вручную синхронизации с Microsoft Active Directory (см. раздел 3.1.9).

В рабочей области страницы расположены:

- Панель **Подключения**. Содержит таблицу с подключениями и кнопки и . В таблице доступны выбор подключения, а также сортировка подключений по нажатию на название колонки. При нажатии обновятся данные в таблице, при нажатии откроется блок параметров для настройки автоматического обновления данных. В таблице отображаются следующие статусы подключений:

  — выполняется синхронизация с Microsoft Active Directory;

  — синхронизация с Microsoft Active Directory завершилась с предупреждением;

  — подключение к LDAP-серверам или синхронизация с Microsoft Active Directory завершились с ошибкой.
- Панель **<Название подключения>**. Содержит данные о выбранном подключении, а также сообщения о возникших ошибках и предупреждениях.

3.1.3. Создание учетной записи

Если аутентификация пользователя будет выполняться через LDAP, перед созданием учетной записи необходимо настроить этот тип аутентификации (см. раздел 3.1.7).

После создания учетная запись не может быть удалена. Если требуется запретить пользователю вход в систему, необходимо заблокировать его учетную запись (см. раздел 3.1.5).

► Чтобы создать учетную запись пользователя:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.
2. В панели инструментов нажмите кнопку **Добавить пользователя**.

   Откроется страница **Новый пользователь**.
3. В блоке параметров **Учетные данные** выберите тип аутентификации.

4. Если вы выбрали локальную аутентификацию, введите логин и пароль пользователя.

   Примечание. Если требуется, чтобы пользователь сменил пароль при первом входе в систему, установите флажок.

5. Если вы выбрали LDAP-аутентификацию, введите доменное имя пользователя и по ссылке **Выбрать домен** выберите LDAP-подключение.
6. Нажмите кнопку **Создать**.

Учетная запись пользователя создана.

3.1.4. Изменение данных пользователя

- Чтобы изменить данные пользователя:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.
2. Выберите учетную запись пользователя, данные которого необходимо изменить.
3. В панели инструментов нажмите кнопку **Изменить данные**.

   Откроется страница **Редактировать информацию о пользователе**.
4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Данные пользователя изменены.

3.1.5. Блокирование и разблокирование учетной записи

- Чтобы заблокировать учетную запись:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.
2. В списке выберите пользователя, учетную запись которого необходимо заблокировать.

   Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.
3. Нажмите кнопку **Заблокировать**.

Учетная запись пользователя заблокирована.

- Чтобы разблокировать учетную запись:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

Откроется страница **Пользователи**.

2. В списке выберите пользователя, учетную запись которого необходимо разблокировать.

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

3. Нажмите кнопку **Разблокировать**.

Учетная запись пользователя разблокирована.

3.1.6. Экспорт данных пользователей в текстовый файл

► Чтобы экспортировать данные пользователей:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. Выберите учетные записи пользователей для экспорта.

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

3. Нажмите кнопку **Экспорт**.
4. В открывшемся окне выберите вариант экспорта выбранных учетных записей и подтвердите экспорт.

   Браузер загрузит текстовый файл с данными пользователей.

Данные пользователей экспортированы.

3.1.7. Создание LDAP-подключения

Для обеспечения защищенного соединения с LDAP-серверами необходимо установить доверенный сертификат корневого центра сертификации на сервер MP 10 Core в хранилище Local Computer\Trusted Root Certification Authorities.

► Чтобы создать LDAP-подключение:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

   Откроется страница **Настройка LDAP-подключений**.

3. В панели инструментов нажмите кнопку **Добавить подключение**.

Откроется страница **Новое LDAP-подключение**.

4. Введите название LDAP-подключения.
5. В блоке параметров **Серверы** в поле **Адрес** введите IP-адрес или FQDN LDAP-сервера.

   Примечание. Если требуется устанавливать защищенное соединение с LDAP-сервером, адрес необходимо вводить в зависимости от типа доверенного сертификата (он выпускается или для IP-адреса, или для FQDN).
6. В поле **Порт** введите номер порта.
7. Если требуется устанавливать защищенное соединение с LDAP-сервером, установите флажок **SSL**.

   Примечание. Вы можете добавлять дополнительные серверы, нажимая +. При потере соединения с одним сервером запрос аутентификации может быть обработан другим сервером. После заполнения полей вы можете проверить соединение (см. раздел 3.1.11) с LDAP-серверами.
8. В поле **Домены** введите DNS-имя домена, NetBIOS-имя домена или UPN-суффикс.
9. В поле **База поиска** введите имя записи каталога, начиная с которой выполняется поиск учетных записей пользователей.

   Примечание. Вы можете автоматически загрузить имена доменов и параметры базы поиска, нажав кнопку **Запросить данные с сервера** и указав данные учетной записи с правами доступа на чтение данных о пользователях.
10. Если требуется, настройте синхронизацию с Microsoft Active Directory (см. раздел 3.1.8).
11. Нажмите кнопку **Сохранить**.

LDAP-подключение создано.

3.1.8. Настройка синхронизации с Microsoft Active Directory

Вы можете настраивать синхронизацию при создании LDAP-подключения (см. раздел 3.1.7) на странице **Новое LDAP-подключение** или при его изменении (см. раздел 3.1.10) на странице **Изменение параметров LDAP-подключения**. Перед настройкой синхронизации необходимо создать в Microsoft Active Directory учетную запись с правами на чтение данных о пользователях и группах пользователей.

► Чтобы настроить синхронизацию с Microsoft Active Directory:

1. Включите синхронизацию с Microsoft Active Directory.
2. В блоке параметров **Учетная запись** введите логин и пароль служебной учетной записи с правами на чтение данных о пользователях и группах пользователей Active Directory.
3. Если необходимо, включите синхронизацию по расписанию и по ссылке настройте расписание.

Примечание. Синхронизация также может быть запущена вручную (см. раздел 3.1.9) на странице **Настройка LDAP-подключений**.

4. В блоке **Соответствие ролей и групп** в раскрывающихся списках выберите группы Microsoft Active Directory, соответствующие ролям пользователей.
5. Нажмите кнопку **Сохранить**.

   Синхронизация с Microsoft Active Directory настроена.

3.1.9. Запуск вручную синхронизации с Microsoft Active Directory

► Чтобы вручную запустить синхронизацию с Microsoft Active Directory:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

   Откроется страница **Настройка LDAP-подключений**.
3. Выберите LDAP-подключение.
4. Нажмите кнопку **Запустить синхронизацию**.

   В таблице отобразится значок .

Синхронизация с Microsoft Active Directory запущена вручную.

По завершении синхронизации:

— если синхронизация была выполнена успешно — значок статуса пропадет, в панели **<Название подключения>** время последней синхронизации изменится на актуальное;

— если синхронизация была выполнена с предупреждениями — значок статуса сменится на , в панели **<Название подключения>** отобразится текст предупреждения;

— если синхронизация была выполнена с ошибками — значок статуса сменится на , в панели **<Название подключения>** отобразится текст ошибки.

3.1.10. Изменение параметров LDAP-подключения

► Чтобы изменить параметры LDAP-подключения:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

Откроется страница **Настройка LDAP-подключений**.

3. Выберите LDAP-подключение.
4. В панели инструментов нажмите кнопку **Изменить подключение**.

   Откроется страница **Изменение параметров LDAP-подключения**.
5. Внесите изменения.

   Примечание. После внесения изменений рекомендуется проверить подключение (см. раздел 3.1.11).
6. Нажмите кнопку **Сохранить**.

Параметры LDAP-подключения изменены.

3.1.11. Проверка LDAP-подключения

При проверке LDAP-подключения устанавливается пробное соединение с LDAP-серверами. Вы можете проверять подключение при его создании (см. раздел 3.1.7) на странице **Новое LDAP-подключение** или изменении его параметров (см. раздел 3.1.10) на странице **Изменение параметров LDAP-подключения**.

► Чтобы проверить LDAP-подключение:

1. Нажмите кнопку **Проверить соединение**.

   Откроется окно **Проверка соединения**.
2. Введите логин и пароль пользователя с правами доступа на чтение данных о пользователях.
3. Нажмите кнопку **Проверить**.

   Результаты проверки отобразятся в окне **Проверка соединения**.
4. Нажмите кнопку **Закрыть**.

LDAP-подключение проверено.

3.1.12. Удаление LDAP-подключения

► Чтобы удалить LDAP-подключение:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.
2. В главном меню в разделе **Пользователи** выберите пункт **Настройка LDAP-подключений**.

   Откроется страница **Настройка LDAP-подключений**.

3. Выберите LDAP-подключение.
4. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

LDAP-подключение удалено.

3.2. Управление ролями

В разделе приведены описание страницы **Роли**, инструкции по созданию, изменению и удалению ролей.

В этом разделе

3.2.1. Страница Роли

Страница **Роли** предназначена для работы с ролями и привилегиями. В панели инструментов страницы находятся следующие кнопки:

- **Создать** — для создания роли (см. раздел 3.2.2);
- **Редактировать** — для изменения доступных для роли привилегий (см. раздел 3.2.4);
- **Создать копию** — для создания роли на основе существующей роли (см. раздел 3.2.3);
- **Удалить** — для удаления роли (см. раздел 3.2.5);
- **Назначить** — для назначения роли пользователям (см. раздел 3.3.1).

В рабочей области страницы расположены:

- Панель **Роли**. Содержит список ролей по приложениям. При выборе роли в панели **Привилегии** отобразятся доступные для роли привилегии.
- Панель **Привилегии**. Содержит список привилегий, доступных для выбранной роли.
- Панель **<Название роли>**. Содержит описание выбранной роли, ссылку для просмотра учетных записей всех пользователей, которым назначена выбранная роль, а также ссылку для настройки прав доступа к активам и инцидентам для пользователей с выбранной ролью.

3.2.2. Создание роли

► Чтобы создать роль:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Создание роли**.

4. В раскрывающемся списке выберите приложение, для которого необходимо создать роль.

5. Введите название роли.

6. В блоке параметров **Права доступа** укажите флажки для тех привилегий, которые будет иметь создаваемая роль.

7. Нажмите кнопку **Создать**.

Роль создана.

3.2.3. Создание роли на основе существующей роли

► Чтобы создать роль на основе существующей:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. Выберите роль, на основе которой будет создана новая роль.

4. В панели инструментов нажмите кнопку **Создать копию**.

   Откроется окно **Создание роли**.

5. Введите название роли.

6. В блоке параметров **Права доступа** укажите флажки для тех привилегий, которые будет иметь создаваемая роль.

7. Нажмите кнопку **Создать**.

