MaxPatrol SIEM версия 8.0

Руководство администратора

Дата редакции документа: 20.10.2023

Содержание

1. Об этом документе

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

Руководство адресовано специалистам, администрирующим MaxPatrol SIEM.

Комплект документации MaxPatrol SIEM включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации и событиями информационной безопасности.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol SIEM для сбора событий с источников и аудита активов.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol SIEM.
- PDQL-запросы для анализа активов — содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в MaxPatrol SIEM.
- Руководство разработчика — содержит рекомендации по созданию правил нормализации, обогащения, агрегации и корреляции событий, описание утилит MaxPatrol SIEM SDK для их отладки, а также информацию о доступных в MaxPatrol SIEM функциях сервиса REST API.

2. О MaxPatrol SIEM

Positive Technologies MaxPatrol SIEM (далее также — MaxPatrol SIEM) — это система, которая предназначена для сбора, хранения и анализа данных о событиях, происходящих в IT-инфраструктуре организации. Это позволяет обеспечивать мониторинг информационной безопасности как всей инфраструктуры, так и отдельных подразделений, узлов и приложений.

MaxPatrol SIEM предоставляет следующие основные возможности:

- **Инвентаризация активов.** Система регулярно собирает данные о сетевых узлах и связях между ними.
- **Сбор данных о событиях.** В качестве источника событий может выступать любое поддерживаемое оборудование или ПО.
- **Анализ событий для выявления инцидентов ИБ.** Набор специальных правил, на основе которых выполняется анализ, постоянно пополняется экспертами Positive Technologies.
- **Управление инцидентами ИБ.** Система помогает организовать работу по расследованию инцидентов информационной безопасности и устранению их последствий.
- **Визуализация данных.** Сводная информация об активах, событиях и инцидентах отображается в веб-интерфейсе системы в виде диаграмм и таблиц.

MaxPatrol SIEM предоставляет также дополнительные возможности:

- **Пакеты экспертизы.** Использование базы знаний, разработанной экспертами Positive Technologies. База содержит данные о самых современных тактиках и техниках хакерских атак и помогает выявлять даже сложные нетиповые атаки.
- **Автоматизация работы с активами.** Система может автоматически устанавливать значимость активов и сроки актуальности данных об активах, полученных в результате сканирования IT-инфраструктуры.
- **Репутационные списки.** Актуальная информация о вредоносных IP-адресах и хеш-суммах опасных файлов используется для предотвращения инцидентов.
- **Повторная проверка событий.** Ретроспективная корреляция полученных ранее событий после добавления новых правил или обновления данных табличных списков; ретроспективный поиск индикаторов компрометации.
- **Отправка уведомлений.** Оповещение операторов об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных, собираемых событиях, а также о выявляемых инцидентах ИБ.
- **Интеграция с PT NAD.** Регистрация инцидентов на основе сессий и атак.

В этом разделе

Архитектура MaxPatrol SIEM (см. раздел 2.1)

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

2.1. Архитектура MaxPatrol SIEM

MaxPatrol SIEM 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. Для высокопродуктивных систем (более 3000 событий в секунду) рекомендуется распределенная установка MaxPatrol SIEM.

В этом разделе

2.1.1. Компонент MaxPatrol 10 Core

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

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

2.1.2. Компонент MaxPatrol SIEM Server

Компонент MaxPatrol SIEM Server (далее также — MP SIEM Server) выполняет основные функции по обработке событий безопасности:

— нормализацию, агрегацию, обогащение и корреляцию событий;

— автоматическое создание инцидентов;

— создание активов из событий;

— привязку событий к активам.

2.1.3. Компонент MaxPatrol SIEM Events Storage

Компонент MaxPatrol SIEM Events Storage (далее также — MP SIEM Events Storage) обеспечивает централизованное хранение информации о событиях безопасности.

2.1.4. Компонент MaxPatrol 10 Collector

Компонент MaxPatrol 10 Collector (далее также — MP 10 Collector) сканирует активы IT-инфраструктуры организации и собирает события с источников. MP 10 Collector имеет модульную структуру. Модули сканирования позволяют обнаруживать узлы и их открытые сетевые сервисы и проводить специализированные проверки в режиме теста на проникновение.

MP 10 Collector 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.

MP 10 Collector управляет модулями и обеспечивает мониторинг их состояния, а также передачу данных между модулями и компонентом MP SIEM Server.

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

2.1.5. Компонент MaxPatrol NAD Sensor

Компонент MaxPatrol NAD Sensor (далее также — MP NAD Sensor) выполняет комплексный анализ сетевого трафика на уровнях L2—L7 сетевой модели OSI и собирает данные о соединениях.

В состав компонента MP NAD Sensor входят модули Core Agent, DPI Event Collector и продукт Positive Technologies Network Attack Discovery (далее также — PT NAD).

В отличие от обычной версии PT NAD в MP NAD Sensor:

— захваченный трафик не сохраняется на диск (нет хранилища файлов PCAP);

— метаданные трафика хранятся не больше суток;

— скорость захвата трафика ограничена 1 Гбит/с.

2.1.6. Компонент Knowledge Base

Компонент Knowledge Base — это единая база знаний для продуктов Positive Technologies. Knowledge Base содержит пакеты экспертизы (наборы правил и табличных списков), макросы и схему полей событий, сведения о возможном ПО на активах. Также вместе с Knowledge Base поставляются утилиты SDK для работы с данными базы.

2.1.7. Компонент PT Management and Configuration

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

— сервис единого входа в продукты Positive Technologies, развернутые в инфраструктуре организации;

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

— интеграцию с Microsoft Active Directory, включая аутентификацию пользователей и синхронизацию прав доступа;

— управление иерархией продуктов Positive Technologies;

— журналирование действий пользователей;

— прием, анонимизацию, шифрование и отправку телеметрических данных.

2.1.8. Компонент PT Update and Configuration Service

Компонент PT Update and Configuration Service (далее также — PT UCS) — это сервис онлайн-обновления компонентов MaxPatrol SIEM. PT UCS обеспечивает проверку наличия, загрузку и установку новых версий компонентов, а также обновление пакетов экспертизы, макросов и схемы полей событий.

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 SIEM. PT UCS загружает новые версии компонентов с глобального сервера обновлений Positive Technologies и с помощью модуля Salt Master отправляет их модулям Salt Minion для установки.

2.1.9. Компонент PT Cybsi Provider

Компонент PT Cybsi Provider (далее также — PT CP) обеспечивает доставку данных об угрозах информационной безопасности и индикаторах компрометации, специфичных для отдельной организации в данный момент времени. Индикаторы компрометации — это артефакты, наблюдаемые в сети или в операционной системе и указывающие на вредоносную активность в инфраструктуре.

В качестве источника данных об угрозах информационной безопасности и индикаторах компрометации PT CP поддерживает репутационные сервисы компаний «Лаборатория Касперского», Positive Technologies, Group-IB, платформы MISP Threat Sharing и системы PT CybSI. Также PT CP поддерживает получение данных в формате STIX 2.0 по протоколу TAXII. Лицензии на репутационные сервисы компаний «Лаборатория Касперского» и Group-IB необходимо приобретать у производителей (подробнее на сайтах kaspersky.ru и group-ib.ru).

2.1.10. Компонент PT Retro Correlator

Компонент PT Retro Correlator (далее также — PT RC) выполняет повторную проверку полученных ранее событий при помощи правил корреляции. В состав компонента входят службы mpagent.service и siemserver-retrocontroller.service.

2.2. Алгоритм работы MaxPatrol SIEM и схема взаимодействия компонентов

Алгоритм работы MaxPatrol SIEM:

1. Коллекторы собирают данные об IT-инфраструктуре предприятия:

   — модули компонента MP 10 Collector сканируют IT-инфраструктуру, собирают сведения о сетевых узлах и события с источников;

   — компонент MP NAD Sensor собирает сведения о сетевых соединениях.

   Собранные данные коллекторы передают в MP SIEM Server и MP 10 Core. Переданные события используются в MP SIEM Server для нормализации, агрегации, обогащения и корреляции.

2. Компонент MP 10 Core обрабатывает и хранит результаты сканирования с подробной информацией об обнаруженных ОС, ПО, службах, портах и прочими сведениями об узлах и связях между ними. Также компонент хранит параметры задач на сбор данных, профилей сканирования и транспортов, данные и сценарии справочников и осуществляет контроль доступа к этим данным, связываясь с остальными компонентами системы для выполнения пользовательских запросов.

3. Компонент MP SIEM Server обрабатывает входящий поток событий, приводит их к единому формату в соответствии с правилами нормализации и группирует их согласно правилам агрегации. Он также связывает события с активами и, при необходимости, создает новые активы на основе событий. Затем дополняет данные о событиях, используя правила

обогащения или табличные списки, и анализирует поток нормализованных событий по правилам корреляции для выявления и регистрации событий информационной безопасности. MP SIEM Server передает компоненту MP SIEM Events Storage поступившие события в исходном (необработанном) и в нормализованном виде для хранения.

Примечание. Нормализация событий может выполняться на сервере MP 10 Collector. Для этого необходимо установить на сервер MP 10 Collector облегченную версию MP SIEM Server — «SIEM на коллекторе». События, нормализованные на таком сервере MP 10 Collector, передаются для агрегации, обогащения и корреляции на основной MP SIEM Server.

4. Компонент Knowledge Base содержит базу знаний, необходимых MaxPatrol SIEM для структурирования сведений, собранных от источников событий и объектов инфраструктуры.
5. Компонент PT MC обеспечивает доступ к системе через сервис единого входа и журналирует действия пользователей.
6. Для управления системой, просмотра данных, построения отчетов и мониторинга пользователь подключается к компоненту MP 10 Core через веб-интерфейс в соответствии с правами, которые назначены в PT MC.
7. Компонент PT CP доставляет данные об угрозах информационной безопасности и индикаторах компрометации.
8. Компонент PT RC обеспечивает возможность ретроспективной проверки полученных ранее событий, используя новые правила корреляции и данные из табличных списков.
9. Компонент PT UCS обеспечивает обновление компонентов системы и базы знаний.

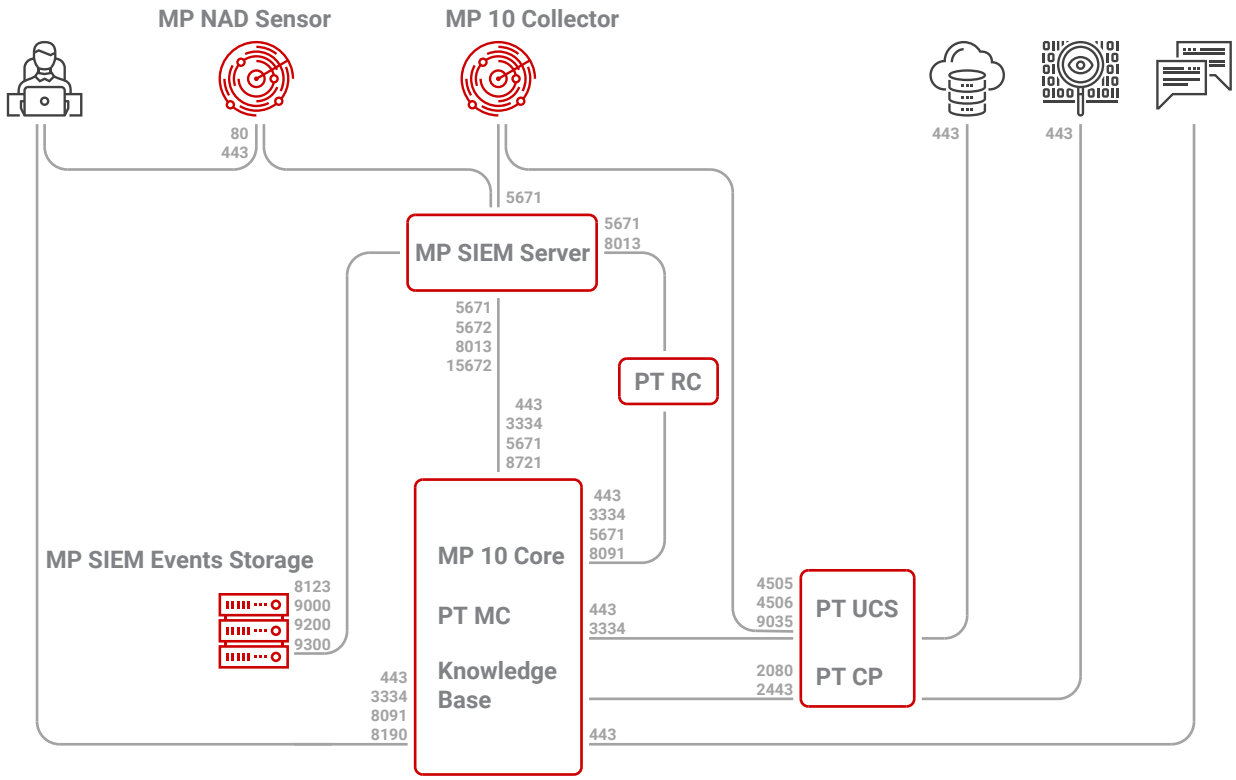

Рисунок 1. Взаимодействие компонентов MaxPatrol SIEM

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

Таблица 1. Компоненты и порты взаимодействия

Источник	Получатель	TCP-порт
Рабочая станция пользователя, ПО для загрузки данных уведомлений	MP 10 Core	443
MP SIEM Server	MP 10 Core	443, 3334, 5671, 8721
PT UCS	MP 10 Core	443, 3334
PT RC	MP 10 Core	443, 5671
Рабочая станция пользователя	Knowledge Base	8091, 8190
PT RC	Knowledge Base	8091

Источник	Получатель	TCP-порт
Рабочая станция пользователя, компонент PT RC	PT MC	3334
MP 10 Core	MP SIEM Server	5671, 5672, 15672
MP 10 Collector, MP NAD Sensor	MP SIEM Server	5671
Knowledge Base	MP SIEM Server	8013
PT RC	MP SIEM Server	8013, 5671
MP SIEM Server	MP SIEM Events Storage	8123, 9000, 9200, 9300
Рабочая станция пользователя	MP NAD Sensor	80, 443
MP 10 Core, MP SIEM Server, MP SIEM Events Storage, MP 10 Collector	PT UCS	4505, 4506, 9035
PT UCS	Глобальный сервер обновлений	443
MP 10 Core	PT CP	2080, 2443
PT CP	Репутационный сервис, предоставляющий данные об угрозах ИБ и индикаторах компрометации	443

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

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

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

3. Предоставление прав доступа

В MaxPatrol SIEM 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, источники, события и инциденты, доступ к которым получат пользователи с этой ролью.

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

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

При развертывании MaxPatrol SIEM 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, источникам, событиям и инцидентам в соответствии с производственными задачами пользователя.

В этом разделе даны инструкции по предоставлению доступа к активам, источникам, событиям и инцидентам. Подробная информация об учетных записях пользователей, их ролях и привилегиях, а также инструкции по работе с ними приведены в руководстве администратора PT MC.

В этом разделе

О приложениях PT MC (см. раздел 3.1)

Предоставление доступа к событиям (см. раздел 3.2)

Предоставление доступа к активам, инцидентам и источникам (см. раздел 3.3)

См. также

Возможности привилегии «Расширенные полномочия» (см. приложение B)

3.1. О приложениях PT MC

При развертывании MaxPatrol SIEM в PT MC регистрируются следующие приложения:

- **Management and Configuration.** Приложение предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления площадками и связями между ними. По умолчанию приложение содержит стандартные роли **Администратор** и **Пользователь**.
- **MaxPatrol 10.** Приложение предназначено для настройки сбора данных об IT-инфраструктуре предприятия и работы с активами, источниками, событиями и инцидентами. По умолчанию приложение содержит стандартные роли **Администратор** и **Оператор**.
- **Knowledge Base.** Приложение предназначено для работы с пакетами экспертизы, макросами и схемой полей событий. По умолчанию приложение содержит стандартную роль **Администратор**.

3.2. Предоставление доступа к событиям

► Чтобы предоставить доступ к событиям:

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

   Откроется страница **Права доступа**.

2. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к событиям.
3. В панели **<Название роли>** по ссылке **Редактировать** откройте окно **Доступ к событиям**.
4. В раскрывающемся списке **Доступ** выберите необходимый тип доступа.
5. Если вы выбрали ограниченный доступ к событиям, введите условия фильтрации.

   Примечание. Вы можете скопировать условия фильтрации, нажав ссылку **Вставить условие из сохраненного запроса** и выбрав условия фильтрации из списка.

6. Нажмите кнопку **Сохранить**.

Доступ к событиям предоставлен.

3.3. Предоставление доступа к активам, инцидентам и источникам

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

► Чтобы предоставить доступ к активам:

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

   Откроется страница **Права доступа**.

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

3. В панели **<Название роли>** по ссылке **Редактировать** откройте окно **Доступ к активам, инцидентам и источникам**.

4. В раскрывающемся списке **Доступ** выберите необходимый тип доступа.

5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы активов, к которым необходимо предоставить доступ.

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

6. Нажмите кнопку **Сохранить**.

Доступ к активам предоставлен.

4. Распределенный поиск и репликация событий

После создания связей между площадками (подробное описание см. в Руководстве администратора PT MC) вы сможете настроить связи между приложениями MaxPatrol 10, предназначенные для выполнения следующих задач.

Распределенный поиск событий

Связь обеспечивает в интерфейсе локального приложения работу с событиями, собранными в других приложениях. Эти события будут доступны для поиска и фильтрации, группировки и агрегации, отображения на виджетах и выпуска по ним отчетов. Вместе с тем данные об этих событиях не реплицируются между хранилищами связанных приложений.

Для работы с распределенным поиском вы можете предоставить пользователю следующие привилегии:

— **Распределенный поиск событий.** Разрешает просмотр полученных распределенным поиском событий на странице **События** и на виджетах, а также выпуск отчетов по таким событиям. Привилегия доступна для ролей в приложении MaxPatrol 10.

  Внимание! Пользователю с привилегией **Распределенный поиск событий** будут доступны все события, собранные как на локальной площадке, так и на площадках связанных приложений. Права доступа к событиям, указанные для ролей пользователя на странице **Система** → **Права доступа**, будут проигнорированы.

— **Просмотр правил репликации и связей для распределенного поиска.** Разрешает просмотр созданных связей распределенного поиска на странице **Площадки**. Привилегия доступна для ролей в приложении PT MC.

— **Добавление, изменение и удаление правил репликации и связей для распределенного поиска.** Разрешает управление связями распределенного поиска на странице **Площадки**. Привилегия доступна для ролей в приложении PT MC.

Перед настройкой связей для распределенного поиска на каждой площадке необходимо:

1. Обеспечить сетевое взаимодействие через TCP-порты 9200 и 9300 между серверами MP SIEM Server и MP SIEM Events Storage связываемых приложений.
2. Указать IP-адрес или FQDN сервера MP SIEM Events Storage в качестве значения параметра `ClusterSeedHost` компонента MP SIEM Server.
3. Повторно запустить настройку компонента MP 10 Core:
   `/opt/deployer/bin/Restart-Configuration.ps1 -RoleTypeId Core`

Не рекомендуется создавать связи для распределенного поиска между приложениями в низконагруженной конфигурации MaxPatrol SIEM.

Репликация событий

Связь обеспечивает репликацию данных о событиях из одного приложения в другое согласно установленному правилу. После репликации эти события будут доступны в приложении-получателе независимо от сетевой доступности приложения-отправителя.

Для работы с правилами репликации вы можете предоставить пользователю следующие привилегии:

— **Просмотр правил репликации и связей для распределенного поиска.** Разрешает просмотр правил репликации на странице **Площадки**. Привилегия доступна для ролей в приложении PT MC.

— **Добавление, изменение и удаление правил репликации и связей для распределенного поиска.** Разрешает управление правилами репликации на странице **Площадки**. Привилегия доступна для ролей в приложении PT MC.

Перед добавлением правила, а также для его дальнейшей работы необходимо обеспечить сетевое взаимодействие через TCP-порт 443 между серверами MP 10 Core связываемых приложений.

При работе с правилами репликации событий необходимо учитывать ряд ограничений:

— между двумя приложениями можно создать только одно правило;

— правила не должны формировать направленный цикл;

— по умолчанию приложение-получатель не выполняет агрегацию, обогащение, корреляцию и привязку реплицированных событий к активам.

Примечание. Вы можете разрешить агрегацию (параметр `RemoteEventsSkipAggregator`), обогащение (параметр `RemoteEventsSkipEnricher`), корреляцию (параметр `RemoteEventsSkipCorrelator`) и привязку реплицированных событий к активам (параметр `RemoteEventsSkipResolver`) в приложении-получателе.

В этом разделе

Добавление связей для распределенного поиска (см. раздел 4.1)

Удаление связи для распределенного поиска (см. раздел 4.2)

Добавление правила репликации событий (см. раздел 4.3)

Изменение правила репликации событий (см. раздел 4.4)

Удаление правила репликации событий (см. раздел 4.5)

4.1. Добавление связей для распределенного поиска

- Чтобы добавить связи:

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

     Откроется страница **Площадки**.
  3. На схеме выберите приложение.
  4. В панели **Приложение MaxPatrol 10** выберите вкладку **Распределенный поиск**.
  5. В панели инструментов нажмите кнопку **Добавить связи**.

