MaxPatrol SIEM версия 27.6

Руководство администратора

© Positive Technologies, 2026.

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

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

Документ может быть изменен без предварительного уведомления.

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

Дата редакции документа: 10.09.2026

Содержание

1. Об этом документе ... 10
2. О MaxPatrol SIEM ... 11
   - 2.1. Архитектура MaxPatrol SIEM ... 12
     - 2.1.1. Компонент MaxPatrol 10 Core ... 12
     - 2.1.2. Компонент MaxPatrol SIEM Server ... 13
     - 2.1.3. Компонент MaxPatrol SIEM Events Storage ... 13
     - 2.1.4. Компонент MaxPatrol 10 Collector ... 13
     - 2.1.5. Компонент MaxPatrol NAD Sensor ... 14
     - 2.1.6. Компонент Knowledge Base ... 14
     - 2.1.7. Компонент Positive Technologies Management and Configuration ... 14
     - 2.1.8. Компонент PT Threat Intelligence Feeds ... 15
     - 2.1.9. Компонент PT Update and Configuration Service ... 15
     - 2.1.10. Компонент PT Retro Correlator ... 15
     - 2.1.11. Локальный сервер обновлений ... 15
   - 2.2. Алгоритм работы MaxPatrol SIEM и схема взаимодействия компонентов ... 16
3. Предоставление прав доступа ... 23
   - 3.1. О приложениях PT MC ... 24
   - 3.2. Предоставление доступа к событиям ... 24
   - 3.3. Предоставление доступа к активам, инцидентам и источникам ... 25
   - 3.4. Предоставление доступа к задачам на сбор данных ... 26
4. Распределенный поиск и репликация событий ... 27
   - 4.1. Добавление связей для распределенного поиска ... 29
   - 4.2. Удаление связи для распределенного поиска ... 29
   - 4.3. Добавление правила репликации событий ... 30
   - 4.4. Изменение правила репликации событий ... 30
   - 4.5. Удаление правила репликации событий ... 31
   - 4.6. Настройка защищенного подключения для кросс-кластерного поиска ... 31
5. Управление политиками ... 35
   - 5.1. Создание правила для значимости активов ... 36
   - 5.2. Создание правила для сроков актуальности данных ... 37
   - 5.3. Создание правила для активности активов ... 37
   - 5.4. Создание правила для потока событий с источников ... 38
6. Мониторинг источников событий ... 39
   - 6.1. Просмотр списка активов и источников событий ... 39
   - 6.2. Экспорт данных мониторинга источников в CSV-файл ... 39
   - 6.3. Создание правила для политики активности активов ... 40
   - 6.4. Создание правила для политики потока событий с источников ... 40
7. Работа с табличными списками ... 42
   - 7.1. Экспорт записей из табличных списков ... 43
   - 7.2. Импорт данных из файла формата CSV ... 43
   - 7.3. Добавление записи в табличный список ... 44
   - 7.4. Удаление записей из табличного списка ... 45
8. Включение и отключение правил корреляции и обогащения событий ... 46

8.1. Отключение правила корреляции ... 46
8.2. Включение правила корреляции ... 47
8.3. Отключение правила обогащения ... 47
8.4. Включение правила обогащения ... 47
9. Мониторинг состояния MaxPatrol SIEM ... 49
9.1. Страницы раздела «Управление системой» ... 49
9.2. Удаление недоступного коллектора ... 51
9.3. Настройка количества подзадач, одновременно выполняемых модулем ... 52
9.4. Мониторинг работы правил корреляции ... 52
10. Лимит EPS: условия и ограничения лицензионного контроля ... 54
11. Сбор телеметрических данных ... 56
12. Мониторинг ресурсов в Grafana ... 57
12.1. Настройка дашбордов в Grafana на отдельном сервере ... 58
12.2. Работа с дашбордом хранилища событий Elasticsearch ... 61
12.3. Работа с дашбордом хранилища событий LogSpace ... 65
12.4. Работа с дашбордом SIEM Aggregator ... 71
12.5. Работа с дашбордом SIEM Correlator ... 71
12.6. Работа с дашбордом SIEM Enricher ... 72
12.7. Работа с дашбордом SIEM Normalizer ... 74
12.8. Работа с дашбордом SIEM Pipeline metrics ... 74
12.9. Работа с дашбордом SIEM Receiver ... 76
12.10. Работа с дашбордом SIEM Renderer ... 76
12.11. Работа с дашбордом SIEM Router ... 78
12.12. Работа с дашбордом SIEM Storage ... 79
12.13. Работа с дашбордом Host metrics ... 80
12.14. Работа с дашбордом SqlStorage ... 82
13. Удаление истории изменения активов ... 86
14. Изменение сроков актуальности данных сканирования активов ... 89
15. Ротация результатов сканирования, импорта и ручного ввода активов ... 90
16. Максимальный размер собранных данных ... 91
17. Тайм-аут для подзадач сбора данных ... 92
18. Оптимизация выполнения PDQL-запросов для высоконагруженных систем ... 93
19. Резервное копирование данных ... 97
19.1. Особенности создания резервной копии роли SqlStorage ... 98
19.2. Создание резервной копии данных ... 98
19.3. Создание резервной копии индексов Elasticsearch на Linux ... 99
19.4. Создание резервной копии данных хранилища LogSpace ... 101
19.5. Создание резервной копии пользовательских определений роли RMQ Message Bus ... 102
19.6. О резервном копировании данных о площадках и их связях ... 102
20. Восстановление данных из резервной копии ... 103
20.1. Восстановление данных компонентов MaxPatrol SIEM на Linux из резервной копии ... 103
20.2. Восстановление индексов Elasticsearch из резервной копии на Linux ... 107
20.2.1. Восстановление всех индексов Elasticsearch из резервной копии на Linux ... 108
20.2.2. Восстановление индексов Elasticsearch, созданных за определенный период, из резервной копии на Linux ... 109
20.3. Восстановление данных хранилища LogSpace из резервной копии ... 109

20.4. Восстановление пользовательских определений роли RMQ Message Bus ... 110
20.5. О восстановлении резервной копии данных о площадках и их связях ... 111
21. Индексы Elasticsearch: ротация, архивация, перемещение, удаление, использование политик ILM ... 112
21.1. Просмотр списка индексов ... 114
21.2. Настройка ротации индексов ... 114
21.3. Архивация индексов ... 114
21.3.1. Создание хранилища для архивных индексов ... 115
21.3.2. Архивация индексов на Linux ... 115
21.3.3. Архивация индексов по расписанию ... 115
21.4. Восстановление индекса из архива ... 116
21.5. Удаление архивных индексов ... 116
21.5.1. Удаление архивных индексов на Linux ... 116
21.5.2. Удаление архивных индексов по расписанию ... 117
21.6. Удаление индекса без архивации ... 117
21.7. Перемещение индексов на Linux ... 117
21.8. Настройка политик ILM при смене конфигурации MaxPatrol SIEM ... 119
22. Разделы LogSpace: ротация, перемещение, резервное копирование и восстановление, переключение в режим гибридного хранилища ... 121
22.1. Просмотр списков разделов и архивов LogSpace ... 126
22.2. Удаление разделов и архивов LogSpace ... 126
22.3. Перемещение разделов LogSpace ... 126
22.4. Резервное копирование разделов ... 127
22.5. Архивация разделов ... 128
22.6. Восстановление раздела из архива ... 128
22.7. Перенос данных из Elasticsearch в LogSpace ... 128
22.8. Переключение LogSpace в режим гибридного хранилища ... 131
23. Гибридное хранилище LogSpace: пути к хранилищам, политики переноса данных ... 133
24. Настройка кэш-памяти для индексов LogSpace ... 135
25. Смена паролей служебных учетных записей ... 137
25.1. Смена пароля служебной учетной записи в PostgreSQL ... 137
25.2. Смена паролей служебных учетных записей в RabbitMQ ... 138
25.2.1. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Core на Linux ... 138
25.2.2. RabbitMQ: смена паролей служебных учетных записей компонента MP SIEM Server на Linux ... 139
25.2.2.1. Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на один сервер ... 139
25.2.2.2. Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на разные серверы ... 140
25.2.3. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Microsoft Windows ... 141
25.2.4. RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Linux ... 142
25.3. Смена пароля служебной учетной записи в Grafana ... 143
26. Смена пароля учетной записи администратора RabbitMQ ... 144
27. Настройка журналирования работы MaxPatrol SIEM ... 146

27.1. Настройка журналирования работы компонента MP 10 Core на Linux ... 146
27.2. Настройка журналирования работы компонента MP SIEM Server ... 146
27.3. Настройка журналирования работы компонента MP SIEM Events Storage ... 147
27.4. Настройка журналирования работы компонента MP 10 Collector ... 148
27.5. Настройка журналирования работы LogSpace ... 148
28. Настройка обогащения событий данными геолокации ... 150
29. Просмотр и изменение параметров конфигурации MaxPatrol SIEM ... 152
29.1. Просмотр конфигурации роли ... 153
29.2. Изменение конфигурации роли ... 153
29.3. Управление изменением конфигурации ролей с помощью манифеста ... 155
29.3.1. Изменение конфигурации ролей с помощью манифеста ... 155
29.3.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей ... 156
29.4. Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch ... 160
29.5. Изменение степени сжатия данных в Elasticsearch ... 161
29.6. Регистрация событий при нарушении и восстановлении параметров источников ... 162
29.7. Включение регистрозависимого поиска по схеме полей событий ... 162
29.8. Настройка прокси-сервера для онлайн-активации PT MC ... 163
29.9. Включение AI-поиска по запросам ... 163
29.10. Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol SIEM ... 163
29.11. Изменение времени устаревания активов ... 164
29.12. Отключение правил Declarative Detect ... 165
29.13. Изменение времени хранения индексов Elasticsearch в горячей стадии ... 166
30. Отключение отправки ненормализованных событий облегченной версией компонента MP SIEM Server («SIEM на коллекторе») ... 167
31. Смена алгоритма контроля потока событий ... 168
32. Удаление экземпляра роли Collector ... 169
33. Настройка очереди выпуска отчетов ... 170
34. Пользовательские поля в модели актива ... 171
34.1. Добавление пользовательских полей в модель актива ... 172
34.2. Добавление описания пользовательских полей ... 177
34.3. Изменение имен пользовательских полей ... 179
34.4. Удаление пользовательских полей из модели актива ... 180
35. Работа с инфраструктурами ... 182
35.1. Создание инфраструктуры ... 182
35.2. Изменение названия инфраструктуры ... 182
35.3. Удаление инфраструктуры ... 183
36. Изменение проверок по чек-листу ... 184
37. Диагностика и решение проблем ... 185
37.1. Обмен данными между компонентами системы ... 187
37.1.1. Диагностика работы RabbitMQ ... 189
37.1.2. Вход в веб-интерфейс RabbitMQ ... 190
37.1.3. Мониторинг потока событий в RabbitMQ ... 191
37.1.4. Очередь storageq не уменьшается ... 191
37.1.5. Очередь siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается ... 192

37.1.6. Очередь storageq растет и начинает уменьшаться только после появления ошибки 193
37.1.7. Очередь siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растет и начинает уменьшаться только после появления ошибки 194
37.1.8. Не удается запустить контейнер RMQ 195
37.1.9. Ошибка «Closing AMQP connection, missed heartbeats from client, timeout» 195
37.1.10. Ошибка «Shovel <Имя> failed to connect (URI: <Адрес>): closed» 196
37.1.11. Ошибка «Unknown CA, error handshake» 196
37.1.12. Ошибка «No route to» 197
37.2. Мониторинг состояния RabbitMQ и Elasticsearch 197
37.3. Ошибка «Объем очередей SIEM Server Messaging Service на узле <FQDN сервера> достиг критического порога» 200
37.4. Ошибка «Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен» 201
37.5. Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога» 202
37.6. Ошибка «Объем свободного места на диске, выделенном для SIEM Messaging Service, достиг критического порога» 202
37.7. Ошибка «Объем свободного места на диске, выделенном для SIEM Events Storage, достиг критического порога» 203
37.8. Ошибка «Компонент Core Messaging Service недоступен. Health Monitoring Service не может получать сообщения от других систем» 204
37.9. Предупреждение «Время выполнения запросов у SIEM Events Storage на узле <FQDN сервера> достигло критического порога» 205
37.10. Система не получает данные от задачи 205
37.11. Отсутствуют события от источников 207
37.12. Задача аудита не собирает сведения об активах 208
37.13. Не приходят уведомления, отправляемые по электронной почте 208
37.14. Ошибка «Sdk пакет <Номер версии> поврежден. Необходимо восстановление» 209
37.15. Не удается импортировать отчет из MaxPatrol 8 209
37.16. Настройка компонентов после изменения IP-адресов или FQDN их серверов 210
37.17. Подсеть Docker-контейнера MaxPatrol SIEM совпадает с одной из подсетей предприятия 211
37.18. Ошибка при установке, переконфигурации или обновлении компонентов в высоконагруженных системах 215
37.19. Задача на сбор данных с коллектором на Windows завершается с ошибкой 215
37.20. Ошибка «Глубина поиска по событиям сокращена до 7 дней» 216
37.21. Ошибка «Запуск задач на сбор событий отключен» 217
37.22. Ошибка «Корреляция событий отключена» 217
37.23. Ошибка «Доля свободного дискового пространства, выделенного для табличных списков в <Название компонента> на узле <Название узла>, достигла 5%» 218
37.24. Большое количество запросов к DNS-серверу от Docker-контейнеров сервера MP 10 Core 219
37.25. Установка модуля Salt Minion завершается с ошибкой 220
37.26. Не отображаются события в веб-интерфейсе после установки или обновления MaxPatrol SIEM 220
37.27. Ошибка при загрузке шаблона для экспорта записей в формате XLSX 221
37.28. Ошибка при проверке подключения 222
37.29. Ошибка при обновлении роли Deployer 222
37.30. Ошибка при создании резервной копии данных LogSpace после обновления Astra Linux 223