Роль создана.

3.2.4. Изменение роли

Вы можете изменять роли, созданные пользователями. Стандартные роли недоступны для изменения.

► Чтобы изменить роль:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели **Роли** выберите роль пользователя.

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

4. В панели инструментов нажмите кнопку **Редактировать**.

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

5. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Роль изменена.

3.2.5. Удаление роли

Вы можете удалять роли, созданные пользователями. Стандартные роли недоступны для удаления.

► Чтобы удалить роль:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели **Роли** выберите роль пользователя.

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

4. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Роль удалена.

3.3. Управление правами доступа

Вы можете управлять правами доступа к разделам веб-интерфейса и операциям во всех зарегистрированных в системе приложениях, а также в правами доступа к активам и инцидентам.

Права доступа к разделам веб-интерфейса и операциям в системе назначаются в приложении Management and Configuration и определяются набором доступных привилегий для роли, назначенной пользователю. Права доступа к активам и инцидентам назначаются в приложении MaxPatrol 10 и указываются для роли пользователя.

Если аутентификация пользователей выполняется локально или через LDAP без синхронизации с Microsoft Active Directory, вы можете назначать:

- роли в нескольких приложениях одному пользователю — при создании его учетной записи (см. раздел 3.1.3) на странице **Новый пользователь** или изменении его данных (см. раздел 3.1.4) на странице **Изменение данных пользователя**;
- роли в одном приложении (см. раздел 3.3.1) нескольким пользователям — на странице **Роли и права доступа**;
- роли в нескольких приложениях (см. раздел 3.3.2) нескольким пользователям — на странице **Пользователи**.

Если учетные записи пользователей синхронизируются с Microsoft Active Directory, назначение им ролей в приложении Management and Configuration недоступно. Назначать роли таким пользователям необходимо в Microsoft Active Directory, добавляя их в группы, соответствующие требуемых ролям.

В этом разделе

3.3.1. Назначение пользователям ролей одного приложения

► Чтобы назначить пользователям роли:

1. В главном меню нажмите ⋮⋮⋮ и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Роли**.

   Откроется страница **Роли и права доступа**.

3. В панели **Роли** выберите роли, которые необходимо назначить пользователям.

   Примечание. В панели **Роли** вы можете выбрать роли только одного приложения.

4. В панели инструментов нажмите кнопку **Назначить**.
5. Во всплывающем окне установите флажки для тех пользователей, которым необходимо назначить выбранные роли.
6. Нажмите кнопку **Назначить выбранные роли пользователям**.

Пользователям назначены роли.

3.3.2. Назначение пользователям ролей нескольких приложений

► Чтобы назначить пользователям роли:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.
2. Выберите учетные записи пользователей, которым необходимо назначить роли.

   Примечание. Вы можете выбирать несколько учетных записей подряд, нажимая клавишу Shift, или несколько отдельных учетных записей, нажимая клавишу Ctrl.
3. В панели инструментов нажмите кнопку **Роли в приложениях**.

   Откроется окно **Роли пользователей**.
4. В раскрывающемся списке **<Название приложения>** установите флажки для назначаемых пользователям ролей.
5. Нажмите кнопку **Сохранить**.

Пользователям назначены роли.

3.3.3. Предоставление пользователям доступа к активам и инцидентам

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

► Чтобы предоставить пользователям доступ к активам:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **MaxPatrol 10**.
2. В главном меню в разделе **Система** выберите пункт **Права доступа**.

   Откроется страница **Права доступа**.
3. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к активам.

4. В панели **<Название роли>** по ссылке **Редактировать** откройте окно **Доступ к активам, инцидентам и источникам**.
5. В раскрывающемся списке **Доступ** выберите необходимый тип доступа.
6. 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.
7. Нажмите кнопку **Сохранить**.

Пользователям предоставлен доступ к активам.

3.4. Страница Журнал действий пользователей

Страница **Журнал действий пользователей** предназначена для просмотра записей о действиях пользователей (см. раздел 3.5).

В рабочей области страницы расположены:

- Панель **Действия**. Содержит список возможных действий пользователей. При выборе действия в панели **Действия пользователей** отобразятся записи о выбранном действии.
- Панель **Пользователи**. Содержит список учетных записей пользователей и кнопку для их быстрого поиска. При выборе учетной записи в панели **Действия пользователей** отобразятся записи о действиях пользователя с выбранной учетной записью.
- Панель **Действия пользователей**. Содержит таблицу с записями, ссылку со значком и кнопки , и . В таблице доступны выбор записи, а также сортировка записей по времени регистрации действий. При нажатии ссылки со значком открывается всплывающее окно для выбора периода просмотра записей. При нажатии в верхней части панели открывается поле для быстрого поиска записей, при нажатии обновятся данные в таблице, при нажатии откроется блок параметров для настройки автоматического обновления данных.
- Панель **<Дата и время действия>**. Содержит данные о выбранной записи.

3.5. Просмотр записей о действиях пользователей

Чтобы просмотреть записи о действиях пользователя:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.
2. В главном меню выберите раздел **Журнал действий**.

   Откроется страница **Журнал действий пользователя**.

3. В панели **Пользователи** выберите пользователя, записи о действиях которого необходимо просмотреть.
4. В панели **Действия** выберите группу действий, записи о которых необходимо просмотреть.
5. Если требуется, выберите период для просмотра записей, нажав  .

   В панели **Действия пользователей** отобразится список записей о действиях пользователя.

3.6. Смена пароля учетной записи Administrator с помощью командной строки Microsoft Windows

В случае невозможности сменить пароль учетной записи `Administrator` через веб-интерфейс (например, при утере пароля), вы можете сменить пароль в командной строке Microsoft Windows.

- Чтобы сменить пароль учетной записи `Administrator`:

  1. На сервере MP 10 Core остановите службу MC Identity and Access Management Service.
  2. В интерфейсе командной строки Microsoft Windows от имени администратора выполните команды:

     ```
     cd C:\Program Files\Positive Technologies\Management And Configuration
     \IdentityAndAccessManagement
     IAM.Host.exe resetpassword
     ```

     Интерфейс командной строки выведет сообщение:

     ```
     Please enter new password
     ```
  3. Введите новый пароль.

     Интерфейс командной строки выведет сообщение:

     ```
     Password successfully changed
     ```
  4. Запустите службу MC Identity and Access Management Service.

  Пароль учетной записи `Administrator` сменен.

4. Иерархия площадок

В этом документе площадкой называется развернутая конфигурация MaxPatrol VM, выполняющая задачи по мониторингу информационной безопасности отдельного подразделения (подразделений) или всего предприятия в целом.

Иерархия площадок — представление связей между площадками в виде дерева, построенное на основе организационной структуры предприятия. Иерархия всегда содержит главную площадку и один или несколько уровней площадок, структурно подчиненных главной.

Информация об иерархии площадок отображается на странице **Иерархия площадок**, которая содержит панели для отображения связей между площадками (в виде графа) и параметров площадки, выбранной на графе. С помощью панели инструментов вы можете добавлять площадки в иерархию и удалять их, изменять параметры подключения площадок.

Построение иерархии выполняется в интерфейсе главной площадки. Сначала необходимо добавить в иерархию площадки, непосредственно подчиненные главной, затем остальные площадки, непосредственно подчиненные уже добавленным. Площадка может быть частью только одной иерархической инсталляции.

Учетные записи пользователей MaxPatrol VM постоянно синхронизируются между всеми площадками иерархии. Пользователи каждой площадки при наличии прав доступа могут через главное меню MaxPatrol VM войти на другую площадку. По умолчанию учетные записи не имеют прав доступа на другую площадку, поэтому для входа от их имени необходимо назначить им подходящие роли. Также необходимо обеспечить сетевое взаимодействие через порты 80/TCP, 443/TCP, 3333/TCP, 3334/TCP, 8091/TCP, 8190/TCP между рабочими станциями пользователей и серверами компонентов MP 10 Core, PT MC, Knowledge Base других площадок.

> **Примечание.** В списке пользователей логины учетных записей, принадлежащих пользователям других площадок иерархии, оканчиваются на "@<Псевдоним другой площадки>" (например, Administrator@SOC).

Перед построением иерархии необходимо:

- синхронизировать по протоколу NTP время между серверами PT MC всех площадок;
- убедиться, что на всех площадках развернуты одинаковые версии MaxPatrol VM;
- обеспечить сетевое взаимодействие через порты 8703/TCP и 3334/TCP между сервером компонента PT MC главной площадки и серверами компонентов PT MC остальных площадок.

В этом разделе

Резервное копирование данных об иерархии и их восстановление (см. раздел 4.4)

Инфраструктуры площадки (см. раздел 4.5)

4.1. Добавление площадки в иерархию

► Чтобы добавить площадку в иерархию:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Иерархия площадок**.

   Откроется страница **Иерархия площадок**.

3. В панели инструментов нажмите кнопку **Зарегистрировать площадку**.

   Откроется окно **Новая площадка**.

4. В раскрывающемся списке **Вышестоящая площадка** выберите площадку, которая будет вышестоящей для добавляемой в иерархию.

5. В поле **Название новой площадки** введите название добавляемой в иерархию площадки.

   Примечание. После добавления площадки это название будет отображаться на графе иерархии, в главном меню компонента PT MC добавленной площадки, а также при нажатии .

6. В поле **Псевдоним площадки** введите псевдоним добавляемой площадки.

   Примечание. Псевдоним может содержать только буквы английского алфавита, цифры, дефис и знак подчеркивания. Псевдоним используется в качестве значения поля при построении PDQL-запроса, поэтому должен быть уникальным для каждой площадки в пределах одной иерархической инсталляции.

7. В поле **Адрес** введите значение параметра `HostAddress` конфигурации компонента PT MC добавляемой площадки.

8. Нажмите кнопку **Подключиться**.

   Откроется страница входа на добавляемую площадку.

9. Введите логин и пароль администратора PT MC добавляемой площадки и нажмите кнопку **Войти**.

10. В открывшемся окне **Разрешить подключение к площадке <Название подключаемой площадки>?** нажмите кнопку **Разрешить**.

    Примечание. Если вы добавляете площадку с помощью браузера Microsoft Internet Explorer, в отрывшемся окне необходимо скопировать токен доступа и ввести его в поле **Токен доступа** в окне **Новая площадка**.

11. Нажмите кнопку **Сохранить**.

Новая площадка отобразится на графе иерархии.

Площадка добавлена в иерархию.

4.2. Изменение параметров подключения площадки

► Чтобы изменить параметры подключения площадки:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Иерархия площадок**.