     Откроется окно **Новые связи для распределенного поиска**.
  6. Укажите связанные приложения:

     - Если требуется, чтобы в выбранном приложении были доступны события из других приложений, — выберите эти приложения в раскрывающемся списке **По другим приложениям**.
     - Если требуется, чтобы события выбранного приложения были доступны в других приложениях, — выберите эти приложения в раскрывающемся списке **По этому приложению**.
  7. Нажмите кнопку **Добавить**.

     Новые связи появятся на схеме и в панели **Приложение MaxPatrol 10**.

  Связи добавлены.

4.2. Удаление связи для распределенного поиска

- Чтобы удалить связь:

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

     Откроется страница **Площадки**.
  3. На схеме выберите приложение.
  4. В панели **Приложение MaxPatrol 10** выберите вкладку **Распределенный поиск**.
  5. Выберите связь.

Примечание. Вы можете выбрать несколько связей подряд с помощью клавиши Shift или нескольких отдельных связей с помощью клавиши Ctrl.

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

Связь удалена.

4.3. Добавление правила репликации событий

Перед добавлением правила необходимо убедиться, что в приложении-отправителе вам доступны страница **События** и группы активов, события на которых нужно реплицировать.

- Чтобы добавить правило:

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

   Откроется страница **Площадки**.
3. На схеме выберите приложение, которое будет отправлять реплицированные события.
4. В панели **Приложение MaxPatrol 10** выберите вкладку **Репликация событий**.
5. В панели инструментов нажмите кнопку **Добавить правило репликации**.

   Откроется окно **Новое правило репликации**.
6. В поле **Получатель** укажите приложение, которое будет получать реплицированные события.
7. Нажмите кнопку **Настроить репликацию событий**.

   Откроется страница **События**.
8. В панели **Группы** выберите группы активов, события которых нужно реплицировать.
9. Если требуется, в панели **Фильтры** выберите фильтр событий.
10. Нажмите кнопку **Завершить настройку**.
11. Нажмите кнопку **Добавить**.

    Новое правило репликации появится на схеме и в панели **Приложение MaxPatrol 10**.

Правило добавлено.

4.4. Изменение правила репликации событий

Перед изменением правила необходимо убедиться, что в приложении-отправителе вам доступны страница **События** и группы активов, репликацию событий которых нужно изменить.

- Чтобы изменить правило:

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

     Откроется страница **Площадки**.
  3. На схеме выберите приложение.
  4. В панели **Приложение MaxPatrol 10** выберите вкладку **Репликация событий**.
  5. Выберите правило.
  6. В панели инструментов нажмите кнопку **Редактировать**.

     Откроется окно **Правило репликации**.
  7. Нажмите кнопку **Настроить репликацию событий**.

     Откроется страница **События**.
  8. Внесите изменения.
  9. Нажмите кнопку **Завершить настройку**.
  10. Нажмите кнопку **Сохранить**.

  Правило изменено.

4.5. Удаление правила репликации событий

- Чтобы удалить правило:

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

     Откроется страница **Площадки**.
  3. На схеме выберите приложение.
  4. В панели **Приложение MaxPatrol 10** выберите вкладку **Репликация событий**.
  5. Выберите правило.
  6. В панели инструментов нажмите кнопку **Удалить** и подтвердите удаление.

  Правило удалено.

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 SIEM предусмотрен механизм для автоматизации контроля за регулярностью сканирования активов — политики. Политика состоит из совокупности правил, которые автоматически устанавливают значимость активов или сроки актуальности и устаревания данных об активах, полученных в результате сканирования IT-инфраструктуры методами аудита и пентеста. Опасные уязвимости на активах, данные о которых редко обновляются, могут быть выявлены слишком поздно. Вы можете оценить количество активов, данные о которых не были получены вовремя, с помощью виджета **Актуальность данных об активах**, а также найти их с помощью PDQL-запроса.

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

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

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

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

В этом разделе

Применение изменений в политиках (см. раздел 5.8)

Отмена изменений в черновике политики (см. раздел 5.9)

5.1. Страница «Политики»

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

- **Создать правило** — для создания правила;
- **Редактировать** — для изменения параметров правила (см. раздел 5.4);
- **Копировать** — для создания правила на основе имеющегося правила (см. раздел 5.5);
- **Удалить** — для удаления правила (см. раздел 5.7);
- **Включить** — для включения правила в работу (см. раздел 5.6);
- **Отключить** — для приостановки работы правила (см. раздел 5.6).

В рабочей области страницы расположены:

- Панель **Список политик**. Содержит список политик и предназначена для выбора политики, применения изменений (см. раздел 5.8), а также отмены неприменённых изменений (см. раздел 5.9). При выборе политики составляющие ее правила отобразятся в центральной панели. Если политика имеет неприменённые изменения, на левой границе строки с названием политики отобразится желтая полоска, в правой части строки — кнопка для отмены изменений, а в нижней части панели — кнопка **Применить изменения**. Если выполняется применение изменений, слева от названия политики отобразится значок .
- Центральная панель. Содержит таблицу с правилами и предназначена для выбора правила и изменения порядка применения правил. При выборе правила сведения о нем отобразятся в правой части страницы в панели **<Название правила>**. В таблице отображаются следующие состояния правил:

  — правило работает;

  — правило остановлено;

  — правило работает с предупреждением;

  — правило не работает из-за ошибки. Такой же значок отобразится слева от названия политики с этим правилом.
- Панель **<Название правила>**. Содержит сведения о правиле, а также отображает сообщения о его работе.

5.2. Создание правила для значимости активов

- Чтобы создать правило:

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

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

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

     Примечание. Вы можете отфильтровать активы с помощью PDQL-запроса.
  6. В раскрывающемся списке выберите значимость актива.
  7. Нажмите кнопку **Сохранить**.

  Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.8).

5.3. Создание правила для сроков актуальности данных

- Чтобы создать правило:

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

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

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

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

  Правило создано.

Система начнет использовать правило только после применения изменений в политике (см. раздел 5.8).

5.4. 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 5.8).

5.5. 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 5.8).

5.6. 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 5.8).

- 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 5.8).

5.7. Удаление правила

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

- Чтобы удалить правило:

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

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

  Правило удалено.

Система перестанет использовать правило только после применения изменений в политике (см. раздел 5.8).

5.8. Применение изменений в политиках

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

- Чтобы применить изменения, внесенные в несколько политик:

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

     Откроется окно **Применение изменений**.

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

  Изменения применены.

5.9. Отмена изменений в черновике политики

- Чтобы отменить изменения:

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

  Изменения отменены.

6. Мониторинг источников событий

Для уменьшения вероятности пропуска инцидентов ИБ необходимо своевременно отслеживать состояние источников событий и потока данных от них. Качество и непрерывность сбора данных с источников влияют на оперативность выявления инцидентов и принятия решений.

Данные от источников передаются в MaxPatrol SIEM напрямую (без посредников) или через промежуточный актив — форвардер (например, через контроллер домена). Форвардер, кроме пересылки данных от других активов, также может отправлять данные от находящихся в нем источников.

Источники и форвардеры появляются в системе автоматически, по мере сбора событий с активов и их идентификации. На странице **Мониторинг источников** пользователь системы может просмотреть состояние источников и параметры потока данных от них или состояние форвардеров и параметры находящихся в них источников. Ссылка для выбора типа элементов (источников или форвардеров) находится в верхней части рабочей области страницы.

Если вы выбрали по ссылке работу с источниками, рабочая область страницы **Мониторинг источников** содержит:

— панель **Источники** для поиска источников, которые находятся на активах выбранной группы и вложенных в нее групп;

— панель **Фильтры** для фильтрации источников по условию наличия или отсутствия предупреждений;

— панель управления с возможностью настраивать, отключать или включать предупреждения для источника, удалять источники из списка, экспортировать и обновлять список источников, искать источники в списке;

— центральную панель с таблицей источников, а также со ссылкой для настройки периода отображения (по времени последнего получения данных от источника).

Если вы выбрали по ссылке работу с форвардерами, рабочая область страницы **Мониторинг источников** содержит:

— панель **Форвардеры** для поиска форвардеров, которые содержатся в выбранной группе активов и вложенных в нее группах;

— панель **Фильтры** для фильтрации форвардеров по условию наличия или отсутствия предупреждений;

— панель управления с возможностью настраивать, отключать или включать предупреждения для форвардера, удалять форвардеры из списка, экспортировать и обновлять список форвардеров, искать форвардеры в списке;

— центральную панель с таблицей форвардеров, а также со ссылкой для настройки периода отображения (по времени последнего получения данных от форвадера).

Примечание. По умолчанию на странице **Мониторинг источников** отображаются все источники (форвардеры), связанные с группами активов, к которым оператору предоставлен доступ.

В этом разделе

6.1. Просмотр списка источников и списка потоков событий от источника

- Чтобы просмотреть список источников:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **MaxPatrol 10**.

     Откроется главная страница.

  2. В главном меню в разделе **Сбор данных** выберите пункт **Мониторинг источников**.

     Откроется страница **Мониторинг источников**.

  В центральной панели отображена таблица со списком источников.

Для каждого источника в таблице указаны значения параметров. Вы можете сортировать список, нажимая на название колонки (параметра). Нажимая в правом верхнем углу страницы, вы можете отображать и скрывать колонки таблицы.

Примечание. Срок хранения данных, полученных от источника, 30 дней.

Для автоматизации мониторинга потока событий от источников или форвардеров вы можете создавать предупреждения для отслеживания наличия событий, средней скорости потока событий и задержки в получении события коллектором. Состояние предупреждения отображается в столбце **Контроль** соответствующим значком:

— параметры потока событий находятся в пределах допустимых значений;

— параметры потока событий вышли за пределы допустимых значений;

— предупреждение отключено.

При наведении курсора мыши на значок предупреждения во всплывающем окне отображается информация об отслеживаемых параметрах потока событий.

> **Примечание.** Источник автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Также удаляются данные, полученные от источника.

Также вы можете настраивать отправку уведомлений для получения по электронной почте информации о потоке событий от источника или форвардера.

- Чтобы просмотреть список потоков событий от источника,

  откройте страницу со списком потоков событий двойным щелчком мыши на строке с названием источника.

6.2. Просмотр списка форвардеров и списка источников форвардера

- Чтобы просмотреть список форвардеров:

  1. В главном меню нажмите и в раскрывшемся меню выберите пункт **MaxPatrol 10**.

     Откроется главная страница.

  2. В главном меню в разделе **Сбор данных** выберите пункт **Мониторинг источников**.

     Откроется страница **Мониторинг источников**.

  В центральной панели отображена таблица со списком форвардеров.

Для каждого форвардера в таблице указаны значения параметров. Вы можете сортировать список, нажимая на название колонки (параметра). Нажимая в правом верхнем углу страницы, вы можете отображать и скрывать колонки таблицы.

> **Примечание.** Срок хранения данных, полученных от форвардера, 30 дней.

Для автоматизации мониторинга потока событий от источников или форвардеров вы можете создавать предупреждения для отслеживания наличия событий, средней скорости потока событий и задержки в получении события коллектором. Состояние предупреждения отображается в столбце **Контроль** соответствующим значком:

— параметры потока событий находятся в пределах допустимых значений;

— параметры потока событий вышли за пределы допустимых значений;

— предупреждение отключено.

При наведении курсора мыши на значок предупреждения во всплывающем окне отображается информация об отслеживаемых параметрах потока событий.

> **Примечание.** Форвардер автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Также удаляются данные, полученные от форвардера.

Также вы можете настраивать отправку уведомлений для получения по электронной почте информации о потоке событий от источника или форвардера.

- Чтобы просмотреть список источников форвардера,

  откройте страницу со списком источников двойным щелчком мыши на строке с названием форвадера.

6.3. Создание предупреждения для отслеживания наличия событий

- Чтобы создать предупреждение для отслеживания наличия событий:

  1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

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

  2. В панели инструментов нажмите кнопку **Настроить предупреждения**.

     Откроется страница **Настройка предупреждений для источника <Название источника>**.

  3. Включите отслеживание наличия событий.
  4. По ссылкам укажите период, в котором необходимо отслеживать наличие событий, с учетом часового пояса.
  5. Нажмите кнопку **Добавить**.

Примечание. Вы можете добавлять до десяти периодов. Периоды не должны пересекаться.

6. Нажмите кнопку **Сохранить**.

Предупреждение создано. Отслеживание наличия событий запущено.

6.4. Создание предупреждения для отслеживания средней скорости потока событий

► Чтобы создать предупреждение для отслеживания средней скорости потока событий:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

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

2. В панели инструментов нажмите кнопку **Настроить предупреждения**.

   Откроется страница **Настройка предупреждений для источника <Название источника>**.

3. Включите отслеживание средней скорости потока событий.
4. По ссылке выберите, какие значения средней скорости необходимо отслеживать (абсолютные или относительные).
5. По ссылкам укажите интервал, в котором необходимо отслеживать среднюю скорость, с учетом часового пояса.
6. В поле правее введите продолжительность периода для вычисления средней скорости.

   Примечание. Продолжительность периода для вычисления средней скорости не должна превышать продолжительность интервала, в котором необходимо отслеживать среднюю скорость.

7. Если вы выбрали отслеживание абсолютного значения средней скорости потока событий, в полях **Минимум** и **Максимум** введите пороговые значения средней скорости.
8. Если вы выбрали отслеживание относительного значения средней скорости потока событий, в полях **Уменьшение** и **Увеличение** введите пороговые значения в процентах относительно средней скорости.
9. Нажмите кнопку **Добавить**.

   Примечание. Вы можете добавлять до десяти периодов. Периоды не должны пересекаться.

10. Нажмите кнопку **Сохранить**.

Предупреждение создано. Отслеживание средней скорости потока событий запущено.

6.5. Создание предупреждения для отслеживания задержки в получении события коллектором

- Чтобы создать предупреждение для отслеживания задержки в получении события коллектором:

  1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

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

  2. В панели инструментов нажмите кнопку **Настроить предупреждения**.

     Откроется страница **Настройка предупреждений для источника <Название источника>**.

  3. Включите отслеживание задержки в получении события коллектором.
  4. Введите значение задержки и по ссылке укажите единицу измерения времени (минуты или часы).
  5. Нажмите кнопку **Сохранить**.

  Предупреждение создано. Отслеживание задержки в получении события коллектором запущено.

6.6. Остановка и повторный запуск отслеживания потока событий

Вы можете остановить отслеживание потока событий от источника или форвардера (например, на время проведения плановых работ по техническому обслуживанию актива).

- Чтобы остановить отслеживание потока событий:

  1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

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

  2. В панели инструментов нажмите кнопку **Отключение предупреждения**.

     Слева от названия источника (форвардера) отобразится значок ⃠.

  Отслеживание потока событий остановлено.

- Чтобы запустить отслеживание потока событий:

  1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

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

2. В панели инструментов нажмите кнопку **Включение предупреждения**.

   Слева от названия источника (форвардера) отобразится значок ✔.

Отслеживание потока событий запущено.

6.7. Удаление источника (форвардера) из списка

Источник (форвардер) автоматически удаляется из списка, если от него не поступают события в течение 30 дней и для него не настроено предупреждение. Вы также можете удалить источник (форвардер) из списка вручную.

► Чтобы удалить источник (форвардер) из списка вручную:

1. На странице **Мониторинг источников** в центральной панели выберите строку с названием источника (форвардера).

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

2. Нажмите кнопку **Настроить предупреждения**.

   Откроется страница **Настройка предупреждений для источника <Название источника>**.

3. Убедитесь, что отключено отслеживание наличия событий, средней скорости потока событий и задержки в получении события коллектором.
4. Нажмите кнопку **Сохранить**.
5. Нажмите кнопку **Удалить источник** или кнопку **Удалить форвардер** и подтвердите удаление.

Источник (форвардер) удален из списка.

6.8. Экспорт списка источников (форвардеров) в текстовый файл

Вы можете экспортировать в текстовый файл список всех источников (форвардеров) или список выбранных источников (форвардеров).

- Чтобы экспортировать список всех источников (форвардеров):

  1. На странице **Мониторинг источников** в панели инструментов нажмите кнопку **Экспортировать список**.
  2. В открывшемся окне выберите вариант экспорта списка всех источников (форвардеров).
  3. Нажмите кнопку **Экспортировать**.

     Браузер загрузит текстовый файл со списком источников (форвардеров).

  Список всех источников (форвардеров) экспортирован в текстовый файл.

- Чтобы экспортировать список выбранных источников (форвардеров):

  1. На странице **Мониторинг источников** в центральной панели выберите строки с названиями источников (форвардеров).

     Примечание. Вы можете выбирать несколько строк подряд, нажимая клавишу Shift, или несколько отдельных строк, нажимая клавишу Ctrl.
  2. Нажмите кнопку **Экспортировать список**.
  3. В открывшемся окне выберите вариант экспорта выбранных источников (форвардеров).
  4. Нажмите кнопку **Экспортировать**.

     Браузер загрузит текстовый файл со списком источников (форвардеров).

  Список выбранных источников (форвардеров) экспортирован в текстовый файл.

6.9. Обновление списка источников (форвардеров)

Вы можете обновлять список источников (форвардеров) вручную или настраивать автоматическое обновление списка.

- Чтобы обновить список источников (форвардеров) вручную,

  в верхней правой части страницы **Мониторинг источников** нажмите .

- Чтобы настроить автоматическое обновление списка источников (форвардеров):

  1. В верхней правой части страницы **Мониторинг источников** нажмите .
  2. В открывшемся окне установите флажок **Автоматически обновлять** и выберите период обновления.

  Автоматическое обновление списка источников (форвардеров) настроено.

7. Мониторинг состояния MaxPatrol SIEM

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

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

В этом разделе

7.1. Страница «Управление системой»

Страница **Управление системой** предназначена для просмотра состояния лицензии, управления коллекторами сбора данных, а также для просмотра информации об используемой базе знаний по уязвимостям и обновления этой базы вручную.

В рабочей области страницы расположены центральная панель и панель **Компоненты**, в которой доступны следующие разделы.

О системе

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

Конвейеры

Раздел предназначен для просмотра подробной информации о конвейерах обработки событий, для их переименования и удаления. При выборе раздела в центральной панели отобразится таблица с конвейерами. Для каждого конвейера в таблице указаны статус, псевдоним, доменное имя и IP-адреса сервера MP SIEM Server, версии MP SIEM Server и установленной на нем схемы полей событий, семейство ОС сервера.

Вы можете сортировать список, нажимая на названия колонок таблицы, а также обновлять список с помощью значка в правой верхней части таблицы. При выборе конвейера подробная информация о нем появится в боковой панели, в том числе перечень подключенных к нему коллекторов.

Один из конвейеров является главным, поскольку через компонент MP SIEM Events Storage этого конвейера выполняются все запросы по фильтрации событий, в том числе хранящихся в других конвейерах (кросс-кластерный поиск). Слева от доменного имени сервера MP SIEM Server главного конвейера отображается значок .

В таблице отображаются следующие статусы конвейера:

— **Доступен** — конвейер работает в нормальном режиме;

— **Недоступен** — MP 10 Core не получает отклика от компонента MP SIEM Server конвейера.

В панели инструментов находятся следующие кнопки:

— **Переименовать** — для изменения псевдонима конвейера.

— **Удалить** — для удаления конвейера из списка.

Примечание. Невозможно удалить конвейер, к которому подключены коллекторы, а также единственный конвейер в списке.

Коллекторы

Раздел предназначен для просмотра подробной информации о коллекторах, для обновления их версий и удаления недоступных коллекторов. При выборе раздела в центральной панели отобразится таблица с коллекторами. Для каждого коллектора в таблице указаны название, версия, статус, роли, а также имя, IP-адреса и семейство ОС сервера.

Вы можете сортировать список, нажимая на названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая в правой верхней части таблицы. Для поиска коллектора в списке вы можете нажать и ввести в поле поиска параметр коллектора. При выборе коллектора система отображает подробную информацию о нем в боковой панели, в том числе перечень модулей коллектора.

В таблице отображаются следующие статусы коллектора:

— **Доступен** — коллектор работает в нормальном режиме;

— **С ограничениями** — коллектор работает в режиме ограниченной функциональности по причине нехватки свободного места на жестком диске;

— **Недоступен** — MP 10 Core не получает отклика от коллектора более 10 минут;

— **Обновляется** — коллектор обновляется;

— **Удаляется** — коллектор удаляется из списка.

В панели инструментов находятся следующие кнопки:

— **Удалить** — для удаления недоступного коллектора (см. раздел 7.2). Если после удаления коллектор начнет присылать данные, он снова будет отображаться в списке.

— **Обновить версию** — для обновления версии коллектора.

Обработка активов

Раздел предназначен для просмотра информации о работе служб MP 10 Core на различных этапах обработки данных об активах.

Для каждого этапа в таблице указаны название используемой службы, длина очереди, время ожидания обработки, номера пакетов в очереди, номера последних обработанных пакетов и средняя скорость обработки пакетов за 5 минут.

См. также

Удаление недоступного коллектора (см. раздел 7.2)

7.2. Удаление недоступного коллектора

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

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

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

► Чтобы удалить коллектор из списка:

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

   Откроется страница **Управление системой**.

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

   В рабочей области страницы отобразится таблица со списком коллекторов.

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

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

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

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

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

Коллектор удален из списка.