37.31. Слишком много открытых файлов при создании резервной копии или восстановлении данных LogSpace ... 223
37.32. Настройка LimitMEMLOCK для исправления ошибки ENOMEM при использовании LogSpace ... 224
37.33. Ошибки, связанные с конфигурацией LogSpace ... 225
37.34. Ошибки взаимодействия служб MaxPatrol SIEM с LogSpace ... 228
37.35. Защита LogSpace от принудительной остановки службой OOM Killer ... 229
37.36. На коллекторах накапливается и не разбирается очередь событий ... 230
37.37. Ошибка при обновлении роли, связанная с именем Docker-контейнера ... 231
37.38. Ошибка «There is no application package with following properties: WithHidden True Id <Идентификатор пакета приложения>» при обновлении MaxPatrol SIEM ... 232
37.39. Ошибки, связанные с сертификатом MP 10 Collector на Microsoft Windows ... 233
37.40. Ошибка «The repository <Ссылка на репозиторий> does not have a Release file» ... 234
37.41. Диагностика и решение проблем при работе с Elasticsearch ... 235
37.41.1. Индексы Elasticsearch находятся в состоянии red ... 235
37.41.2. Служба Elasticsearch останавливается через некоторое время после запуска ... 236
37.41.3. Индексы Elasticsearch не переходят из горячей стадии в теплую ... 237
37.41.4. Ошибки Elasticsearch при замедлении его работы и потере отображения данных ... 237
37.42. Справочная информация ... 239
37.42.1. Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки ... 240
37.42.2. Сбор информации о нагрузке на файловую систему и запущенных процессах ... 240
37.42.3. Просмотр статуса службы ... 241
37.42.4. Проверка доступности сетевого порта сервера ... 241
37.42.5. Деактивация PT MC ... 241
37.42.6. Проверка работоспособности Elasticsearch ... 242
37.42.6.1. Проверка прав доступа и портов ... 242
37.42.6.2. Расположение индексов Elasticsearch ... 242
37.42.6.3. Диагностика Elasticsearch на основании запросов к API ... 242
37.42.7. Создание дампа памяти процесса ... 245
37.42.8. Расположение файлов журналов ... 247
37.42.9. Расположение временных файлов аудита ... 249
37.42.10. Параметры мониторинга обработки активов ... 250
37.42.11. Экспорт конфигурационных параметров ролей в файл ... 252
37.42.12. Экспорт и импорт пользовательских профилей ... 252
37.42.13. Управление системой с помощью утилиты deployer ... 256
37.42.14. Настройка мандатного контроля целостности для Astra Linux ... 258
37.42.15. Расположение пользовательских сертификатов ... 259
37.42.16. Реорганизация данных в таблицах СУБД PostgreSQL ... 259
37.42.17. Удаление неиспользуемых пакетов ролей ... 261
37.42.18. Добавление исключений в Kaspersky Endpoint Security для БД PostgreSQL ... 261
37.42.19. Особенности обновления Astra Linux при использовании хранилища LogSpace ... 262
37.42.20. Просмотр версии LogSpace ... 263

38. О технической поддержке 264
Приложение А. Привилегии и роли MaxPatrol SIEM 268
Приложение Б. Параметры конфигурации компонентов MaxPatrol SIEM на Linux 271
Приложение В. Параметры проверок по чек-листу 306
Приложение Г. О проверке серверов перед установкой ролей 311
Приложение Д. Возможности привилегии «Расширенные полномочия» 313
Предметный указатель 314

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 и обновлению 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

Компонент MaxPatrol 10 Core (см. раздел 2.1.1)

Компонент MaxPatrol SIEM Server (см. раздел 2.1.2)

Компонент MaxPatrol SIEM Events Storage (см. раздел 2.1.3)

Компонент MaxPatrol 10 Collector (см. раздел 2.1.4)

Компонент MaxPatrol NAD Sensor (см. раздел 2.1.5)

Компонент Knowledge Base (см. раздел 2.1.6)

Компонент Positive Technologies Management and Configuration (см. раздел 2.1.7)

Компонент PT Threat Intelligence Feeds (см. раздел 2.1.8)

Компонент PT Update and Configuration Service (см. раздел 2.1.9)

Компонент PT Retro Correlator (см. раздел 2.1.10)

Локальный сервер обновлений (см. раздел 2.1.11)

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;
- поддержка 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:

— нормализация, агрегация, обогащение и корреляция событий;

— автоматическое создание инцидентов;

— создание активов из событий;

— привязка 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 открытые сетевые сервисы на них, а также проводить специализированные проверки в режиме теста на проникновение.

MP 10 Collector собирает следующую информацию об активах:

— название;

— версия и производитель операционной системы;

— установленные обновления ОС;

— список установленного ПО;

— параметры ОС и ПО;

— учетные записи пользователей и их привилегии;

— данные об аппаратном обеспечении;

— информацию о запущенных сетевых сервисах и службах ОС;

— сведения о параметрах сети и средствах 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. Также вместе с Knowledge Base поставляются утилиты SDK для работы с данными базы.

2.1.7. Компонент Positive Technologies Management and Configuration

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

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

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

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

— управление иерархией продуктов Positive Technologies;

— журналирование действий пользователей;

— управление лицензиями продуктов Positive Technologies;

— прием, анонимизацию, шифрование и отправку телеметрических данных.

2.1.8. Компонент PT Threat Intelligence Feeds

Компонент PT Threat Intelligence Feeds (далее также — PT Feeds) 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 Feeds поддерживает репутационные сервисы компаний «Лаборатория Касперского», Positive Technologies, платформы MISP Threat Sharing и системы PT CybSI. Также PT Feeds поддерживает получение данных в формате STIX 2.1 по протоколу TAXII. Лицензию на репутационные сервисы компании «Лаборатория Касперского» необходимо приобретать у производителя (подробнее на сайте kaspersky.ru).

2.1.9. Компонент PT Update and Configuration Service

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

- обновление данных об угрозах информационной безопасности и индикаторах компрометации для компонента PT Feeds;
- проверку наличия и загрузку дистрибутива с новыми версиями компонентов с глобального сервера обновлений Positive Technologies.

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

2.1.10. 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 mp agent.service и siemserver-retrocontroller.service.

2.1.11. Локальный сервер обновлений

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

2.2. Алгоритм работы MaxPatrol 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 Feeds 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 данных для компонента PT Feeds и загрузку дистрибутивов с новыми версиями компонентов.
10. Компонент BAD обеспечивает обнаружение аномального поведения пользователей или сущностей в IT-инфраструктуре организации и оценку степени риска событий с помощью моделей машинного обучения.
11. Локальный сервер обновлений обеспечивает загрузку и передачу обновлений с глобального сервера обновлений Positive Technologies при отсутствии прямого доступа к интернету.
12. Локальные агенты OTEL собирают сведения со всех компонентов системы и отправляют данные в коллектор OTEL. Коллектор собирает данные и записывает их в хранилище. Полученные метрики направляются в сервис VictoriaMetrics, который является частью роли Observability в приложении PT MC.

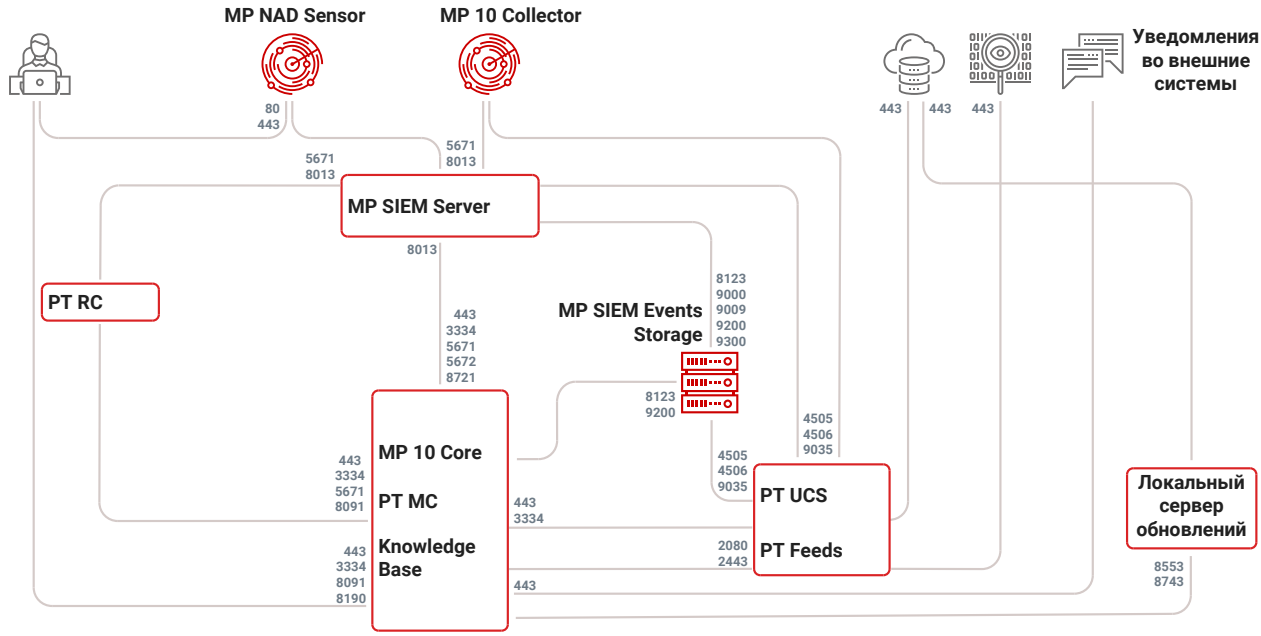


Рисунок 1. Взаимодействие компонентов MaxPatrol SIEM

Для получения обновлений межсетевой экран сервера компонента PT UCS не должен блокировать адреса глобальных серверов обновлений Positive Technologies — update.ptsecurity.ru и update.ptsecurity.com. Для обеспечения сетевого взаимодействия компонентов MaxPatrol 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, 5672, 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
Рабочая станция пользователя, компонент PT RC	PT MC	3334
MP 10 Core	MP SIEM Server	8013
MP 10 Collector, MP NAD Sensor	MP SIEM Server	5671, 8013
Knowledge Base	MP SIEM Server	8013
PT RC	MP SIEM Server	8013, 5671
MP 10 Core	MP SIEM Events Storage	8123[1], 9200[2]
MP SIEM Server	MP SIEM Events Storage	8123[1], 9000, 9009, 9200[2], 9300
MP SIEM Events Storage	MP SIEM Events Storage	9000, 9009 (только для кросс-кластерного поиска между хранилищами событий LogSpace)
MP SIEM Events Storage	MP SIEM Events Storage	9200, 9300 (только для кросс-кластерного поиска между хранилищами событий Elasticsearch)
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

1 При использовании компонента MP SIEM Events Storage с хранилищем событий LogSpace.

2 При использовании компонента MP SIEM Events Storage с хранилищем событий Elasticsearch.

Источник	Получатель	TCP-порт
Docker Registry	Deployer	5000
PT UCS, локальный сервер обновлений	Глобальный сервер обновлений	443
MP 10 Core	PT Feeds	2080, 2443
PT Feeds	Репутационный сервис, предоставляющий данные об угрозах ИБ и индикаторах компрометации	443
PT MC	Локальный сервер обновлений	8553, 8743
Локальные агенты OTEL	Коллектор OTEL	4318

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

Перечень портов, необходимых для установки и работы MaxPatrol BAD, представлен в документации MaxPatrol BAD.

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.

Для возможности репликации событий необходимо обеспечить сетевое взаимодействие через TCP-порты 5671 и 5672 между серверами MP 10 Core связываемых приложений, а также между серверами MP SIEM Server связываемых приложений.

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

Открытые порты, используемые службами MaxPatrol SIEM

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

Таблица 2. Открытые порты служб

Служба	Порты
ai.assistant.proxy	8738
archivemanager	8737

Служба	Порты
assets.groups	8730
assets.identity	8721
assets.input	8731
assets.processing	8723
assets.projections	8799
assets.scans	8722
assets.temporalreadmodel	8782
assets.triggers	8733
collector-agent (Management and Configuration)	54528, 54529
collector-agent (Core)	4317—4320, 55679—55680
collector-server	4317, 4318
consul-server	8320-8322
contentservice	8727
core-groups	8787
core-triggers	8834
core-chromium	9232
core.analytics.reportsdelivery	8762
core.apigateway	8711
core.assets.compliance.control	8724
core.contentdeployer	8586
core.deployment.configuration	8740
core.events	8776
core.events.monitoring	8706
core.events.triggers	8707
core.healthmonitoring	8774
core.healthmonitoring.agent	8773
core.incidents	8781
core.incidents.triggers	8779
core.incidentsreadmodel	8777
core.pipeline.control.service	8729
core.portal	8712

Служба	Порты
core.scanning	8769
core.siem-querying	8050
core.siemmanager	8990
core.tables	8735
core.tenants	8703
core.topology	8775
core.topology.analyzer	8705
help-portal-maxpatrol (Core)	4211
help-portal-maxpatrol (Management and Configuration)	3336
kb-apigateway	8190
kb-consul	8531
kb-contentdeployer	8195
kb-ui	8091
kb-validationservice	8095
mc-apigateway	8709
mc-consul	8511
mc-portal	8710
messagebus-rabbitmq	4369, 5671, 5672, 15671, 15672
observability.grafana	9002
platform-policies	8852
platform-branding (Management and Configuration)	3335
platform-branding (Knowledge Base)	8092
platform.branding (Core)	4210
storage-pgadmin	9001
storage-postgres	5432
storage-victorialogs	9428
storage-victoriametrics	8428
task-manager	10239
telemetry.adapter.victoriametrics	9339
ti-feeds	2443
ui.am-app	4204

Служба	Порты
ui.hcc-app	4212
ui.infosec-platform	3334
ui.infosec-platform-dashboards	4207
ui.infosec-platform-edr-adapter	4301
ui.infosec-platform-mp10	4202
ui.infosec-platform-navbar	4201
ui.infosec-platform-reports	3208
ui.infosec-platform-siem-api	4206
ui.infosec-platform-mc	4300
ui.platform-services	4209
ui.vm-app	4205
vulnerabilities-processing	8811

3. Предоставление прав доступа

В MaxPatrol 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, инциденты и задачи на сбор событий, 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 событиям (см. раздел 3.2), активам, инцидентам, источникам (см. раздел 3.3) и задачам на сбор данных (см. раздел 3.4) в соответствии с производственными задачами пользователя.

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

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

Предоставление доступа к задачам на сбор данных (см. раздел 3.4)

См. также

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

3.1. О приложениях PT MC

При развертывании MaxPatrol SIEM в PT MC регистрируются следующие приложения:

- Management and Configuration — предназначено для управления учетными записями и ролями пользователей во всех приложениях системы, а также для управления площадками и связями между ними. Подробную информацию о площадка и связях см. в разделе «Площадки и связи между ними» Руководства администратора PT MC. По умолчанию содержит стандартные роли **Администратор** (с полными правами), **Пользователь** (с правами на просмотр и изменение информации в личном профиле) и **Оператор** (с правами на просмотр всей информации в приложении). Приложение также предоставляет пользователю возможность регистрировать, переименовывать и удалять приложения из системы. Для этого роль пользователя должна содержать соответствующие привилегии — **Переименование приложений** и **Добавление и удаление приложений**. Для повышения безопасности вы можете настроить в системе обязательное подтверждение регистрации приложений, установленных неавторизованными пользователями, в соответствии с инструкцией «Включение подтверждения регистрации приложений» Руководства администратора PT MC.
- MaxPatrol 10 — предназначено для настройки сбора данных об IT-инфраструктуре предприятия и работы с активами, источниками, событиями и инцидентами. По умолчанию приложение содержит стандартные роли **Администратор** (с полными правами на просмотр и изменение данных в приложении), **Оператор** (с ограниченными правами на просмотр и изменение данных) и **Наблюдатель** (с правами только на просмотр данных). Вы можете просмотреть список привилегий, доступных для этих ролей, на странице **Система** → **Права доступа**.
- Knowledge Base — 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>** в блоке параметров **Доступ к событиям** нажмите .
4. В открывшемся окне 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>** в блоке параметров **Доступ к активам, инцидентам и источникам** нажмите .
  4. В открывшемся окне в раскрывающемся списке **Доступ** выберите необходимый тип доступа.
  5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы активов, к которым необходимо предоставить доступ.