   Откроется страница **Иерархия площадок**.

3. На графе иерархии выберите площадку, параметры подключения которой необходимо изменить.

4. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется окно **<Название площадки>**.

5. Внесите изменения.

6. Если вы изменили адрес площадки, нажмите кнопку **Подключиться** и разрешите подключение.

7. Нажмите кнопку **Сохранить**.

Параметры подключения площадки изменены.

4.3. Удаление площадки из иерархии

► Чтобы удалить площадку из иерархии:

1. В главном меню нажмите и в раскрывшемся меню выберите пункт **Management and Configuration**.

   Откроется страница **Пользователи**.

2. В главном меню выберите раздел **Иерархия площадок**.

   Откроется страница **Иерархия площадок**.

3. На графе иерархии выберите площадку, которую нужно удалить.

4. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

   Примечание. Если вы удаляете площадку с помощью браузера Microsoft Internet Explorer, для подтверждения удаления необходимо нажать на кнопку **Получить токен** и ввести полученный токен в поле **Токен доступа**.

Площадка удалена из иерархии.

4.4. Резервное копирование данных об иерархии и их восстановление

Для оперативного восстановления иерархии рекомендуется своевременно выполнять резервное копирование данных.

После построения иерархии рекомендуется создать резервную копию данных компонентов PT MC и MP 10 Core, расположенных на всех площадках. При последующих изменениях иерархии (например, после добавления площадки в иерархию) рекомендуется создавать резервные копии данных компонентов PT MC и MP 10 Core, расположенных на главной площадке и на добавленной в иерархию площадке.

Восстановление данных необходимо начинать с главной площадки. Данные подчиненных главной площадок можно восстанавливать в любом порядке, независимо от уровня площадки в иерархии.

> Внимание! Сервер, на котором будут восстановлены данные PT MC, должен иметь такое же FQDN (при его отсутствии — такой же IP-адрес), которое имел сервер PT MC на момент создания резервной копии. Также при восстановлении данных компонента PT MC главной площадки необходимо до начала восстановления закрыть на его сервере порт 8703/TCP для входящих соединений, по окончании восстановления открыть этот порт.

4.5. Инфраструктуры площадки

При сканировании IT-инфраструктуры предприятия важно правильно идентифицировать активы. Сканирование одним агентом 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 агентом 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

4.5.1. 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.

4.5.2. 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.

4.5.3. 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.

5. Управление политиками

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

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

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

При создании, удалении, включении и отключении правил, а также при изменении их параметров или порядка система не изменяет политику сразу, она создает черновик политики. После внесения всех изменений их необходимо применить. В зависимости от количества объектов применение изменений может занимать продолжительное время (до нескольких суток).

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

В MaxPatrol VM доступны следующие политики.

Для сроков актуальности данных

Правила политики автоматически устанавливают сроки актуальности и устаревания данных об активах, полученных в результате сканирования IT-инфраструктуры предприятия методом аудита или пентеста. Используя результат применения политики, можно оперативно находить активы, данные о которых неактуальны или скоро станут неактуальными.

Для статусов уязвимостей

Правила политики автоматически изменяют статус экземпляров уязвимостей, определяют срок их устранения или исключения из проверки. Результат применения политики (например, перечень запланированных к устранению уязвимостей) можно выпускать в виде отчета по расписанию и отправлять по электронной почте системному администратору.

Для отметки "важная"

Правила политики автоматически отмечают экземпляры уязвимостей как важные. Например, важными могут быть отмечены наиболее опасные для IT-инфраструктуры предприятия уязвимости, активы с важными уязвимостями — найдены с помощью PDQL-запроса.

В этом разделе

5.1. Страница Политики

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

- **Создать правило** — для создания правила;
- **Редактировать** — для изменения параметров правила (см. раздел 5.5);
- **Копировать** — для создания правила на основе имеющегося правила (см. раздел 5.6);
- **Удалить** — для удаления правила (см. раздел 5.8);
- **Включить** — для включения правила в работу (см. раздел 5.7);
- **Отключить** — для приостановки работы правила (см. раздел 5.7).

В рабочей области страницы расположены:

- Панель **Список политик**. Содержит список политик и предназначена для выбора политики, применения изменений (см. раздел 5.9), а также отмены неприменных изменений (см. раздел 5.10). При выборе политики составляющие ее правила отобразятся в центральной панели. Если политика имеет неприменные изменения, на левой границе строки с названием политики отобразится желтая полоска, в правой

части строки — кнопка ⋮ для отмены изменений, а в нижней части панели — кнопка **Применить изменения**. Если выполняется применение изменений, слева от названия политики отобразится значок ◌.

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

— Панель **<Название правила>**. Содержит сведения о правиле.

Если правило содержит ошибки (например, указанная в правиле группа активов была удалена), значок состояния правила в центральной панели сменится на ❗. Такой же значок отобразится слева от названия политики, содержащей это правило.

5.2. Создание правила для сроков актуальности данных

► Чтобы создать правило:

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

   Откроется страница **Политики**.

2. В панели инструментов нажмите кнопку **Создать правило** и в раскрывшемся меню выберите:

   — если вы хотите указать сроки актуальности данных, собираемых модулями audit, — пункт **Для сроков актуальности данных (аудит)**;

   — если вы хотите указать сроки актуальности данных, собираемых модулями pentest, — пункт **Для сроков актуальности данных (пентест)**.

   Откроется страница **Создание правила**.

3. Введите название правила.
4. В раскрывающемся списке выберите группы активов, для которых необходимо указать сроки актуальности данных.

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

5. Если требуется, измените значения по умолчанию для сроков актуальности данных.
6. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.3. Создание правила для отметки "важная"

► Чтобы создать правило:

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

Откроется страница **Политики**.

2. В панели инструментов нажмите кнопку **Создать правило** и в раскрывшемся меню выберите пункт **Для отметки важная**.

   Откроется страница **Создание правила**.

3. Введите название правила.
4. В поле **Фильтр уязвимостей** введите запрос на языке PDQL для поиска экземпляров уязвимостей, которые необходимо отметить как важные.

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

5. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.4. Создание правила для статусов уязвимостей

- Чтобы создать правило:

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

   Откроется страница **Политики**.

2. В панели инструментов нажмите кнопку **Создать правило** и в раскрывшемся меню выберите пункт **Для статусов уязвимостей**.

   Откроется страница **Создание правила**.

3. Введите название правила.
4. В поле **Фильтр уязвимостей** введите запрос на языке PDQL для поиска тех экземпляров уязвимостей, которым необходимо изменить статусы.

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

5. В раскрывающемся списке выберите действие, которое необходимо сделать с экземплярами уязвимостей.
6. Если требуется исключить из мониторинга экземпляры уязвимостей, в раскрывающемся списке **Уточнение к статусу** выберите причину исключения.
7. Нажмите кнопку **Сохранить**.

Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.5. Изменение правила

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

► Чтобы изменить правило:

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

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

   Откроется окно **Редактирование правила <Название правила>**.
5. Внесите изменения.
6. Нажмите кнопку **Сохранить**.

Правило изменено.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.6. Копирование правила

► Чтобы скопировать правило:

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

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

   Откроется окно **Создание правила**.
5. Если требуется, внесите изменения.
6. Нажмите кнопку **Сохранить**.

Правило скопировано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.7. Включение и отключение правила

- Чтобы включить правило:

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

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

  Правило включено. Система начнет использовать правило только после применения изменений в политике (см. раздел 5.9).

- Чтобы отключить правило:

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

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

  Правило отключено. Система перестанет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.8. Удаление правила

Вы можете удалить только пользовательские правила, стандартные правила удалить невозможно.

- Чтобы удалить правило:

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

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

  Правило удалено.

Система перестанет использовать правило только после применения изменений в политике (см. раздел 5.9).

5.9. Применение изменений в политиках

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

- Чтобы применить изменения:

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

     Откроется окно **Применение изменений**.

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

  Изменения применены.

5.10. Отмена изменений в политике

- Чтобы отменить изменения:

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

  Изменения отменены.

6. Отправка уведомлений

Уведомления MaxPatrol VM содержат информацию об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных, выявляемых инцидентах ИБ и состоянии системы.

Вы можете автоматизировать отправку уведомлений, создавая задачи на странице **Уведомления**.

В этом разделе

6.1. Страница Уведомления

Страница **Уведомления** предназначена для работы с задачами для отправки уведомлений. В панели инструментов страницы находятся следующие кнопки:

- **Создать** — для создания задачи;
- **Копировать** — для создания задачи на основе существующей задачи (см. раздел 6.8);
- **Редактировать** — для изменения параметров задачи (см. раздел 6.9);
- **Удалить** — для удаления задачи (см. раздел 6.10);
- **Остановить** — для остановки задачи (см. раздел 6.7);
- **Запустить** — для запуска задачи после ее остановки (см. раздел 6.7).

  Примечание. После создания задачи она запускается автоматически.

В рабочей области страницы расположены:

— Панель **Типы уведомлений**. Содержит перечень разделов по типам объектов, для которых доступно создание задач. При выборе типа в центральной панели отобразятся задачи, созданные для объектов этого типа.

— Центральная панель. Содержит таблицу с задачами.

— Панель **<Название задачи>**. Содержит данные о выбранной задаче.

6.2. Создание задачи для отправки уведомления об изменении общего числа активов

► Чтобы создать задачу для отправки уведомления об изменении общего числа активов:

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

   Откроется страница **Уведомления**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.

3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об изменении общего числа активов**.
5. Если необходимо, снимите флажок **Создание активов** или **Удаление активов**.
6. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
7. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
8. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об изменении общего числа активов создана.

6.3. Создание задачи для отправки уведомления об изменениях в группах активов

► Чтобы создать задачу для отправки уведомления об изменениях в группах активов:

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

   Откроется страница **Уведомления**.

2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.

3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **Об изменениях в группах активов**.
5. Если необходимо, снимите флажок **Добавление активов в группу** или **Исключение активов из группы**.
6. В раскрывающемся списке **В группах** выберите те группы активов, об изменениях которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об изменениях в группах активов создана.

6.4. Создание задачи для отправки уведомления об инцидентах

► Чтобы создать задачу для отправки уведомления об инцидентах:

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

   Откроется страница **Уведомления**.

2. В панели инструментов нажмите кнопку **Создать**.

Откроется окно **Новое уведомление**.

3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **О состоянии инцидентов**.
5. В раскрывающемся списке **В группах** выберите те группы активов, об инцидентах которых система будет отправлять уведомление.
6. В раскрывающемся списке **Фильтр** выберите фильтр инцидентов.
7. В блоке параметров **Уведомление при срабатывании** в поле **Кому** укажите адреса электронной почты получателей уведомления.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления об инцидентах создана.