7.3. Мониторинг работы правил корреляции

MaxPatrol SIEM отслеживает объем оперативной памяти, занимаемой правилами корреляции, и количество срабатываний для каждого правила. На основании результатов мониторинга система приостанавливает работу правила корреляции в следующих случаях:

— Если все правила занимают более 95% от объема оперативной памяти, выделенной для их работы (по умолчанию 60 ГБ). В этом случае система начинает последовательно приостанавливать работу отдельных правил до тех пор, пока не освободится 20% от объема выделенной памяти.

— Если отдельное правило срабатывает слишком часто (по умолчанию более 300 раз за час).

Система автоматически не запускает приостановленные правила — их необходимо запускать вручную. Также приостановленные правила запустятся в случае перезапуска службы SIEM Server correlator.

Отдельные правила можно добавлять в список исключений. Система не приостанавливает работу этих правил, если они срабатывают слишком часто, и приостанавливает их работу в последнюю очередь, когда освобождает выделенную для работы правил оперативную память. Для включения правил в список исключений необходимо добавить их системные названия в текстовый файл (каждое название в отдельной строке) и указать путь к файлу в качестве значения параметра `ProtectedRulesPath`.

Вы можете изменять объем оперативной памяти, выделенной для работы правил корреляции (параметр `MonitoringOomMemoryLimit`), или вовсе отключить отслеживание объема оперативной памяти, занимаемой правилами (параметр `MonitoringOomEnabled`).

Также вы можете изменять период для подсчета количества срабатываний правил корреляции (параметр `MonitoringOvertriggerPeriod`), максимальное количество срабатываний за этот период, которое не приведет к остановке правила (параметр `MonitoringOvertriggerThreshold`), или вовсе отключить отслеживание количества срабатываний для всех правил (параметр `MonitoringOvertriggerEnabled`).

8. Сбор телеметрических данных

В MaxPatrol SIEM реализован сбор телеметрических данных о производительности микросервисов компонента MP 10 Core и действиях пользователя. Это необходимо для дальнейшего развития продукта и повышения качества экспертизы.

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

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

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

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

9. Резервное копирование данных

Вы можете создавать резервные копии данных компонентов MP 10 Core, PT MC, Knowledge Base и MP SIEM Server с помощью сценариев. Также вы можете создавать резервные копии индексов Elasticsearch. При создании резервной копии данных и при их последующем восстановлении из резервной копии должны совпадать конфигурации MaxPatrol SIEM, версии компонента MaxPatrol SIEM и языки интерфейса ОС.

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

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

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

В этом разделе

9.1. Создание резервной копии данных роли на Linux

- Чтобы создать резервную копию данных,

  запустите сценарий резервного копирования данных:

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

Например:

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

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

9.2. Создание резервной копии индексов Elasticsearch на Linux

Если в системе запущена задача архивации индексов по расписанию, перед созданием резервной копии необходимо ее остановить.

Для регистрации хранилища резервной копии индексов в Elasticsearch используется утилита `es_initrepo`, которую необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

- Чтобы создать резервную копию индексов Elasticsearch на Linux:

1. Укажите путь к каталогу для хранения резервной копии индексов:

   ```
   /opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу для хранения резервной копии индексов>"
   ```

   Внимание! Резервную копию индексов и копии индексов, создаваемые при архивации по расписанию, необходимо хранить в разных каталогах. Во избежание переполнения корневой файловой системы рекомендуется для хранения резервной копии смонтировать к каталогу отдельное дисковое устройство.

   Утилита `es_initrepo` зарегистрирует в Elasticsearch хранилище резервной копии индексов и свяжет его с указанным каталогом. После регистрации хранилища интерфейс терминала Linux выведет сообщение:

   ```
   Repository <Название хранилища> created successfully.
   ```

   Примечание. Команда также перезапустит службы Elasticsearch. После перезапуска Elasticsearch начнет восстанавливать индексы и будет некоторое время недоступен.

2. Создайте резервную копию индексов:

   - Если требуется выполнить резервное копирование индексов, созданных за определенный период, выполните команду:

     ```
     /opt/estools/bin/es_backup_tool -cmd backup -from <Дата начала периода> -to <Дата окончания периода> -host 127.0.0.1 -port 9200 -di false
     ```

     Примечание. Даты начала и окончания периода необходимо указывать в формате <День.Месяц.Год> (например, 27.03.2020).

   - Если требуется выполнить резервное копирование индексов, с момента создания которых прошло не меньше определенного количества дней, выполните команду:

     ```
     /opt/estools/bin/es_backup_tool -cmd backup -t <Количество дней> -host 127.0.0.1 -port 9200 -di false
     ```

     Примечание. Значение параметра `-t` должно быть больше нуля.

- Если требуется создать резервную копию всех индексов, выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd full_backup -host 127.0.0.1 -port 9200
  ```

  Утилита `es_backup_tool` сформирует из индексов, созданных системой за каждые сутки, отдельные файлы резервной копии. После создания каждого из этих файлов интерфейс терминала отобразит сообщение:

  ```
  snapshot_<Дата создания индексов> created successfully
  ```

Резервная копия индексов Elasticsearch на Linux создана.

Если задача архивации индексов по расписанию была остановлена, после создания резервной копии необходимо заново зарегистрировать хранилище архивных индексов и запустить задачу.

9.3. Создание резервной копии данных хранилища LogSpace

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

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

- Чтобы создать резервную копию данных,

  на сервере с ролью Event Storage выполните команду:

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

  Например:

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

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

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

9.4. О резервном копировании данных о площадках и их связях

После регистрации всех площадок и добавления необходимых связей рекомендуется создать резервную копию данных компонентов PT MC и MP 10 Core, расположенных на всех площадках. При последующих изменениях в схеме площадок (например, после регистрации новой площадки или добавления связей) рекомендуется создавать резервные копии данных компонентов PT MC и MP 10 Core, расположенных на главной площадке, на зарегистрированной площадке, а также на тех площадках, связи с которыми были изменены, удалены или добавлены.

10. Восстановление данных из резервной копии

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

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

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

В этом разделе

10.1. Восстановление данных компонентов MaxPatrol SIEM на Linux из резервной копии

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

Если при создании резервной копии компоненты MP SIEM Server и MP SIEM Events Storage находились на отдельных серверах, при восстановлении данных необходимо также выделить для этих компонентов отдельные серверы.

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

- Чтобы восстановить данные компонентов на Linux:

  1. Установите роль Deployer.
  2. Если при создании резервной копии компоненты MP SIEM Server и MP SIEM Events Storage были установлены на отдельных серверах, установите на серверы этих компонентов модули Salt Minion.
  3. Для каждой роли в следующей последовательности SqlStorage → Observability → Management and Configuration → Knowledge Base → RMQ Message Bus → Core → SIEM Storage → SIEM Server → Collector выполните сценарий:

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

     Например:

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

  4. Восстановите данные роли Deployer:

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

     Например:

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

  5. Для каждой роли в каталоге `/var/lib/deployer/role_instances/<Название роли>` в файле `instance.yaml` в качестве значения параметра `HostId` укажите идентификатор Salt Minion.
  6. Для каждой роли в каталоге `/var/lib/deployer/role_instances/<Название роли>` в файлах `params.yaml` и `params.default.yaml` в качестве значений параметров, содержащих FQDN, укажите FQDN серверов, на которые будут установлены соответствующие роли.

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

  7. Установите роль SqlStorage.
  8. Восстановите данные роли SqlStorage:

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

     Например:

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

  9. Установите роли Management and Configuration и Knowledge Base.
  10. Восстановите данные роли Knowledge Base:

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

  11. Установите роли RMQ Message Bus и Core.

12. Восстановите данные роли Core:

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

13. Установите роль SIEM Storage.

14. Установите роли RMQ Message Bus и SIEM Server.

15. Восстановите данные роли SIEM Server:

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

Данные компонентов восстановлены.

10.2. Восстановление индексов Elasticsearch из резервной копии на Linux

При восстановление индексов Elasticsearch из резервной копии на Linux вы можете восстановить как все индексы, так и индексы, созданные за определенный период.

> **Внимание!** Восстановление индексов, созданных за определенный период, возможно только на том сервере, где была создана резервная копия этих индексов.

Если в системе запущена задача архивации индексов по расписанию, перед восстановлением индексов из резервной копии необходимо ее остановить.

Для регистрации хранилища резервной копии индексов в Elasticsearch используется утилита `es_initrepo`, которую необходимо запускать в интерфейсе терминала от имени суперпользователя (root).

В этом разделе

Восстановление всех индексов Elasticsearch из резервной копии на Linux (см. раздел 10.2.1)

Восстановление индексов Elasticsearch, созданных за определенный период, из резервной копии на Linux (см. раздел 10.2.2)

10.2.1. Восстановление всех индексов Elasticsearch из резервной копии на Linux

- Чтобы восстановить индексы Elasticsearch из резервной копии на Linux:

  1. На сервере MP SIEM Server остановите службу SIEM Server storage и все службы Elasticsearch:

     ```
     systemctl stop -a elasticsearch* siemserver-storage.service
     ```

  2. Удалите каталог с индексами:

     ```
     rm -rf /<Путь к каталогу индексов>/*
     ```

3. Запустите все службы Elasticsearch:
   ```
   systemctl start -a elasticsearch*
   ```
4. Запустите службу SIEM Server storage для загрузки шаблона индекса:
   ```
   systemctl start siemserver-storage.service
   ```
5. Остановите службу SIEM Server storage:
   ```
   systemctl stop siemserver-storage.service
   ```
6. Укажите путь к каталогу с резервной копией индексов:
   ```
   /opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу с резервной копией индексов>"
   ```
   Утилита `es_initrepo` зарегистрирует в Elasticsearch хранилище резервной копии индексов и свяжет его с указанным каталогом. После регистрации хранилища интерфейс терминала Linux выведет сообщение:
   ```
   Repository <Название хранилища> created successfully.
   ```
   Примечание. Команда также перезапустит службы Elasticsearch. После перезапуска Elasticsearch начнет восстанавливать индексы и будет некоторое время недоступен.
7. Восстановите индексы из файла резервной копии:
   ```
   /opt/estools/bin/es_backup_tool -cmd full_restore
   ```
   После восстановления данных из файла интерфейс терминала отобразит сообщение:
   ```
   restored snapshot: snapshot_<Дата создания индексов>
   ```
8. Запустите службу SIEM Server storage:
   ```
   systemctl start siemserver-storage.service
   ```

Индексы Elasticsearch восстановлены из резервной копии на Linux.

Если задача архивации индексов по расписанию была остановлена, после восстановления данных из резервной копии необходимо заново зарегистрировать хранилище архивных индексов и запустить задачу.

10.2.2. Восстановление индексов Elasticsearch, созданных за определенный период, из резервной копии на Linux

- Чтобы восстановить индексы Elasticsearch, созданные за определенный период, из резервной копии на Linux:

  1. Укажите путь к каталогу с резервной копией индексов:
     ```
     /opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу с резервной копией индексов>"
     ```
     Утилита `es_initrepo` зарегистрирует в Elasticsearch хранилище резервной копии индексов и свяжет его с указанным каталогом. После регистрации хранилища интерфейс терминала Linux выведет сообщение:
     ```
     Repository <Название хранилища> created successfully.
     ```

Примечание. Команда также перезапустит службы Elasticsearch. После перезапуска Elasticsearch начнет восстанавливать индексы и будет некоторое время недоступен.

2. Восстановите индексы из файла резервной копии:

   ```
   /opt/estools/bin/es_backup_tool -cmd restore -host 127.0.0.1 -port 9200 -arc
   snapshot_<Дата создания индексов>
   ```

   После восстановления данных из файла интерфейс терминала отобразит сообщение:

   ```
   restored snapshot: snapshot_<Дата создания индексов>
   ```

   Примечание. При вводе команды вы можете использовать символы подстановки: звездочка (*) заменяет любое количество символов, вопросительный знак (?) — один отдельный символ.

Индексы Elasticsearch восстановлены из резервной копии на Linux.

Если задача архивации индексов по расписанию была остановлена, после восстановления данных из резервной копии необходимо заново зарегистрировать хранилище архивных индексов и запустить задачу.

10.3. Восстановление данных хранилища LogSpace из резервной копии

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

- Чтобы восстановить данные из резервной копии:

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

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

  2. На сервере с ролью Event Storage выполните команду:

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

     Например:

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

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

  Данные из резервной копии восстановлены.

10.4. О восстановлении резервной копии данных о площадках и их связях

Восстановление данных необходимо начинать с главной площадки. Данные остальных площадок можно восстанавливать в любом порядке.

Сервер, на котором будут восстановлены данные PT MC, должен иметь такое же доменное имя (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 TCP-порт 8703 для входящих соединений, по окончании восстановления открыть этот порт.

11. Индексы Elasticsearch: ротация, архивация, перемещение, удаление, использование политик ILM

Индексы Elasticsearch хранят информацию о событиях информационной безопасности. При продолжительной обработке событий, а также при расширении IT-инфраструктуры предприятия (увеличении количества активов и потока событий от них) имеющееся свободное место на жестких дисках сервера MP SIEM Events Storage будет уменьшаться, что может привести к необходимости подключения новых жестких дисков или отдельной системы хранения данных. С помощью утилит, устанавливаемых при развертывании системы, вы можете:

— просматривать список индексов;

— настраивать ротацию индексов;

— архивировать индексы по расписанию и восстанавливать их из архива;

— удалять архивные индексы по расписанию;

— удалять индексы без архивации.

Также вы можете перемещать индексы в новое хранилище. Утилиты для просмотра, ротации, архивации и удаления индексов находятся на сервере MP SIEM Events Storage.

Если MP SIEM Events Storage установлен на Linux, указанные в инструкциях команды необходимо выполнять в интерфейсе терминала от имени суперпользователя (root).

Ротация

Максимальный объем дискового пространства, выделяемый для хранения индексов, автоматически вычисляется при установке и обновлении компонента MP SIEM Events Storage и равен 92% от общего объема дискового пространства. По умолчанию срок хранения индексов — 365 дней. Утилита ротации `tailcutter` автоматически запускается каждые 30 минут и при превышении этих значений удаляет старые индексы. Вы можете изменить максимальный объем дискового пространства, выделяемый для хранения индексов, и срок их хранения.

> **Примечание.** Если ранее для ротации индексов вы создавали задачи для их архивации и последующего удаления по расписанию, необходимо удалить эти задачи и настроить ротацию индексов с помощью утилиты.

Архивация и удаление

Утилита `es_backup_tool` создает из исходных индексов архивные, сохраняет их в отдельное хранилище, а исходные индексы удаляет из Elasticsearch. Архивные индексы не используются системой, но при необходимости могут быть восстановлены в любой момент. Кроме того, утилита может удалять ставшие ненужными архивные индексы, удалять исходные индексы без архивации.

Вы можете настроить расписание запуска утилиты `es_backup_tool` с помощью планировщика заданий и указать количество дней с момента создания индекса до его архивации и удаления. Архивация индексов создает дополнительную нагрузку на Elasticsearch, поэтому ее рекомендуется выполнять в период наименьшей нагрузки на систему. Перед созданием задачи для архивации индексов необходимо создать хранилище архивных индексов.

Перемещение

Перемещение индексов может потребоваться в случае нехватки свободного места на жестких дисках сервера MP SIEM Events Storage и, как следствие, подключения новых жестких дисков или отдельной системы хранения данных.

Использование политик ILM

В сверхнагруженной конфигурации индексы Elasticsearch необходимо хранить на двух типах накопителей данных — жестких дисках и твердотельных накопителях. Объем твердотельных накопителей позволяет хранить индексы хранилища в горячей стадии от нескольких дней до недели. Затем индексы автоматически переходят в теплую стадию и хранятся на жестких дисках. Для разделения индексов на разные типы накопителей в хранилище событий Elasticsearch используются политики ILM.

Настройка политик ILM происходит автоматически после установки системы и запуска компонента MP SIEM Events Storage. После настройки политик необходимо перезапустить службу SIEM server storage с помощью команды `systemctl restart siemserver-storage`.

> **Примечание.** Время хранения индексов автоматически определяется из расчета 1 час на каждые 250 ГБ. Для горячей стадии учитывается только объем твердотельных накопителей.

Рекомендуется проверить значения параметров политики ILM после переустановки или обновления системы. Для смены или восстановления значений параметров необходимо внести изменения в файл политик `/var/lib/storage/siem_*_policy.json` по образцу из файла `/var/lib/storage/siem_*_policy.json.expample`. После сохранения файла необходимо перезапустить службу SIEM server storage.

В этом разделе

Просмотр списка индексов (см. раздел 11.1)

Настройка ротации индексов (см. раздел 11.2)

Архивация индексов (см. раздел 11.3)

11.1. Просмотр списка индексов

- Чтобы просмотреть список индексов, используемых системой,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd listindex
  ```

- Чтобы просмотреть список архивных индексов,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd listarchive
  ```

11.2. Настройка ротации индексов

Вы можете изменять срок хранения индексов для событий (параметр `TailcutterTtl`) и для счетчиков событий (параметр `TailcutterTtlc`), а также максимальный объем дискового пространства, выделяемый для хранения всех индексов (параметр `TailcutterDbspace`).

11.3. Архивация индексов

Вы можете запускать архивацию индексов вручную или настроить архивацию по расписанию. Перед архивацией индексов необходимо создать для них хранилище.

В этом разделе

11.3.1. Создание хранилища для архивных индексов

- Чтобы создать хранилище для архивных индексов,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/estools/bin/es_initrepo --host 127.0.0.1 --port 9200 --repopath "<Путь к каталогу для хранения архивных индексов>"
  ```

  По завершении создания хранилища появится сообщение:

  ```
  Repository ptsiem_backup created successfully.
  ```

11.3.2. Архивация индексов на Linux

- Чтобы архивировать индексы, созданные за определенный период,

  выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd backup -from <Дата начала периода> -to <Дата окончания периода>
  ```

  Примечание. Даты начала и окончания периода необходимо указывать в формате <День.Месяц.Год> (например, 27.03.2020).

- Чтобы архивировать индексы, с момента создания которых прошло не меньше определенного количества дней,

  выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd backup -t <Количество дней>
  ```

11.3.3. Архивация индексов по расписанию

- Чтобы настроить архивацию индексов по расписанию,

  в планировщике заданий cron на Linux создайте задачу:

  ```
  <Расписание> /opt/estools/bin/es_backup_tool -cmd backup -t <Дней до архивации> >> /opt/estools/log/es_backup.log
  ```

  где:

  <Дней до архивации> — количество дней с момента создания индекса до его архивации;

  <Расписание> — периодичность запуска утилиты с помощью планировщика заданий.

  Примечание. Описание планировщика заданий cron на Debian (параметров команды `crontab`) приведено на сайте debian.org.

Например, для запуска еженедельной (в каждое воскресенье в 1 час 30 минут) архивации индексов, с момента создания которых прошло 30 дней, необходимо в планировщике заданий cron на Linux создать задачу:

```
30 1 * * 7 /opt/estools/bin/es_backup_tool -cmd backup -t 30 >> /opt/estools/log/es_backup.log
```

11.4. Восстановление индекса из архива

- Чтобы восстановить индекс из архива,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/estools/bin/es_backup_tool.sh -cmd restore -arc snapshot_<Дата архивации индекса>
  ```

  Примечание. При вводе команды вы можете использовать символы подстановки: звездочка (*) заменяет любое количество символов, вопросительный знак (?) — один отдельный символ.

11.5. Удаление архивных индексов

Вы можете удалять архивные индексы вручную или настроить их удаление по расписанию.

В этом разделе

11.5.1. Удаление архивных индексов на Linux

- Чтобы удалить архивные индексы, созданные за определенный период,

  выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd cleanarchive -from <Дата начала периода> -to <Дата окончания периода>
  ```

  Примечание. Даты начала и окончания периода необходимо указывать в формате <День.Месяц.Год> (например, 27.03.2020).

- Чтобы удалить архивные индексы, с момента создания которых прошло не меньше определенного количества дней,

  выполните команду:

  ```
  /opt/estools/bin/es_backup_tool -cmd cleanarchive -t <Количество дней>
  ```

11.5.2. Удаление архивных индексов по расписанию

- Чтобы настроить удаление архивных индексов по расписанию,

  в планировщике заданий cron на Linux создайте задачу:

  ```
  <Расписание> /opt/estools/bin/es_backup_tool -cmd cleanarchive -t <Дней до удаления> >> /opt/estools/log/es_backup.log
  ```

  где:

  <Дней до удаления> — количество дней с момента создания индекса до его удаления;

  <Расписание> — периодичность запуска утилиты с помощью планировщика заданий.

  Примечание. Описание планировщика заданий cron на Debian (параметров команды `crontab`) представлено на сайте debian.org.

Например, для запуска еженедельного (в каждое воскресенье в 2 часа 30 минут) удаления индексов, с момента создания которых прошло 100 дней, необходимо в планировщике заданий cron на Linux создать задачу:

```
30 2 * * 7 /opt/estools/bin/es_backup_tool -cmd cleanarchive -t 100 >> /opt/estools/log/es_backup.log
```

11.6. Удаление индекса без архивации

- Чтобы удалить индекс,

  в интерфейсе терминала Linux выполните команду:

  - если MaxPatrol SIEM развернут в конфигурации для средненагруженных или высоконагруженных систем:
    ```
    /opt/estools/bin/es_backup_tool -cmd deleteindex --index <Тип индекса>_<Дата создания>
    ```
  - если для сверхнагруженных:
    ```
    /opt/estools/bin/es_backup_tool -cmd deleteindex --index <Тип индекса>_<Дата создания>*
    ```

    Примечание. При вводе команды вы можете использовать символы подстановки: звездочка (*) заменяет любое количество символов, вопросительный знак (?) — один отдельный символ.