     Примечание. Вы можете искать группы активов с помощью поля поиска и выбирать группы активов, устанавливая флажки напротив них.
  6. Нажмите кнопку **Сохранить**.

  Доступ к активам предоставлен.

3.4. Предоставление доступа к задачам на сбор данных

- Чтобы предоставить доступ к задачам на сбор данных:

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

     Откроется страница **Права доступа**.

  2. В панели **Роли** выберите роль тех пользователей, которым необходимо предоставить доступ к задачам на сбор данных.

  3. В панели **<Название роли>** в блоке параметров **Доступ к задачам на сбор данных** нажмите  .

  4. В открывшемся окне в раскрывающемся списке **Доступ** выберите необходимый тип доступа.

  5. Если вы выбрали ограниченный доступ, в раскрывающемся списке выберите группы задач на сбор данных, к которым необходимо предоставить доступ.

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

  6. Нажмите кнопку **Сохранить**.

  Доступ к задачам предоставлен.

4. 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.

> **Внимание!** Распределенный поиск событий возможен только между хранилищами одного типа: все связанные приложения должны использовать либо хранилище Elasticsearch, либо LogSpace. Распределенный поиск событий между хранилищами Elasticsearch и LogSpace невозможен.

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. Если используется хранилище событий LogSpace — разрешить сетевое подключение серверов MP SIEM Server и MP 10 Core к серверам всех MP SIEM Events Storage на площадке по TCP-порту 8123, разрешить сетевое подключение между серверами всех MP SIEM Events Storage на площадке по TCP-портам 9000, 9009.
2. Если используется хранилище событий Elasticsearch — разрешить сетевое подключение серверов MP SIEM Server и MP 10 Core к серверам всех MP SIEM Events Storage на площадке по TCP-порту 9200, разрешить сетевое подключение между серверами всех MP SIEM Events Storage на площадке по TCP-портам 9200, 9300.
3. Повторно запустить настройку компонента MP 10 Core:

```
deployer instance reconfigure -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 необходимо обеспечить сетевое взаимодействие через TCP-порты 443, 5671, 5672 между серверами MP 10 Core связываемых приложений и через TCP-порты 5671, 5672 между серверами MP SIEM Server 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)

Настройка защищенного подключения для кросс-кластерного поиска (см. раздел 4.6)

4.1. Добавление связей для распределенного поиска

► Чтобы добавить связи:

1. В главном меню нажмите и выберите **Management and Configuration**.
2. В главном меню выберите **Площадки**.

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

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

4.2. Удаление связи для распределенного поиска

► Чтобы удалить связь:

1. В главном меню нажмите и выберите **Management and Configuration**.
2. В главном меню выберите **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. Нажмите **Удалить** и подтвердите удаление.

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 выберите **Management and Configuration**.
2. В главном меню выберите **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 **Добавить правило репликации**.

   Откроется окно **Новое правило репликации**.
6. В поле **Получатель** укажите приложение, которое будет получать реплицированные события.
7. Нажмите **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 **Завершить настройку**.
11. Нажмите **Добавить**.

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

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 выберите **Management and Configuration**.
2. В главном меню выберите **Площадки**.

   Откроется страница **Площадки**.
3. На схеме выберите приложение.
4. В панели **Приложение MaxPatrol 10** выберите вкладку **Репликация событий**.

5. Выберите правило.
6. Нажмите **Редактировать**.

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

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

4.5. Удаление правила репликации событий

- Чтобы удалить правило:

  1. В главном меню нажмите  и выберите **Management and Configuration**.
  2. В главном меню выберите **Площадки**.

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

4.6. Настройка защищенного подключения для кросс-кластерного поиска

Вы можете настроить защищенное подключение, чтобы использовать кросс-кластерный поиск событий. Кросс-кластерный поиск позволяет выполнять из одного приложения MaxPatrol SIEM фильтрацию событий, которые собираются, обрабатываются и хранятся в разных конвейерах.

Перед настройкой защищенного подключения необходимо:

1. Если используется хранилище событий LogSpace — разрешить сетевое подключение серверов MP SIEM Server и MP 10 Core к серверам всех MP SIEM Events Storage на площадке по TCP-порту 8123, разрешить сетевое подключение между серверами всех MP SIEM Events Storage на площадке по TCP-портам 9000, 9009.
2. Если используется хранилище событий Elasticsearch — разрешить сетевое подключение серверов MP SIEM Server и MP 10 Core к серверам всех MP SIEM Events Storage на площадке по TCP-порту 9200, разрешить сетевое подключение между серверами всех MP SIEM Events Storage на площадке по TCP-портам 9200, 9300.

Для настройки защищенного подключения можно использовать пользовательский сертификат безопасности, который должен отвечать следующим требованиям:

— использовать алгоритм подписи SHA-256;

— использовать алгоритм шифрования ключей RSA;

— соответствовать формату PEM;

— использовать отдельные файлы для хранения сертификата центра сертификации (ЦС), пользовательского сертификата и закрытого ключа;

— иметь заголовок `BEGIN CERTIFICATE` без дополнительных заголовков;

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

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

— включать область применения сертификата Digital Signature или Key Encipherment;

— содержать в расширении Subject Alternative Name (SAN) запись об IP-адресе компонента, для которого предназначен сертификат;

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

Настройка защищенного подключения для MP SIEM Events Storage с хранилищем событий LogSpace

► Чтобы настроить защищенное подключение к MP SIEM Events Storage для кросс-кластерного поиска:

1. Выполните одно из действий:

   • Если нужно использовать стандартный сертификат, скопируйте файлы `rootCA.crt`, `logpace_auth.crt` и `logspace_auth.key` из каталога `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` роли Event Storage главного конвейера в аналогичные каталоги для остальных ролей Event Storage.

   • Если нужно использовать пользовательский сертификат, разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей Event Storage.

2. Выполните одно из действий:

   • Если нужно использовать стандартный сертификат, скопируйте файл `rootCA.crt` в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей SIEM Server и Core.

- Если нужно использовать пользовательский сертификат, разместите файлы сертификата ЦС в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей SIEM Server и Core.

3. Измените конфигурацию каждой роли Event Storage:

   ```
   EnableLogspaceSecurity: [x]
   LogspaceCACertificatePath: <Полный путь к файлу с цепочкой корневых сертификатов>
   LogspaceCertificatePath: <Полный путь к файлу пользовательского сертификата>
   LogspaceKeyPath: <Полный путь к файлу закрытого ключа>
   ```

4. Измените конфигурацию каждой роли SIEM Server:

   ```
   EnableLogspaceSecurity: [x]
   LogspaceCertificateCA: <Полный путь к файлу сертификата ЦС>
   ```

5. Измените конфигурацию роли Core:

   ```
   EnableEventStorageSecurity: [x]
   EventStorageAuthCertificateCA: <Имя файла сертификата ЦС>
   ```

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

Настройка защищенного подключения для MP SIEM Events Storage с хранилищем событий Elasticsearch

- Чтобы настроить защищенное подключение к MP SIEM Events Storage для кросс-кластерного поиска:

1. Выполните одно из действий:

   - Если нужно использовать стандартный сертификат, скопируйте файлы `rootCA.crt`, `elasticsearch_auth.crt` и `elasticsearch_auth.key` из каталога `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` роли SIEM Storage главного конвейера в аналогичные каталоги для остальных ролей SIEM Storage.
   - Если нужно использовать пользовательский сертификат, разместите файлы сертификата ЦС, пользовательского сертификата и закрытого ключа в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей SIEM Storage.

2. Выполните одно из действий:

   - Если нужно использовать стандартный сертификат, скопируйте файл `rootCA.crt` в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей SIEM Server и Core.
   - Если нужно использовать пользовательский сертификат, разместите файлы сертификата ЦС в каталогах `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs` для ролей SIEM Server и Core.

3. Измените конфигурацию каждой роли SIEM Storage:

   ```
   ElasticSearchCACertificatePath: <Полный путь к файлу с цепочкой корневых сертификатов>
   ElasticSearchCertificatePath: <Полный путь к файлу пользовательского сертификата>
   ElasticSearchKeyPath: <Полный путь к файлу закрытого ключа>
   EnableElasticsearchSecurity: [x]
   ```

4. На всех серверах с установленной ролью SIEM Storage измените конфигурацию службы siem-storage:

   ```
   dpkg-reconfigure siem-storage
   ```

5. Измените конфигурацию каждой роли MP SIEM Server:

   ```
   EnableElasticsearchSecurity: [x]
   ElasticsearchCertificateCA: <Полный путь к файлу сертификата ЦС>
   ```

6. Измените конфигурацию роли Core:

   ```
   EnableEventStorageSecurity: [x]
   EventStorageAuthCertificateCA: <Имя файла сертификата ЦС>
   ```

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

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.

Порядок применения правил

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

Применение изменений в политиках

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

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

Типы политик

Работа с правилами

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

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

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

В таблице в центральной панели отображаются состояния правил:

 — правило работает;

 — правило остановлено;

 — правило работает с предупреждением;

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

В этом разделе

Создание правила для значимости активов (см. раздел 5.1)

Создание правила для сроков актуальности данных (см. раздел 5.2)

Создание правила для активности активов (см. раздел 5.3)

Создание правила для потока событий с источников (см. раздел 5.4)

5.1. Создание правила для значимости активов

- Чтобы создать правило:

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

     Примечание. Вы можете указать группы активов и отфильтровать активы с помощью PDQL-запроса. По ссылке **Вставить условие** доступны стандартные фильтры.
  6. Выберите значимость, которую правило будет назначать активам.
  7. Нажмите **Сохранить**.

  Правило создано. Система начнет использовать его только после применения изменений в политике (см. раздел 5).

5.2. Создание правила для сроков актуальности данных

- Чтобы создать правило:

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

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

  Правило создано. Система начнет использовать его только после применения изменений в политике (см. раздел 5).

5.3. Создание правила для активности активов

- Чтобы создать правило:

  1. В главном меню выберите **Система** → **Политики**.
  2. В панели **Список политик** выберите политику для активности активов.
  3. Нажмите **Создать правило**.
  4. Введите название правила.
  5. Выберите активы, которые необходимо проверять на соответствие требованиям.

     Примечание. Вы можете ввести условие фильтрации активов на языке PDQL в поле **Фильтр активов**.
  6. В панели **Контроль активности активов** в блоке параметров **Период контроля** выберите тип проверяемых узлов.

     Для правила будет задан период контроля, рекомендуемый для выбранного типа узлов.
  7. Нажмите **Сохранить**.

  Правило создано. Система начнет использовать его только после применения изменений в политике (см. раздел 5).

5.4. Создание правила для потока событий с источников

► Чтобы создать правило:

1. В главном меню выберите **Система** → **Политики**.
2. В панели **Список политик** выберите политику для потока событий с источников.
3. Нажмите **Создать правило**.
4. Введите название правила.
5. Выберите активы, которые необходимо проверять на соответствие требованиям.

   Примечание. Вы можете ввести условие фильтрации активов на языке PDQL в поле **Фильтр активов**.
6. Во всплывающем окне по кнопке **Добавить источник** в иерархическом списке установите флажки напротив источников, для которых необходимо контролировать поток событий, и нажмите кнопку **Добавить**.
7. Для каждого добавленного источника выберите тип проверяемых узлов.

   Для источников будут заданы период контроля, частота проверки и допустимый поток событий, рекомендуемые для выбранных типов узлов.

   Примечание. По кнопке вы можете изменять рекомендуемые параметры контроля — устанавливать максимальную и минимальную границы для потока событий по количеству событий в секунду (EPS) или по количеству событий за период. Вы также можете контролировать отклонение потока событий относительно среднего значения (в процентах). Среднее значение потока в этом случае рассчитывается за период в текущих или предыдущих сутках, ближайший к периоду, указанному в поле **Период контроля**. Рассчитать среднее значение потока событий для указанного периода контроля вы можете по кнопке .
8. Нажмите **Сохранить**.

Правило создано. Система начнет использовать его только после применения изменений в политике (см. раздел 5).

6. Мониторинг источников событий

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

На странице **Мониторинг источников** вы можете просматривать состояние активов, к которым применены правила политик мониторинга источников, создавать правила для политик мониторинга источников, а также экспортировать данные мониторинга источников в файл формата CSV.

MaxPatrol SIEM анализирует данные от источников один раз в минуту — проверяет наличие событий от источника и величину задержки между появлением события на источнике и его поступлением в конвейер обработки событий. Решение об отсутствии активности источника принимается по истечении интервала времени, заданного с помощью параметра **Частота проверки**. Например, при частоте проверки 60 минут отсутствие событий будет зафиксировано только при условии, что в течение всех 60 минут от источника не поступило ни одного события.

В этом разделе

Просмотр списка активов и источников событий (см. раздел 6.1)

Экспорт данных мониторинга источников в CSV-файл (см. раздел 6.2)

Создание правила для политики активности активов (см. раздел 6.3)

Создание правила для политики потока событий с источников (см. раздел 6.4)

6.1. Просмотр списка активов и источников событий

- Чтобы просмотреть список активов и источников событий:

  1. В главном меню выберите **Сбор данных** → **Мониторинг источников**.
  2. В верхней части страницы по ссылке выберите активы.

     В центральной панели отобразится таблица активов и источников на них.

6.2. Экспорт данных мониторинга источников в CSV-файл

Данные мониторинга источников могут быть представлены в виде таблицы активов. Вы можете экспортировать отфильтрованные и сгруппированные данные из таблицы в файл формата CSV для последующего анализа.

- Чтобы экспортировать данные мониторинга по активам:

  1. В главном меню выберите **Сбор данных** → **Мониторинг источников**.
  2. В верхней части страницы по ссылке выберите активы.

3. Если требуется, в таблице выберите отдельные источники на активах.

   Примечание. Вы также можете отфильтровать активы, выбрав группу активов в панели **Источники** и фильтр активов в панели **Фильтры**.

4. Нажмите **Экспорт** и в раскрывшемся меню выберите вариант экспорта.

6.3. Создание правила для политики активности активов

- Чтобы создать правило:

  1. В главном меню выберите **Сбор данных** → **Мониторинг источников**.
  2. В верхней части страницы по ссылке выберите активы.
  3. В панели инструментов нажмите кнопку **Создать правило для политики** и в раскрывшемся меню выберите пункт **Активность активов**.
  4. Введите название правила.
  5. Выберите активы, которые необходимо проверять на соответствие требованиям.

     Примечание. Вы можете ввести условие фильтрации активов на языке PDQL в поле **Фильтр активов**.

  6. В панели **Контроль активности активов** в блоке параметров **Период контроля** выберите тип проверяемых узлов.

     Для правила будет задан период контроля, рекомендуемый для выбранного типа узлов.

  7. Нажмите кнопку **Сохранить**.

  Правило создано. Система начнет использовать его только после применения изменений в политике (см. раздел 5).

6.4. Создание правила для политики потока событий с источников