6.5. Создание задачи для отправки уведомления о состоянии MaxPatrol VM

► Чтобы создать задачу для отправки уведомления о состоянии MaxPatrol VM:

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

   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся блоке **Сообщать** выберите **О состоянии системы**.
5. В раскрывающемся списке **Опасность** выберите тип сообщений, отправляемых системой самодиагностики.
6. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
7. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.

8. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
9. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о состоянии системы создана.

6.6. Создание задачи для отправки уведомления о выполнении задач сбора данных

► Чтобы создать задачу для отправки уведомления о выполнении задач сбора данных:

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

   Откроется страница **Уведомления**.
2. В панели инструментов нажмите кнопку **Создать**.

   Откроется окно **Новое уведомление**.
3. В поле **Название** введите название уведомления.
4. В раскрывающемся списке **Сообщать** выберите **О задачах сбора данных**.
5. Если необходимо, снимите флажок **О начале выполнения** или **О завершении**.
6. В раскрывающемся списке **Задачи** выберите те задачи сбора данных, о начале и (или) завершении которых система будет отправлять уведомление.
7. В блоке параметров **Уведомление при срабатывании** настройте способ отправки уведомления:
   - Если необходимо отправлять уведомление по электронной почте, включите отправку уведомления по электронной почте и в поле **Кому** укажите адреса электронной почты получателей уведомления.
   - Если необходимо отправлять уведомление с помощью POST-запроса, включите отправку уведомления с помощью POST-запроса и введите адрес сервера для получения POST-запроса.
8. В блоке параметров **Макс.частота** выберите, как часто система будет отправлять уведомление.
9. В раскрывающемся списке **Часовой пояс** выберите часовой пояс, подходящий для времени отправки уведомления и для отображения в тексте уведомления.
10. Нажмите кнопку **Сохранить**.

Задача для отправки уведомления о выполнении задач сбора данных создана.

6.7. Остановка и повторный запуск задачи для отправки уведомления

- Чтобы остановить задачу для отправки уведомления:
  1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

     Откроется страница **Уведомления**.
  2. В центральной панели выберите задачу.
  3. В панели инструментов нажмите кнопку **Остановить**.

  Задача для отправки уведомления остановлена.
- Чтобы запустить задачу для отправки уведомления:
  1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

     Откроется страница **Уведомления**.
  2. В центральной панели выберите задачу.
  3. В панели инструментов нажмите кнопку **Запустить**.

  Задача для отправки уведомления запущена.

6.8. Создание новой задачи на основе существующей задачи

- Чтобы создать новую задачу на основе существующей:
  1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

     Откроется страница **Уведомления**.
  2. В центральной панели выберите задачу.
  3. В панели инструментов нажмите кнопку **Копировать**.

     Откроется окно **Новое уведомление**.
  4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

  Новая задача создана на основе существующей.

6.9. Изменение задачи для отправки уведомления

- Чтобы изменить задачу для отправки уведомления:
  1. В главном меню в разделе **Система** выберите пункт **Уведомления**.

     Откроется страница **Уведомления**.
  2. В центральной панели выберите задачу.

3. В панели инструментов нажмите кнопку **Редактировать**.

   Откроется окно **Редактировать уведомление**.

4. Внесите необходимые изменения и нажмите кнопку **Сохранить**.

Задача для отправки уведомлений изменена.

6.10. Удаление задачи для отправки уведомления

► Чтобы удалить задачу для отправки уведомления:

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

   Откроется страница **Уведомления**.

2. В центральной панели выберите задачу.
3. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

Задача для отправки уведомлений удалена.

7. Мониторинг состояния MaxPatrol VM

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

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

В этом разделе

7.1. Просмотр состояния лицензии и версии компонента MP 10 Core

Для корректной работы MaxPatrol VM необходима действующая лицензия. Индикатор состояния системы сигнализирует о том, что до истечения срока действия лицензии осталось 14 дней, а также об истечении срока действия лицензии и ее отсутствии.

► Чтобы просмотреть состояние лицензии и версию компонента MP 10 Core:

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

   Откроется страница **Управление системой**.

2. В панели **Компоненты** выберите пункт **О системе**.

   В рабочей области страницы отобразится информация о текущей лицензии системы и версии компонента MP 10 Core.

7.2. Просмотр состояния агентов

Агенты обеспечивают поступление данных в систему. Если агент недоступен или имеются проблемы в его работе, индикатор состояния сигнализирует об этом. Например, система предупреждает о приближении объема свободного дискового пространства к пороговому значению. Когда объем свободного места на диске достигает порогового значения, агент переходит в режим работы с ограниченной функциональностью (см. раздел 7.4).

- Чтобы просмотреть состояние агента:

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

     Откроется страница **Управление системой**.

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

     В рабочей области страницы отобразится таблица со списком агентов.

Для каждого агента в таблице указаны название, версия, статус, роли, а также IP-адреса и семейство ОС сервера. Вы можете сортировать список, нажимая на названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая ⚙ в правой верхней части таблицы. Для поиска агента в списке вы можете нажать 🔍 и ввести в поле поиска параметр агента.

> **Примечание.** При выборе агента система отображает подробную информацию о нем в боковой панели с названием агента.

Система отображает следующие статусы агента:

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

Вы можете удалить из списка (см. раздел 7.3) только недоступные агенты. Если после удаления агент начнет присылать данные, он снова будет отображаться в списке.

7.3. Удаление недоступного агента

Агент, который был установлен в системе, а затем выведен из ее состава (например, по причине неисправности сервера агента), автоматически не удаляется из списка агентов и продолжает отображаться в интерфейсе со статусом **Недоступен**. Такой агент необходимо удалить из списка вручную. После удаления агента будут автоматически остановлены:

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

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

► Чтобы удалить агент из списка:

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

   Откроется страница **Управление системой**.

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

   В рабочей области страницы отобразится таблица со списком агентов.

3. Выберите агент 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 агент используется запущенными задачами.

   Статус удаляемого агента изменится на **Удаляется**. По завершении удаления агент не будет отображаться в списке.

Агент удален из списка.

7.4. Отслеживание агентом объема дискового пространства

Агент собирает данные и передает их для обработки компоненту MP 10 Core. При работе MaxPatrol VM скорость входящего потока данных агента может превышать скорость исходящего потока. В этом случае агент временно сохраняет данные на жестком диске для последующей отправки компонентам системы.

При отсутствии свободного дискового пространства агент переходит в неработоспособное состояние. Поэтому агент постоянно отслеживает объем дискового пространства и при его изменении может перейти в один из режимов работы с ограниченной функциональностью:

— SafeMode1 — агент выполняет запущенные задачи, но не запускает новые задачи.

— SafeMode2 — агент останавливает выполнение запущенных задач и не запускает новые задачи.

Примечание. Агент отслеживает объем дискового пространства только в тех разделах, где находятся создаваемые им файлы.

При переходе в режимы SafeMode1 или SafeMode2 статус агента на странице **Управление системой** изменяется на **safe**. Запуск вручную задач для сбора данных на агенте завершается с ошибкой.

> **Примечание.** По умолчанию после установки агент настроен на переход в режим SafeMode2 при уменьшении объема свободного дискового пространства до 20 480 МБ.

В этом разделе

Настройка отслеживания агентом объема дискового пространства на Windows (см. раздел 7.4.1)

Настройка отслеживания агентом объема дискового пространства на Debian (см. раздел 7.4.2)

7.4.1. Настройка отслеживания агентом объема дискового пространства на Windows

Вы можете настраивать отслеживание агентом свободного и (или) занятого дискового пространства (занимаемого как всеми файлами раздела диска, так и только файлами, создаваемыми агентом).

Команды необходимо выполнять в интерфейсе командной строки Microsoft Windows от имени администратора.

- Чтобы настроить отслеживание агентом объема дискового пространства на Windows,

  выполните команду:

  ```
  coreagentcfg <Где отслеживать> <Пороговое значение><Единицы порогового значения> <Что отслеживать>
  ```

  где:

  <Где отслеживать> — название параметра утилиты coreagentcfg;

  Примечание. Название параметров, определяющих отслеживание агентом дискового пространства, начинается со слов "AgentMonitoring".

  <Единицы порогового значения> — байты ("`M`" — для мегабайтов, "`G`" — для гигабайтов, "`T`" — для терабайтов) или проценты (`%`);

  Примечание. Пороговое значение должно быть положительным числом.

  <Что отслеживать> — для отслеживания свободного дискового пространства необходимо указать `free`, для отслеживания занятого дискового пространства — `used`.

Примеры команд:

— `coreagentcfg AgentMonitoringCacheWarn 100G used`

Если суммарный размер файлов, создаваемых агентом в разных разделах диска, превысит 100 ГБ, агент перейдет в режим SafeMode1.

— `coreagentcfg AgentMonitoringDiskLogsAlarm 95% used`

Если суммарный размер всех файлов раздела, на котором находятся файлы журналов агента, превысит 95% от его объема, агент перейдет в режим SafeMode2.

— `coreagentcfg AgentMonitoringCacheWarn 100G free`

Если объем свободной дисковой памяти в тех разделах диска, где находятся создаваемые агентом файлы, уменьшится до 100 ГБ, агент перейдет в режим SafeMode1.

— `coreagentcfg AgentMonitoringDiskStorageAlarm 5% free`

Если объем свободной дисковой памяти в том разделе диска, где находятся файлы базы данных агента, уменьшится до 5% от общего объема раздела, агент перейдет в режим SafeMode2.

7.4.2. Настройка отслеживания агентом объема дискового пространства на Debian

Вы можете настраивать отслеживание агентом свободного и (или) занятого дискового пространства (занимаемого как всеми файлами раздела диска, так и только файлами, создаваемыми агентом).

Команды необходимо выполнять в интерфейсе командной строки Microsoft Windows от имени администратора.