11.7. Перемещение индексов на Linux

- Чтобы переместить индексы:

  1. Остановите все задачи сканирования сети и сбора данных.
  2. На сервере MP SIEM Server остановите службу SIEM Server storage:
     ```
     systemctl stop siemserver-storage
     ```
  3. На сервере MP SIEM Events Storage остановите все службы Elasticsearch:
     ```
     systemctl stop elasticsearch_*
     ```
  4. Переместите все файлы из каталога с индексами Elasticsearch в каталог нового хранилища, например:
     ```
     mv <Путь к каталогу с индексами Elasticsearch>/* <Путь к каталогу нового хранилища>
     ```

     Например:
     ```
     mv /data/* /storage/
     ```
  5. На сервере с установленной ролью Deployer запустите сценарий:
     ```
     /var/lib/deployer/role_packages/pt_SiemStorage_<Номер версии>/install.sh
     ```
  6. В открывшемся окне нажмите кнопку **Yes**.
  7. В открывшемся окне выберите вариант с идентификатором приложения MaxPatrol 10.
  8. В открывшемся окне выберите вариант с названием экземпляра роли SIEM Storage.

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

     Откроется страница со списком параметров.
  10. Измените значение параметра `PathData`:
      ```
      PathData: <Путь к каталогу нового хранилища>
      ```

11. Нажмите кнопку **OK**.

    По завершении изменения конфигурации появится сообщение `Deployment configuration successfully applied`.

12. Нажмите кнопку **OK**.
13. На сервере MP SIEM Server запустите службу SIEM Server storage:

    ```
    systemctl start siemserver-storage
    ```

14. На сервере MP SIEM Events Storage запустите все службы Elasticsearch:

    ```
    systemctl --all start elasticsearch_*
    ```

15. Запустите остановленные задачи.

Индексы перемещены.

12. Разделы LogSpace: ротация, резервное копирование и восстановление

Данные в хранилище LogSpace разбиты на разделы. Каждый раздел хранит информацию о событиях информационной безопасности за одни сутки. Для работы с разделами хранилища вы можете использовать набор утилит dbtools, который устанавливается вместе с ролью Event Storage и включает в себя утилиты backup_tool и tailcutter.

Ротация

Максимальный объем дискового пространства, выделяемый для хранения разделов, автоматически вычисляется при установке и обновлении роли Event Storage и равен 92% от общего объема дискового пространства. По умолчанию срок хранения разделов — 365 дней. Утилита ротации tailcutter удаляет из хранилища разделы, срок хранения или размер которых превышает значения, указанные в конфигурационных параметрах (см. приложение А) `TailcutterTtl`, `TailcutterTtlc` и `TailcutterDbspace` роли Event Storage. По умолчанию утилита запускается с помощью планировщика cron один раз в 30 минут. Задача на запуск создается в cron автоматически при установке утилиты. После запуска утилита сначала удаляет разделы таблицы events, срок хранения которых превышает значение параметра `TailcutterTtl`, затем удаляет разделы таблицы counters, срок хранения которых превышает значение параметра `TailcutterTtlc`. Далее утилита проверяет наличие свободного дискового пространства и, в случае превышения разделами объема, указанного в параметре `TailcutterDbspace`, удаляет самые старые разделы из таблиц events и counters. Утилита удаляет старые разделы до тех пор, пока занимаемый ими объем не станет меньше значения параметра `TailcutterDbspace`.

После установки утилита tailcutter хранится в каталоге `/opt/dbtools/bin/tailcutter`. Вы можете настроить ее параметры, изменяя конфигурацию роли Event Storage согласно инструкции (см. раздел 15.1) или используя соответствующие ключи при запуске утилиты из командной строки.

Таблица 2. Ключи для запуска утилиты tailcutter

Ключ	Описание	Значение по умолчанию
`--help`	Вывод справочной информации о ключах, с которыми можно запускать утилиту tailcutter	—
`--database <Название базы данных>`	Название базы данных	`siem`
`--dbspace <Объем дискового пространства в процентах или гигабайтах>`	Максимальный объем дискового пространства, выделяемый для разделов хранилища. Обязательный ключ	`92%`

Ключ	Описание	Значение по умолчанию
`--ttl <Количество дней>`	Срок хранения разделов таблицы events. Обязательный ключ	`365`
`--ttlc <Количество дней>`	Срок хранения разделов таблицы counters. Если значение ключа не указано, оно принимается равным значению ключа `--ttl`	`5`
`--log <Путь к файлу журнала>`	Путь к файлу журнала утилиты tailcutter	`/opt/dbtools/log/tailcutter.log`
`--loglevel <Уровень журналирования>`	Уровень журналирования событий утилиты tailcutter. Возможные значения — `DEBUG`, `INFO`, `WARNING`, `ERROR` или `CRITICAL`	`INFO`

Резервное копирование и восстановление

Утилита backup_tool предназначена для резервного копирования (см. раздел 9.3) и восстановления (см. раздел 10.3) данных хранилища LogSpace. Кроме того, утилита может удалять разделы и показывать списки существующих разделов и архивов хранилища.

После установки утилита хранится в каталоге `/opt/dbtools/bin`. Вы можете настроить ее параметры, используя соответствующие ключи при запуске утилиты из командной строки.

Таблица 3. Ключи для запуска утилиты backup_tool

Ключ	Описание	Значение по умолчанию
`--help`	Вывод справочной информации о ключах, с которыми можно запускать утилиту backup_tool	—
`--database <Название базы данных>`	Название базы данных	`siem`
`--database_type <Тип базы данных>`	Тип хранилища	`logspace`
`-repopath <Путь к каталогу>`	Путь к каталогу для сохранения резервной копии данных хранилища	`/db_backup`
`--log <Имя файла>`	Путь к файлу журнала утилиты backup_tool	`tailcutter.log`

Ключ	Описание	Значение по умолчанию
`--loglevel <Уровень журналирования>`	Уровень журналирования событий утилиты backup_tool. Возможные значения — `DEBUG`, `INFO`, `WARNING`, `ERROR` или `CRITICAL`	`INFO`
`--time`	Допустимый срок хранения разделов, в днях. Разделы, срок хранения которых превышает указанное в ключе значение, будут удалены	—
`--part <Название раздела>`	Название раздела, который необходимо удалить с помощью команды `deletepart`	—
`--from`	Начало периода, за который необходимо удалить архивы, в формате ГГГГММДД	—
`--to`	Окончание периода, за который необходимо удалить архивы, в формате ГГГГММДД	—
`--cmd deletepart`	Команда для удаления раздела. Название раздела необходимо указать после команды с помощью ключа `--part`	—
`--cmd listpart`	Вывод списка разделов хранилища	—
`--cmd listarchive`	Вывод списка архивов хранилища	—
`--cmd cleanarchive`	Удаление архивов хранилища. После команды необходимо указать в днях срок хранения, при превышении которого необходимо удалять архивы (с помощью ключа `--time`), или период, за который необходимо удалить архивы (с помощью ключей `--from` и `--to`)	—

В этом разделе

Просмотр списков разделов и архивов LogSpace (см. раздел 12.1)

Удаление разделов и архивов LogSpace (см. раздел 12.2)

12.1. Просмотр списков разделов и архивов LogSpace

- Чтобы просмотреть список разделов хранилища LogSpace,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/dbtools/bin/backup_tool --cmd listpart
  ```

- Чтобы просмотреть список архивов хранилища LogSpace,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/dbtools/bin/backup_tool --cmd listarchive
  ```

12.2. Удаление разделов и архивов LogSpace

- Чтобы удалить раздел хранилища LogSpace,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/dbtools/bin/backup_tool --cmd deletepart --part <Название раздела>
  ```

- Чтобы удалить архивы, которые хранятся дольше определенного количества дней,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/dbtools/bin/backup_tool --cmd cleanarchive --time <Количество дней>
  ```

- Чтобы удалить архивы хранилища LogSpace за определенный период времени,

  в интерфейсе терминала Linux выполните команду:

  ```
  /opt/dbtools/bin/backup_tool --cmd cleanarchive --from <Нижняя граница периода в формате
  ГГГГММДД> --to <Верхняя граница периода в формате ГГГГММДД>
  ```

13. Смена паролей служебных учетных записей

Для выполнения своих функций компоненты MaxPatrol SIEM 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 SIEM логины и пароли служебных учетных записей устанавливаются в значения по умолчанию.

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

В этом разделе

13.1. Смена пароля служебной учетной записи в PostgreSQL

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

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

  1. На сервере с установленной ролью SqlStorage выполните команду:

     ```
     docker exec -it $(docker ps | awk '/storage-postgres/ {print $NF}') psql -U pt_system -d postgres -c "ALTER USER pt_system WITH PASSWORD '<Новый пароль>'"
     ```

  2. Измените конфигурацию роли SqlStorage:

     ```
     PgPassword: <Новый пароль>
     ```

  3. Измените конфигурации ролей Management and Configuration, Knowledge Base и Core:

     ```
     PostgrePassword: <Новый пароль>
     ```

  Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 15.1.2)

13.2. Смена паролей служебных учетных записей в RabbitMQ

> **Внимание!** Приведенные ниже инструкции не предназначены для смены паролей служебных учетных записей компонентов MP SIEM Server и MP 10 Collector, установленных на одном сервере («SIEM на коллекторе»).

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

В конфигурации для низконагруженных систем используется только один брокер RabbitMQ. В конфигурациях для средненагруженных, высоконагруженных и сверхнагруженных систем используется два брокера RabbitMQ. Один из них устанавливается на сервер MP 10 Core и обеспечивает обмен данными между службами всех компонентов MaxPatrol SIEM, другой — на сервер MP SIEM Server и обеспечивает обмен данными только между его службами.

В этом разделе

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Core на Linux (см. раздел 13.2.1)

RabbitMQ: смена паролей служебных учетных записей компонента MP SIEM Server на Linux (см. раздел 13.2.2)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Microsoft Windows (см. раздел 13.2.3)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Linux (см. раздел 13.2.4)

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

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

- Чтобы сменить пароль служебной учетной записи MP 10 Core:

  1. На сервере MP 10 Core измените конфигурации (см. раздел 15.1.2) ролей Core и RMQ Message Bus:

     ```
     RMQPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

     Пароль изменен.

13.2.2. RabbitMQ: смена паролей служебных учетных записей компонента MP SIEM Server на Linux

Компонент MP SIEM Server на Linux для работы в RabbitMQ использует две служебных учетных записи. Одна запись предназначена для доступа к RabbitMQ, установленному на сервер MP 10 Core, другая — для доступа к RabbitMQ, установленному на сервер MP SIEM Server. По умолчанию обе учетных записи имеют одинаковый логин `siem` и пароль `P@ssw0rd`.

Порядок действий по смене паролей зависит от конфигурации MaxPatrol SIEM и от операционных систем серверов MP SIEM Server и MP 10 Core.

В этом разделе

Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на один сервер (см. раздел 13.2.2.1)

Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на разные серверы (см. раздел 13.2.2.2)

13.2.2.1. Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на один сервер

Если компоненты MP SIEM Server и MP 10 Core установлены на Linux на один сервер, обе учетных записи используются для доступа к одному и тому же брокеру RabbitMQ и по умолчанию имеют одинаковый логин.

- Чтобы сменить пароли служебных учетных записей MP SIEM Server:

  1. На сервере MP 10 Core измените конфигурации ролей Core и RMQ Message Bus:
     ```
     RMQSiemPassword: <Новый пароль>
     ```
  2. Перезапустите Docker-контейнер роли RMQ Message Bus:
     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
     docker-compose down
     docker-compose up -d
     ```
  3. Измените конфигурацию роли SIEM Server:
     ```
     GlobalRabbitPassword: <Новый пароль>
     RMQPassword: <Новый пароль>
     ```

  Пароли изменены.

См. также

Изменение конфигурации роли (см. раздел 15.1.2)

13.2.2.2. Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на разные серверы

Если компоненты MP SIEM Server и MP 10 Core установлены на разные серверы, одна учетная запись используется для доступа к RabbitMQ, установленному на сервер MP 10 Core, другая — для доступа к RabbitMQ, установленному на сервер MP SIEM Server.

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

  1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере MP 10 Core:

     ```
     RMQSiemPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

  3. Измените конфигурацию роли SIEM Server:

     ```
     RMQPassword: <Новый пароль>
     ```

  Пароль изменен.

- Чтобы сменить пароль служебной учетной записи для подключения к RabbitMQ, установленному на сервер MP SIEM Server:

  1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере MP SIEM Server:

     ```
     RMQSiemPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

  3. Измените конфигурацию роли SIEM Server:

     ```
     GlobalRabbitPassword: <Новый пароль>
     ```

  4. Если компонент MP 10 Core установлен на Linux, измените конфигурацию роли Core:

     ```
     RMQSiemPassword: <Новый пароль>
     ```

  Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 15.1.2)

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

По умолчанию логин служебной учетной записи компонента MP 10 Collector на Microsoft Windows для доступа к RabbitMQ — `mpx_agent`, пароль — `P@ssw0rd`.

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

  1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере MP 10 Core:

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

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

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

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

  Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 15.1.2)

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

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

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

  1. Измените конфигурацию роли RMQ Message Bus, установленной на сервере MP 10 Core:

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

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

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

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

  Пароль изменен.

См. также

Изменение конфигурации роли (см. раздел 15.1.2)

14. Настройка журналирования работы MaxPatrol SIEM

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

В этом разделе

14.1. Настройка журналирования работы компонента MP 10 Core на Linux

Настройка выполняется отдельно для каждой службы компонента.

- Чтобы настроить журналирование:

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

     ```
     Logging_Threshold=<Уровень журналирования>
     ```

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

  2. Выполните команды:

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

  Журналирование настроено.

14.2. Настройка журналирования работы компонента MP SIEM Server

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию служба SIEM Server health monitor записывает в журнал сообщения уровня `debug`, все остальные службы — уровня `info`. Размер каждого файла журнала ограничен 100 МБ, каждая служба хранит последние 10 таких файлов.

Файл `siem.conf`, используемый для настройки журналирования, находится на сервере MP SIEM Server в каталоге `/opt/mpxsiem/etc`.

- Чтобы настроить журналирование:

  1. В файле `siem.conf` в секции `<Название службы>` → `logger` измените значения параметров:

     `"level": <Уровень журналирования>`

     Примечание. Возможные значения `fatal`, `error`, `warning`, `info`, `debug` и `trace`.

     `"nfiles": <Максимальное количество сохраняемых файлов журналов>`

     `"size_limit": <Максимальный размер файла журнала (в байтах)>`

     Примечание. Если требуется сохранять записи обо всех событиях, произошедших за сутки, в один файл журнала, необходимо указать значение параметра `size_limit` равным нулю.

  2. В интерфейсе терминала от имени суперпользователя (root) выполните команду для перезапуска службы, параметры журналирования которой были изменены:

     `systemctl siemserver-<Название службы>.service restart`

  Журналирование настроено.

14.3. Настройка журналирования работы компонента MP SIEM Events Storage

Вы можете настраивать уровень журналирования и параметры ротации файлов журнала. По умолчанию в журнал записываются события уровня `debug`, размер каждого файла журнала ограничен 128 МБ на Linux, общий объем файлов журналов для каждого узла Elasticsearch ограничен 2 ГБ.

Для настройки журналирования вам потребуется файл `log4j2.properties`, который находится на сервере MP SIEM Events Storage в каталоге `/etc/elasticsearch/<Имя узла Elasticsearch>`.

- Чтобы настроить журналирование:

  1. В файле `log4j2.properties` измените значения параметров:

     `logger.action.level = <Уровень журналирования>`

     Примечание. Возможные значения `off`, `error`, `warn`, `info`, `debug`, `trace` и `all`.

     `appender.rolling.policies.size.size = <Максимальный размер файла журнала (в мегабайтах)>MB`

     `appender.rolling.strategy.action.condition.nested_condition.exceeds = <Максимальный общий объем файлов журналов для каждого узла Elasticsearch (в гигабайтах)>GB`

  2. В интерфейсе терминала от имени суперпользователя (root) выполните команду для перезапуска службы Elasticsearch:

     `systemctl --all restart elastic*service`

  Журналирование настроено.

14.4. Настройка журналирования работы компонента MP 10 Collector на Microsoft Windows

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

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

- Чтобы настроить журналирование:

  1. В файле `agent.log.xml` измените значение атрибута `level` параметра `config` → `root`:

     ```
     <Название журналируемого компонента коллектора> level="<Уровень журналирования>"
     ```

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

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

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

  3. Перезапустите службу Core Agent.

  Журналирование настроено.

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

15. Просмотр и изменение параметров конфигурации MaxPatrol SIEM

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

В этом разделе

15.1. Просмотр и изменение конфигурации компонентов MaxPatrol SIEM на Linux

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

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

В этом разделе

См. также

15.1.1. Просмотр конфигурации роли

- Чтобы просмотреть конфигурацию роли:

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

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

     Откроется страница со списком параметров (см. приложение А).
  6. По завершении просмотра нажмите кнопку **Cancel**.
  7. В окне для выбора набора параметров нажмите кнопку **Cancel**.

15.1.2. Изменение конфигурации роли

- Чтобы изменить конфигурацию роли:

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

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

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

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

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

Конфигурация роли изменена.

15.1.3. Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch

- Чтобы изменить объем оперативной памяти:

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

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

   Откроется страница со списком параметров (см. приложение А).
6. Измените значение параметра **ClusterConfigurationProfile** на **Manual**.
7. В качестве значений параметров **MasterNodeHeapSize**, **ClientNodeHeapSize** и **DataNodeHeapSize** введите объем оперативной памяти, выделяемый для главного узла, клиентского узла и узла данных соответственно.

   Примечание. Минимальное значение параметров `MasterNodeHeapSize` и `ClientNodeHeapSize` — 2 ГБ, параметра `DataNodeHeapSize` — 8 ГБ. Суммарный объем оперативной памяти всех узлов кластера, умноженный на коэффициент 1,7, не должен превышать объем оперативной памяти сервера MP SIEM Events Storage.
8. Нажмите кнопку **OK**.
9. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

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

Объем оперативной памяти изменен.

15.1.4. Изменение степени сжатия данных в Elasticsearch

Elasticsearch позволяет изменять степень сжатия сохраняемых данных за счет использования одного из алгоритмов — LZ4 (по умолчанию) или DEFLATE.

- Чтобы выбрать алгоритм сжатия данных:

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

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

     Откроется страница со списком параметров (см. приложение А).
  6. Измените значение параметра **ElasticsearchCompression**:
     - Если вы хотите использовать для сжатия сохраняемых данных алгоритм LZ4, выберите значение **default**.
     - Если вы хотите использовать для сжатия сохраняемых данных алгоритм DEFLATE, выберите значение **best_compression**.
  7. Нажмите кнопку **OK**.
  8. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

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

  Алгоритм сжатия данных выбран и будет применен к новым индексам.

15.1.5. Регистрация событий при нарушении и восстановлении параметров источников

- Чтобы включить регистрацию событий при нарушении и восстановлении параметров источников:

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

4. В открывшемся окне выберите вариант с названием экземпляра роли.

   Откроется окно для выбора набора параметров.

5. Выберите вариант **Advanced configuration**.

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

6. Установите флажок **SendAlertsToSiem**.
7. Нажмите кнопку **OK**.
8. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

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

9. Нажмите кнопку **OK**.

Регистрация событий при нарушении и восстановлении параметров источников включена.

15.1.6. Настройка SMTP-сервера для отправки уведомлений по электронной почте

Уведомления MaxPatrol SIEM содержат информацию об изменениях в IT-инфраструктуре предприятия, о работе задач сбора данных, собираемых событиях и параметрах потока событий, а также о выявляемых инцидентах ИБ и состоянии системы. Вы можете настроить отправку уведомлений по электронной почте, указав при создании задачи адреса получателей уведомления. Подробнее о создании задач для отправки уведомлений см. Руководство оператора. Перед созданием задачи необходимо настроить SMTP-сервер.

► Чтобы настроить SMTP-сервер для отправки уведомлений по электронной почте:

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

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

2. Запустите сценарий:

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

3. В открывшемся окне нажмите кнопку **Yes**.
4. В открывшемся окне выберите вариант с идентификатором приложения роли.
5. В открывшемся окне выберите вариант с названием экземпляра роли.

   Откроется окно для выбора набора параметров.

6. Выберите вариант **Advanced configuration**.

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

7. Укажите значения параметров:

   ```
   SmtpHost: <IP-адрес или FQDN SMTP-сервера>
   SmtpPassword: <Пароль служебной учетной записи для подключения MP 10 Core к SMTP-серверу>
   SmtpPort: <Порт SMTP-сервера для входящих подключений от MP 10 Core>
   SmtpSender: <Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте>
   SmtpUser: <Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу>
   ```

   Примечание. Для публичных почтовых сервисов значения параметров `SmtpSender` и `SmtpUser` должны совпадать.

8. Если необходима проверка валидности сертификата при подключении к SMTP-серверу, в качестве значения параметра `SmtpIgnoreCertificateValidation` выберите `True`.

9. В качестве значения параметра `SmtpSecureSocketOptions` выберите вариант шифрования при подключении к SMTP-серверу.

10. Нажмите кнопку **OK**.