- Чтобы создать правило:

  1. В главном меню выберите **Сбор данных** → **Мониторинг источников**.

     Откроется страница **Мониторинг источников**.

  2. В верхней части страницы по ссылке выберите активы.
  3. В панели инструментов нажмите **Создать правило для политики** и в раскрывшемся меню выберите пункт **Поток событий с источников**.

     Откроется страница **Создание правила**.

  4. Введите название правила.

5. Выберите активы, которые необходимо проверять на соответствие требованиям.

   Примечание. Вы можете ввести условие фильтрации активов на языке PDQL в поле **Фильтр активов**.

6. Во всплывающем окне по кнопке **Добавить источник** в иерархическом списке установите флажки напротив источников, для которых необходимо контролировать поток событий, и нажмите кнопку **Добавить**.

7. Для каждого добавленного источника выберите тип проверяемых узлов.

   Для источников будут заданы период контроля, частота проверки и допустимый поток событий, рекомендуемые для выбранных типов узлов.

   Примечание. По кнопке вы можете изменять рекомендуемые параметры контроля — устанавливать максимальную и минимальную границы для потока событий по количеству событий в секунду (EPS) или по количеству событий за период. Вы также можете контролировать отклонение потока событий относительно среднего значения (в процентах). Среднее значение потока в этом случае рассчитывается за период в текущих или предыдущих сутках, ближайший к периоду, указанному в поле **Период контроля**. Рассчитать среднее значение потока событий для указанного периода контроля вы можете по кнопке .

8. Нажмите кнопку **Сохранить**.

Правило создано. Система начнет использовать его только после применения изменений в политике (см. раздел 5).

7. Работа с табличными списками

Табличный список — двумерный массив данных, хранящийся в памяти MaxPatrol SIEM и доступный для использования в правилах корреляции и правилах обогащения.

Ключевая колонка — это колонка, значения в которой являются идентификаторами записей табличного списка. Если ключевых колонок несколько, то запись идентифицируется по совокупности значений всех ключевых колонок.

Работать с табличными списками вы можете на странице **Табличные списки**. В зависимости от назначения существуют следующие типы табличных списков:

- Данные об активах — предназначены для хранения информацией об активах, используемой в правилах обогащения и корреляции. Заполняются данными из модели активов и автоматически обновляются при изменении состояния активов.
- Заполняются правилами корреляции — предназначены для хранения данных, используемых в правилах обогащения и корреляции. Заполняются автоматически при выполнении правил корреляции. Вы можете вручную добавить или изменить записи в табличных списках, выполнить импорт данных из файла формата CSV или очистить табличный список.
- Заполняются правилами обогащения — предназначены для хранения данных, используемых в правилах обогащения и корреляции. Заполняются автоматически при выполнении правил обогащения. Вы можете вручную добавить или изменить записи в табличных списках, выполнить импорт данных из файла формата CSV или очистить табличный список.
- Репутационные списки — предназначены для хранения репутационных списков, получаемых из системы Cyber Security Intelligence. Табличные списки заполняются и обновляются автоматически при изменении репутационных списков. Данные из списков могут использоваться в правилах обогащения.
- Справочник — предназначены для хранения справочной информации, используемой в правилах обогащения и корреляции. Через веб-интерфейс Knowledge Base вы можете вручную добавить или изменить записи в табличных списках, выполнить импорт данных из файла формата CSV или очистить табличный список.

Вы можете экспортировать записи из любого табличного списка в файл формата CSV, XLSX, JSON или XML.

В этом разделе

Экспорт записей из табличных списков (см. раздел 7.1)

Импорт данных из файла формата CSV (см. раздел 7.2)

Добавление записи в табличный список (см. раздел 7.3)

Удаление записей из табличного списка (см. раздел 7.4)

7.1. Экспорт записей из табличных списков

- Чтобы экспортировать записи из табличного списка:

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

     Откроется страница **Табличные списки**.

  2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

  3. В панели **Табличные списки** выберите табличный список.

  4. Если нужно экспортировать отдельные записи табличного списка, выберите строки с этими записями.

     Примечание. Для выбора нескольких строк подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных строк — клавишу Ctrl.

  5. Нажмите **Экспорт** и в раскрывшемся меню выберите вариант экспорта.

  6. В открывшемся окне выберите формат файла для экспорта записей.

     Примечание. Вы можете создать задачу на экспорт выбранных записей табличного списка по кнопке **Создать задачу на экспорт**.

  7. Нажмите кнопку **Экспортировать**.

  Файл сохранен на вашем компьютере.

7.2. Импорт данных из файла формата CSV

Поддерживается импорт данных из файлов формата CSV в кодировке UTF-8. В первой строке файла нужно указать наименования колонок, в качестве разделителя данных в строке нужно использовать точку с запятой (;).

Файл для импорта должен содержать значения для ключевых колонок табличного списка. Значения ячеек должны удовлетворять требованиям: для типа данных DateTime — дата должна находиться в интервале от 1970-01-01 00:00:00 до 2106-02-07 06:28:15; для Number — число должно находиться в интервале от –9223372036854775807 до 9223372036854775807; для String — длина строки не должна превышать 16 382 символов (65 531 байт).

- Чтобы выполнить импорт данных в табличный список для правил корреляции или обогащения:

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

     Откроется страница **Табличные списки**.

  2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
4. Выберите вкладку **Записи**.
5. Нажмите кнопку **Импорт**.
6. В открывшемся окне по ссылке **выбрать** укажите расположение файла с данными для импорта.

   Примечание. Для выбора файла с данными вы можете перетащить его в окно **Импорт табличного списка** в область **Загрузить файл CSV**.
7. Нажмите кнопку **Импортировать**.
8. При появлении сообщения об окончании процедуры импорта нажмите кнопку **Закрыть**.

Данные импортированы. Строки с уникальным значением ключевых колонок добавлены в конец табличного списка. Строки с существующими в табличном списке значениями ключевых колонок перезаписаны.

7.3. Добавление записи в табличный список

► Чтобы добавить запись в табличный список для правил обогащения или корреляции:

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

   Откроется страница **Табличные списки**.
2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
4. Выберите вкладку **Записи**.
5. Нажмите кнопку **Редактировать содержимое**.
6. В открывшемся окне выберите вариант **Приостановить все связанные правила** и нажмите кнопку **Далее**.
7. В панели инструментов вкладки нажмите кнопку **Добавить**.
8. В добавленной строке заполните ячейки в соответствии с типом данных колонок табличного списка и нажмите ✓.
9. В нижней части вкладки нажмите кнопку **Закончить редактирование**.

Запись добавлена в табличный список.

7.4. Удаление записей из табличного списка

- Чтобы удалить записи из табличного списка для правил корреляции или обогащения:

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

     Откроется страница **Табличные списки**.

  2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.
  3. В панели **Табличные списки** выберите табличный список для правил корреляции или обогащения.
  4. Выберите вкладку **Записи**.
  5. Нажмите кнопку **Редактировать содержимое**.
  6. В открывшемся окне выберите вариант **Приостановить все связанные правила** и нажмите кнопку **Далее**.
  7. Выберите одну или несколько записей.

     Примечание. Для выбора нескольких строк подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных строк — клавишу Ctrl.

  8. Нажмите кнопку **Удалить** и подтвердите удаление.
  9. В нижней части вкладки нажмите кнопку **Закончить редактирование**.

  Записи удалены из табличного списка.

8. Включение и отключение правил корреляции и обогащения событий

Корреляция событий — это процесс обнаружения событий информационной безопасности путем анализа потока нормализованных событий. При обнаружении в потоке событий такой их последовательности, которая указана в условии одного из заранее настроенных правил корреляции, регистрируется корреляционное событие.

Обогащение событий — заполнение полей нормализованных, агрегированных и корреляционных событий согласно правилам обогащения. Поля заполняются данными, указанными в правиле обогащения или полученными из табличных списков.

На странице **Правила корреляции** вы можете включать и отключать правила корреляции событий, на странице **Правила обогащения** — правила обогащения событий.

В этом разделе

Отключение правила корреляции (см. раздел 8.1)

Включение правила корреляции (см. раздел 8.2)

Отключение правила обогащения (см. раздел 8.3)

Включение правила обогащения (см. раздел 8.4)

8.1. Отключение правила корреляции

Вы можете отключать правила корреляции со статусами «Включено» и «Приостановлено».

- Чтобы отключить правило корреляции:

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

     Откроется страница **Правила корреляции**.

  2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

  3. В панели **Список правил корреляции** выберите одно или несколько правил.

     Примечание. Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил — клавишу Ctrl.

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

  Правило корреляции отключено, конвейер не будет использовать его для корреляции событий.

8.2. Включение правила корреляции

Вы можете включать правила корреляции со статусом «Отключено» и «Приостановлено».

- Чтобы включить правило корреляции:

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

     Откроется страница **Правила корреляции**.

  2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

  3. В панели **Список правил корреляции** выберите одно или несколько правил.

     Примечание. Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил — клавишу Ctrl.

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

  Правило корреляции включено, конвейер начнет использовать его для корреляции событий.

8.3. Отключение правила обогащения

Вы можете отключать правила обогащения со статусом «Включено».

- Чтобы отключить правило обогащения:

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

     Откроется страница **Правила обогащения**.

  2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

  3. В панели **Список правил обогащения** выберите одно или несколько правил.

     Примечание. Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил — клавишу Ctrl.

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

  Правило обогащения отключено, конвейер не будет использовать его для обогащения событий.

8.4. Включение правила обогащения

Вы можете включать правила обогащения со статусом «Отключено».

► Чтобы включить правило обогащения:

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

   Откроется страница **Правила обогащения**.

2. Если установлено несколько конвейеров обработки событий, по ссылке выберите конвейер.

3. В панели **Список правил обогащения** выберите одно или несколько правил.

   Примечание. Для выбора нескольких правил подряд вы можете использовать клавишу Shift, для выбора нескольких отдельных правил — клавишу Ctrl.

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

Правило обогащения включено, конвейер начнет использовать его для обогащения событий.

9. 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

Страницы раздела «Управление системой» (см. раздел 9.1)

Удаление недоступного коллектора (см. раздел 9.2)

Настройка количества подзадач, одновременно выполняемых модулем (см. раздел 9.3)

Мониторинг работы правил корреляции (см. раздел 9.4)

9.1. Страницы раздела «Управление системой»

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

Страница «Конвейеры»

На странице **Конвейеры** вы можете просматривать информацию о конвейерах MP SIEM Server, которые обеспечивают обработку событий в системе. Для перехода на страницу необходимо в главном меню выбрать **Система** → **Управление системой** → **Конвейеры**.

Панель инструментов содержит следующие кнопки:

- **Изменить** — для изменения псевдонима конвейера;
- **Удалить** — для удаления недоступного конвейера из списка.

В рабочей области страницы отображается таблица со списком конвейеров. Для каждого конвейера в таблице указаны статус, псевдоним, имя узла, версии установленной системы и схемы полей событий, семейство ОС сервера, IP-адреса и подключения. Вы можете сортировать список, нажимая названия колонок таблицы. Нажатием вы можете обновить информацию о конвейерах. При выборе конвейера система отображает подробную информацию о нем в боковой панели с названием конвейера.

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

В колонке **Статус** отображается статус конвейера:

Доступен — конвейер работает в нормальном режиме;

Недоступен — MP 10 Core не получает отклика от конвейера более 10 минут.

Страница «Коллекторы»

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

Панель инструментов содержит следующие кнопки:

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

В рабочей области страницы отображается таблица со списком коллекторов. Для каждого коллектора в таблице указаны статус, название, имя узла, версия, роли, а также семейство ОС сервера и IP-адреса сетевых интерфейсов сервера MP 10 Collector, которые доступны для внешнего подключения. Вы можете сортировать список, нажимая названия колонок таблицы, а также отображать и скрывать отдельные колонки, нажимая в правой верхней части таблицы. Для поиска коллектора в списке вы можете нажать и ввести в поле для поиска параметр коллектора. При выборе коллектора система отображает подробную информацию о нем, его модулях и их потоках в боковой панели с названием коллектора.

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

В колонке **Статус** отображается статус коллектора:

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

Страница «Обработка активов»

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

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

Страница «О системе»

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

9.2. 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.

9.3. Настройка количества подзадач, одновременно выполняемых модулем

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

► Чтобы настроить количество одновременно выполняемых подзадач:

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

   Откроется страница **Управление системой**.

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

   В рабочей области страницы отобразится таблица со списком коллекторов.

3. Выберите коллектор.

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

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

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

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

Количество одновременно выполняемых подзадач настроено.

9.4. 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`).

10. Лимит EPS: условия и ограничения лицензионного контроля

Для каждой лицензии MaxPatrol SIEM действует лимит EPS (количества событий в секунду). Поток событий, который поступает в MaxPatrol SIEM от всех источников, не должен превышать этот лимит больше допустимого. Диапазон допустимого превышения описан ниже.

Однократное превышение лимита EPS больше допустимых значений запускает льготный период. В этот период система ежедневно проверяет последние 90 дней до текущей даты включительно: если за это время средний поток событий за сутки превысит лимит 20 раз (не подряд, а в любые 20 дней из 90), функции MaxPatrol SIEM будут ограничены. Чтобы выйти из льготного периода, необходимо соблюдать лимит EPS в течение 90 дней подряд.

Вы можете следить за соблюдением лимита EPS на странице **Лицензии** PT MC и с помощью виджета **Средний поток событий**. Если лимит будет превышен больше допустимого, система сообщит об этом с помощью уведомлений.

Поток событий и допустимое превышение

MaxPatrol SIEM использует следующие показатели для лицензионного контроля:

- **Средний поток событий за сутки.** Это основной показатель для проверок: если он хотя бы раз превысит лимит больше допустимого, начнется льготный период. Если этот показатель превысит лимит больше допустимого 20 раз за 90 дней, функции MaxPatrol SIEM будут ограничены. Допустимое превышение — 30% лимита EPS, установленного для лицензии.
- **Средний поток событий за неделю.** Не используется для проверок и ограничений, служит, чтобы предупреждать администратора о проблеме с помощью уведомлений. Допустимое превышение — 20% лимита EPS, установленного для лицензии.
- **Средний поток событий за месяц.** Не используется для проверок и ограничений, служит, чтобы предупреждать администратора о проблеме с помощью уведомлений. Допустимое превышение — 10% лимита EPS, установленного для лицензии.