► Чтобы настроить отслеживание агентом занятого объема дискового пространства на Debian:

1. измените файл `/opt/mpxagent/config.json`:

   • если вы хотите настроить отслеживание агентом свободного дискового пространства, в секцию `cop` → `monitoring` → `disk` → `usage_control` добавьте следующую строку:

   ```
   "<Где отслеживать>": { "free": { "<В какой режим переходит агент>": { "<Единицы порогового значения>": <Пороговое значение>}}}
   ```

   • если вы хотите настроить отслеживание агентом дискового пространства, занимаемого всеми файлами раздела диска, в секцию `cop` → `monitoring` → `disk` → `usage_control` добавьте следующую строку:

   ```
   "<Где отслеживать>": { "used": { "<В какой режим переходит агент>": { "<Единицы порогового значения>": <Пороговое значение>}}}
   ```

- если вы хотите настроить отслеживание агентом дискового пространства, занимаемого только создаваемыми агентом файлами, в секцию `cop` → `monitoring` → `cash` → `usage_control` добавьте следующую строку:

  ```
  "overall": { "used": { "<В какой режим переходит агент>": { "<Единицы порогового значения>": <Пороговое значение>}}}
  ```

  где:

  <Где отслеживать> — название варианта отслеживания, выбор варианта зависит от вида создаваемых агентом файлов (см. таблицу ниже);

  <В какой режим переходит агент> — для перехода агента в режим SafeMode1 при достижении порогового значения необходимо указать `warn`, SafeMode2 — `alarm`;

  <Единицы порогового значения> — мегабайты (`megabytes`) или проценты (`percent`).

  Примечание. Пороговое значение должно быть положительным числом.

2. Перезапустите службу агента:

   ```
   systemctl restart mpxagent.service
   ```

Отслеживание агентом занятого объема дискового пространства на Debian настроено.

Примеры строк:

— `"storage": { "free": {"warn": {"megabytes": 204800}, "alarm": {"megabytes": 102400}}}`

Если объем свободного дискового пространства в том разделе диска, где находятся файлы базы данных агента, уменьшится до 204 800 МБ, агент перейдет в режим SafeMode1, до 102 400 МБ — в режим SafeMode2.

— `"logs": { "used": { "warn": {"percent": 85}, "alarm": {"percent": 95}}}`

Если суммарный размер всех файлов раздела, на котором находятся файлы журналов агента, превысит 85% от его объема, агент перейдет в режим SafeMode1, 95% — в режим SafeMode2.

— `"overall": { "used": {"warn": {"megabytes": 102400}, "alarm": {"megabytes": 204800}}}`

Если суммарный размер файлов, создаваемых агентом в разных разделах диска, превысит 102 400 МБ, агент перейдет в режим SafeMode1, 204 800 МБ — в режим SafeMode2.

Таблица 3. Список вариантов отслеживания дисковой памяти

Вариант отслеживания	Раздел для отслеживания
`logs`	Раздел с файлами журналов агента
`queue`	Раздел с файлами очереди сообщений
`storage`	Раздел с файлами БД агента
`overall`	Все разделы с файлами агента

8. Резервное копирование данных

Для создания резервной копии данных компонентов MP 10 Core, PT MC, Knowledge Base и MP 10 Agent вам потребуется файл сценария `backup_all_in_one_win.ps1` из комплекта поставки. При создании резервной копии данных и их последующем восстановлении должны совпадать версии компонентов MaxPatrol VM и языки интерфейса ОС. Также требуется наличие не менее 200 ГБ свободного места на жестком диске сервера.

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

Файл сценария необходимо запускать в интерфейсе командной строки Windows PowerShell от имени администратора.

- Чтобы создать резервную копию данных,

  запустите сценарий резервного копирования данных:

  ```
  powershell -ExecutionPolicy ByPass -File backup_all_in_one_win.ps1 <Путь к папке для размещения резервной копии данных>
  ```

  Внимание! Убедитесь, что путь к папке содержит только буквы английского алфавита и (или) цифры и не содержит пробелов.

  Примечание. Вы можете не указывать путь к папке для размещения резервной копии данных. В этом случае сценарий разместит резервную копию данных в папке `C:\backup_<Название компонента продукта>`.

  По завершении резервного копирования сценарий создаст архив `<Название компонента>-<Дата создания резервной копии>-R<Номер версии продукта>.zip`. Резервная копия данных создана.

9. Восстановление данных из резервной копии

Для восстановления данных компонентов MP 10 Core, PT MC, Knowledge Base и MP 10 Agent из резервной копии вам потребуется файл сценария `restore_all_in_one_win.ps1` из комплекта поставки. При создании резервной копии данных и их последующем восстановлении должны совпадать версии компонентов MaxPatrol VM и языки интерфейса ОС. Также требуется наличие не менее 200 ГБ свободного места на жестком диске сервера.

Восстанавливать данные необходимо на сервере, содержащим только установленную ОС. Файл сценария необходимо запускать в интерфейсе командной строки Windows PowerShell от имени администратора.

- Чтобы восстановить данные из резервной копии:

  1. Создайте папку для размещения резервной копии данных.

     Внимание! Убедитесь, что путь к папке содержит только буквы английского алфавита и (или) цифры и не содержит пробелов.

  2. В созданную папку распакуйте архив с резервной копией данных.
  3. В файле `<Путь к папке с резервной копией данных>\CoreInstallParams.xml` измените значения параметров:

     ```
     <param id="HostAddress" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     <param id="PtkbFeatureHost" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     <param id="PtmcHostAddress" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     ```

  4. В файле `<Путь к папке с резервной копией данных>\PtmsInstallParams.xml` измените значения параметров:

     ```
     <param id="HostAddress" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     ```

  5. В файле `<Путь к папке с резервной копией данных>\PtkbInstallParams.xml` измените значения параметров:

     ```
     <param id="HostAddress" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     <param id="IdentityServerAddress" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     <param id="CoreAddress" value="<IP-адрес или FQDN сервера для восстановления данных>" />
     ```

  6. Запустите установку компонентов MP 10 Core, PT MC и Knowledge Base с параметрами из XML-файлов:

     ```
     & .\MPXCoreSetup.exe /silent /variables
     PARAMETERSFILE=<Путь к папке с резервной копией данных>\CoreInstallParams.xml
     PTMS_PARAMETERSFILE=<Путь к папке с резервной копией данных>\PtmsInstallParams.xml
     PTKB_PARAMETERSFILE=<Путь к папке с резервной копией данных>\PtkbInstallParams.xml
     ```

  7. По завершении установки перезапустите сессию Windows PowerShell.

8. Если перед созданием резервной копии система имела пароли служебных учетных записей, отличные от паролей по умолчанию, восстановите эти пароли вручную (см. раздел 10).
9. Запустите сценарий восстановления данных из резервной копии:

   ```
   powershell -ExecutionPolicy ByPass -File restore_all_in_one_win.ps1 <Путь к папке с резервной копией данных>
   ```

Данные восстановлены из резервной копии.

Восстановленные данные компонента MP 10 Core содержат идентификаторы всех агентов, входивших в состав системы на момент создания резервной копии. Если после восстановления система не найдет агенты с этими идентификаторами (например, агенты были удалены или переустановлены), в интерфейсе отобразится ошибка "Компонент <Имя агента> на узле <IP-адрес или FQDN сервера агента> недоступен". Рекомендуется удалить недоступные агенты (см. раздел 7.3).

10. Смена паролей служебных учетных записей

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

Вы можете сменить пароли служебных учетных записей. Команды для смены паролей необходимо вводить в интерфейсе командной строки Microsoft Windows от имени администратора, в интерфейсе терминала Debian от имени суперпользователя (root).

В этом разделе

10.1. Смена пароля служебной учетной записи в PostgreSQL

При установке компонента MP 10 Core в PostgreSQL создается служебная учетная запись с правами администратора. По умолчанию логин служебной учетной записи — `pt_system`, пароль — `P@ssw0rdP@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи в PostgreSQL,

  выполните команды:

```
cd "C:\Program Files\Positive Technologies\Common\PostgreSQL12\bin"
set PGPASSWORD=<Старый пароль>
psql -U pt_system -d postgres -c "ALTER USER pt_system WITH PASSWORD '<Новый пароль>'"
corecfg set -p PostgrePassword <Новый пароль>
mccfg set -p PostgrePassword <Новый пароль>
kbcfg set -p PostgrePassword <Новый пароль>
```

10.2. Смена пароля служебной учетной записи в MongoDB на Microsoft Windows

При установке компонента MP 10 Core в MongoDB создается служебная учетная запись с правами администратора. По умолчанию логин этой служебной учетной записи — `admin`, пароль — `P@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи в MongoDB на Microsoft Windows,

  выполните команды:

```
mongodbcfg set -p SuperuserPassword <Новый пароль>
corecfg set -p MongoDbPassword <Новый пароль>
```

10.3. 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 (см. раздел 10.3.1)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Agent (см. раздел 10.3.2)

10.3.1. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Core

По умолчанию логин служебной учетной записи компонента MP 10 Core в RabbitMQ — `mpx_core`, пароль — `P@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи компонента MP 10 Core,

  выполните команды:

  ```
  cd "C:\Program Files\Positive Technologies\Common\RabbitMQ\rabbitmq_server-<Номер версии>
  \sbin"
  rabbitmqctl change_password mpx_core "<Новый пароль>"
  corecfg set -p RMQPassword <Новый пароль> ServicesRMQPassword <Новый пароль>
  ```

10.3.2. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Agent

По умолчанию логин служебной учетной записи компонента MP 10 Agent в RabbitMQ — `mpx_agent`, пароль — `P@ssw0rd`.

- Чтобы сменить пароль служебной учетной записи компонента MP 10 Agent:

  1. На сервере компонента MP 10 Core выполните команды:

     ```
     cd "C:\Program Files\Positive Technologies\Common\RabbitMQ\rabbitmq_server-<Номер версии>
     \sbin"
     rabbitmqctl change_password mpx_agent "<Новый пароль>"
     ```

  2. На сервере каждого компонента MP 10 Agent выполните команду:

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

  Пароль служебной учетной записи компонента MP 10 Agent сменен.

11. Настройка журналирования работы MaxPatrol VM

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

В этом разделе

11.1. Настройка журналирования работы компонента MP 10 Core

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. Настройка выполняется отдельно для каждой службы компонента. Названия и расположение файлов, которые требуются для настройки журналирования, приведены в разделе "Расположение файлов для настройки журналирования работы компонента MP Core" (см. приложение Г).

- Чтобы настроить журналирование работы компонента MP 10 Core,

  в файле конфигурации для параметров `log4net` → `root` → `level`, `log4net` → `appender name="FileAppender"` → `maxSizeRollBackups` и `log4net` → `appender name="FileAppender"` → `maximumFileSize` измените значение атрибута `value`:

  ```
  <level value="<Уровень журналирования>" />
  ```

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

  ```
  <maxSizeRollBackups value="<Максимальное количество сохраняемых файлов журналов>" />
  <maximumFileSize value="<Максимальный размер файла журнала (в мегабайтах)>MB" />
  ```

При обновлении системы значения всех параметров журналирования будут автоматически изменены на значения по умолчанию.