11. В открывшемся окне нажмите кнопку **Submit**, чтобы подтвердить новые значения параметров.

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

12. Нажмите кнопку **OK**.

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

SMTP-сервер настроен.

16. Отключение отправки ненормализованных событий облегченной версией компонента MP SIEM Server («SIEM на коллекторе»)

По умолчанию компонент MP SIEM Server, установленный на сервере MP 10 Collector, отправляет в основной MP SIEM Server как нормализованные, так и ненормализованные события. Если требуется, вы можете отключить отправку ненормализованных событий.

- Чтобы отключить отправку ненормализованных событий:

  1. В конфигурационном файле измените значение параметра `normalizer` → `store_unnormalized_raw`:

     - Если облегченная версия компонента установлена на сервере Microsoft Windows, в конфигурационном файле `C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\config\siem.conf` облегченной версии MP SIEM Server измените значение параметра `normalizer` → `store_unnormalized_raw`:

       ```
       "store_unnormalized_raw": false
       ```

     - Если облегченная версия компонента MP SIEM Server установлена на сервере Linux, в конфигурационном файле `/opt/siem/etc/siem.conf` измените значение параметра `normalizer` → `store_unnormalized_raw`:

       ```
       "store_unnormalized_raw": false
       ```

  2. Перезапустите службу SIEM Server normalizer облегченной версии MP SIEM Server:

     - Если компонент установлен на Microsoft Windows, используйте для перезапуска стандартные средства операционной системы.
     - Если компонент установлен на Linux, используйте для перезапуска команду `systemctl restart siemserver-normalizer.service`.

  Отправка ненормализованных событий отключена.

17. Настройка обогащения событий данными геолокации

MaxPatrol SIEM поддерживает обогащение событий данными из базы MaxMind GeoIP для определения местоположения узлов по их IP-адресу.

► Чтобы настроить обогащение событий данными геолокации:

1. Скопируйте файлы базы данных MaxMind GeoIP на сервер MP SIEM Server.
2. На сервере с установленной ролью Deployer распакуйте архив `pt_SiemServer_<Номер версии>.tar.gz` из комплекта поставки:
3. Запустите сценарий:

   `pt_SIEM Server_<Номер версии>/install.sh`
4. В открывшемся окне нажмите кнопку **Yes**.
5. В открывшемся окне нажмите кнопку **Yes**.
6. В открывшемся окне выберите вариант с названием экземпляра роли.

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

   Откроется страница со списком параметров (см. приложение А).
8. В параметре `GeoIPDBPathASN` укажите путь к файлу `GeoLite2-ASN.mmdb` на сервере MP SIEM Server.
9. В параметре `GeoIPDBPathCity` укажите путь к файлу `GeoLite2-City.mmdb` на сервере MP SIEM Server.
10. Установите флажок **GeoIPEnable**.
11. Если требуется, измените параметры обогащения событий данными геолокации.
12. Нажмите кнопку **OK**.

    Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
13. Нажмите кнопку **OK**.
14. Если требуется, исключите подсети из обогащения данными геолокации, добавив их IP-адреса в конфигурационный файл `siem.conf` в раздел `exclude_ip`.

Внимание! Перечень исключенных подсетей сбрасывается до значений, установленных по умолчанию, после каждого запуска сценария `install.sh`.

15. Если в конфигурационный файл `siem.conf` были внесены изменения, выполните команду:

    ```
    systemctl restart siemserver-enricher.service
    ```

Обогащение событий данными геолокации настроено.

Таблица 4. Параметры обогащения событий данными геолокации

Параметр	Описание
`GeoIPFieldDstASN`	Заполнять ли поля с номером автономной системы (ASN) узла назначения
`GeoIPFieldDstCity`	Формат данных о городе узла назначения. Может принимать значения `en`, `ru`, `skip`
`GeoIPFieldDstCountry`	Формат данных о стране узла назначения. Может принимать значения `en`, `ru`, `iso`, `skip`
`GeoIPFieldDstOrg`	Формат данных об организации узла назначения. Может принимать значения `en`, `skip`
`GeoIPFieldSrcASN`	Заполнять ли поля с номером автономной системы (ASN) узла-источника
`GeoIPFieldSrcCity`	Формат данных о городе узла-источника. Может принимать значения `en`, `ru`, `skip`
`GeoIPFieldSrcCountry`	Формат данных о стране узла-источника. Может принимать значения `en`, `ru`, `iso`, `skip`
`GeoIPFieldSrcOrg`	Формат данных об организации узла-источника. Может принимать значения `en`, `skip`
`GeoIPRewriteData`	Заменять ли содержимое предзаполненных полей события с данными геолокации на данные MaxMind GeoIP

18. Пользовательские поля в модели актива

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

После добавления полей и ввода их значений пользователи системы смогут:

— просматривать значения добавленных полей в карточке и миникарточке актива;

— вводить поисковые запросы с учетом добавленных полей;

— осуществлять выборку, группировку и отбор по значениям добавленных полей (PDQL-запрос).

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

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

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

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

В этом разделе

18.1. Добавление пользовательских полей в модель актива

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

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

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

► Чтобы добавить пользовательские поля в модель актива:

1. В файле `UserModel.xml` в качестве значения атрибута `Version` элементов `layer id="UserModel"`, `layer id="UserDescriptions"` и значения атрибута `Version` элемента `Dsl` укажите версию пользовательской модели.

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

   Например:

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

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

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

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

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

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

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

   Например:

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

5. Если необходимо, добавьте описание пользовательских полей (см. раздел 18.2).

6. Перезапустите службы.

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

Пользовательские поля добавлены в модель актива.

18.2. Добавление описания пользовательских полей

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

► Чтобы добавить описание пользовательских полей:

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

   Например, для активов на ОС Microsoft Windows укажите:

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

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

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

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

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

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

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

   Например:

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

Описание пользовательских полей добавлено.

18.3. Изменение имен пользовательских полей

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

► Чтобы изменить имена пользовательских полей:

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

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

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

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

   Например:

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

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

Имена пользовательских полей изменены.

18.4. Удаление пользовательских полей из модели актива

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

- Чтобы удалить пользовательские поля из модели актива:

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

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

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

     Например:

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

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

  Пользовательские поля удалены из модели актива.

19. Работа с инфраструктурами

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

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

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

В этом разделе

19.1. 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.

19.2. 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.

19.3. 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.

20. Изменение проверок по чек-листу

- Чтобы изменить проверки на Linux:

  1. На сервере MP 10 Core в каталоге `/var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли Core>/config/usagemonitoring` создайте копию файла `check_settings.default.yaml` — файл `check_settings.yaml`.
  2. В файле `check_settings.yaml` измените необходимые параметры (см. приложение Б).
  3. Перезапустите контейнер core-usage-monitoring:

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

  Проверки изменены.

См. также

Параметры проверок по чек-листу (см. приложение Б)

21. Диагностика и решение проблем

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

В этом разделе

Не удается сканировать узлы из подсети предприятия (см. раздел 21.20)

Справочная информация (см. раздел 21.21)

21.1. Уведомления о состоянии системы

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

Предусмотрены следующие цветовые индикаторы уведомлений:

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

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

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

21.2. Обмен данными между компонентами системы

Для обмена данными между службами компонентов MaxPatrol SIEM используется брокер сообщений RabbitMQ. В общем случае в системе реализован следующий порядок обмена данными (сообщениями) между службами:

1. При подключении к брокеру службы-отправители создают необходимые точки обмена сообщениями, службы-получатели создают необходимые очереди сообщений и связывают очереди с точками обмена с помощью ключей маршрутизации. Далее службы поддерживают постоянное соединение с брокером.
2. Получив сообщение, брокер уведомляет об этом службу-отправителя и направляет сообщение в точку обмена. Сообщение содержит ключ маршрутизации, поэтому точка обмена пересылает полученное сообщение только в указанную в ключе очередь.
3. Как только сообщение становится первым в очереди, брокер отправляет его службе-получателю. Обработав сообщение, служба-получатель уведомляет об этом брокер.
4. После получения уведомления брокер удаляет из очереди отправленное сообщение. Если брокер не получает уведомление, он не удаляет сообщение из очереди и будет отправлять его до тех пор, пока не получит уведомление.

   Примечание. Служба может быть одновременно и отправителем, и получателем сообщений.

В конфигурации для низконагруженных систем используется только один брокер RabbitMQ. Он устанавливается вместе с компонентами (на один сервер) и обеспечивает как обмен данными между службами одного компонента, так и обмен данными между службами разных компонентов MaxPatrol SIEM.

В конфигурациях для средненагруженных или высоконагруженных систем используются два брокера. Один из них устанавливается на сервер MP 10 Core и обеспечивает обмен данными между службами MP 10 Core, а также между службами разных компонентов MaxPatrol SIEM. Другой брокер устанавливается на сервер MP SIEM Server и обеспечивает обмен данными только между его службами.

Поскольку события от активов тоже пересылаются между службами в виде сообщений RabbitMQ, проблемы в работе службы-получателя (например, ее незапланированная остановка) при постоянном потоке событий могут привести к существенному росту количества сообщений в очереди. Это уменьшает доступные системе память ОЗУ или свободное место на диске сервера MP SIEM Server, прежде всего в конфигурациях для средненагруженных или высоконагруженных систем. Для диагностики проблемы важно понимать, откуда очередь получает события и куда их отправляет.

> **Примечание.** Подробное описание процесса обработки событий см. в Руководстве разработчика.

Таблица 5. Очереди RabbitMQ и связанные с ними службы MP SIEM Server

Имя очереди	Служба-отправитель	Служба-получатель
pt.mpx.siem.receiver.incoming	Core Agent	SIEM Server receiver
normalizeq	SIEM Server receiver	SIEM Server normalizer
aggregatorq	SIEM Server normalizer	SIEM Server aggregator
event.resolve	SIEM Server aggregator	SIEM Server resolver
enricherq	SIEM Server resolver	SIEM Server enricher
routerq	SIEM Server enricher	SIEM Server router
correlatorq	SIEM Server router	SIEM Server correlator
notifierq	SIEM Server router	SIEM Server correlator
storageq	SIEM Server normalizer, SIEM Server resolver, SIEM Server router	SIEM Server storage

Приведенные в таблице очереди принадлежат брокеру MP SIEM Server.

В этом разделе

Вход в RabbitMQ (см. раздел 21.2.1)

Мониторинг потока событий в RabbitMQ (см. раздел 21.2.2)

Очередь storageq не уменьшается (см. раздел 21.2.3)

Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается (см. раздел 21.2.4)

Очередь storageq растет и начинает уменьшаться только после появления ошибки (см. раздел 21.2.5)

Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растет и начинает уменьшаться только после появления ошибки (см. раздел 21.2.6)

21.2.1. Вход в RabbitMQ

Перед входом в RabbitMQ необходимо убедиться, что правила межсетевого экрана разрешают входящее соединение от рабочей станции администратора к серверу RabbitMQ через порт 15672/TCP.

- Чтобы войти в RabbitMQ:

  1. В адресной строке браузера введите:
     `http://<IP-адрес или FQDN сервера RabbitMQ>:15672`

     Откроется страница входа в RabbitMQ.
  2. Введите логин `siem` и пароль.

     Примечание. По умолчанию пароль служебной учетной записи — `P@ssw0rd`.
  3. Нажмите кнопку **Login**.

     Отобразится страница **Overview**.

  Вход в RabbitMQ выполнен.

21.2.2. Мониторинг потока событий в RabbitMQ

Каждое сообщение в RabbitMQ может содержать несколько событий. Среднее количество событий в одном сообщении — 48, максимально возможное — 64.

Вы можете отслеживать обработку системой потока событий на следующих страницах интерфейса RabbitMQ:

— **Overview**. На странице в раскрывающемся блоке **Totals** отображаются графики количества сообщений, поступивших в брокер за указанный период, и скорости потока сообщений за этот период. В раскрывающемся блоке **Nodes** отображается информация об используемых памяти ОЗУ, месте на диске, а также о количестве используемых брокером дескрипторов файла и сокета.

— **Exchanges**. На странице отображается таблица точек обмена, в столбцах **Message rate in** и **Message rate out** приводятся входная и, соответственно, выходная скорости потока сообщений, проходящего через точку.

— **Queues**. На странице отображается таблица очередей сообщений:

- В столбце **Ready** приводится количество неотправленных, но готовых к отправке сообщений в очереди.
- В столбце **Unacked** приводится количество отправленных, но не удаленных брокером сообщений. Брокер удалит их из очереди после получения от службы уведомления об обработке.
- В столбце **Total** приводится общее количество сообщений в очереди.

21.2.3. Очередь storageq не уменьшается

Возможные причины

Возможными причинами проблемы являются неработоспособность компонента MP SIEM Events Storage или его сетевая недоступность.

Решение

► Чтобы решить проблему:

1. На сервере MP SIEM Events Storage проверьте статус служб (см. раздел 21.21.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. раздел 21.12).
2. Убедитесь, что параметр `ElasticsearchHost` компонента MP SIEM Server равен IP-адресу или FQDN сервера MP SIEM Events Storage.
3. Убедитесь, что порт 9200/TCP сервера MP SIEM Events Storage доступен для входящих соединений от сервера MP SIEM Server.
4. Создайте файл дампа памяти (см. раздел 21.21.7) службы SIEM Server storage.
5. Перезапустите службу SIEM Server storage.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

- файлы `siem.conf`, `/etc/opt/siem/siem/params.yaml` и `/etc/opt/siem/siem-server/params.yaml`;
- файл дампа памяти (см. раздел 21.21.7) службы SIEM Server storage;
- файлы журналов Elasticsearch, RabbitMQ, служб SIEM Server storage и SIEM Server frontend.

21.2.4. Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается

Возможные причины

Возможными причинами проблемы являются неработоспособность RabbitMQ или остановка службы MP SIEM Server, обрабатывающей сообщения очереди.

Решение

- Чтобы решить проблему:

  1. В веб-интерфейсе RabbitMQ на странице **Overview** проверьте наличие ошибок. Если ошибки присутствуют перейдите к их устранению (подробнее см. на сайте rabbitmq.com).
  2. Проверьте статус служб (см. раздел 21.21.3) MP SIEM Server. Если служба остановлена, запустите ее.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

- снимок экрана, содержащий страницу **Queues** веб-интерфейса RabbitMQ;
- снимок экрана, содержащий параметры очереди и таблицу с получателями сообщений (в раскрывающемся блоке **Consumers)**;
- результат запроса о статусе служб (см. раздел 21.21.3) MP SIEM Server;
- файлы журналов MP SIEM Server и RabbitMQ;
- снимок экрана страницы **Система** → **Мониторинг обработки событий**.

21.2.5. Очередь storageq растет и начинает уменьшаться только после появления ошибки

Возможные причины

Возможной причиной проблемы является несоответствие производительности MP SIEM Server и MP SIEM Events Storage входящему потоку событий. В этом случае MaxPatrol SIEM не успевает обработать события, что приводит к накоплению сообщений в очереди. Последующее срабатывание системы автоматического мониторинга (с появлением ошибки) останавливает отправку и прием событий, очередь начинает уменьшаться. После уменьшения размера очереди до определенного значения система возобновляет отправку и прием событий, что может опять привести к накоплению сообщений в очереди. Такое накопление очереди до появления ошибки и ее последующее уменьшение могут повторяться.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что аппаратные характеристики серверов MP SIEM Server и MP SIEM Events Storage соответствуют минимальным требованиям к конфигурации.
  2. Убедитесь, что объем раздела подкачки (см. раздел 21.21.1) на сервере MP SIEM Events Storage равен нулю.
  3. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. раздел 21.21.5). Если таких индексов более 900, необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 11).
  4. Убедитесь, что центральный процессор, ОЗУ и жесткие диски серверов MP SIEM Server и MP SIEM Events Storage не испытывают высокой нагрузки от запущенных процессов (см. раздел 21.21.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки Positive Technologies, приложив снимки экрана.
  5. Убедитесь, что скорость потока событий от источников соответствует развернутой конфигурации системы.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

- файлы журналов MP SIEM Server и MP SIEM Events Storage, RabbitMQ;
- аппаратные характеристики серверов MP SIEM Server и MP SIEM Events Storage;
- данные о нагрузке на центральный процессор, ОЗУ и жесткие диски (см. раздел 21.21.2) сервера MP SIEM Events Storage;
- результат запроса о состоянии индексов (см. раздел 21.21.5);
- снимок экрана страницы **Система** → **Мониторинг обработки событий**.

21.2.6. Очередь pt.mpx.siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растет и начинает уменьшаться только после появления ошибки

Возможные причины

Возможной причиной проблемы является несоответствие производительности MP SIEM Server и MP SIEM Events Storage входящему потоку событий. В этом случае MaxPatrol SIEM не успевает обработать события, что приводит к накоплению сообщений в очереди. Последующее срабатывание системы автоматического мониторинга (с появлением ошибки) останавливает отправку и прием событий, очередь начинает уменьшаться. После уменьшения размера очереди до определенного значения система возобновляет отправку и прием событий, что может опять привести к накоплению сообщений в очереди. Такое накопление очереди до появления ошибки и ее последующее уменьшение могут повторяться.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что скорость потока событий от источников соответствует развернутой конфигурации системы.
  2. Убедитесь, что центральный процессор, ОЗУ и жесткие диски серверов MP SIEM Server и MP SIEM Events Storage не испытывают высокой нагрузки от запущенных процессов (см. раздел 21.21.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки Positive Technologies, приложив снимки экрана.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файлы журналов MP SIEM Server и RabbitMQ;

— файл конфигурации `siem.conf`;

— снимок экрана страницы **Система** → **Мониторинг обработки событий**;

— данные о нагрузке (см. раздел 21.21.2) на центральный процессор, ОЗУ и жесткие диски сервера MP SIEM Server.

21.3. Мониторинг состояния RabbitMQ и Elasticsearch

MaxPatrol SIEM с помощью службы SIEM Server health monitor автоматически отслеживает состояние брокера сообщений RabbitMQ и хранилища событий Elasticsearch. На основании результатов мониторинга поток данных, поступающих в систему, может быть временно ограничен.

Служба содержат модули проверки и модули действия. Модуль проверки отслеживает параметры состояния и при превышении их пороговых значений отправляет предупреждение, сообщение об ошибке или запрашивает выполнение определенного действия. Модуль действия периодически проверяет наличие такого запроса и при его обнаружении может ограничить поток данных, поступающий в RabbitMQ, а также остановить прием данных службой SIEM Server receiver.

Для настройки модулей вам потребуются файлы конфигурации службы SIEM Server health monitor. Файлы содержат JSON-объекты, необходимые для настройки того или иного модуля. Каждый объект состоит из набора параметров (пар «ключ — значение»). После изменения параметров необходимо перезапустить службу. После обновления системы значения параметров возвращаются в используемые по умолчанию.

Параметры конфигурации службы SIEM Server health monitor

Ниже описано назначение JSON-объектов, содержащих параметры модулей проверки (секция `checks`) и модулей действия, приведен алгоритм работы модулей.

rabbitmq → poll_period

Параметр `poll_period` определяет частоту запросов для проверки статуса RabbitMQ и свободного места на диске (объект `disk_size`), для мониторинга длины очереди (объект `queues_size`) и объема памяти ОЗУ, занимаемой очередями (объект `queues_memory`). В случае обнаружения статуса «failed» модуль сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

По умолчанию запросы отправляются каждые 30 секунд.

rabbitmq → disk_size

Объект содержит параметры для настройки мониторинга свободного места на логическом диске, занимаемом виртуальным узлом RabbitMQ. По умолчанию модуль проверки запрашивает объем свободного места каждые 30 секунд (параметр `poll_period`).

По результатам запроса модуль:

— если диск содержит меньше 40 ГБ (параметр `limits` → `warn`), но больше 30 ГБ (параметр `limits` → `min`) свободного места — предупреждает об этом службу SIEM Server health monitor;

— если диск содержит меньше 30 ГБ (параметр `limits` → `min`) свободного места — сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

Объем свободного места будет увеличиваться после остановки отправки данных. Если он становится больше 30 ГБ (параметр `limits` → `min`), модуль проверки отзывает запросы на остановку.

rabbitmq → queues_size

Объект содержит параметры для настройки мониторинга очереди `pt.mpx.siem.receiver.incoming`. По умолчанию модуль проверки запрашивает количество сообщений в очереди каждые 30 секунд (параметр `poll_period`).

По результатам запроса модуль:

— если в очереди находится больше 1000 сообщений (параметр `limits` → `warn`), но меньше 2000 сообщений (параметр `limits` → `max`) — предупреждает об этом службу SIEM Server health monitor;

— если в очереди находится больше 2000 сообщений (параметр `limits` → `max`) — сообщает об ошибке и запрашивает остановку приема данных службой SIEM Server receiver.

Количество сообщений в очереди будет уменьшаться после остановки отправки данных. Если в очереди становится меньше 500 сообщений (параметр `limits` → `min`), модуль проверки отзывает запрос на остановку.

rabbitmq → queues_memory

Объект содержит параметры для настройки мониторинга объема памяти ОЗУ, используемого очередями виртуального узла RabbitMQ. По умолчанию модуль проверки запрашивает объем используемой памяти каждые 30 секунд (параметр `poll_period`).