  Примечание. Превышение лимита EPS в пределах допустимого не запускает льготный период и не приводит к ограничениям.

Ограничение функций

Если в течение льготного периода средний поток событий за сутки превысит лимит больше допустимого 20 раз, будут применены следующие ограничения:

- глубина поиска по событиям сократится до 7 дней;
- отключится запуск задач на сбор событий;
- отключится корреляция событий.

Восстановление функций

Чтобы восстановить полную функциональность MaxPatrol SIEM, нужно устранить нарушение лимита EPS — ограничения будут автоматически сняты в течение двух часов.

> **Внимание!** После снятия ограничений льготный период все еще будет действовать, повторное превышение лимита снова приведет к ограничению функций. Чтобы выйти из льготного периода, необходимо соблюдать лимит EPS в течение 90 дней подряд.

11. Сбор телеметрических данных

В MaxPatrol SIEM реализован сбор телеметрических данных о производительности микросервисов компонента MP 10 Core, о параметрах работы моделей машинного обучения BAD, об активах и о 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). Сбор параметров работы моделей машинного обучения BAD также осуществляется по расписанию (по умолчанию один раз в час). Данные об активах собираются еженедельно. Все собранные и обезличенные телеметрические данные хранятся в каталоге `/var/lib/deployed-roles/mc-application/observability/data/telemetry/files` в виде файлов в различных форматах.

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

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

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

12. Мониторинг ресурсов в Grafana

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

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

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

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

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

В веб-интерфейсе Grafana вы можете получать информацию о ключевых метриках:

— серверов, на которых установлены компоненты MaxPatrol SIEM,

— СУБД PostgreSQL,

— хранилища событий Elasticsearch,

— хранилища событий LogSpace.

Вы также можете отслеживать параметры работы отдельных служб MaxPatrol SIEM. Для этого по адресу `https://<IP-адрес или FQDN сервера PT MC>:3334/grafana/dashboards` доступны следующие дашборды:

— SIEM Aggregator;

— SIEM Correlator;

— SIEM Enricher;

— SIEM Normalizer;

— SIEM Pipeline metrics;

— SIEM Receiver;

— SIEM Renderer;

— SIEM Router;

— SIEM Storage.

Данные с этих дашбордов могут быть использованы для отправки в службу технической поддержки Positive Technologies с целью последующего их анализа.

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

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

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

В этом разделе

Настройка дашбордов в Grafana на отдельном сервере (см. раздел 12.1)

Работа с дашбордом хранилища событий Elasticsearch (см. раздел 12.2)

Работа с дашбордом хранилища событий LogSpace (см. раздел 12.3)

Работа с дашбордом SIEM Aggregator (см. раздел 12.4)

Работа с дашбордом SIEM Correlator (см. раздел 12.5)

Работа с дашбордом SIEM Enricher (см. раздел 12.6)

Работа с дашбордом SIEM Normalizer (см. раздел 12.7)

Работа с дашбордом SIEM Pipeline metrics (см. раздел 12.8)

Работа с дашбордом SIEM Receiver (см. раздел 12.9)

Работа с дашбордом SIEM Renderer (см. раздел 12.10)

Работа с дашбордом SIEM Router (см. раздел 12.11)

Работа с дашбордом SIEM Storage (см. раздел 12.12)

Работа с дашбордом Host metrics (см. раздел 12.13)

Работа с дашбордом SqlStorage (см. раздел 12.14)

12.1. Настройка дашбордов в Grafana на отдельном сервере

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

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

Добавление дашборда с метриками VictoriaMetrics

- Чтобы добавить дашборд с метриками VictoriaMetrics:

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

   Примечание. По умолчанию для доступа к VictoriaMetrics используется TCP-порт 8428. Вы можете посмотреть параметры роли с текущими значениями на сервере с установленной ролью Observability с помощью команды `deployer params get -<Идентификатор экземпляра роли Observability>`.
6. В поле **Authentication method** выберите вариант **Basic Authentication**.
7. В поле **User** укажите логин учетной записи для доступа к VictoriaMetrics из значения параметра MetricsUser роли Observability.

   Значение по умолчанию: `admin`.
8. В поле **Password** укажите пароль из значения параметра `MetricsPassword` роли Observability.

   Значение по умолчанию: `P@ssw0rd`.
9. В блоке **TLS settings** выполните одно из следующих действий:
   - Если вы используете собственный сертификат или автоматически установленный сертификат из состава дистрибутива MaxPatrol SIEM, установите флажок **Add self-signed certificate** и в поле **CA Certificate** введите содержимое файла сертификата.

     Примечание. Файл автоматически установленного сертификата `rootCA.crt` находится на сервере с ролью Observability в каталоге `/var/lib/deployed-roles/<Идентификатор приложения>/<Идентификатор экземпляра роли Observability>/certs`.
   - Если политика информационной безопасности вашей организации позволяет не проверять подлинность сертификата, установите флажок **Skip TLS certificate validation**.
10. Нажмите **Save & test**.

    Появится сообщение об успешном добавлении источника данных.
11. В главном меню выберите **Dashboards**.

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

    Дашборд с метриками VictoriaMetrics появится в списке дашбордов Grafana.

Добавление дашборда с журналом VictoriaLogs

- Чтобы добавить дашборд с журналом VictoriaLogs:

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

   Примечание. По умолчанию для доступа к VictoriaLogs используется TCP-порт 9428.
9. В блоке **Auth** включите **Basic Auth**.
10. Выполните одно из следующих действий:
    - Если вы используете доверенный сертификат для сайта MaxPatrol SIEM, включите **With CA Cert**.
    - Если политика информационной безопасности вашей организации позволяет не проверять подлинность сертификата, включите **Skip TLS Verify**.
11. В поле **User** укажите логин учетной записи для доступа к журналам VictoriaLogs.

    Значение по умолчанию: `admin`.
12. В поле **Password** укажите пароль из значения параметра `LogsPassword` роли Observability.

    Значение по умолчанию: `P@ssw0rd`.
13. Если вы используете доверенный сертификат для сайта MaxPatrol SIEM, в поле **CA Cert** введите содержимое файла доверенного сертификата.

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

14. Нажмите **Save & test**.

    Появится сообщение об успешном добавлении источника данных.

15. В главном меню выберите **Dashboards**.
16. Нажмите **New** → **New dashboard**.
17. Нажмите **Add visualization**.
18. Выберите источник данных VictoriaLogs.
19. В правой части страницы выберите тип отображения данных **Logs**.
20. В правой части страницы в раскрывающемся блоке **Panel options** укажите имя и описание дашборда.
21. В правой части страницы в раскрывающемся блоке **Logs** включите **Show timestamps**.
22. В центральной части страницы нажмите **Add query**.
23. В поле **Quick start** выполните одно из следующих действий:
    - Для вывода всех данных введите `*`.
    - Для фильтрации данных введите запрос на языке LogQL.
24. Нажмите **Save dashboard**.

    Дашборд с журналом VictoriaLogs появится в списке дашбордов Grafana.

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

12.2. Работа с дашбордом хранилища событий Elasticsearch

В MaxPatrol SIEM реализован сбор метрик из хранилища событий Elasticsearch. Это позволяет отслеживать состояние хранилища и оперативно реагировать на инциденты. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели хранилища, кластера, узлов, JVM, пула потоков и индексов.

В верхней панели дашборда вы можете выбрать FQDN сервера, кластер и один или несколько узлов кластера.

Виджеты Main

Секция содержит следующие виджеты для мониторинга основных показателей хранилища:

— **Cluster health.** Виджет представляет собой цветовой индикатор с текстовым описанием состояния кластера. Предусмотрены следующие индикаторы уведомлений:

  • **RED** — кластер не работает полностью или частично (хотя бы один из первичных шардов недоступен). Если кластер отвечает на запросы, результаты поиска в ответах будут неполными;

  • **YELLOW** — кластер работает, но нет доступа хотя бы к одной из копий шардов. Результаты поиска в ответах кластера полные, но, если появятся другие недоступные шарды, кластер перестанет работать;

  • **GREEN** — корректная работа кластера (все шарды доступны).

— **Cluster nodes.** Виджет отображает общее количество узлов (cluster nodes) и количество узлов данных (data nodes) в кластере.

— **All shards.** Виджет отображает количество всех шардов кластера.

— **Active shards.** Виджет отображает количество активных шардов кластера.

— **Active primary shards.** Виджет отображает количество активных первичных шардов кластера.

— **Initializing shards.** Виджет отображает количество инициализируемых шардов кластера. Значение отличается от нуля, когда создаются новые индексы и их шарды распределяются по узлам кластера.

— **Unassigned shards.** Виджет отображает количество неназначенных шардов кластера, хранящиеся данные в которых являются недоступными. При корректной работе хранилища количество неназначенных шардов равно нулю.

— **Unassigned delayed shards.** Виджет отображает количество отложенных к назначению шардов кластера.

— **Relocating shards.** Виджет отображает количество перемещаемых шардов кластера.

— **Breaker trips.** Виджет отображает количество прерываний в кластере для предотвращения использования чрезмерного объема памяти.

— **HTTP connections.** Виджет отображает количество подключений по протоколу HTTP на выбранных узлах кластера.

— **Cluster connections.** Виджет отображает количество открытых TCP-подключений на выбранных узлах кластера для внутренней связи кластера.

— **Open files.** Виджет отображает количество открытых файловых дескрипторов на выбранных узлах кластера.

— **Documents.** Виджет отображает количество активных (active) и удаленных (deleted) документов.

— **Pending cluster tasks.** Виджет отображает количество незавершенных задач в кластере.

— **JVM memory usage.** Виджет представляет собой круговую диаграмму, которая отражает объем использованной на выбранных узлах кластера памяти JVM в процентах. Если значение на графике превышает 75%, необходимо оптимизировать использование памяти.

— **JVM heap usage.** Виджет представляет собой круговую диаграмму, которая отражает используемый на выбранных узлах кластера размер кучи JVM в процентах.

— **Available disk space.** Виджет представляет собой круговую диаграмму, которая отражает объем использования на выбранных узлах кластера доступного дискового пространства в процентах.

Виджеты Cluster

Секция содержит следующие виджеты для мониторинга показателей кластера:

— **Cluster health.** Виджет представляет собой график, который показывает информацию о состоянии кластера за выбранный период времени. Цветовая индикация состояния совпадает с индикацией в одноименном виджете в блоке **Main**.

— **Pending tasks.** Виджет представляет собой график, который показывает информацию о количестве незавершенных задач кластера за выбранный период времени.

— **Breaker trips.** Виджет представляет собой график, который показывает информацию о количестве прерываний для предотвращения использования чрезмерного объема памяти за выбранный период времени.

Виджеты Nodes

Секция содержит следующие виджеты для мониторинга состояния узлов кластера:

— **Open files.** Виджет представляет собой график, который показывает информацию о количестве открытых файловых дескрипторов на выбранных узлах кластера за выбранный период времени.

— **Documents.** Виджет представляет собой график, который показывает информацию о количестве активных и удаленных документов на выбранных узлах кластера за выбранный период времени.

— **Completed operations.** Виджет представляет собой график, который показывает информацию о количестве завершенных за минуту операций каждого типа на выбранных узлах кластера за выбранный период времени.

— **Operation time.** Виджет представляет собой график, который показывает информацию о количестве времени выполнения операций каждого типа на выбранных узлах кластера.

— **Available disk space.** Виджет представляет собой график, который показывает информацию о размере доступного дискового пространства на выбранных узлах кластера за выбранный период времени.

— **Cluster I/O.** Виджет представляет собой график, который показывает информацию о количестве байтов, отправленных и полученных по сети для внутренней связи кластера, на выбранных узлах кластера за выбранный период времени.

— **Cache evictions.** Виджет представляет собой график, который показывает информацию о количестве вытеснений из кэша запросов и кэша данных значений, которые дольше всего не запрашивались, на выбранных узлах кластера за выбранный период времени.

— **Cache size.** Виджет представляет собой график, который показывает информацию о размере кэша запросов и кэша данных на выбранных узлах кластера за выбранный период времени в байтах.

— **Connections.** Виджет представляет собой график, который показывает информацию о количестве открытых подключений по протоколам HTTP и TCP за выбранный период времени.

Виджеты JVM

Секция содержит следующие виджеты для мониторинга показателей JVM:

— **Garbage collection count.** Виджет представляет собой график, который показывает информацию о количестве срабатываний сборщика мусора на выбранных узлах кластера за выбранный период времени.

— **Garbage collection elapsed time.** Виджет представляет собой график, который показывает информацию о приблизительном времени, затраченном на сбор мусора, за выбранный период времени.

— **Loaded classes.** Виджет представляет собой график, который показывает информацию о количестве загруженных JVM классов за выбранный период времени.

— **Thread count.** Виджет представляет собой график, который показывает информацию о количестве JVM потоков за выбранный период времени.

— **Heap memory.** Виджет представляет собой график, который показывает информацию о размере кучи JVM на выбранных узлах кластера за выбранный период времени для следующих типов памяти:

  • объем выделенной (committed) памяти;

  • объем используемой (used) памяти;

  • максимальный объем (max) памяти, который может быть выделен.

— **Non-heap memory.** Виджет представляет собой график, который показывает информацию об объеме используемой (used) и выделенной (committed) памяти стека JVM на выбранных узлах кластера за выбранный период времени.

— **Pool memory.** Виджет представляет собой график, который показывает распределение максимального (max) и используемого (used) объема памяти по пулам на выбранных узлах кластера за выбранный период времени.

Виджеты Thread pools

Секция содержит следующие виджеты для мониторинга показателей пула потоков:

- **Queued tasks.** Виджет представляет собой график, который показывает информацию о количестве задач в очереди в пуле потоков на выбранных узлах кластера за выбранный период времени.
- **Finished tasks.** Виджет представляет собой график, который показывает информацию о количестве завершенных за минуту задач в пуле потоков на выбранных узлах кластера за выбранный период времени.
- **Threads.** Виджет представляет собой график, который показывает информацию о количестве потоков в пуле потоков на выбранных узлах кластера за выбранный период времени.

Виджеты Indexes

Секция содержит следующие виджеты для мониторинга показателей индексов хранилища:

- **Indexes with the longest operation time.** Виджет представляет собой график, который показывает топ-10 индексов по времени выполнения операций за выбранный период времени.
- **Indexes with most completed operations.** Виджет представляет собой график, который показывает топ-10 индексов по количеству выполненных операций за выбранный период времени.
- **Indexes with the largest shards.** Виджет представляет собой график, который показывает топ-10 индексов по размеру за выбранный период времени.

12.3. Работа с дашбордом хранилища событий LogSpace

В MaxPatrol SIEM реализован сбор данных из хранилища событий LogSpace. Это позволяет отслеживать состояние хранилища и оперативно реагировать на инциденты. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели хранилища, базы данных и операций с ее таблицами, а также показатели дискового пространства и кэша.

В верхней панели дашборда вы можете выбрать FQDN сервера, экземпляр роли Event Storage и период обновления виджетов в минутах.

Виджеты Service parameters

Секция содержит следующие виджеты для мониторинга основных показателей хранилища:

— **LogSpace status.** Виджет отображает текстовое описание состояния хранилища. Могут отображаться следующие состояния:

  • **Active** — хранилище включено;

  • **Down** — хранилище выключено.

— **LogSpace uptime.** Виджет отображает время работы хранилища событий с его последней перезагрузки в часах, минутах и секундах.

— **Database size.** Виджет отображает размер базы данных хранилища LogSpace.

— **Threads.** Виджет отображает количество потоков в процессе LogSpace.

— **Free disk space.** Виджет отображает объем свободного места на диске, где установлено хранилище. Если хранилище LogSpace находится на нескольких дисках, значение будет неполным.

— **Connections.** Виджет представляет собой график, который показывает информацию о количестве соединений следующих типов:

  • **TCP** — открытые TCP-соединения от клиентов к хранилищу;

  • **HTTP** — открытые HTTP-соединения от клиентов к хранилищу;

  • **Interserver** — открытые HTTP-соединения типа «сервер — сервер» (кросс-доменных запросов).

— **File Open and Seek.** Виджет представляет собой график, который показывает информацию о следующих показателях:

  • **Files Open** — количество файлов, открытых для чтения или записи;

  • **Seek** — количество установленных смещений файлового дескриптора для последующего чтения.

— **RAM usage.** Виджет представляет собой график, который показывает информацию об объеме оперативной памяти сервера, используемой сервисами хранилища, за выбранный период времени.

— **Queries.** Виджет представляет собой график, который показывает информацию о количестве следующих типов принятых запросов за выбранный период времени:

  - **Query** — принятые SQL-запросы;
  - **Selectquery** — принятые SQL-запросы `SELECT`;
  - **Insertquery** — принятые SQL-запросы `INSERT`.

— **Cancellations.** Виджет представляет собой график, который показывает информацию о количестве операций следующих типов за выбранный период времени:

  - **RejectedInserts** — добавление информации в таблицу было отменено из-за превышения максимального количества партиций в сегменте;
  - **MergeInsteadInsert** — добавление информации в таблицу отложено из-за объединения партиций: слишком много партиций в одном из сегментов таблицы;
  - **QueryPostponed** — выполнение запроса отложено из-за запросов с более высоким приоритетом.

Виджеты Database

Секция содержит следующие виджеты для мониторинга показателей базы данных:

— **Threads.** Виджет представляет собой график, который показывает информацию о количестве потоков в процессе LogSpace за выбранный период времени.

— **Buffer reads and writes.** Виджет представляет собой график, который показывает информацию о количестве следующих типов операций за выбранный период времени:

  - **read** — данные файла прочитаны в буфер ввода;
  - **write** — данные из буфера вывода записаны в файл.

— **Memory tracking.** Виджет представляет собой график, который показывает информацию об объеме памяти, используемой конвейером обработки запросов, за выбранный период времени.

— **Buffer reads and write (bytes).** Виджет представляет собой график, который показывает информацию об объеме прочитанных и записанных данных за выбранный период времени (в байтах):

  - **read** — объем прочитанных данных;
  - **write** — объем записанных данных.

Виджеты Disk

Секция содержит следующие виджеты для мониторинга показателей дискового пространства:

— **File descriptors.** Виджет представляет собой график, который показывает информацию о количестве файловых дескрипторов, открытых процессами LogSpace, за выбранный период времени.

— **Read details.** Виджет представляет собой график, который показывает информацию о количестве следующих типов данных за выбранный период времени:

- **SelectedParts** — секции, из которых были запущены процессы чтения;
- **SelectedRanges** — диапазоны ячеек, прочитанных из таблицы;
- **SelectedMarks** — ячейки, прочитанные из таблицы.

— **Size.** Виджет представляет собой графическое и текстовое отображение следующих типов данных:

- **Database Size** — общий размер базы данных LogSpace;
- **Data + stack size** — общий размер данных и стека процесса LogSpace;
- **Text size** — размер секции исполняемых инструкций процесса LogSpace.

Если объем оперативной памяти, занятой процессом LogSpace, приблизится к физическому объему оперативной памяти, работа сервиса замедлится (в некоторых случаях до полной остановки).

— **Files opened for reading and writing.** Виджет представляет собой график, который показывает информацию о количестве следующих типов файлов за выбранный период времени:

- **read** — файлы, открытые для чтения;
- **write** — файлы, открытые для записи.

— **Reads and writes.** Виджет представляет собой график, который показывает информацию о количестве следующих типов файлов за выбранный период времени:

- **read** — прочтения из файла;
- **write** — записи в файл.

Виджеты Table operations

Секция содержит следующие виджеты для мониторинга показателей операций с таблицами БД:

— **Queries.** Виджет представляет собой график, который показывает информацию о количестве следующих типов запросов за выбранный период времени:

- **SQL query accepted** — принятые SQL-запросы;
- **SelectQuery** — принятые SQL-запросы `SELECT`;
- **InsertQuery** — принятые SQL-запросы `INSERT`.

— **Merge.** Виджет представляет собой график, который показывает информацию о следующих показателях таблиц MergeTree за выбранный период времени:

- **Merge** — количество слияний в таблицах MergeTree;
- **MergeTreeDataWriterRows** — размер данных, записанных в строках;
- **MergeTreeDataWriterBlocks** — размер данных, записанных в блоках;
- **MergeTreeDataWriterBlocksAlreadySorted** — размер записанных блоков предварительно отсортированной информации. В таблицу добавлен блок данных, отсортированный в естественном для таблицы порядке: дополнительная сортировка не требуется. Блоки, добавленные в таблицы UnsortedMergeTree, не учитываются;
- **MergedRows** — размер слияний в строках.

— **External aggregation.** Виджет представляет собой график, который показывает информацию о следующих показателях внешней агрегации за выбранный период времени:

- **ExternalSortWritePart** — ресурсоемкое слияние с использованием внешней сортировки; при этом части сортированных данных выгружаются на диск;
- **ExternalSortMerge** — ресурсоемкое слияние с использованием внешней сортировки; при этом данные с диска загружаются для дальнейшего слияния;
- **ExternalAggregationWritePart** — ресурсоемкая двухуровневая агрегация с выгрузкой данных или части данных на диск (внешняя агрегация, аналогичная внешней сортировке). При этом данные первого уровня агрегации выгружаются на диск;
- **ExternalAggregationMerge** — ресурсоемкая внешняя агрегация. Второй уровень агрегации с загрузкой частично агрегированых данных с диска.

— **Merge (bytes).** Виджет представляет собой график, который показывает информацию о следующих показателях слияний за выбранный период времени (в байтах):

  - **MergeTreeDataWriterUncompressedBytes** — исходный размер записанных данных (до сжатия, размер данных в памяти);
  - **MergeTreeDataWriterCompressedBytes** — конечный размер записанных данных (после сжатия, размер данных на диске);
  - **MergedUncompressedBytes** — размер слияния. В счетчиках слияний заложено усиление записи; средний коэффициент усиления можно оценить как соотношение количества записанных строк и объединенных строк.

— **External aggregation (bytes).** Виджет представляет собой график, который показывает информацию о следующих показателях внешней агрегации за выбранный период времени (в байтах):

  - **ExternalAggregationCompressedBytes** — размер выгруженных на диск данных после сжатия (расход дискового пространства);
  - **ExternalAggregationUncompressedBytes** — размер выгруженных на диск данных (высвобождение оперативной памяти).

Виджеты Cache

Секция содержит следующие виджеты для мониторинга показателей кэша:

— **Hits and misses.** Виджет представляет собой график, который показывает информацию о попаданиях и промахах при чтении из кэша для следующих показателей за выбранный период времени:

  - **MarkCacheHits** — попадание при чтении из кэша маркеров;
  - **IdDictCacheHits** — попадание при чтении из кэша словарей;
  - **IndexCacheHits** — попадание при чтении из кэша индексов;
  - **FullTxtCacheHits** — попадание при чтении из кэша полнотекстовых индексов;
  - **MarkCacheMisses** — промах при чтении из кэша маркеров;
  - **IdDictCacheMisses** — промах при чтении из кэша словарей;
  - **IndexCacheMisses** — промах при чтении из кэша индексов;
  - **FullTxtCacheMisses** — промах при чтении из кэша полнотекстовых индексов.

— **Size and limits.** Виджет представляет собой график, который показывает информацию о размере и ограничениях кэша за выбранный период времени:

  - **MarkCacheSize** — размер кэша маркеров;
  - **IdDictCacheSize** — размер кэша словарей;
  - **IndexCacheSize** — размер кэша индексов;

- **FullTxtCacheSize** — размер кэша полнотекстовых индексов;
- **MarkCacheLimit** — ограничение кэша маркеров;
- **IdDictCacheLimit** — ограничение кэша словарей;
- **IndexCacheLimit** — ограничение кэша индексов;
- **FullTxtCacheLimit** — ограничение кэша полнотекстовых индексов.

— **Items.** Виджет представляет собой график, который показывает информацию о количестве записей в кэше следующих типов за выбранный период времени:

- **MarkCacheItems** — записи в кэше маркеров;
- **IdDictCacheItems** — записи в кэше словарей;
- **IndexCacheItems** — записи в кэше индексов;
- **FullTxtCacheItems** — записи в кэше полнотекстовых индексов.

12.4. Работа с дашбордом SIEM Aggregator

В MaxPatrol SIEM реализован сбор метрик службы Aggregator. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana:

— **Rule match event count.** Виджет отображает количество событий, соответствующих определенному правилу.

— **Rule-specific processed event count.** Виджет отображает количество событий, обработанных определенным правилом.

— **Rule-specific pass-through event count.** Виджет отображает количество событий, пропущенных определенным правилом.

— **Rule-specific dropped event count.** Виджет отображает количество событий, отброшенных определенным правилом.

— **Rule-generated event count.** Виджет отображает количество событий, сформированных по определенному правилу.

12.5. Работа с дашбордом SIEM Correlator

В MaxPatrol SIEM реализован сбор метрик службы Correlator. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana:

— **Correlation instances (per min).** Виджет отображает количество созданных экземпляров корреляции за минуту.

— **Service instance count in memory.** Виджет отображает количество экземпляров службы в памяти.

12.6. Работа с дашбордом SIEM Enricher

В MaxPatrol SIEM реализован сбор метрик службы Enricher. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели взаимодействия службы с БД табличных списков (FPTA), а также показатели самой службы Enricher.

Виджеты Rule Diagnostics

Секция содержит следующие виджеты:

Tabular list processing time (including queries processed locally). Виджет отображает время на обработку табличного списка.

Tabular list query execution time. Виджет отображает время выполнения запроса к табличному списку.

Tabular list query execution and build time. Виджет отображает время на построение и выполнение запроса к табличному списку.

Виджеты FPTA usage statistics

Секция содержит следующие виджеты:

- **Queries per second (QPS).** Виджет отображает количество запросов в секунду.
- **Inserts per second.** Виджет отображает суммарное количество вставок в секунду.
- **Full scans per second.** Виджет отображает суммарное количество полных сканирований в секунду.
- **Tabular list removals per second (table_removes).** Виджет отображает количество удалений из табличных списков в секунду на основе правил.
- **Average tabular list TTL cleanup time.** Виджет отображает среднее время, затраченное на очистку таблиц по TTL.

Виджеты FPTA queries

Секция содержит следующие виджеты:

- **Average tabular list query execution and build time.** Виджет отображает среднее время, потраченное на запрос в FPTA.
- **Average tabular list query execution time.** Виджет отображает среднее время выполнения запроса в FPTA.
- **Rule-based query count (query_exec).** Виджет отображает количество запросов по правилам.
- **Rule-based query count (query_full_scans).** Виджет отображает количество запросов по правилам (query_full_scans).

— **Rule-based insert count (table_inserts).** Виджет отображает количество вставок по правилам.

— **Rule-based remove query count (table_removes).** Виджет отображает количество запросов на удаление по правилам.

— **Rule-based range check count (query_checked_ranges).** Виджет отображает количество запросов проверки range по правилам.

— **TTL deletion query count.** Виджет отображает количество запросов на удаление записей из табличных списков по TTL.

— **TTL deleted record count.** Виджет отображает количество записей, удаленных из табличных списков по TTL.

Виджеты Enricher

Секция содержит следующие виджеты:

— **Processed event count.** Виджет отображает количество событий, обработанных службой.

— **Rule-dropped event count.** Виджет отображает суммарное количество событий, отброшенных правилами.

— **Rule-specific dropped event count.** Виджет отображает количество событий, отброшенных определенным правилом.

— **Skipped event count.** Виджет отображает количество пропущенных событий.

— **Cached record count.** Виджет отображает количество записей в кэше.

— **Cache miss ratio.** Виджет отображает долю промахов кэша в процентах.

— **Cache query count.** Виджет отображает количество обращений в кэш.

— **Cache miss count.** Виджет отображает количество записей, не найденных в кэше.

— **Expired query cache record count.** Виджет отображает количество событий с истекшим сроком хранения в кэше запросов.

— **Cache error count.** Виджет отображает количество ошибок в кэше.

— **FPTA change checks by watchdog (count).** Виджет отображает общее количество проверок изменений в FPTA.

— **Types of FPTA change checks by watchdog.** Виджет отображает виды отслеживаемых изменений в FPTA.

— **Context preparation calls for watchdog.** Виджет отображает количество запросов для получения дополнительной информации об изменениях, обнаруженных в FPTA.

12.7. Работа с дашбордом SIEM Normalizer

В MaxPatrol SIEM реализован сбор метрик службы Normalizer. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana:

- **Normalization status event count.** Виджет отображает количество нормализованных и ненормализованных событий.
- **Unnormalized event percentage.** Виджет отображает долю ненормализованных событий в потоке событий в процентах.
- **Source-specific normalized event count.** Виджет отображает количество нормализованных событий от источника.
- **Source-specific unnormalized event count.** Виджет отображает количество ненормализованных событий от источника.
- **Rule-specific dropped event count.** Виджет отображает количество событий, отброшенных определенным правилом.

12.8. Работа с дашбордом SIEM Pipeline metrics

В MaxPatrol SIEM реализован сбор метрик служебных процессов. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели служб, процессов, брокера сообщений RabbitMQ и баз данных FPTA.

Виджеты General

Секция содержит следующие виджеты для мониторинга основных показателей работы служб:

- **Service uptime (hours).** Виджет отображает время работы служб в часах.
- **Handler IO throughput.** Виджет отображает количество сообщений, обработанных службами за секунду.
- **Total IO throughput.** Виджет отображает количество всех сообщений, принятых службами за секунду.
- **Incoming flow (EPS).** Виджет отображает входящий поток событий.
- **Outgoing flow (EPS).** Виджет отображает исходящий поток событий.
- **Average event processing time.** Виджет отображает среднее время, затраченное службой на обработку события.
- **Service-processed event count.** Виджет отображает количество событий, успешно обработанных службами.
- **Service RAM (RSS) usage.** Виджет отображает объем оперативной памяти (RSS), используемой службами.

— **Service RAM (shared) usage.** Виджет отображает объем оперативной памяти (shared), используемой службами.

— **Service CPU usage (%).** Виджет отображает использование ресурсов центрального процессора службами в процентах.

— **Service CPU usage duration.** Виджет отображает продолжительность использования центрального процессора службами.

— **Slow event count (per min).** Виджет отображает количество событий в минуту, время обработки которых службами preaggregator, router, enricher и normalizer превысило установленный лимит.

Виджеты Workers

Секция содержит следующие виджеты для мониторинга основных показателей служебных процессов:

— **Worker count.** Виджет отображает количество процессов, используемых службами.

— **Worker start count.** Виджет отображает количество запусков процесса.

— **Events per worker.** Виджет отображает количество событий, обработанных одним процессом службы за минуту.

— **Worker restart count.** Виджет отображает количество перезапусков процессов.

Виджеты RMQ