11.2. Настройка журналирования работы компонента MP 10 Agent

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

Примечание. Не рекомендуется изменять уровень журналирования без указания службы технической поддержки "Позитив Текнолоджиз".

► Чтобы настроить журналирование работы компонента MP 10 Agent:

1. В файле `agent.log.xml` измените значение атрибута `level` параметра `config` → `root`:
   ```
   <Название журналируемого компонента агента> 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 работы компонента MP 10 Agent настроено.

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

11.3. Настройка журналирования работы компонентов сторонних производителей

Вы можете настраивать ротацию файлов журнала MongoDB, PostgreSQL и RabbitMQ. По умолчанию размер каждого файла журнала ограничен 200 МБ, сохраняются последние 10 файлов.

Для настройки ротации вам потребуется утилита `C:\Program Files (x86)\Positive Technologies\Common\Logrotate\.install\logrotatecfg.exe`. Утилита ротации автоматически запускается каждый час и проверяет размер файлов журнала. Вы можете изменить периодичность запуска утилиты с помощью планировщика заданий Microsoft Windows.

► Чтобы настроить ротацию файлов журнала,

выполните команду:

```
logrotatecfg set -p RotateSize <Размер файла журналов> RotateCount <Максимальное количество сохраняемых файлов журналов>
```

где <Размер файла журнала> — размер файла журнала, при превышении которого файл будет запущен в ротацию. Для указания единиц количества информации необходимо вводить G для гигабайт, M для мегабайт, k для килобайт.

Например, если необходимо настроить ротацию файла журнала при превышении им размера 500 мегабайт и с максимальным количеством сохраняемых (ротируемых) файлов — 15, выполните следующую команду:

```
logrotatecfg set -p RotateSize 500M RotateCount 15
```

12. Изменение конфигурации компонентов MaxPatrol VM на Microsoft Windows

Для изменения конфигурации компонентов вам потребуются утилиты, которые входят в комплект поставки и включены в дистрибутивы компонентов. После развертывания системы путь к исполняемому файлу утилиты добавляется в переменную окружения PATH.

Таблица 4. Список компонентов и поставляемых с ними утилит

Компонент	Утилита
MP 10 Core	`corecfg.exe`
PT MC	`mccfg.exe`
Knowledge Base	`kbcfg.exe`
MP 10 Agent	`coreagent.exe`
RabbitMQ	`rabbitmqcfg.exe`
MongoDB	`mongodbcfg.exe`
Salt Minion	`saltcfg.exe`
Компоненты сторонних производителей	`logrotatecfg.exe`

Также с помощью утилит вы можете просматривать краткое описание параметров конфигурации (см. приложение А) и их текущие значения.

Таблица 5. Команды утилит MaxPatrol VM

Команда	Действие
`set`	Ввод значений параметров (соответствующие службы перезапускаются автоматически)
`get`	Вывод значений параметров (значения выводятся в одинарных кавычках)
`list`	Вывод описания параметров
`version`	Вывод версии компонента
`start`	Запуск остановленных служб компонента
`stop`	Остановка служб компонента
`restart`	Перезапуск служб компонента

Вы можете изменять значения параметров двумя способами: вручную вводя названия параметров и их новые значения или указывая путь к XML-файлу с новыми значениями. Утилиты необходимо запускать в интерфейсе командной строки Microsoft Windows от имени администратора.

В этом разделе

12.1. Изменение значений параметров вручную

- Чтобы изменить значения параметров вручную,

  выполните команду:

  ```
  <Название утилиты> set -p <Название параметра 1> <Значение параметра 1>
  <Название параметра 2> <Значение параметра 2> … <Название параметра N>
  <Значение параметра N>
  ```

  Например:

  ```
  corecfg set -p PtkbFeatureEnabled true PtkbFeatureHost core.example.com
  ```

12.2. Изменение значений параметров с помощью XML-файла

- Чтобы изменить значения параметров с помощью XML-файла:

  1. Создайте XML-файл в кодировке UTF-8:

     ```
     <?xml version="1.0" encoding="utf-8"?>
     <params>
         <param id="Название параметра 1" value="Значение параметра 1" />
         <param id="Название параметра 2" value="Значение параметра 2" />
         ....
         <param id="Название параметра N" value="Значение параметра N" />
     </params>
     ```

  2. Выполните команду:

     ```
     <Название утилиты> set -f <Путь к XML-файлу>
     ```

13. Изменение конфигурации компонента PT UCS

Для изменения конфигурации вам потребуется утилита `configure-install-params`, которая входит в комплект поставки и находится в архиве с дистрибутивами компонента. Утилиту необходимо запускать в терминале Debian от имени суперпользователя (root).

Описание параметров конфигурации приведено в приложении "Параметры конфигурации компонента PT UCS" (см. приложение Б).

- Чтобы изменить конфигурацию компонента PT UCS:

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

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

  2. Запустите утилиту конфигурирования:

     ```
     cd /<Путь к каталогу для распаковки архива>/ucs-debian<Номер версии Debian>-<Номер версии MaxPatrol VM>
     ./configure-install-params -a
     ```

  3. На открывшейся странице измените значения параметров на новые.
  4. Нажмите кнопку **OK**.
  5. Выполните команду:

     ```
     dpkg-reconfigure ucs-pt
     ```

  Конфигурация компонента PT UCS изменена.

14. Пользовательские поля в модели актива

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

После добавления полей и ввода их значений пользователи системы смогут:

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

Перед добавлением пользовательских полей на сервере MP 10 Core в папке `C:\ProgramData\Positive Technologies\MaxPatrol 10 Core\Config\Layers` 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.

В этом разделе

14.1. Добавление пользовательских полей в модель актива

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

► Чтобы добавить пользовательские поля в модель актива:

1. На сервере MP 10 Core в файле `C:\ProgramData\Positive Technologies \MaxPatrol 10 Core\Config\Layers\UserModel.xml` в качестве значения атрибута `version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели.
   - Если вы добавляете пользовательские поля впервые, скопируйте значение атрибута `Version` элемента `Dsl`, содержащегося в файле `C:\ProgramData\Positive Technologies\MaxPatrol 10 Core\Config\Layers\ModelMigrations.xml`, добавьте единицу к последней цифре скопированного значения и укажите полученное значение в файле `UserModel.xml` в качестве версии пользовательской модели (например, `version="19.0.20206.1"`).
   - Если вы добавляете пользовательские поля повторно, добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.2"`).

     Например:

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

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

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

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

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

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

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

   Например:

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

5. Если необходимо, добавьте описание пользовательских полей (см. раздел 14.2).
6. Перезапустите следующие службы:
   - Core Assets Processing;
   - Core Assets Temporal Read Model;
   - Core Assets Identification;
   - Core Assets Projections;
   - Core Assets Scans;
   - Core Scanning;
   - Core Tables;
   - Core Topology;
   - Core Topology Analyzer.

Пользовательские поля добавлены в модель актива.

14.2. 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. На сервере MP 10 Core в файле `C:\ProgramData\Positive Technologies \MaxPatrol 10 Core\Config\Layers\UserModel.xml` для элемента `layer id="UserDescriptions"` → `Entities` добавьте дочерний элемент `Entity` с атрибутом `Name`. В качестве значения атрибута `Name` укажите алиас типа актива.

   Например, для активов на ОС Microsoft Windows укажите:

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

Примечание. Названия алиасов по типу актива содержатся в файле `C:\ProgramData\Positive Technologies\MaxPatrol 10 Core\Config\Layers\AssetAliases.xml`.

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

   Например:
```
<Entity Name="OperatingSystem.Windows.WindowsHost">
    <Properties>
        <Property Name="UF_AssetNumber">
            <Title>Инвентарный номер актива в реестре</Title>
        </Property>
        <Property Name="UF_AssetOwner">
            <Title>Ответственный за актив</Title>
        </Property>
        <Property Name="UF_AssetRevisionDate">
            <Title>Дата последней ревизии актива</Title>
        </Property>
    </Properties>
</Entity>
```

Описание пользовательских полей добавлено.

14.3. 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. На сервере MP 10 Core в файле `C:\ProgramData\Positive Technologies\MaxPatrol 10 Core\Config\Layers\UserModel.xml` в качестве значения атрибута `version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели. Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.3"`).
2. Для элемента `layer id="UserModel"` → `Dsl` → `Migrations` добавьте дочерний элемент `Group` с атрибутом `Version`. В качестве значения атрибута `Version` укажите версию пользовательской модели, например:
```
<Group Version="19.0.20206.3">
```

```
</Group>
```

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

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

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

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

   Например:

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

5. Перезапустите следующие службы:

   - Core Assets Processing;
   - Core Assets Temporal Read Model;
   - Core Assets Identification;
   - Core Assets Projections;
   - Core Assets Scans;
   - Core Scanning;
   - Core Tables;
   - Core Topology;
   - Core Topology Analyzer.

Имена пользовательских полей изменены.

14.4. 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. На сервере MP 10 Core в файле `C:\ProgramData\Positive Technologies \MaxPatrol 10 Core\Config\Layers\UserModel.xml` в качестве значения атрибута `version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели.

Для этого добавьте единицу к последней цифре текущего значения версии пользовательской модели и укажите полученное значение (например, `version="19.0.20206.4"`).

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