По результатам запроса модуль:

— если используемый объем больше 4 ГБ (параметр `limits` → `warn`), но меньше 6 ГБ (параметр `limits` → `max`) — предупреждает об этом службу SIEM Server health monitor;

— если используемый объем больше 6 ГБ (параметр `limits` → `max`) — сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

После остановки отправки данных объем используемой памяти будет уменьшаться. Если он становится меньше 4 ГБ (параметр `limits` → `min`), модуль проверки отзывает запросы на остановку.

elasticsearch → poll_period

Параметр `poll_period` определяет частоту запросов для проверки статуса Elasticsearch и свободного места на диске (объект `disk_size`). В случае обнаружения статуса «red» модуль сообщает об ошибке, а также запрашивает остановку отправки данных от коллекторов и приема данных службой SIEM Server receiver.

По умолчанию запросы отправляются каждые 30 секунд.

elasticsearch → disk_size

Объект содержит параметры для настройки мониторинга свободного места на логическом диске, занимаемом узлами RabbitMQ. По умолчанию модуль проверки запрашивает объем свободного места каждые 30 секунд (параметр `poll_period`).

По результатам запроса модуль:

— если диск содержит меньше 200 ГБ (параметр `limits` → `warn`), но больше 60 ГБ (параметр `limits` → `min`) свободного места — предупреждает об этом службу SIEM Server health monitor;

— если диск содержит меньше 60 ГБ (параметр `limits` → `min`) свободного пространства — сообщает об ошибке, а также запрашивает остановку отправки данных коллекторами и приема данных службой SIEM Server receiver.

Объем свободного места будет увеличиваться после остановки отправки данных. Если он становится больше 60 ГБ (параметр `limits` → `min`), модуль проверки отзывает запросы на остановку.

agent

Объект содержит параметры для управления потоком данных, отправляемых коллектором. По умолчанию модуль действия каждые 30 секунд (параметр `check_period`) проверяет наличие запроса на остановку отправки данных. При наличии запроса модуль запрещает коллектору отправлять данные в течение 40 секунд (параметр `timeout`). Если при следующих проверках модуль не обнаруживает ранее существовавший запрос, он снова отправляет коллектору запрет, причем длительность запрета при каждой последующей отправке уменьшается на 5 секунд (параметр `timeout_step`). Когда длительность запрета станет равна нулю, модуль прекращает его отправку.

receiver

Объект содержит параметры для управления потоком данных, принимаемых службой SIEM Server receiver. По умолчанию модуль действия каждые 30 секунд (параметр `check_period`) проверяет наличие запроса на остановку приема данных. При наличии запроса модуль запрещает службе принимать данные в течение 40 секунд (параметр `timeout`). Если при следующих проверках модуль не обнаруживает ранее существовавший запрос, он снова отправляет службе запрет, причем длительность запрета при каждой последующей отправке уменьшается на 5 секунд (параметр `timeout_step`). Когда длительность запрета станет равна нулю, модуль прекращает его отправку.

21.4. Ошибка «Объем очередей SIEM Server Messaging Service на узле <FQDN сервера> достиг критического порога»

Возможные причины

Возможной причиной ошибки является неспособность компонентов MP SIEM Server и MP SIEM Events Storage вовремя обрабатывать входящий поток сообщений или неисправность компонентов.

Решение

- Чтобы решить проблему:

  1. Если присутствует ошибка «Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен», устраните ее (см. раздел 21.5).
  2. Войдите в RabbitMQ (см. раздел 21.2.1) и проверьте состояние очередей (см. раздел 21.2.2):
     - Если количество сообщений не уменьшается, перейдите к решению проблемы «Очередь <Название очереди> не уменьшается».
     - Если количество сообщений уменьшается, перейдите к решению проблемы «Очередь <Название очереди> растет и начинает уменьшаться только после появления ошибки».

21.5. Ошибка «Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен»

Возможные причины

Возможными причинами ошибки являются сетевая недоступность MP SIEM Events Storage, обработка компонентом сложного запроса или инициализация Elasticsearch после перезагрузки, вызванной срабатыванием системы автоматического мониторинга. Указанные ниже действия по решению проблемы рекомендуется выполнять только в том случае, если ошибка не исчезает в течение 15 минут.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что для MP 10 Core задан правильный IP-адрес или FQDN компонента MP SIEM Events Storage.
  2. Убедитесь, что сетевой порт 9200/TCP сервера MP SIEM Events Storage доступен (см. раздел 21.21.4) для MP 10 Core.
  3. На сервере MP SIEM Events Storage проверьте статус служб (см. раздел 21.21.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. раздел 21.12).
  4. Проверьте состояние индексов Elasticsearch (см. раздел 21.21.5). Если в Elasticsearch есть индексы в состоянии red, перейдите к решению этой проблемы (см. раздел 21.11).

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— результат выполнения каждого шага инструкции по решению проблемы;

— файлы журналов Elasticsearch;

— данные о нагрузке на центральный процессор, ОЗУ и жесткие диски (см. раздел 21.21.2) серверов MP SIEM Server и MP SIEM Events Storage;

— результат запроса о состоянии индексов (см. раздел 21.21.5).

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

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

Возможные причины

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

Решение

- Чтобы решить проблему:

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

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

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

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файл журнала службы Core Health Monitoring;

— снимок экрана, отображающий свободное место на логическом диске.

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

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

Возможные причины

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

Решение

- Чтобы решить проблему:

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

     ```
     df -h /var/lib/rabbitmq
     ```

     Интерфейс терминала отобразит имя диска и его параметры.

3. Убедитесь, что этот логический диск занят только файлами, необходимыми для работы ОС и MaxPatrol SIEM. Если диск содержит другие файлы и каталоги, удалите их.
4. Перезапустите службу SIEM Health Monitoring.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файлы журналов служб SIEM Health Monitoring, SIEM Health Monitor;

— снимок экрана, отображающий свободное место на логическом диске.

21.8. Ошибка «Объем свободного места на диске, выделенном для SIEM Events Storage, достиг критического порога»

Перед появлением ошибки система отображает предупреждение «Заканчивается свободное место на диске, выделенном для SIEM Events Storage».

Возможные причины

Причиной ошибки является уменьшение свободного места на логическом диске, занимаемом индексами Elasticsearch.

Решение

► Чтобы решить проблему:

1. Убедитесь, что аппаратные характеристики сервера MP SIEM Events Storage соответствуют минимальным требованиям к конфигурации.
2. Убедитесь, что логический диск с индексами занят только файлами, необходимыми для работы ОС и MaxPatrol SIEM. Если диск содержит другие файлы и папки, удалите их.
3. Проверьте свободное место на логическом диске с индексами Elasticsearch. Если на диске менее 40 ГБ свободного места, настройте архивацию индексов по расписанию (см. раздел 11.3).
4. Проверьте свободное место на логическом диске с архивными индексами. Если на диске отсутствует свободное место, настройте удаление архивных индексов по расписанию.
5. На сервере MP 10 Core перезапустите службу Core Health Monitoring.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файл журнала службы Core Health Monitoring;

— снимок экрана, отображающий свободное место на логическом диске.

См. также

Удаление индекса без архивации (см. раздел 11.6)

21.9. Ошибка «Компонент Core Messaging Service недоступен. Health Monitoring Service не может получать сообщения от других систем»

Возможные причины

Причиной ошибки является прекращение работы RabbitMQ.

Решение

- Чтобы решить проблему:

  1. Проверьте состояние службы RabbitMQ (см. раздел 21.21.3). Если служба остановлена, запустите ее вручную.
  2. Проверьте доступность страницы входа в RabbitMQ (см. раздел 21.2.1). Если страница недоступна, сообщите об этом в службу технической поддержки Positive Technologies, приложив журналы службы RabbitMQ.

21.10. Предупреждение «Время выполнения запросов у SIEM Events Storage на узле <FQDN сервера> достигло критического порога»

Возможные причины

Производительность и объем жестких дисков не соответствуют входящему потоку событий. Также производительность может снижаться при обработке сложных запросов или событий с нетиповой структурой.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что аппаратные характеристики сервера MP SIEM Events Storage соответствуют минимальным требованиям к конфигурации.
  2. Убедитесь, что объем раздела подкачки (см. раздел 21.21.1) на сервере MP SIEM Events Storage равен нулю.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

- о нагрузке на файловую систему и запущенных процессах (см. раздел 21.21.2);
- файлы журналов служб Core Health Monitoring, SIEM Server Health Monitor и Elasticsearch;
- файлы журналов (см. раздел 21.21.2) служб SIEM Server storage и SIEM Server frontend, собранные в режиме расширенного журналирования;
- снимок экрана страницы **Система** → **Мониторинг обработки событий**;
- аппаратные характеристики сервера MP SIEM Events Storage, включая информацию об уровне RAID-массива и параметрах жестких дисков.

21.11. Индексы Elasticsearch находятся в состоянии red

Индексы Elasticsearch предназначены для хранения данных о событиях информационной безопасности и их последующего поиска. Если не удается прочитать данные из индекса, его состояние сменится на red. В такой индекс нельзя ни записать данные, ни считать их из него.

Возможные причины

Возможной причиной проблемы является незапланированное завершение записи данных на диск (например, в случае аварийного выключения питания сервера, сбоя в работе файловой системы или сбора данных о событиях во время обновления MaxPatrol SIEM). Также индексы находятся в состоянии red во время инициализации Elasticsearch (например, после перезагрузки сервера), что является корректным поведением системы (после инициализации все индексы должны находиться в состоянии green или yellow).

Решение

Перед выполнением инструкции необходимо убедиться, что службы Elasticsearch запущены (см. раздел 21.21.3) и не менее 15 минут находятся в статусе `active (running)`.

► Чтобы решить проблему:

1. На сервере MP SIEM Events Storage выполните команду:
   ```
   curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true
   ```
2. Если индексы все еще находятся в состоянии (см. раздел 21.21.5) `red`, повторно выполните команду:
   ```
   curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true
   ```
   Примечание. Рекомендуется выполнять команду повторно не более двух раз.
3. Если требуется оперативно восстановить работоспособность системы, удалите индексы (см. раздел 11.6), которые находятся в состоянии `red`.

   Внимание! При удалении индексов будут потеряны сохраненные в них данные.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— данные о состоянии (см. раздел 21.21.5) индексов и шардов (фрагментов индексов);

— время запуска каждой команды `curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true`;

— файлы журналов Elasticsearch, SIEM Health Monitor.

21.12. Служба Elasticsearch останавливается через некоторое время после запуска

Возможные причины

Возможными причинами незапланированной остановки службы являются внезапный сбой в ее работе или недостаточный объем памяти ОЗУ сервера MP SIEM Events Storage.

Решение

► Чтобы решить проблему:

1. Запустите службу вручную.

   Примечание. После запуска службы начнется процесс инициализации Elasticsearch, которая может занять до 15 минут. По завершении инициализации все индексы должны находится в состоянии (см. раздел 21.21.5) green или yellow.

2. Зафиксируйте время повторной остановки службы.
3. Если MP SIEM Events Storage установлен на Linux, убедитесь, что суммарный объем памяти ОЗУ, выделяемый для всех узлов кластера (параметры DataNodeHeapSize, ClientNodeHeapSize и MasterNodeHeapSize (см. приложение А)), не превышает 58% от объема памяти ОЗУ сервера.
4. Убедитесь, что объем раздела подкачки (см. раздел 21.21.1) на сервере MP SIEM Events Storage равен нулю.
5. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. раздел 21.21.5). Если таких индексов более 900, необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 11).

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— период остановки службы, точное время каждой остановки;

— скорость потока событий;

— файл /tmp/hs_err_pid.log (на Linux);

— аппаратные характеристики сервера MP SIEM Events Storage, включая информацию об уровне RAID-массива и параметрах жестких дисков.

21.13. Система не получает данные от задачи

Возможные причины

Возможными причинами проблемы являются ошибки в работе компонентов системы, неправильная настройка профиля для сбора данных, сбои в работе источника событий, а также сбор событий с неподдерживаемых источников.

Решение

► Чтобы решить проблему:

1. Убедитесь, что задача запущена.
2. Проверьте наличие ошибок (см. раздел 21.1) системы автоматического мониторинга. Если ошибки присутствуют, устраните их.
3. Проверьте, что источник событий поддерживается системой. Если источник не поддерживается, система не сможет получать от него данные.

   Примечание. Список поддерживаемых источников приведен в Руководстве по настройке источников.
4. Скачайте журнал задачи (см. Руководство оператора) и проверьте наличие в нем строк с параметром `PackCount`. Если такие строки отсутствуют, проверьте наличие сетевого соединения между коллектором и источником.
5. Проверьте журнал задачи на наличие ошибок. Если ошибки присутствуют, убедитесь, что профиль задачи и параметры источника настроены правильно (см. Руководство по настройке источников).
6. На странице **Система** → **Управление системой** → **Коллекторы** проверьте статус коллектора. Если коллектор имеет статус «Недоступен», сохраните файлы его журналов для последующей отправки в службу технической поддержки.
7. Проверьте очереди в RabbitMQ (см. раздел 21.2.1). Если количество сообщений в очередях не уменьшается, сделайте снимок экрана со списком очередей для последующей отправки в службу технической поддержки.
8. Проверьте состояние Elasticsearch (см. раздел 21.21.6). Если Elasticsearch имеет статус «red», перейдите к решению проблемы «Индексы Elasticsearch находятся в состоянии red» (см. раздел 21.11).
9. Проверьте состояние служб (см. раздел 21.21.3) MP SIEM Server. Если служба остановлена, запустите ее вручную.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

- файлы журналов задачи и коллектора;
- название и версию источника;
- снимок экрана с очередями RabbitMQ;
- файлы журналов служб MP SIEM Server, которые были запущены вручную;
- сведения о том, поступали ли ранее данные от этого источника.

21.14. Отсутствуют события от источников

Возможные причины

Возможными причинами проблемы являются неправильная настройка источника событий или задачи по сбору данных, а также сбои в работе системы, возникающие при выполнении сбора, обработки или хранении событий.

Решение

- Чтобы решить проблему:

  1. На странице **События** в панели **Фильтры** выберите фильтр **Все события**. Если на странице отобразились ожидаемые события, рекомендуется проверить условия, используемые для фильтрации (см. документ Синтаксис языка запроса PDQL).
  2. Убедитесь, что источники событий поддерживаются системой и правильно настроены (см. Руководство по настройке источников).
  3. Скачайте журнал задачи (см. Руководство оператора) и проверьте наличие в нем строк с параметрами `PackCount` и `RawCount`. Если такие строки отсутствуют, обратитесь в службу технической поддержки Positive Technologies.
  4. На странице **Система** → **Мониторинг обработки событий** проверьте наличие входящего потока событий от источников. Если события отсутствуют, обратитесь в службу технической поддержки Positive Technologies.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

- предупреждения и ошибки (см. раздел 21.1) системы автоматического мониторинга;
- файлы журналов задачи, от которой ожидается поступление данных;
- снимок экрана, содержащий страницу **Задачи** с запущенными задачами;
- информацию о статусе служб (см. раздел 21.21.3) MP SIEM Server;
- файлы журналов MP SIEM Server, MP SIEM Events Storage и RabbitMQ;

— снимок экрана, содержащий страницу **Queues** веб-интерфейса RabbitMQ;

— HAR-файл с данными об открытии страницы **События**.

21.15. Задача аудита не собирает сведения об активах

Возможные причины

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

Решение

- Чтобы решить проблему:

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

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файлы журналов задачи аудита, собранные с уровнем журналирования debug;

— название и версию источника;

— снимки экрана с данными о правах доступа и привилегиях учетной записи, используемой для аудита.

21.16. Не приходят уведомления, отправляемые по электронной почте

- Чтобы решить проблему:

  1. Откройте файлы журналов `Notifications.log` и `Triggers.log`, расположенные на серверах PT MC и MP 10 Core соответственно.
  2. Если журналы содержат сообщения об ошибках (например, `Can't send email to <Адрес электронной почты>. Reason: Failure sending mail.; Unable to connect to the remote server; No connection could be made because the`

target machine actively refused it), убедитесь, что значения параметров SmtpHost, SmtpPort, SmtpUser и SmtpPassword роли Core соответствуют значениям параметров для подключения к серверу электронной почты.

3. Если журналы содержат сообщения об отправке (например, Email ["Название задачи"] "Название события" was sent to "Адрес электронной почты"), обратитесь к системному администратору предприятия для проверки параметров сервера электронной почты и просмотра его журналов на наличие ошибок.

21.17. Ошибка «Sdk пакет <Номер версии> поврежден. Необходимо восстановление»

Ошибка может возникнуть во время обновления компонента MP 10 Core.

Решение

Для решения проблемы вам потребуется архив packages\siem-sdk.<Номер версии>.tar.gz из комплекта поставки.

- Чтобы решить проблему:

1. После обновления MP 10 Core в папке C:\ProgramData\Positive Technologies\Knowledge Base\SiemSdks создайте папку <Номер версии пакета>.
2. Распакуйте архив siem-sdk.<Номер версии>.tar.gz в папку <Номер версии пакета>.
3. Войдите в Knowledge Base.
4. В меню **SIEM** выберите пункт **Выбор версии SDK**.
5. На отрывшейся странице в центральной панели выберите последнюю версию SDK и нажмите кнопку **Восстановить**.

21.18. Не удается импортировать отчет из MaxPatrol 8

Возможные причины

Возможными причинами проблемы являются сбои при создании отчета в MaxPatrol 8 или при его обработке в MaxPatrol SIEM.

Решение

- Чтобы решить проблему:

  1. Убедитесь, что MaxPatrol 8 как источник событий правильно настроен (см. Руководство по настройке источников).
  2. Скачайте журнал задачи (см. Руководство оператора). Если в журнале есть строки с ошибками `Failed to convert report scan.xml` или `mp_scan_converter.conversion_error.ConversionError: Errors in the hosts`, произошел сбой при обработке данных отчета. Необходимо обратиться в службу технической поддержки Positive Technologies.

Если выполнение указанных выше шагов не решило проблему, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— снимки экрана, содержащие параметры создания отчета в MaxPatrol 8;

— файлы журнала задачи по импорту данных отчета из MaxPatrol 8;

— файлы из папки `not processed` (находится в одной папке с файлом отчета);

— файл с консолидированными результатами сканирования, выполненного в MaxPatrol 8.

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

Для взаимодействия между собой компоненты системы используют IP-адреса или FQDN серверов, на которых они установлены. Эти сетевые параметры указываются администратором при установке компонента и сохраняются в его конфигурации. Если во время работы системы IP-адрес или FQDN сервера изменился, взаимодействие между компонентами нарушится, поскольку в конфигурации компонента будет храниться прежнее значение параметра. Для восстановления взаимодействия необходимо в качестве значений параметров компонентов указать актуальные IP-адреса или FQDN серверов.

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

— `CoreAddress` и `RMQHost` компонента MP SIEM Server на Linux;

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

Если был изменен IP-адрес или FQDN сервера MP SIEM Events Storage, необходимо указать актуальные значения параметров `SiemElasticsearchHost` компонента MP 10 Core и `ElasticsearchHost` компонента MP SIEM Server на Linux, а также выполнить команду `dpkg-reconfigure siem-storage` на сервере MP SIEM Events Storage.

21.20. Не удается сканировать узлы из подсети предприятия

Проблема

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

Возможные причины

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

Решение

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

Команды из инструкции необходимо выполнять в интерфейсе терминала Linux.

- Чтобы изменить подсеть докер-контейнера:

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

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

     Пример конфигурационного файла с параметрами подсетей:
     ```
     {
       "log-driver": "json-file",
       "log-opts": {
         "max-size": "100m",
         "max-file": "2",
     ```

```
    "compress": "true"
  },
  "dns-opts": ["ndots:1"],
  "bip": "10.10.0.1/24",
  "default-address-pools": [
    {
      "base": "10.0.0.0/20",
      "size": "24"
    }
  ]
}
```

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

Подсеть Docker-контейнера изменена.

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

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

21.21. Справочная информация

В разделе приведены рекомендации по выполнению шагов инструкций.

В этом разделе

21.21.1. Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки

- Чтобы просмотреть данные о распределении памяти ОЗУ,

  выполните команду:

  ```
  free -h
  ```

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

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

- Чтобы отключить раздел подкачки,

  выполните команду:

  ```
  swapoff -a
  ```

21.21.2. Сбор информации о нагрузке на файловую систему и запущенных процессах

- Чтобы собрать информацию о нагрузке на файловую систему,

  выполните команду:

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

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

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

- Чтобы собрать информацию о запущенных в системе процессах,

  выполните команду:

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

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

21.21.3. Просмотр статуса службы

- Чтобы просмотреть статус служб (Docker-контейнеров ролей) компонентов MP 10 Core, PT MC и Knowledge Base,

  выполните команду:

  ```
  docker ps --format "table {{.Names}}\t{{.State}}\t{{.Status}}"
  ```

- Чтобы просмотреть статус служб MP SIEM Server на Linux,

  выполните команду:

  ```
  systemctl --all status siemserver*service
  ```

- Чтобы просмотреть статус служб MP SIEM Events Storage на Linux,

  выполните команду:

  ```
  systemctl --all status elastic*service
  ```

- Чтобы просмотреть статус службы (Docker-контейнера роли) RabbitMQ на Linux,

  выполните команду:

  ```
  docker ps --filter "name=rabbitmq" --format "table {{.Names}}\t{{.State}}\t{{.Status}}"
  ```

21.21.4. Проверка доступности сетевого порта сервера

- Чтобы проверить доступность сетевого порта сервера,

  выполните команду:

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

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

21.21.5. Просмотр состояния индексов Elasticsearch

Во время инициализации Elasticsearch (например, после перезагрузки сервера) индексы находятся в состоянии `red`, что является корректным поведением системы (после инициализации все индексы должны сменить состояние на `green` или `yellow`). Поэтому рекомендуется просматривать состояние индексов через 15 минут после запуска всех служб Elasticsearch.