Секция содержит следующие виджеты для мониторинга основных показателей брокера сообщений RabbitMQ:

— **Total RMQ queue size.** Виджет отображает суммарный размер очередей брокера в сообщениях.

— **Individual RMQ queue sizes.** Виджет отображает размеры отдельных очередей RabbitMQ в сообщениях.

— **Non-empty RMQ message read time.** Виджет отображает время, затраченное службой на чтение непустого сообщения RabbitMQ.

— **RMQ message send time.** Виджет отображает время, затраченное службой на отправку сообщения в RabbitMQ.

— **RMQ message confirmation time.** Виджет отображает время, затраченное службой на подтверждение сообщения в RabbitMQ.

— **Unconfirmed RMQ message count.** Виджет отображает количество сообщений, для которых не получено подтверждение в RabbitMQ.

— **RMQ confirmation wait time.** Виджет отображает время, затраченное службой на ожидание подтверждения сообщения в RabbitMQ.

Виджеты FPTA

Секция содержит следующие виджеты для мониторинга основных показателей баз данных FPTA:

- **FPTA page count.** Виджет отображает количество страниц, используемых службой (available, garbage, used) в FPTA.
- **Total FPTA tabular list size.** Виджет отображает общий размер табличных списков, используемых службами в FPTA.
- **FPTA service error count.** Виджет отображает количество ошибок служб при работе с FPTA.
- **FPTA tabular list size.** Виджет отображает размеры табличных списков, используемых службами в FPTA.

12.9. Работа с дашбордом SIEM Receiver

В MaxPatrol SIEM реализован сбор метрик службы Receiver. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana:

- **Incoming packet count.** Виджет отображает количество входящих пакетов.
- **Broken message count.** Виджет отображает количество битых сообщений.
- **Broken packet count.** Виджет отображает количество битых пакетов.
- **Packet processing duration (mcs).** Виджет отображает время обработки пакета.

12.10. Работа с дашбордом SIEM Renderer

В MaxPatrol SIEM реализован сбор метрик службы Renderer. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели взаимодействия службы с FPTA, а также показатели самой службы Renderer.

Виджеты FPTA management

Секция содержит следующие виджеты:

- **Average FPTA rule duration.** Виджет отображает среднее время, потраченное на правило в FPTA.
- **Rule-based query count (query_exec).** Виджет отображает количество запросов по правилам.
- **Rule-based query count (query_full_scans).** Виджет отображает количество запросов по правилам, которые ушли в full scan.

— **Rule-based insert count (table_inserts).** Виджет отображает количество вставок в табличные списки по правилам.

— **Rule-based range check count (query_checked_ranges).** Виджет отображает количество запросов проверки range по правилам.

— **Rule-based remove query count (table_removes).** Виджет отображает количество запросов на удаление по правилам.

Виджеты Database management

Секция содержит следующие виджеты:

— **Database search and result count.** Виджет отображает количество успешных поисков в базе данных.

— **Database search without result count.** Виджет отображает количество неуспешных поисков в базе данных.

— **Total database search count (non-cached).** Виджет отображает общее количество поисков событий в базе данных (вне кэша).

— **Database search time.** Виджет отображает время поиска в базе данных.

— **Event count dropped due to limits.** Виджет отображает количество событий, отброшенных из-за достижения максимального допустимого количества запросов в базу данных.

— **Query count during rendering.** Виджет отображает количество запросов во время рендеринга.

Виджеты Renderer

Секция содержит следующие виджеты:

— **Renderer task queue size.** Виджет отображает размер очереди задач службы.

— **Correlation count queued for rendering.** Виджет отображает количество корреляций в очереди на обработку службой.

— **Correlation rendering time by rules.** Виджет отображает время обработки службой корреляций по правилам.

— **Correlation rendering failures (count).** Виджет отображает количество неуспешных попыток обработки корреляций.

— **Unrenderable correlation count.** Виджет отображает абсолютное количество корреляций, которые не удалось обработать.

— **Cache miss count.** Виджет отображает количество промахов кэша.

— **Cached event count.** Виджет отображает количество событий, добавленных в кэш.

— **Cache eviction count.** Виджет отображает количество событий, удаленных из кэша.

— **Number of events generated based on a specific rule.** Виджет отображает количество событий, созданных по определенному правилу.

— **Partially rendered correlation count.** Виджет отображает количество частично обработанных корреляций.

12.11. Работа с дашбордом SIEM Router

В MaxPatrol SIEM реализован сбор метрик службы Router. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели взаимодействия службы с FPTA, а также показатели самой службы Router.

Виджеты Rule diagnostics

Секция содержит следующие виджеты:

Tabular list processing time (including queries processed locally). Виджет отображает время на обработку табличного списка.

Tabular list query execution time. Виджет отображает время выполнения запроса к табличному списку.

Tabular list query execution and build time. Виджет отображает время на построение и выполнение запроса к табличному списку.

Виджеты FPTA usage statistics

Секция содержит следующие виджеты:

— **Rule-based queries per second (query_exec).** Виджет отображает количество запросов за секунду.

— **Rule-based queries per second (query_full_scans).** Виджет отображает количество запросов по правилам query_full_scans за секунду.

— **Regex table query count.** Виджет отображает количество запросов с использованием regex table за минуту.

Виджеты FPTA queries

Секция содержит следующие виджеты:

— **Average tabular list query execution time.** Виджет отображает среднее время выполнения запроса в FPTA.

— **Average tabular list query execution and build time (exec_span).** Виджет отображает среднее время, затраченное на построение и выполнение запроса в FPTA.

— **Rule-based query count (query_full_scans).** Виджет отображает количество запросов по правилам (query_full_scans).

— **Rule-based query count (query_exec).** Виджет отображает количество запросов по правилам (query_exec).

— **Rule-based range check count (query_checked_ranges).** Виджет отображает количество запросов по правилам (query_checked_ranges).

Виджеты Router

Секция содержит следующие виджеты:

— **Event emits per second.** Виджет отображает количество переданных событий за секунду.

— **Rule-specific event emit count.** Виджет отображает количество переданных событий по определенному правилу.

— **Cached record count.** Виджет отображает количество записей в кэше.

— **Cache miss count.** Виджет отображает количество промахов кэша.

— **Cache query count.** Виджет отображает количество запросов к кэшу.

— **Cache miss ratio.** Виджет отображает долю промахов кэша в процентах.

— **Expired cached record count.** Виджет отображает количество записей в кэше с истекшим сроком хранения.

— **Empty cache query count.** Виджет отображает количество запросов на очистку кэша.

— **Cache error count.** Виджет отображает количество ошибок в кэше.

— **FPTA change checks by watchdog (count).** Виджет отображает общее количество проверок изменений в FPTA.

— **Types of FPTA change checks by watchdog.** Виджет отображает виды отслеживаемых изменений в FPTA.

— **Context preparation calls for watchdog.** Виджет отображает количество запросов для получения дополнительной информации об изменениях, обнаруженных в FPTA.

12.12. Работа с дашбордом SIEM Storage

В MaxPatrol SIEM реализован сбор метрик службы Storage. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana:

— **Average insert time.** Виджет отображает среднее время вставок.

— **Database insert query count.** Виджет отображает количество запросов на вставку.

— **Accepted counter number.** Виджет отображает количество принятых счетчиков.

— **Query elapsed time.** Виджет отображает время, затраченное на запросы в базу данных.

— **Average Elasticsearch _refresh time.** Виджет отображает среднее время, затраченное на выполнение запроса _refresh к хранилищу Elasticsearch.

— **Savepoint duration.** Виджет отображает время, затраченное на точки сохранения.

— **Backend HTTP request processing time.** Виджет отображает время обработки HTTP-запроса.

— **Dropped event count.** Виджет отображает количество отброшенных событий.

12.13. Работа с дашбордом Host metrics

В MaxPatrol SIEM реализован сбор метрик производительности узла. Это позволяет отслеживать нагрузку на аппаратное обеспечение и оперативно реагировать на изменения в нагрузке на отдельные компоненты системы. Собранные данные выводятся на виджеты дашборда в веб-интерфейсе Grafana. Виджеты сгруппированы по секциям, отображающим показатели загруженности системы, в том числе для отдельных контейнеров.

В верхней панели дашборда вы можете выбрать сетевой интерфейс, сервер и диск.

Виджеты System

Секция содержит следующие виджеты для мониторинга загруженности сервера:

— **Number of CPUs.** Виджет отображает количество ядер и потоков процессора.

— **Memory.** Виджет отображает количество оперативной памяти в системе.

— **SWAP.** Виджет отображает размер сгенерированного файла подкачки.

— **Network.** Виджет отображает сетевой интерфейс, который использует сервер.

— **Disk.** Виджет отображает состояние выбранного дискового устройства:

- **free** — объем свободного места на диске;
- **reserved** — объем места на диске, зарезервированного под файловую систему;
- **used** — объем используемого места на диске;
- **total** — общий объем диска.

— **CPU usage.** Виджет отображает загруженность процессора.

— **Average CPU load per 1 min.** Виджет отображает показатель общей загруженности системы за период времени. Загруженность системы выражается в соотношении всех запущенных процессов и реально исполняемых процессов. Виджет позволяет отобразить загруженность системы за 1, 5 и 15 минут работы.

— **Memory usage.** Виджет отображает общую загруженность оперативной памяти и ее использование под различные нужды:

- **free** — количество незадействованной оперативной памяти;
- **used** — количество используемой оперативной памяти;

- **buffered** — количество оперативной памяти, используемой под сетевые буферы;
- **cached** — количество оперативной памяти, используемой под дисковый кэш.

— **File system usage.** Виджет отображает загруженность файловой системы.

— **Disk read speed.** Виджет отображает скорость чтения данных с выбранного диска.

— **Disk write speed.** Виджет отображает скорость записи данных на выбранный диск.

— **Disk load.** Виджет отображает текущую загруженность диска.

— **SWAP usage.** Виджет отображает загруженность файла подкачки.

— **Network input.** Виджет отображает скорость передачи входящих по сети данных.

— **Network output.** Виджет отображает скорость передачи исходящих по сети данных.

— **CPU per core.** Виджет отображает загруженность ядер процессора.

— **File system parameters.** Виджет отображает список физических и виртуальных дисков, их точки монтирования и тип файловой системы.

— **Disk I/O load.** Виджет отображает загруженность диска в течение установленного периода времени.

— **Disk write speed.** Виджет отображает скорость записи данных на диск и скорость чтения данных с диска.

— **Processes by state.** Виджет отображает состояние запущенных в системе процессов:

- **running** — исполняемые в данный момент процессы;
- **blocked** — завершенные процессы;
- **idle** — запущенные процессы, не исполняемые в данный момент;
- **sleeping** — процессы, находящиеся в режиме ожидания для продолжения работы.

— **TCP connections by state.** Виджет отображает состояние сетевых соединений по протоколу TCP:

- **ESTABLISHED** — установленные сетевые соединения;
- **TIME_WAIT** — сетевые соединения, находящиеся в режиме ожидания;
- **LISTEN** — порты, которые прослушиваются сервисами на сервере;
- **CLOSE_WAIT** — сетевые соединения, ожидающие завершения передачи данных от удаленной стороны;
- **FIN_WAIT2** — сетевые соединения, отправившие запрос на завершение передачи данных и ожидающие подтверждения удаленной стороны;
- **TIME_WAIT** — сетевые соединения, отправившие последнее подтверждение при закрытии;
- **SYN_WAIT** — сетевые соединения, отправившие запрос SYN и ожидающие ответа удаленной стороны.

— **Network flow.** Виджет отображает загруженность выбранного сетевого интерфейса, а также скорость приема и передачи данных.

— **Container restarts.** Виджет отображает количество перезапусков контейнеров системы.

— **Container uptime.** Виджет отображает время, в течение которого контейнеры находятся в запущенном состоянии после последнего перезапуска.

Виджеты Containers

Секция содержит виджеты мониторинга производительности для конкретных контейнеров, развернутых на сервере. Доступны следующие виджеты:

— **CPU usage.** Виджет отображает загруженность процессора.

— **Memory usage.** Виджет отображает количество задействованной контейнерами оперативной памяти.

— **Disk write speed.** Виджет отображает скорость записи данных на выбранный диск.

— **Disk read speed.** Виджет отображает скорость чтения данных с выбранного диска.

— **Network input.** Виджет отображает скорость передачи входящих по сети данных.

— **Network output.** Виджет отображает скорость передачи исходящих по сети данных.

12.14. Работа с дашбордом SqlStorage

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

— **Databases.** Виджет отображает общие данные о базах данных:

- **count** — количество баз данных в СУБД;
- **size** — общий размер всех баз данных;
- **temp bytes** — объем временных файлов, создаваемых СУБД для обработки запросов.

— **Transaction rate.** Виджет отображает количество транзакций в секунду:

- **commit** — количество успешных транзакций;
- **rollback** — количество отмененных транзакций.

— **Checkpoint write time.** Виджет отображает время записи изменений из временного хранилища в основную базу данных. По умолчанию запись происходит каждые пять минут.

— **Checkpoint by request.** Виджет отображает время записи изменений из временного хранилища в основную базу данных вне очереди.

— **Checkpoint count.** Виджет отображает количество записей в основную базу данных с момента последнего перезапуска СУБД:
  - **timed** — записи по расписанию;
  - **req** — записи вне очереди.
— **Checksum fail.** Виджет отображает количество несовпадений контрольных сумм в табличных списках и в записанных на диск файлах.
— **No rollback.** Виджет отображает процент успешно проведенных транзакций в базах данных с момента перезапуска СУБД.
— **Cache hit.** Виджет отображает процент запросов, обработанных с помощью буферного кэша без обращения к памяти диска.
— **Deadlocks.** Виджет отображает количество взаимных блокировок между запросами к одним и тем же табличным спискам.
— **Checkpoint hit.** Виджет отображает соотношение записей в базы данных по расписанию и записей вне очереди.
— **Operation speed.** Виджет отображает количество операций определенного типа в секунду:
  - **return** — запрошенные у СУБД записи;
  - **fetch** — записи, возвращаемые СУБД в результате применения фильтров;
  - **insert** — вставленные записи;
  - **delete** — удаленные записи;
  - **update** — измененные записи.
— **SqlStorage settings: size.** Виджет отображает заданные для роли SqlStorage параметры:
  - **effective_cache_size** — объем дискового кэша на узле, на котором развернута СУБД. Параметр влияет на работу планировщика запросов;
  - **shared_buffers** — объем буферного кэша, с помощью которого СУБД обрабатывает запросы;

- **wal_buffers** — объем кэша, выделенного под журнал предзаписи;
- **work_mem** — объем кэша, выделенного под запросы пользователя.

— **SqlStorage settings: limits.** Виджет отображает заданные для роли SqlStorage лимиты:

- **autovacuum_analyze_threshold** — количество изменений строк, после которого запускается операция `autovacuum_analyze`;
- **max_connections** — максимальное количество установленных соединений;
- **max_parallel_workers** — максимальное количество параллельных вычислений для выполнения одного запроса.

— **SqlStorage settings: time.** Виджет отображает заданное для роли SqlStorage время:

- **autovacuum_naptime** — интервал между операциями `autovacuum`. Параметр задает время, которое должно пройти между двумя операциями `autovacuum`, даже если лимит изменений строк превышен;
- **checkpoint_timeout** — интервал между записями по расписанию.

— **Database size.** Виджет отображает семь самых объемных баз данных:

- **max** — наибольший размер базы данных с момента перезапуска СУБД;
- **current** — текущий размер базы данных. Показатель может быть меньше максимального после выполнения операции `vacuum_full`.

— **Database temporary file size.** Виджет отображает шесть баз данных с самыми объемными временными файлами.

— **Sessions.** Виджет отображает количество сервисных соединений:

- **idle** — установленные неактивные соединения;
- **active** — установленные активные соединения;