```
<Group Version="19.0.20206.4">
</Group>
```

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

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

4. Для элемента `ChangeEntity` добавьте дочерние элементы `RemoveProperty` (по количеству удаляемых пользовательских полей) с атрибутом `Property`. В качестве значения атрибута `Property` укажите имя удаляемого поля.

   Например:

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

5. Перезапустите следующие службы:
   - Core Assets Processing;
   - Core Assets Temporal Read Model;
   - Core Assets Identification;
   - Core Assets Projections;
   - Core Assets Scans;
   - Core Scanning;
   - Core Tables;
   - Core Topology;
   - Core Topology Analyzer.

Пользовательские поля удалены из модели актива.

15. Изменение проверок по чек-листу

Описание параметров проверок приведено в разделе "Параметры проверок по чек-листу".

- Чтобы изменить проверки:

  1. На сервере MP 10 Core в папке `C:\ProgramData\Positive Technologies \MaxPatrol 10 Core\Config\UsageMonitoring` создайте копию файла `check_settings.default.yaml` — файл `check_settings.yaml`.
  2. В файле `check_settings.yaml` измените необходимые параметры.
  3. Перезапустите службу Core Usage Monitoring.

  Проверки изменены.

16. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

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

Вы можете получать техническую поддержку на портале support.ptsecurity.com или по телефону. Запросы на портале — основной способ обращений за технической поддержкой.

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

В этом разделе

16.1. Техническая поддержка на портале

Портал support.ptsecurity.com предоставляет вам возможность создавать запросы на техническую поддержку.

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

Портал support.ptsecurity.com содержит статьи базы знаний, новости обновлений продуктов "Позитив Текнолоджиз", ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

16.2. Техническая поддержка по телефону

Вы можете связаться со службой технической поддержки по телефону +7 495 744 01 44.

Техническая поддержка по телефону предоставляется на русском и английском языках.

Сотрудники технической поддержки по телефону могут выполнить оперативную диагностику, ответить на простые вопросы или уточнить текущий статус работ по ранее созданному запросу.

Если решить вопрос по телефону в разумное время (15—20 минут) невозможно, создайте запрос на портале support.ptsecurity.com. Запрос на портале, созданный и обновляемый по рекомендациям специалиста технической поддержки, гарантирует дальнейшие работы по вашему обращению.

16.3. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний. Сотрудники технической поддержки работают по имеющимся запросам и принимают обращения по телефону с понедельника по пятницу с 9:00 до 19:00 UTC+3.

16.4. Как служба технической поддержки работает с запросами

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

В этом разделе

Предоставление информации для технической поддержки (см. раздел 16.4.1)

Типы запросов (см. раздел 16.4.2)

Время реакции и приоритизация запросов (см. раздел 16.4.3)

Выполнение работ по запросу (см. раздел 16.4.4)

16.4.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста "Позитив Текнолоджиз" нужно предоставить:

- номер лицензии на использование продукта;
- файлы журналов и другие наборы диагностических данных, хранящихся в продукте;
- снимки экрана;
- результаты выполнения рекомендаций специалиста технической поддержки;
- каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

"Позитив Текнолоджиз" не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

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

16.4.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

"Позитив Текнолоджиз" поставляет пакеты обновления продукта в течение срока действия лицензии на продукт.

"Позитив Текнолоджиз" не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

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

16.4.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 6).

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

Таблица 6. Время реакции на запрос и время его обработки

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

Уровень значимости запроса	Критерии значимости запроса	Время реакции на запрос	Время обработки запроса
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

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

16.4.4. Выполнение работ по запросу

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

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

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

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

Работы по запросу считаются выполненными, если:

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

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

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

— проблема классифицирована как неподдерживаемая.

Приложение А. Параметры конфигурации компонентов MaxPatrol VM на Microsoft Windows

Раздел содержит описание параметров конфигурации компонентов MaxPatrol VM на Microsoft Windows. Инструкции по изменению параметров приведены в разделе "Изменение конфигурации компонентов MaxPatrol VM на Microsoft Windows" (см. раздел 12).

Таблица 7. Параметры конфигурации компонента MP 10 Core

Параметр	Описание	Значение по умолчанию
`CollectCorrelationTelemetry`	Если запущен сбор данных (параметр `CollectTelemetry` равен `True`), собираются (`True`) или не собираются (`False`) данные о срабатывании правил корреляции	`True`
`CollectProductTelemetry`	Если запущен сбор данных (параметр `CollectTelemetry` равен `True`), собираются (`True`) или не собираются (`False`) данные о версиях служб MaxPatrol VM	`True`
`CollectTelemetry`	Система собирает (`True`) или не собирает (`False`) данные о своей работе	`False`
`ConsiderEventsImportance`	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (`True`) или по расписанию (`False`)	`True`
`DefaultAssetTtl`	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	`90.00:00:00`
`DefaultLocale`	Интерфейс MaxPatrol VM отображается на русском (`ru-RU`) или английском (`en-US`) языке	`ru-RU`
`EmailNotificationRetryCount`	Максимальное количество попыток отправки сообщения на SMTP-сервер	`10`

Параметр	Описание	Значение по умолчанию
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
MicroservicesCertificateThumb	Отпечаток сертификата, используемого службами MP 10 Core для взаимодействия между собой	7EA87DDE95A95FD2D2BA8C9C1237110A9177DA46
MongoDbAuthSource	Имя базы данных, где хранятся учетные данные пользователей СУБД MongoDB	admin
MongoDbHost	IP-адрес или FQDN сервера СУБД MongoDB	localhost
MongoDbLogin	Логин служебной учетной записи для подключения MP 10 Core к СУБД MongoDB	admin
MongoDbPassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД MongoDB	P@ssw0rd
MongoDbPort	Порт сервера СУБД MongoDB для входящих подключений от MP 10 Core	27017
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	—
PtkbFeatureHost	IP-адрес или FQDN сервера Knowledge Base	localhost

Параметр	Описание	Значение по умолчанию
PtmcHostAddress	IP-адрес или FQDN сервера PT MC	localhost
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O
RMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	C:\Program Files\Positive Technologies\MaxPatrol 10 Core \.install\scripts\Certificates \RMQ_Core_Client.p12
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SaltMasterHost	IP-адрес или FQDN сервера с модулем SaltMaster	—
SaltMasterPort	Порт сервера с модулем SaltMaster для входящих подключений от MP 10 Core	9035
SendTelemetry	Система отправляет (True) или не отправляет (False) собранные данные в "Позитив Текнолоджиз"	False
ServicesRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
ServicesRMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd
ServicesRMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O

Параметр	Описание	Значение по умолчанию
ServicesRMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	C:\Program Files\Positive Technologies\MaxPatrol 10 Core\.install\scripts\Certificates\RMQ_Core_Client.p12
ServicesRMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
ServicesRMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
ServicesRMQVirtualHost	Имя виртуального узла RabbitMQ	/
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
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
SmtpSender	Значение поля "Отправитель" в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpSslEnabled	Для подключения к SMTP-серверу службы MP 10 Core используют защищенное (True) или незащищенное (False) соединение	False
SmtpUseDefaultCredentials	Для аутентификации на SMTP-сервере используются логин и пароль служебной учетной записи Network Service (True) или логин и пароль, указанные в параметрах SmtpUser и SmtpPassword (False)	True
SmtpUser	Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—

Параметр	Описание	Значение по умолчанию
SSLCertificateThumb	Отпечаток сертификата для веб-сайта компонентов MP 10 Core и PT MC	805A6F12A9BF2978BCC718D718DB7E9F269E2D53
SsoClientId	Идентификатор для регистрации приложения MaxPatrol 10 в PT MC	mpx
SsoClientSecret	Ключ для регистрации приложения MaxPatrol 10 в PT MC	eea74278-ff80-4268-9934-51de0a2c8d7e
StopOnMicroserviceError	Службы MP 10 Core останавливаются (True) или не останавливаются (False) при возникновении ошибки в их работе	False
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsePtbkServer	MP 10 Core проверяет (True) или не проверяет (False) наличие обновления базы знаний об уязвимостях в Knowledge Base	True

Таблица 8. Параметры конфигурации компонента MP 10 Agent

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами агента. При достижении порогового значения агент переходит в режим SafeMode1	—

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов агента. При достижении порогового значения агент переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	20480M 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 сообщений. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди сообщений. При достижении порогового значения агент переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode2	—
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных агента. При достижении порогового значения агент переходит в режим SafeMode1	—

Параметр	Описание	Значение по умолчанию
AgentName	Имя агента в веб-интерфейсе MaxPatrol VM	FQDN сервера MP 10 Agent
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\.install\scripts\Certificates\rootCA.crt
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\.install\scripts\Certificates\RMQ_Agent_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	C:\Program Files (x86)\Positive Technologies\MaxPatrol 10 Agent\.install\scripts\Certificates\RMQ_Agent_Client.key
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Agent к RabbitMQ	P@ssw0rd
RMQPort	Порт сервера RabbitMQ для входящих подключений от MP 10 Agent	5671
RMQUser	Логин служебной учетной записи для подключения MP 10 Agent к RabbitMQ	mpx_agent
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
SSLEnabled	MP 10 Agent подключается к RabbitMQ через защищенное (True) или незащищенное (False) соединение	True

Таблица 9. Параметры конфигурации компонента Knowledge Base

Параметр	Описание	Значение по умолчанию
`ClientId`	Идентификатор для регистрации приложения Knowledge Base в PT MC	`ptkb`
`ClientSecret`	Ключ для регистрации приложения Knowledge Base в PT MC	`secret`
`CoreAddress`	IP-адрес или FQDN сервера MP 10 Core	`localhost`
`DatabaseBackupFolder`	Путь к папке для хранения резервной копии БД	`C:\ProgramData\Positive Technologies\Knowledge Base\ \data\backup`
`DatabaseConnectionString`	Строка для подключения к БД PostgreSQL	—
`DefaultLocale`	Интерфейс Knowledge Base отображается на русском (`ru-RU`) или английском (`en-US`) языке	—
`DeploymentType`	Тип развертывания Knowledge Base	—
`DisplayName`	Название приложения Knowledge Base в PT MC	`Knowledge Base`