- Чтобы просмотреть состояние индексов,

  выполните команду:

  ```
  curl localhost:9200/_cat/indices?v
  ```

  Примечание. Вы можете сохранить данные о состоянии индексов в файл с помощью команды `curl localhost:9200/_cat/indices &> /usr/all_indices_and_errors.txt`.

- Чтобы просмотреть состояние шардов (фрагментов индексов),

  выполните команду:

  ```
  curl localhost:9200/_cat/shards?v
  ```

  Примечание. Вы можете сохранить данные о состоянии шардов в файл с помощью команды `curl localhost:9200/_cat/shards &> /usr/all_indices_and_errors.txt`.

21.21.6. Просмотр состояния Elasticsearch

- Чтобы просмотреть состояние Elasticsearch,

  выполните команду:

  ```
  curl localhost:9200/_cluster/health?pretty
  ```

21.21.7. Создание дампа памяти процесса

- Чтобы создать дамп памяти процесса на Linux:

  1. Определите идентификатор процесса:

     ```
     pgrep <Название процесса>
     ```

     Интерфейс терминала отобразит идентификатор процесса.

  2. Создайте файл дампа:

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

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

  Дамп памяти процесса создан.

21.21.8. Расположение индексов Elasticsearch

Путь к индексам Elasticsearch указан в качестве значения параметра `path.data` в файле `/etc/elasticsearch/<Название узла>/elasticsearch_<Название узла>.yml`.

Путь к архивным индексам указан в качестве значения параметра `path.repo` в файле `/etc/opt/siem/siem-storage/params.yaml`.

21.21.9. Расположение файлов журналов

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

Таблица 6. Расположение файлов журналов компонентов на Linux

Компонент	Путь к файлам
MP 10 Core , PT MC , Knowledge Base , MP 10 Collector	Файлы журналов MP 10 Core , PT MC и Knowledge Base находятся в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/log`, а файл журнала MP 10 Collector — в каталоге `/var/log/core-agent`. Журнал установки находится в файле `<Каталог со сценарием установки install.sh>/install_<Название роли>_<Номер версии>.log`
MP SIEM Server	Файлы журналов находятся в каталогах `opt/siem/log` и `opt/siem/log/<Название службы>/logs`, журнал установки — в файле `<Каталог со сценарием установки install.sh>/install_SiemServer_<Номер версии>.log`
MP SIEM Events Storage	Файлы журналов находятся в каталогах `/var/log/elasticsearch/` и `/es_logs/`, журнал установки — в файле `<Каталог со сценарием установки install.sh>/install_SiemStorage_<Номер версии>.log`
RabbitMQ	Файлы журналов находятся в каталоге `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли RMQ Message Bus>/log`, журнал установки — в файле `<Каталог со сценарием установки install.sh>/install_RmqMessagebus_<Номер версии>.log`
СУБД PostgreSQL	Файлы журналов находятся в каталоге `/var/lib/deployed-roles/<Идентификатор приложения MaxPatrol 10>/<Название экземпляра роли SqlStorage>/log`, журнал установки — в файле: `<Каталог со сценарием установки install.sh>/install_<Название роли>_<Номер версии>.log`

По умолчанию журналы компонента MP SIEM Server содержат информацию уровня debug и info. Если требуется журналировать всю информацию о работе службы, необходимо в файле `siem.conf` в секции `<Название службы>` → `logger` изменить значение параметра `level` на `trace` и перезапустить службу. Расширенное журналирование рекомендуется включать только при диагностике проблем или по запросу службы технической поддержки.

Примечание. Файл `siem.conf` находится в каталоге `/opt/siem/etc`.

21.21.10. Параметры мониторинга обработки активов

Основными показателями обработки активов являются длина очереди, время ожидания в очереди и средняя скорость обработки активов. Для тонкой настройки мониторинга обработки вы можете изменять пороговые значения длины очереди и времени ожидания, а также период вычисления средней скорости обработки активов для каждой стадии обработки. Эти параметры находятся в каталоге `/var/lib/deployed-roles/mp10-application/core-*/images/<Название службы>/config/default.env` и приведены в таблице.

Таблица 7. Параметры мониторинга обработки активов

Стадия обработки	**Служба**	**Длина очереди**		**Время ожидания**		**Период вычисления средней скорости обработки**
		Допустимое значение	**Критическое значение**	**Допустимое значение**	**Критическое значение**	
Обогащение собранных данных	Assets Scans	`QueueLengthAllowedThreshold`	`QueueLengthCriticalThreshold`	`WaitingTimeAllowedThreshold`	`WaitingTimeCriticalThreshold`	`ProcessingSpeedCalculationPeriod`
Идентификация актива	Assets Identification					
Буферизация	Assets Processing	`IdentityCommandsBufferingQueueLengthAllowedThreshold`	`IdentityCommandsBufferingQueueLengthCriticalThreshold`	`IdentityCommandsBufferingWaitingTimeAllowedThreshold`	`IdentityCommandsBufferingWaitingTimeCriticalThreshold`	`IdentityCommandsBufferingProcessingSpeedCalculationPeriod`

Стадия обработки	Служба	Длина очереди		Время ожидания		Период вычисления средней скорости обработки
		Допустимое значение	Критическое значение	Допустимое значение	Критическое значение	
Слияние данных об активах	Assets Processing	AssetsMergingQueueLengthAllowedThreshold	AssetsMergingQueueLengthCriticalThreshold	AssetsMergingWaitingTimeAllowedThreshold	AssetsMergingWaitingTimeCriticalThreshold	AssetsMergingProcessingSpeedCalculationPeriod
Расчет содержимого динамических групп	Assets Processing	DynamicGroupsCalculationQueueLengthAllowedThreshold	DynamicGroupsCalculationQueueLengthCriticalThreshold	DynamicGroupsCalculationWaitingTimeAllowedThreshold	DynamicGroupsCalculationWaitingTimeCriticalThreshold	DynamicGroupsCalculationProcessingSpeedCalculationPeriod
Расчет данных об уязвимостях	Assets Processing	VulnerabilityCalculationQueueLengthAllowedThreshold	VulnerabilityCalculationQueueLengthCriticalThreshold	VulnerabilityCalculationWaitingTimeAllowedThreshold	VulnerabilityCalculationWaitingTimeCriticalThreshold	VulnerabilityCalculationProcessingSpeedCalculationPeriod
Обновление отображаемых данных об активе	Assets Temporal Read Model	QueueLengthAllowedThreshold	QueueLengthCriticalThreshold	WaitingTimeAllowedThreshold	WaitingTimeCriticalThreshold	ProcessingSpeedCalculationPeriod
Обновление табличных списков	Tables					

21.21.11. Просмотр данных о политиках ILM

- Чтобы просмотреть текущее состояние индекса Elasticsearch и список политик ILM, которые к нему применены,

  выполните команду:

  ```
  curl 127.0.0.1:9200/siem_events_<Дата создания индекса>-000001/_ilm/explain?pretty
  ```

- Чтобы просмотреть статус политики ILM,

  выполните команду:

  ```
  curl 127.0.0.1:9200/_ilm/status
  ```

- Чтобы просмотреть текущую политику ILM без указания индекса,

  выполните команду:

  ```
  curl 127.0.0.1:9200/_ilm/policy/siem_events_policy
  ```

21.21.12. Настройка версий объектов, обновляемых на сервере PT UCS

Внимание! Чтобы PT UCS мог загружать обновления объектов с определенных версий и удалять из репозитория устаревшие версии, в блоке **Advanced configuration** параметров компонента должен быть установлен флажок **DeleteObsoleteProductVersions**.

- Чтобы настроить версии объектов, обновляемых на сервере PT UCS:

  1. Выполните команду

     ```
     mv ucs_user_static.conf.example ucs_user_static.conf
     ```

  2. В файле `ucs_user_static.conf` в блоке `product_versions` укажите идентификаторы объектов и их версии, начиная с которых будут скачиваться обновления.

     Примечание. Более ранние версии будут удаляться из локального репозитория сервера PT UCS при следующей загрузке обновлений.

  Версии обновляемых объектов настроены.

  Примечание. После обновления компонента PT UCS настройку необходимо выполнить заново.

22. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

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

Вы можете получать техническую поддержку на портале.

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

В этом разделе

22.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

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

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

Техническая поддержка на портале предоставляется на русском и английском языках.

22.2. Время работы службы технической поддержки

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

22.3. Как служба технической поддержки работает с запросами

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

В этом разделе

22.3.1. Предоставление информации для технической поддержки

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

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

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

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

22.3.2. Типы запросов

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

Вопросы по установке, повторной установке и предстартовой настройке продукта

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

Вопросы по администрированию и настройке продукта

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

Восстановление работоспособности продукта

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

Обновление продукта

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

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

Устранение дефектов продукта

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

22.3.3. Время реакции и приоритизация запросов

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

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

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 8).

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 8. Время реакции на запрос и время его обработки

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

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

22.3.4. Выполнение работ по запросу

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

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

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

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

Работы по запросу считаются выполненными, если:

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

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

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

— проблема классифицирована как неподдерживаемая.

Приложение А. Параметры конфигурации компонентов MaxPatrol SIEM на Linux

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

Таблица 9. Параметры конфигурации роли Deployer

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

Таблица 10. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
`HostAddress`	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
`PgAdminPort`	Порт для доступа к pgAdmin	`9001`
`PgAnalyzeScaleFactor`	Доля от числа кортежей в таблице, которая прибавляется к значению параметра `PgAnalyzeThreshold` при расчете порога срабатывания команды ANALYZE. Например, если значение `PgAnalyzeThreshold` равно 200 000, а значение параметра `PgAnalyzeScaleFactor` равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет 200 000 + 100 000 = 300 000 кортежей	`0.0`
`PgAnalyzeThreshold`	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	`200000`

Параметр	Описание	Значение по умолчанию
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения — HDD или SSD)	HDD
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения — panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5	warning
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgSharedBufferSize	Объем памяти, который сервер баз данных будет использовать для буферов в разделяемой памяти	4GB
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgVacuumNapTime	Минимальная задержка между двумя запусками автоочистки для отдельной базы данных	20min
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB

Таблица 11. Параметры конфигурации роли Observability

Параметр	Описание	Значение по умолчанию
AllowToExportTelemetry	Данные телеметрии отправляются (True) или не отправляются (False) на сервер приема телеметрии	True
CollectorServerHttpPort	Порт для доступа к серверу сбора журналов по протоколу HTTP	4318
DockerRegistry	Порт для доступа к реестру Docker-образов	Адрес сервера компонента MP 10 Core
ExportEnabledFrom	Разрешенное начальное время отправки телеметрии	00:00:00
ExportEnabledTo	Разрешенное конечное время отправки телеметрии	23:59:59
FlusUri	Адрес сервера приема телеметрии	—
InstanceAccessToken	Токен авторизации на сервере приема телеметрии	—
JobExecutingInterval	Интервал запуска работ внутри сервиса Telemetry.Tracker	00:01:00
MetricsHttpPort	Порт для доступа к метрическим данным	8428
MetricsRetention	Время сохранения метрических данных в базе данных	30d
Network	Сетевое имя реестра Docker-образов	observability.network.observability
NetworkDriver	Драйвер Docker-образов	bridge
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	—
PostgrePassword	Пароль служебной учетной записи для доступа к серверу СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432

Параметр	Описание	Значение по умолчанию
PostgreUserName	Логин служебной учетной записи для доступа к серверу СУБД PostgreSQL	pt_system
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	—
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	—
TelemetryFileSize	Максимальный размер файла телеметрии в мегабайтах	50
TelemetryPackSize	Максимальный размер архива в мегабайтах, который можно отправить на сервер приема телеметрии	35

Таблица 12. Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
ActionLogBatchSize	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service единовременно отправляет службе MC User Action Logging Service	100
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
DefaultLocale	Интерфейс PT MC отображается на русском (ru-RU) или английском (en-US) языке	ru-Ru
ExpertDataUpdateMethod	Метод получения обновлений экспертных данных. Возможные значения: Online или Offline	—
HostAddress	IP-адрес или FQDN сервера PT MC	—
IamCookieLifetime	Время жизни неактивной сессии в MaxPatrol SIEM (в часах)	168

Параметр	Описание	Значение по умолчанию
LdapTimeout	Тайм-аут подключения к LDAP-серверу (в миллисекундах)	60000
LogCleanLimit	Максимальное количество сохраняемых записей о действиях пользователей. При превышении заданного значения старые записи будут удалены	1000000
MasterRedirectEnabled	В случае иерархической инсталляции аутентификация пользователя выполняется на главной (флажок установлен) или на локальной (флажок снят) площадке	Флажок снят
PackageManagementPort	Номер порта сервиса управления пакетами Package Management	8585
PackagesSourceCredentialToken	Токен для авторизации на сервере обновлений. Хранится в файле instance-access-token.key и представляет собой набор символов, закодированных с использованием стандарта Base64	—
PackagesSourceUri	Адрес сервера обновлений	—
PostgreHost	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
PostgrePassword	Пароль служебной учетной записи для доступа PT MC к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432
PostgreUserName	Логин служебной учетной записи для доступа PT MC к СУБД PostgreSQL	pt_system
TmSiteAlias	Псевдоним площадки	SITE
TmSiteId	Идентификатор площадки	—
TmTenantManagerId	Идентификатор службы MC Tenant Manager Service	—

Таблица 13. Параметры конфигурации роли Knowledge Base

Параметр	Описание	Значение по умолчанию
ClientId	Идентификатор для регистрации приложения Knowledge Base в PT MC	ptkb
ClientSecret	Ключ для регистрации приложения Knowledge Base в PT MC	secret
CoreAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
DefaultLocale	Интерфейс Knowledge Base отображается на русском (ru-RU) или английском (en-US) языке	—
DeploymentType	Тип развертывания Knowledge Base	—
DetectOutOfSyncWithSIEM	Knowledge Base определяет (флажок установлен) или не определяет (флажок снят) отсутствие синхронизации с MP SIEM Server	Флажок установлен
DisplayName	Название приложения Knowledge Base в PT MC	Knowledge Base
EditableOrigins	Поставщик, атрибуты объектов которого можно изменять	Local
HostAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
OriginNameENG	Полное название поставщика для объектов Knowledge Base на английском языке	Local system
OriginNameRUS	Полное название поставщика для объектов Knowledge Base на русском языке	Локальная система
OriginNickName	Псевдоним поставщика для объектов Knowledge Base	LOC
OriginSystemName	Поставщик объектов Knowledge Base	Local
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost

Параметр	Описание	Значение по умолчанию
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от Knowledge Base	5432
PostgreUserName	Логин служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	pt_system
RestrictedLocales	Не используемый в Knowledge Base язык локализации	KOR
ShowDiffObjectId	Веб-интерфейс Knowledge Base отображает (флажок установлен) или не отображает (флажок снят) идентификаторы объектов (например, при сравнении ревизий БД)	Флажок снят
SiemPackageSourceContentDatabase	Название БД, которая автоматически обновляется с помощью PT UCS	siem_content
SiemPort	Порт сервера MP SIEM Server для входящих подключений от Knowledge Base	8013
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpPassword	Пароль служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от Knowledge Base	25
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Knowledge Base Notification System <NoReply@knowledgebase.com>

Параметр	Описание	Значение по умолчанию
SmtpUseDefaultCredentials	Режим аутентификации SMTP-сервера: флажок установлен — для аутентификации используются логин и пароль служебной учетной записи Network Service (необходимо очистить значения параметров SmtpUser и SmtpPassword); флажок снят — для аутентификации используются логин и пароль, указанные в параметрах SmtpUser и SmtpPassword	Флажок установлен
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics

Таблица 14. Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
ConsiderEventsImportance	В случае изменения IP-адреса актива система обновляет его конфигурацию сразу (флажок установлен) или по расписанию (флажок снят)	Флажок установлен
CybsiAddress	IP-адрес или FQDN сервера PT CP	localhost
CybsiEnabled	MP 10 Core получает (флажок установлен) или не получает (флажок снят) данные от PT CP	Флажок снят
DefaultAssetTtl	Время устаревания активов (<Дни>.<Часы>:<Минуты>:<Секунды>)	90.00:00:00
DefaultLocale	Интерфейс MaxPatrol SIEM отображается на русском (ru-RU) или английском (en-US) языке	ru-RU

Параметр	Описание	Значение по умолчанию
EmailNotificationRetryCount	Максимальное количество попыток отправки сообщения на SMTP-сервер	10
EmailNotificationRetryPeriodSeconds	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	60
HostAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
IncidentAggregationTimeout	Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>)	00:01:00
IncidentIdenticalNotificationLimit	Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент	100
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	—
PtkbUpdateCheckPeriod	Период проверки наличия обновления для базы знаний, используемой в MP 10 Core (<Часы>:<Минуты>:<Секунды>)	00:05:00
RMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP 10 Core к RabbitMQ	P@ssw0rd

Параметр	Описание	Значение по умолчанию
RMQSslCertPassword	Пароль SSL-сертификата RabbitMQ	oxah4kie2O
RMQSslCertPath	Путь к файлу SSL-сертификата RabbitMQ	RMQ_Core_Client.p12
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
SaltMasterHost	IP-адрес или FQDN сервера с модулем Salt Master	—
SaltMasterPort	Порт сервера с модулем Salt Master для входящих подключений от MP 10 Core	9035
SendAlertsToSiem	При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок установлен). Если флажок не установлен, события не регистрируются	Флажок не установлен
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpIgnoreCertificateValidation	MP 10 Core проверяет (False) или не проверяет (True) валидность сертификата при подключении к SMTP-серверу	True
SmtpPassword	Пароль служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от MP 10 Core	25

Параметр	Описание	Значение по умолчанию
SmtpSecureSocketOptions	Варианты шифрования при подключении к SMTP-серверу: — None — шифрование не используется; — Auto — почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется; — SslOnConnect — протоколы SSL или TLS используются при соединении; — StartTls — протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается; — StartTlsWhenAvailable — протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS	Auto
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpUser	Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsageMonitoringCheckingPeriod	Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)	00:15:00

Таблица 15. Параметры конфигурации роли Collector

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	—
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2	—

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentName	Имя коллектора в веб-интерфейсе MaxPatrol SIEM	FQDN сервера MP 10 Collector
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** Брокер RabbitMQ устанавливается на сервер MP 10 Core и обеспечивает обмен сообщениями между компонентами MaxPatrol SIEM	localhost
AgentRMQPassword	Пароль служебной учетной записи для подключения MP 10 Collector к RabbitMQ	P@ssw0rd
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от MP 10 Collector	5671
AgentRMQUser	Логин служебной учетной записи для подключения MP 10 Collector к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	RMQ_Server.crt

Параметр	Описание	Значение по умолчанию
`Agent_RMQ_SSL_CERTIFICATE`	Путь к файлу публичного SSL-сертификата	`RMQ_Agent_Client.crt`
`Agent_RMQ_SSL_Enabled`	MP 10 Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
`Agent_RMQ_SSL_KEY`	Путь к файлу закрытого ключа SSL-сертификата	`RMQ_Agent_Client.key`

Таблица 16. Параметры конфигурации роли SIEM Storage

Параметр	Описание	Значение по умолчанию
`BindHost`	IP-адреса или FQDN сетевых интерфейсов сервера MP SIEM Events Storage. **Примечание.** Elasticsearch обрабатывает входящие запросы, поступающие только на эти сетевые интерфейсы	`0.0.0.0`
`ClientNodeHeapSize`	Объем оперативной памяти, выделяемый для клиентского узла (в гигабайтах). **Примечание.** Перед изменением параметра необходимо выбрать вариант `Manual` в качестве значения параметра `ClusterConfigurationProfile`	`16g`

Параметр	Описание	Значение по умолчанию
`ClusterConfigurationProfile`	Объем оперативной памяти, выделяемый каждому типу узлов кластера Elasticsearch. Для выбора доступны следующие варианты: — `AIO` — значения установлены производителем и соответствуют требованиям конфигурации MaxPatrol SIEM для низконагруженных систем; — `SIEMandStorage` — значения установлены производителем и соответствуют требованиям конфигурации MaxPatrol SIEM для средненагруженных систем; — `Standalone` — значения установлены производителем и соответствуют требованиям конфигурации MaxPatrol SIEM для высоконагруженных систем с потоком событий до 20000 в секунду; — `ManagedStorage` — значения установлены производителем и соответствуют требованиям конфигурации MaxPatrol SIEM для высоконагруженных систем с потоком событий выше 20000 в секунду; — `Manual` — ввод значений вручную (параметры `DataNodeHeapSize`, `ClientNodeHeapSize`, `MasterNodeHeapSize`)	`Standalone`
`DataNodeHeapSize`	Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах). **Примечание.** Перед изменением параметра необходимо выбрать вариант `Manual` в качестве значения параметра `ClusterConfigurationProfile`	`30g`