`EnableMPXAuth`	Аутентификация пользователей выполняется локально (`True`) или через LDAP (`False`)	`True`
`FrontendBindingPort`	Порт для подключения к веб-интерфейсу Knowledge Base	`8091`
`HostAddress`	IP-адрес или FQDN сервера Knowledge Base	`localhost`
`IamPort`	Порт сервера PT MC для входящих подключений от Knowledge Base к службе MC Identity and Access Management Service	`3334`
`IdentityServerAddress`	IP-адрес или FQDN сервера PT MC	`localhost`

Параметр	Описание	Значение по умолчанию
IdentityServerPort	Порт сервера PT MC для входящих подключений от Knowledge Base к службе MC User Action Logging Service	3333
InternalServicePort	Порт для подключения к API Knowledge Base	8190
MaxPortalPort	Порт сервера MP 10 Core для входящих подключений от Knowledge Base	443
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RegistrationId	Идентификатор Knowledge Base для регистрации в службе MC Tenant Manager Service	50dfcc46-fbf1-48f5-909b-ac90ca45567c
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25

Параметр	Описание	Значение по умолчанию
SmtpSender	Значение поля "Отправитель" в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>
SmtpUseDefaultCredentials	Для аутентификации на SMTP-сервере используются логин и пароль служебной учетной записи Network Service (True) или логин и пароль, указанные в параметрах SmtpUser и SmtpPassword (False)	True
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SSLCertificateThumb	Отпечаток сертификата для веб-сайта компонента Knowledge Base	805A6F12A9BF2978BCC718D718DB7E9F269E2D53
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics
TempDataDir	Путь к папке для хранения временных файлов Knowledge Base	C:\ProgramData\Positive Technologies\Knowledge Base\\tmp
TmPort	Порт сервера PT MC для входящих подключений от Knowledge Base к службе MC Tenant Manager Service	8703

Таблица 10. Параметры конфигурации компонента PT MC

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

Параметр	Описание	Значение по умолчанию
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
DataProtectionFilePath	Путь к папке с ключами для шифрования файлов cookies	/ptmc-shared-keys
DefaultLocale	Интерфейс PT MC отображается на русском (ru-RU) или английском (en-US) языке	ru-RU
HostAddress	IP-адрес или FQDN сервера PT MC	localhost
IamCookieLifetime	Продолжительность жизни неактивной сессии в MaxPatrol VM (в часах)	168
IamSecret	Идентификатор для регистрации приложения Management and Configuration в PT MC	—
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000
LogCleanTimeout	Период между проверками количества сохраненных записей о действиях пользователей (в миллисекундах)	5000
MasterRedirectEnabled	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (True) или на локальной (False) площадке	True
MicroservicesCertificateThumb	Отпечаток сертификата, используемого службами MP 10 Core при взаимодействии между собой	7EA87DDE95A95FD2D2BA8C9C1237110A9177DA46
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost

Параметр	Описание	Значение по умолчанию
PostgrePassword	Пароль служебной учетной записи для подключения PT MC к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для подключения PT MC к СУБД PostgreSQL	pt_system
SSLCertificateThumb	Отпечаток сертификата для веб-сайта компонентов MP 10 Core и PT MC	805A6F12A9BF2978BCC718D718DB7E9F269E2D53
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	—
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	—
TokensCertificateThumb	Отпечаток сертификата для подписи и валидации маркеров доступа	805A6F12A9BF2978BCC718D718DB7E9F269E2D53

Таблица 11. Параметры конфигурации утилиты rabbitmqcfg

Параметр	Описание	Значение по умолчанию
AdminPassword	Пароль администратора RabbitMQ	guest
CACertFile	Путь к файлу корневого сертификата	C:\ProgramData\RabbitMQ/tls/rootCA.crt
CertFile	Путь к файлу публичного сертификата	C:\ProgramData\RabbitMQ/tls/RMQ_Server.crt
KeyFile	Путь к файлу закрытого ключа сертификата	C:\ProgramData\RabbitMQ/tls/RMQ_Server.pem

Параметр	Описание	Значение по умолчанию
MEMORY_HIGH_WATERMARK	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в гигабайтах). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ останавливает прием входящих сообщений	10GB
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах). **Примечание.** Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	20
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Таблица 12. Параметры конфигурации утилиты mongodbcfg

Параметр	Описание	Значение по умолчанию
CacheSizeGB	Максимальный размер кэша (в гигабайтах)	1
DBPath	Путь к папке для хранения данных	C:\ProgramData\MongoDB\data\
ListenOnlyLocal	СУБД MongoDB доступна как для локальных, так и для удаленных подключений (False) или только для локальных (True)	True

Параметр	Описание	Значение по умолчанию
LogrotateCommonParamsDir	Путь к файлам конфигурации утилиты logrotate	C:\ProgramData\Positive Technologies\Logrotate\config\ComponentConfigs
SuperuserPassword	Пароль суперпользователя	P@ssw0rd

Таблица 13. Параметры конфигурации утилиты logrotatecfg

Параметр	Описание	Значение по умолчанию
CommonParamsDir	Путь к файлам конфигурации утилиты	C:\ProgramData\Positive Technologies\Logrotate\config\ComponentConfigs
RotateCount	Максимальное количество файлов журналов для компонентов сторонних производителей	10
RotateSize	Максимальный размер файла журнала для компонентов сторонних производителей (G для гигабайтов, M для мегабайтов, k для килобайтов)	200M

Таблица 14. Параметры конфигурации утилиты saltcfg

Параметр	Описание	Значение по умолчанию
SaltMasterHost	IP-адрес или FQDN сервера с модулем SaltMaster	—
SaltMinionLogLevel	Уровень журналирования для службы salt-minion (возможные значения — fatal, error, warn, info, debug или trace)	info

Приложение Б. Параметры конфигурации компонента PT UCS

Раздел содержит описание параметров конфигурации компонента PT UCS. Инструкция по изменению параметров приведена в разделе "Изменение конфигурации компонента PT UCS" (см. раздел 13).

Таблица 15. Параметры конфигурации компонента PT UCS

Параметр	Описание	Значение по умолчанию
`AutoAcceptMinions`	SaltMaster автоматически утверждает запрос на подключение от модулей SaltMinion (флажок установлен) или модули необходимо подключать вручную (флажок снят)	Флажок снят
`AutoDownloadProductsList`	PT UCS автоматически загружает с глобального сервера "Позитив Текнолоджиз" обновления для следующих объектов: — `KB VM DATA` — уязвимостей, условий их возникновения и закрытия, бюллетеней, возможного ПО на активах; — `KB BINARY` — дистрибутивов Knowledge Base; — `SIEM BINARY` — дистрибутивов компонентов на Microsoft Windows.	Установлены флажки `KB VM DATA` и `KB BINARY`
`LogLevel`	Уровень журналирования для служб PT UCS	`info`
`ProxyAddress`	IP-адрес или FQDN прокси-сервера	`proxy.server.fqdn.or.ip`
`ProxyEnabled`	PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений "Позитив Текнолоджиз"	Флажок снят
`ProxyPassword`	Пароль служебной учетной записи для подключения PT UCS к прокси-серверу	—

Параметр	Описание	Значение по умолчанию
`ProxyPort`	Порт прокси-сервера для входящего подключения от PT UCS	`8080`
`ProxyUser`	Логин служебной учетной записи для подключения PT UCS к прокси-серверу	—
`SaltMasterHost`	IP-адрес или FQDN сервера с модулем SaltMaster	—
`SaltMinionLogLevel`	Уровень журналирования для модуля SaltMinion (возможные значения — `fatal`, `error`, `warn`, `info`, `debug` или `trace`)	`info`
`TelemetrySendPeriod`	Расписание отправки в "Позитив Текнолоджиз" собранных данных о работе системы (в формате планировщика заданий cron)	`30 0 * * *`

Приложение B. 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 15).

Таблица 16. Параметры проверок по чек-листу

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

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		`actual_valued_assets_amount`	Максимальное количество неактуальных активов	`3`
Общий параметр для всех проверок	—	`check_period`	Период (в минутах) запуска проверок и обновления их результатов в веб-интерфейсе	`15`

Приложение Г. Расположение файлов для настройки журналирования работы компонента MP 10 Core

Файлы, необходимые для настройки журналирования, находятся в папках с названием службы, расположенных, в свою очередь, в общей папке `C:\Program Files\Positive Technologies\MaxPatrol 10 Core`. Инструкция по настройке журналирования приведена в разделе "Настройка журналирования работы компонента MP Core" (см. раздел 11.1).

Таблица 17. Расположение файлов конфигурации

Служба	Расположение файла
Core Application Registration	Файл `microservice.log4net.config` находится в папке `ApplicationRegistration`
Core Assets Identification	Файл `microservice.log4net.config` находится в папке `Assets.Identity`
Core Assets Premerger	Файл `microservice.log4net.config` находится в папке `Assets.PreMerger`
Core Assets Processing	Файл `log4net.config` находится в папке `Assets.Processing`
Core Assets Projections	Файл `host.log4net.config` находится в папке `Assets.Projections`
Core Assets Scans	Файл `microservice.log4net.config` находится в папке `Assets.Scans`
Core Assets Temporal Read Model	Файл `log4net.config` находится в папке `Assets.TemporalReadModel`
Core Assets Triggers	Файл `log4net.config` находится в папке `Assets.Triggers`
Core Deployment Configuration	Файл `microservice.log4net.config` находится в папке `Deployment.Configuration`
Core Events	Файл `microservice.log4net.config` находится в папке `Events`
Core Events Sources Monitoring	Файл `microservice.log4net.config` находится в папке `Events.Monitoring`
Core Events Triggers	Файл `microservice.log4net.config` находится в папке `Events.Triggers`
Core Groups	Файл `host.log4net.config` находится в папке `Groups`

Служба	Расположение файла
Core Health Monitoring	Файл `microservice.log4net.config` находится в папке `HealthMonitoring`
Core Incidents Management	Файл `log4net.config` находится в папке `Incident`
Core Incidents Read Model	Файл `log4net.config` находится в папке `IncidentReadModel`
Core Licensing	Файл `microservice.log4net.config` находится в папке `Licensing`
Core Notifications Management	Файл `log4net.config` находится в папке `NotificationsManagement`
Core Printing	Файл `microservice.log4net.config` находится в папке `Analytics.Printing`
Core Query Aggregator	Файл `microservice.log4net.config` находится в папке `Analytics.QueryAggregator`
Core Reporting	Файл `microservice.log4net.config` находится в папке `Analytics.Reports`
Core Reporting Delivery	Файл `microservice.log4net.config` находится в папке `Analytics.ReportsDelivery`
Core Scanning	Файл `log4net.config` находится в папке `Scanning`
Core Scopes	Файл `host.log4net.config` находится в папке `Scopes`
Core Tables	Файл `microservice.log4net.config` находится в папке `Tables`
Core Telemetry Collector	Файл `microservice.log4net.config` находится в папке `Telemetry.Collector`
Core Topology	Файл `microservice.log4net.config` находится в папке `Topology`
Core Topology Analyzer	Файл `microservice.log4net.config` находится в папке `Topology.Analyzer`
Core Triggers	Файл `log4net.config` находится в папке `Triggers`
Core Usage Monitoring	Файл `microservice.log4net.config` находится в папке `UsageMonitoring`
Core Users Settings	Файл `microservice.log4net.config` находится в папке `Users.Settings`
Core Watchdog	Файл `microservice.log4net.config` находится в папке `HealthMonitoring.Watchdog.Core`

Служба	Расположение файла
Core Widgets	Файл `microservice.log4net.config` находится в папке `Analytics.Widgets`

Предметный указатель

О компании

"Позитив Текнолоджиз" уже 18 лет создает инновационные решения в сфере информационной безопасности. Продукты и сервисы компании позволяют выявить, верифицировать и нейтрализовать реальные бизнес-риски, которые могут возникать в IT-инфраструктуре предприятий. Наши технологии построены на многолетнем исследовательском опыте и экспертизе ведущих специалистов по кибербезопасности.

Сегодня свою безопасность нам доверяют более 2000 компаний в 30 странах мира. В числе наших клиентов в России — 80% участников рейтинга "Эксперт-400".

POSITIVE TECHNOLOGIES

pt@ptsecurity.com ptsecurity.com