Параметр	Описание	Значение по умолчанию
HighLoad	Кластер Elasticsearch содержит два (флажок снят) или четыре (флажок установлен) узла данных	Флажок снят
HostAddress	IP-адрес или FQDN сервера MP SIEM Events Storage	—
MasterNodeHeapSize	Объем оперативной памяти, выделяемый для главного узла (в гигабайтах). **Примечание.** Перед изменением параметра необходимо выбрать вариант Manual в качестве значения параметра ClusterConfigurationProfile	16g
PathData	Путь к индексам Elasticsearch. Если MaxPatrol SIEM развернут для высоконагруженных систем — путь к индексам, находящимся в теплой стадии	/data
PathDataHot	Путь к индексам, находящимся в горячей стадии	/datahot
PathLog	Путь к файлам журналов	/es_logs
PathRepo	Путь к резервным копиям индексов	/es_backup
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
SetRecomendedDiskScheduler	Для операций ввода-вывода ядро Linux использует планировщик по умолчанию (флажок снят) или планировщик deadline (флажок установлен)	Флажок установлен

Параметр	Описание	Значение по умолчанию
TailcutterDbspace	Максимальный объем дискового пространства, выделяемый для хранения индексов, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)	92%
TailcutterLog	Путь к файлу журнала утилиты tailcutter	/opt/estools/log/tailcutter.log
TailcutterLoglevel	Уровень журналирования работы утилиты tailcutter (возможные значения CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET)	WARNING
TailcutterTtl	Срок хранения индексов для событий (в днях)	365
TailcutterTtlc	Срок хранения индексов для счетчиков событий (в днях)	7

Таблица 17. Параметры конфигурации роли Event Storage

Параметр	Описание	Значение по умолчанию
BindHost	IP-адреса или FQDN сетевых интерфейсов сервера MP SIEM Events Storage. **Примечание.** LogSpace обрабатывает входящие запросы, поступающие только на эти сетевые интерфейсы	0.0.0.0
Database	Название базы данных хранилища LogSpace	siem
PathData	Корневой каталог хранилища LogSpace	/db_data
RotateCount	Максимальное количество сохраняемых файлов журналов	10
RotateSize	Максимальный размер сохраняемых файлов журналов (G для гигабайтов, M для мегабайтов, k для килобайтов)	200M

Параметр	Описание	Значение по умолчанию
TailcutterDbspace	Максимальный объем дискового пространства, выделяемый для разделов хранилища, в гигабайтах (например, 1000) или процентах от общего объема жесткого диска (например, 65%)	92%
TailcutterLog	Путь к файлу журнала утилиты tailcutter	/opt/dbtools/log/tailcutter.log
TailcutterLogLevel	Уровень журналирования работы утилиты tailcutter (возможные значения — CRITICAL, ERROR, WARNING, INFO, DEBUG и NOTSET)	WARNING
TailcutterTtl	Срок хранения разделов для событий (в днях)	365
TailcutterTtlc	Срок хранения разделов для счетчиков событий (в днях)	7

Таблица 18. Параметры конфигурации роли SIEM Server

Параметр	Описание	Значение по умолчанию
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ для подключения MP SIEM Server	mpx
AssetResolverPort	Порт сервера MP 10 Core для подключения службы SIEM Server assets resolution	8721
AUTH_KEY	Путь к файлу закрытого ключа сертификата для аутентификации MP SIEM Server в PT MC	/opt/mpxsiem/etc/authKey.pem
ClusterSeedHost	IP-адрес или FQDN сервера MP SIEM Events Storage для входящих подключений от связанных приложений при выполнении распределенного поиска событий	—

Параметр	Описание	Значение по умолчанию
`ClusterSeedPort`	Порт сервера MP SIEM Events Storage для входящих подключений от связанных приложений при выполнении распределенного поиска событий	`9300`
`CoreAddress`	IP-адрес или FQDN сервера MP 10 Core	`localhost`
`CorePort`	Порт сервера MP 10 Core для подключения MP SIEM Server	`8799`
`CoreRabbitAuthMethod`	Аутентификация MP SIEM Server в брокере RabbitMQ выполняется с помощью логина и пароля (`plain`) или с помощью сертификатов безопасности (`ssl`). **Примечание.** Этот брокер устанавливается на сервер MP 10 Core и обеспечивает обмен сообщениями между компонентами MaxPatrol SIEM	`ssl`
`CoreTableListsSize`	Объем оперативной памяти для хранения табличных списков, заполняемых правилами корреляции (в мегабайтах)	`16384`
`CorrTableListsSize`	Объем оперативной памяти для хранения табличных списков, заполняемых данными об активах, справочной информацией и данными от репутационных сервисов (в мегабайтах)	`4096`
`CounterRefreshInterval`	Период обновления данных о счетчиках производительности (в секундах)	`60`
`CsvSeparator`	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	`;`
`DefaultLogLevel`	Уровень журналирования для служб MP SIEM Server (возможные значения — `fatal`, `error`, `warn`, `info`, `debug` или `trace`)	`info`

Параметр	Описание	Значение по умолчанию
`ElasticsearchAggregationQueryTimeout`	Тайм-аут для поиска событий, подходящих под условия группировки или агрегации (в секундах)	`600`
`ElasticsearchAggregationResponseTimeout`	Тайм-аут выполнения запроса группировки или агрегации событий (в секундах)	`600`
`ElasticsearchAggregationSize`	Максимальное количество групп, отображаемое в результате группировки или агрегации событий	`1000`
`ElasticsearchAPIVersion`	Версия API, используемая для взаимодействия с Elasticsearch	`7.4`
`ElasticsearchCompression`	Алгоритм сжатия данных, используемый в Elasticsearch	`default`
`ElasticsearchCountersLimit`	Максимальное количество записей о счетчиках производительности, получаемых от Elasticsearch (`0` — количество получаемых записей не ограничено)	`0`
`ElasticsearchDefaultQueryTimeout`	Тайм-аут для поиска событий, подходящих под условия фильтрации (в секундах)	`600`
`ElasticsearchDefaultResponseTimeout`	Тайм-аут выполнения запроса фильтрации событий (в секундах)	`600`
`ElasticsearchHost`	IP-адрес или FQDN сервера MP SIEM Events Storage	`localhost`
`ElasticsearchMaxReplySize`	Максимальный размер ответа от Elasticsearch (в байтах)	`524288000`
`EnriTableListsSize`	Объем оперативной памяти для хранения табличных списков, заполняемых правилами обогащения (в мегабайтах)	`8192`
`EventsRefreshInterval`	Период обновления данных о событиях (в секундах)	`60`

Параметр	Описание	Значение по умолчанию
FrontendHost	IP-адрес для прослушивания службой SIEM Server frontend входящих подключений	0.0.0.0
GlobalRabbitHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** Этот брокер RabbitMQ устанавливается на сервер MP SIEM Server и обеспечивает обмен сообщениями между службами MP SIEM Server	127.0.0.1
GlobalRabbitPort	Порт сервера RabbitMQ для входящих соединений от MP 10 Core	5672
HighLoad	Для службы SIEM server storage выделено шесть (флажок установлен) или четыре (флажок снят) потока операционной системы	Флажок снят
LogCount	Максимальное количество файлов журналов MP SIEM Server (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов MP SIEM Server	2
LogSize	Максимальный размер файла журнала MP SIEM Server (в байтах)	104857600
LogSpaceHost	IP-адрес или FQDN сервера MP SIEM Events Storage	localhost
ManagedStorage	Для управления жизненным циклом индексов Elasticsearch используется (флажок установлен) или не используется (флажок снят) технология ILM	Флажок снят
MonitoringOomEnabled	Мониторинг объема оперативной памяти, потребляемой правилами корреляции, выполняется (флажок установлен) или не выполняется (флажок снят)	Флажок установлен

Параметр	Описание	Значение по умолчанию
MonitoringOomMemoryLimit	Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)	60
MonitoringOvertriggerEnabled	Мониторинг количества корреляционных событий, регистрируемых правилами корреляции, выполняется (флажок установлен) или не выполняется (флажок снят)	Флажок установлен
MonitoringOvertriggerPeriod	Период для подсчета количества корреляционных событий, регистрируемых одним правилом корреляции (в секундах)	3600
MonitoringOvertriggerThreshold	Максимальное количество корреляционных событий за период (параметр MonitoringOvertriggerPeriod), регистрируемых одним правилом корреляции и не приводящее к остановке правила	300
ProtectedRulesPath	Путь к файлу со списком правил корреляции, работа которых приостанавливается в последнюю очередь (при мониторинге работы правил корреляции)	—
RemoteEventsSkipAggregator	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) агрегацию реплицированных событий	Флажок установлен
RemoteEventsSkipCorrelator	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) корреляцию реплицированных событий	Флажок установлен
RemoteEventsSkipEnricher	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) обогащение реплицированных событий	Флажок установлен
RemoteEventsSkipResolver	Площадка-получатель выполняет (флажок снят) или не выполняет (флажок установлен) привязку реплицированных событий к активам	Флажок установлен
RMQ_SSL_CA_CERTIFICATE	Путь к файлу корневого SSL-сертификата	/opt/mpxsiem/etc/rootCA.crt

Параметр	Описание	Значение по умолчанию
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	/opt/mpxsiem/etc/RMQ_SIEM_Client.crt
RMQ_SSL_KEY	Путь к файлу закрытого ключа SSL-сертификата	/opt/mpxsiem/etc/RMQ_SIEM_Client.key
RMQDurableQueue	Сообщения, накопленные в очередях RabbitMQ, сохранятся (флажок установлен) или не сохранятся (флажок снят) после перезагрузки брокера	Флажок установлен
RMQHost	IP-адрес или FQDN сервера RabbitMQ. **Примечание.** Этот брокер RabbitMQ устанавливается на сервер MP 10 Core и обеспечивает обмен сообщениями между компонентами MaxPatrol SIEM	localhost
RMQPassword	Пароль служебной учетной записи для подключения MP SIEM Server к брокеру RabbitMQ	P@ssw0rd
RMQPort	Порт сервера RabbitMQ для входящих соединений от MP SIEM Server при аутентификации с помощью логина и пароля (plain)	5672
RMQPortSSL	Порт сервера RabbitMQ для входящих соединений от MP SIEM Server при аутентификации с помощью сертификатов безопасности (ssl)	5671
RMQUser	Логин служебной учетной записи для подключения MP SIEM Server к брокеру RabbitMQ	siem
RowBatchSize	Количество строк табличного списка, экспортируемых (импортируемых) службой SIEM Server frontend из службы (в службу) SIEM Server commander	5000

Параметр	Описание	Значение по умолчанию
SiemOnAgent	Установлена облегченная (флажок установлен) или стандарная (флажок снят) версия MP SIEM Server	Флажок снят
StatsPublishPeriod	Период обновления данных, отображаемых в рабочей области главной страницы MaxPatrol SIEM (в секундах)	30
StorageBackendType	В качестве хралища событий используется Elasticsearch или LogSpace	elasticsearch
StoreNormalizedRaw	Нормализованные события сохраняются с полем body (флажок установлен) или без него (флажок снят)	Флажок установлен
StoreUnnormalizedRaw	Ненормализованные события хранятся (флажок установлен) или не хранятся (флажок снят) в системе	Флажок установлен
TableListsRestorePolicy	Режим работы службы автоматического восстановления данных табличных списков SIEM Server fptarestorer. Для выбора доступны следующие варианты: — disabled — автоматическое восстановление выключено; — fragile — данные будут восстановлены только в том случае, если при восстановлении исключена возможность их потери; — best_effort — в процессе восстановления допустима потеря одной-двух последних записей; — robust — в процессе восстановления допустима потеря всех данных (базы данных могут быть удалены и пересозданы)	best_effort
WebProto	HTTP-запросы к MP 10 Core выполняются через защищенное (https) или незащищенное (http) соединение	https

Таблица 19. Параметры конфигурации роли Retro Correlator

Параметр	Описание	Значение по умолчанию
AgentMonitoringCacheAlarm	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringCacheWarn	Пороговое значение для объема свободного места на всех логических дисках с файлами коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskLogsAlarm	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskLogsWarn	Пороговое значение для объема свободного места на логическом диске с файлами журналов коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskOverallAlarm	Пороговое значение для параметров AgentMonitoringDiskLogsAlarm, AgentMonitoringDiskStorageAlarm, AgentMonitoringDiskQueueAlarm (групповое указание значений)	32768M free
AgentMonitoringDiskOverallWarn	Пороговое значение для параметров AgentMonitoringDiskLogsWarn, AgentMonitoringDiskStorageWarn, AgentMonitoringDiskQueueWarn (групповое указание значений)	—
AgentMonitoringDiskQueueAlarm	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode2	—

Параметр	Описание	Значение по умолчанию
AgentMonitoringDiskQueueWarn	Пороговое значение для объема свободного места на логическом диске с файлами очереди событий. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentMonitoringDiskStorageAlarm	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode2	—
AgentMonitoringDiskStorageWarn	Пороговое значение для объема свободного места на логическом диске с файлами базы данных коллектора. При достижении порогового значения коллектор переходит в режим SafeMode1	—
AgentName	Имя коллектора в веб-интерфейсе MaxPatrol SIEM	FQDN сервера PT RC
AgentRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
AgentRMQPassword	Пароль служебной учетной записи для доступа PT RC к RabbitMQ	P@ssw0rd
AgentRMQPort	Порт сервера RabbitMQ для входящих подключений от MP 10 Collector	5671
AgentRMQUser	Логин служебной учетной записи для доступа PT RC к RabbitMQ	agent
AgentRMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
Agent_RMQ_SSL_CA_Certificate	Путь к файлу корневого SSL-сертификата	rootCA.crt
Agent_RMQ_SSL_Certificate	Путь к файлу публичного SSL-сертификата	RMQ_Agent_Client.crt
Agent_RMQ_SSL_Enabled	MP 10 Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key

Параметр	Описание	Значение по умолчанию
CoreAddress	IP-адрес или FQDN сервера MP 10 Core	localhost
CsvSeparator	Разделитель данных в CSV-файле, используемом для экспорта и импорта табличных списков	;
DefaultLogLevel	Уровень журналирования для служб PT RC (возможные значения — fatal, error, warn, info, debug или trace)	info
HostAddress	IP-адрес или FQDN сервера PT RC	localhost
InternalRMQHost	IP-адрес или FQDN сервера RabbitMQ	localhost
InternalRMQPassword	Пароль служебной учетной записи для доступа к RabbitMQ	P@ssw0rd
InternalRMQPort	Порт сервера RabbitMQ для входящих соединений от PT RC при аутентификации с помощью логина и пароля (plain)	5672
InternalRMQPortSSL	Порт сервера RabbitMQ для входящих соединений от PT RC при аутентификации с помощью сертификатов безопасности (ssl)	5671
InternalRMQUser	Логин служебной учетной для доступа к RabbitMQ	siem
InternalRMQVirtualHost	Имя виртуального узла RabbitMQ	/
KBAddress	IP-адрес или FQDN сервера Knowledge Base	localhost
LogCount	Максимальное количество файлов журналов PT RC (архивированных и неархивированных)	10
LogPlain	Максимальное количество неархивированных файлов журналов PT RC	2
LogSize	Максимальный размер файла журнала PT RC (в байтах)	104857600

Параметр	Описание	Значение по умолчанию
MaxTableListsSize	Максимальный объем оперативной памяти, выделяемый для хранения табличных списков (в мегабайтах)	8192
RetroControllerHost	IP-адрес для входящих подключений от коллектора на Linux	0.0.0.0
SiemServerAddress	IP-адрес или FQDN сервера MP SIEM Server	localhost

Таблица 20. Параметры конфигурации роли RMQ Message Bus

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

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

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

Таблица 21. Параметры конфигурации компонента PT UCS

Параметр	Описание	Значение по умолчанию
`AutoAcceptMinions`	Salt Master автоматически утверждает запрос на подключение от модулей Salt Minion (флажок установлен) или модули необходимо подключать вручную (флажок снят)	Флажок снят
`AutoDownloadProductsList`	PT UCS автоматически загружает с глобального сервера Positive Technologies обновления для следующих объектов: — `KB SIEM DATA` — правил, табличных списков, макросов, схемы полей событий и описаний пакетов экспертизы; — `KB BINARY` — дистрибутивов Knowledge Base; — `KB SDK` — утилит SDK Knowledge Base; — `SIEM BINARY` — дистрибутивов компонентов на Microsoft Windows; — `CYBSI FEED` — данных об угрозах информационной безопасности и индикаторах компрометации для компонента PT CP	Установлены флажки `KB SIEM DATA`, `KB BINARY`, `KB SDK` и `CYBSI FEED`
`LogLevel`	Уровень журналирования для служб PT UCS	`info`
`ProxyAddress`	IP-адрес или FQDN прокси-сервера	`proxy.server.fqdn.or.ip`

Параметр	Описание	Значение по умолчанию
`ProxyEnabled`	PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений Positive Technologies	Флажок снят
`ProxyPassword`	Пароль служебной учетной записи для подключения PT UCS к прокси-серверу	—
`ProxyPort`	Порт прокси-сервера для входящего подключения от PT UCS	`8080`
`ProxyUser`	Логин служебной учетной записи для подключения PT UCS к прокси-серверу	—
`SaltMasterHost`	IP-адрес или FQDN сервера с модулем Salt Master	—
`SaltMinionLogLevel`	Уровень журналирования для модуля Salt Minion (возможные значения — `fatal`, `error`, `warn`, `info`, `debug` или `trace`)	`info`
`TelemetrySendPeriod`	Расписание отправки в Positive Technologies собранных данных о работе системы (в формате планировщика заданий cron)	`30 0 * * *`

Приложение Б. Параметры проверок по чек-листу

В разделе приведены описания параметров и их значения по умолчанию.

Инструкция по изменению проверок приведена в разделе «Изменение проверок по чек-листу» (см. раздел 20).

Таблица 22. Параметры проверок по чек-листу

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
Значимость активов присваивается политикой	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
		valued_assets_minscope	Проверка учитывает (true) или не учитывает (false) минимальное количество выделенных активов	true
		asset_importance_policy	Проверка учитывает (true) или не учитывает (false) наличие хотя бы одного включенного правила политики для присвоения значимости активов	true

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
Данные о значимых активах актуальны (аудит)	AM8-CriticalAssetsActualAudit	valued_assets_refresh_period	Максимальный период запуска задачи на сбор данных (в днях)	7
		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
		actual_valued_assets_amount	Максимальное количество неактуальных активов	3
		manual_asset_actuality_check	Проверка учитывает (true) или не учитывает (false) ручной контроль выполнения периодических задач сбора данных для обеспечения актуальных данных об активах, а также успешности их выполнения	true
		asset_actuality_policy	Проверка учитывает (true) или не учитывает (false) наличие хотя бы одного включенного правила политики для сроков актуальности данных (аудит)	false
Данные о значимых активах актуальны (пентест)	AM9-CriticalAssetsActualPentest	valued_assets_refresh_period	Максимальный период запуска задачи на сбор данных (в днях)	7

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		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
		actual_valued_assets_amount	Максимальное количество неактуальных активов	3
		manual_asset_actuality_check	Проверка учитывает (true) или не учитывает (false) ручной контроль выполнения периодических задач сбора данных для обеспечения актуальных данных об активах, а также успешности их выполнения	true
		asset_actuality_policy	Проверка учитывает (true) или не учитывает (false) наличие хотя бы одного включенного правила политики для сроков актуальности данных (пентест)	false
Проводится расширенный аудит активов (Windows)	SM1-ExtAuditCriticalWindowsAssets	share_objects	Проверка учитывает (true) или не учитывает (false) события системы безопасности Microsoft Windows с идентификаторами 5140 и 5145	true
		process_monitoring_powershell_operations	Проверка учитывает (true) или не учитывает (false) события системы безопасности Microsoft Windows с идентификаторами 4103 и 4104	true

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
		process_monitoring_winevents	Проверка учитывает (true) или не учитывает (false) события системы безопасности Microsoft Windows с идентификатором 4688 и события службы Microsoft Sysmon с идентификатором 1	true
		events_receive_interval	Максимальный период (в часах) между событиями, поступающими от одного и того же актива	120
		valued_assets_definition	Задача собирает данные с активов: — любого уровня значимости — all; — только среднего и высокого уровня — any; — только среднего — medium; — только высокого — high	any
		valued_assets_relative_amount	Минимальная доля (в процентах) от общего количества участвующих в проверке активов, с которых ожидается получение данных	95
Проводится расширенный аудит активов (Linux)	SM3-AuditDCriticalLinuxAssets	events_receive_interval	Максимальный период (в часах) между событиями, поступающими от одного и того же актива	120
		valued_assets_definition	Задача собирает данные с активов: — любого уровня значимости — all; — только среднего и высокого уровня — any;	any

Проверка	Блок параметров	Параметр	Описание	Значение по умолчанию
			— только среднего — `medium`; — только высокого — `high`	
Настроен мониторинг значимых источников событий	`SM4-EventSourcesMonitoring`	`event_sources_monitoring`	Задача собирает данные с активов: — любого уровня значимости — `all`; — только среднего и высокого уровня — `any`; — только среднего — `medium`; — только высокого — `high`	`any`
Общий параметр для всех проверок	—	`check_period`	Период (в минутах) запуска проверок и обновления их результатов в веб-интерфейсе	`15`

Приложение В. Возможности привилегии «Расширенные полномочия»

Раздел содержит описание возможностей привилегии «Расширенные полномочия».

Таблица 23. Возможности привилегии «Расширенные полномочия»

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

Предметный указатель

У

positive
technologies

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