- **wait** — установленные активные соединения, ожидающие в очереди;
- **total backends** — все установленные соединения.

— **Query time.** Виджет отображает самый длинный исполняемый запрос на данный момент.

— **Transaction idle time.** Виджет отображает время самой длинной незакрытой транзакции.

— **Killed.** Виджет отображает количество принудительно отмененных транзакций.

— **Abandoned.** Виджет отображает количество транзакций, отмененных в результате потери соединения.

— **Query state.** Виджет отображает количество установленных соединений в разных статусах за время, прошедшее с перезапуска СУБД.

— **Session breaks.** Виджет отображает количество завершенных соединений за время, прошедшее с перезапуска СУБД.

— **Longest database query time.** Виджет отображает длинные запросы, выполненные с момента перезапуска СУБД, с разделением по базам данных.

— **Idle transactions.** Виджет отображает неактивные соединения с разделением по базам данных.

13. Удаление истории изменения активов

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

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

В ходе ротации удаляются:

— конфигурации активов и данные о состоянии активов до даты ротации;

— информация о вхождении активов в группы до даты ротации;

— данные о состоянии уязвимостей, найденных на активах до даты ротации.

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

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

Возможные последствия

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

— Сведения об активе могут заменяться значениями из версии, ближайшей к дате ротации.

— Данные о привязке актива к группе будут содержать только последнее актуальное состояние.

— Если перед датой ротации актив в последний раз изменялся вручную, а не по результатам аудита, в качестве даты последнего обновления в жизненном цикле на карточке актива будет отображаться дата последнего аудита актива, но состояние актива на эту дату отображаться не будет.

Настройка ротации истории изменения активов

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

Внимание! Исторические данные удаляются безвозвратно, поэтому перед включением ротации настоятельно рекомендуется создать резервную копию базы данных assets_temporal_rm. Инструкцию по созданию резервной копии вы можете найти на сайте postgresql.org.

► Чтобы включить и настроить ротацию истории изменения активов:

1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz` из комплекта поставки:
   ```
   tar xzf pt_core_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_core_<Номер версии>/install.sh
   ```
3. Выберите вариант с идентификатором приложения роли.
4. Выберите вариант с идентификатором экземпляра роли.

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

   Откроется страница со списком параметров (см. приложение Б).
6. Установите флажок `HistoryRotationEnabled`.
7. В качестве значения параметра `HistoryRotationDepth` укажите глубину ротации — период истории изменения активов, данные за который необходимо удалять:
   ```
   <Дни>.<Часы>:<Минуты>:<Секунды>
   ```

   Например:
   ```
   110.00:00:00
   ```

   Внимание! Минимально допустимое значение параметра `HistoryRotationDepth` — 14 дней (`14.00:00:00`).
8. В качестве значения параметра `HistoryRotationCronSchedule` укажите периодичность запуска ротации с помощью планировщика заданий cron:
   ```
   <Минута> <Час> <Число> <Месяц> <День недели>
   ```

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

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

10. Нажмите **Submit**.

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

11. Нажмите кнопку **OK**.

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

Ротация истории изменения активов включена и настроена.

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

14. Изменение сроков актуальности данных сканирования активов

- Чтобы изменить сроки актуальности данных сканирования активов:

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

15. Ротация результатов сканирования, импорта и ручного ввода активов

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

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

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

В ходе ротации устаревшие результаты удаляются пакетами указанного размера.

> **Внимание!** Чтобы освободить дисковое пространство, после выполнения ротации необходимо запустить утилиту pgcompacttable (см. раздел 37.42.16) для БД сервиса Assets.Scans.

Настройка ротации результатов сканирования, импорта и ручного ввода активов

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

- Чтобы настроить ротацию результатов сканирования, импорта и ручного ввода активов,

  измените конфигурацию роли MP 10 Core, указав значения следующих параметров:

  `ScansRotationEnabled`: `True`

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

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

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

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

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

16. Максимальный размер собранных данных

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

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

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

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

> **Внимание!** При выборе значения `MaxScanSizeKb` следует учитывать связанные с этим ограничения на размер Active Directory. Например, при значении `MaxScanSizeKb`, равном 600 000 КБ, поддерживается аудит служб каталогов Active Directory, включающих до 100 000 пользователей и 5000 групп.
>
> **Примечание.** Чтобы снизить требования к размеру памяти при аудите Active Directory, вы можете ограничить количество собираемых активов. Подробности см. в разделе «Microsoft Active Directory в Windows Server 2003—2022: настройка MaxPatrol SIEM» Руководства по настройке источников.

Таблица 3. Максимальный размер собранных данных

Память (ОЗУ)	**Рекомендуемое значение MaxScanSizeKb, КБ**
80 ГБ	800 000
90 ГБ	900 000
100 ГБ	1 000 000

- Чтобы указать максимальный размер собранных данных,

  измените конфигурацию роли MP 10 Core, указав значение параметра `MaxScanSizeKb` в килобайтах.

17. Тайм-аут для подзадач сбора данных

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

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

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

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

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

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

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

18. Оптимизация выполнения PDQL-запросов для высоконагруженных систем

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

Режим работы оптимизации управляется следующими параметрами:

— `AssetGridVersionRangeModeEnabled` — определяет, включена оптимизация (значение `True`) или отключена (значение `False`).

— `AssetGridValidTimePeriodIndexFormat` — определяет режим оптимизации:

- Максимальная оптимизация (значение `IdAndPeriod`). Режим обеспечивает максимальную производительность выполнения PDQL-запросов — скорость их обработки увеличивается в несколько десятков раз.
- Средняя оптимизация (значение `PeriodOnly`). Режим снижает нагрузку на систему при работе с большими объемами данных. Скорость обработки PDQL-запросов увеличивается в несколько раз.

Примечание. По умолчанию в MaxPatrol SIEM версии 27.6 и выше включена оптимизация в максимальном режиме. В версиях ниже 27.6 рекомендуется включить оптимизацию вручную.

Таблица 4. Рекомендации по выбору режима оптимизации

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

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

- Чтобы настроить оптимизацию выполнения PDQL-запросов,

  измените конфигурацию (см. раздел 29.2) роли Core, указав для параметра `AssetGridValidTimePeriodIndexFormat` одно из значений: `IdAndPeriod` или `PeriodOnly`.

Отключение и повторное включение оптимизации выполнения PDQL-запросов

Отключение оптимизации рекомендуется только в отдельных случаях:

— при выполнении миграции PDQL, если процесс зависает или выполняется длительное время;

— при нестабильной инфраструктуре (недостаток ресурсов, проблемы с дисковой подсистемой).

В этих случаях:

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

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

- Чтобы отключить оптимизацию,

  измените конфигурацию (см. раздел 29.2) роли Core, указав для параметра `AssetGridVersionRangeModeEnabled` значение `False`.

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

— созданные индексы не удаляются;

— структура БД не возвращается к базовому сценарию работы;

— ранее выполненные изменения в БД сохраняются.

Повторное включение оптимизации после ее отключения:

— не запускает повторную миграцию данных сервиса TRM;

— не приводит к повторному созданию индексов;

— не вызывает повторного увеличения размера БД, так как изменения уже были внесены ранее и не откатываются;

— только изменяет способ выполнения SQL-поиска в БД.

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

► Чтобы определить размер базы данных сервиса TRM:

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

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

► Чтобы включить и настроить оптимизацию выполнения PDQL-запросов,

измените конфигурацию (см. раздел 29.2) роли Core, указав значения следующих параметров:

`AssetGridVersionRangeModeEnabled`: `True`

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

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

Дополнительные рекомендации

При проблемах с производительностью PDQL-запросов также рекомендуется:

— переводить виджеты в ручной режим обновления;

— уменьшать количество параллельных потоков;

— анализировать и оптимизировать политики;

— избегать использования ресурсоемких операторов (например, `like` с широкими шаблонами).

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

19. 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 и данные хранилища LogSpace. 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.

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

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

Для резервного копирования данных компонентов на Linux необходимо создать резервные копии данных ролей в следующем порядке: 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).

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

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

В этом разделе

Особенности создания резервной копии роли SqlStorage (см. раздел 19.1)

Создание резервной копии данных (см. раздел 19.2)

Создание резервной копии индексов Elasticsearch на Linux (см. раздел 19.3)

Создание резервной копии данных хранилища LogSpace (см. раздел 19.4)

Создание резервной копии пользовательских определений роли RMQ Message Bus (см. раздел 19.5)

О резервном копировании данных о площадках и их связях (см. раздел 19.6)

19.1. Особенности создания резервной копии роли SqlStorage

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

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

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

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

Например:

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

19.2. Создание резервной копии данных

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

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

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

В ходе восстановления данных из резервной копии (см. раздел 20.1) необходимо добавить:

— файлы сертификатов роли Deployer — в каталоги `/opt/deployer/pki/` и `/opt/deployer/pki/trusted_ca/`;

— файлы сертификатов остальных ролей — в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.

Чтобы избежать ошибок в ходе восстановления данных из резервной копии, при сохранении копий файлов пользовательских доверенных сертификатов их необходимо отличать от системных. Для этого вы можете воспользоваться поиском пользовательских сертификатов (см. раздел 37.42.15).

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

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

► Чтобы создать резервную копию данных,

запустите сценарий резервного копирования:

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

Например:

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

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

Например:

`/home/mc-application/sqlstorage`.

19.3. Создание резервной копии индексов Elasticsearch на Linux

Если в системе запущена задача архивации индексов по расписанию, перед созданием резервной копии необходимо ее остановить. Вы можете проверить наличие запущенных задач архивации с помощью команды `ps aux|grep backup_tool`.

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. На сервере с установленной ролью SIEM Storage 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. Каталог для хранения резервной копии не должен располагаться в домашнем каталоге пользователя.

   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
     ```

Если задача архивации индексов по расписанию была остановлена, после создания резервной копии необходимо заново зарегистрировать (см. раздел 21.3.1) хранилище архивных индексов и запустить задачу.

19.4. Создание резервной копии данных хранилища LogSpace

Для резервного копирования данных из хранилища LogSpace используется утилита backup_tool. Она входит в состав пакета dbtools и устанавливается вместе с ролью Event Storage.

Внимание! Если MaxPatrol SIEM установлен на Astra Linux и включен мандатный контроль целостности, после обновления операционной системы может возникнуть ошибка (см. раздел 19.4) при создании резервной копии данных LogSpace. Чтобы этого избежать, необходимо зафиксировать (см. раздел 37.42.19) атрибуты контроля целостности для каталога с данными хранилища.

- Чтобы создать резервную копию данных,

  на сервере с ролью Event Storage выполните одно из следующих действий:

  - Если требуется создать полную резервную копию данных, выполните команду:

    ```
    /usr/local/bin/backup_tool --cmd full_backup
    ```

  - Если требуется создать резервную копию данных за определенный период, выполните команду:

    ```
    /usr/local/bin/backup_tool --cmd backup --from <Начальная дата в формате ГГГГММДД> --to <Конечная дата в формате ГГГГММДД>
    ```

    Например:

    ```
    /usr/local/bin/backup_tool --cmd backup --from 20240504 --to 20240505
    ```

  - Если требуется создать резервную копию данных, с момента формирования которых прошло не меньше определенного количества дней, выполните команду:

    ```
    /usr/local/bin/backup_tool --cmd backup -t <Количество дней>
    ```

    Например:

    ```
    /usr/local/bin/backup_tool --cmd backup -t 7
    ```

    Примечание. При создании частичной копии исходные разделы данных сохраняются. Если вы хотите их удалить, необходимо использовать ключ `--delete part true`.

Вы можете задать каталог для сохранения резервной копии данных с помощью параметра `BackupPath` роли Event Storage. По умолчанию используется каталог `/db_backup`.

См. также

Особенности обновления Astra Linux при использовании хранилища LogSpace (см. раздел 37.42.19)

19.5. Создание резервной копии пользовательских определений роли RMQ Message Bus

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

- Чтобы создать резервную копию,

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

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

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

19.6. 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.

20. 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 и данные хранилища LogSpace. 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

Восстановление данных компонентов MaxPatrol SIEM на Linux из резервной копии (см. раздел 20.1)

Восстановление индексов Elasticsearch из резервной копии на Linux (см. раздел 20.2)

Восстановление данных хранилища LogSpace из резервной копии (см. раздел 20.3)

Восстановление пользовательских определений роли RMQ Message Bus (см. раздел 20.4)

О восстановлении резервной копии данных о площадках и их связях (см. раздел 20.5)

20.1. 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.

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

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

- Чтобы восстановить данные компонентов на Linux:

1. Установите пакеты ролей и экземпляр роли Deployer с помощью сценария `install_all_role_packages.sh`.
2. 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. Восстановите данные роли Deployer:

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

   Например:

   ```
   /var/lib/deployed-roles/Deployment-Application/Deployer/restore.sh /home/deploy-app/Deployer/backup.tar
   ```
4. Запустите сценарий для обновления идентификаторов версий пакетов приложений:

   ```
   deployer maintenance fix -AppPackage
   ```

   По завершении работы сценария отобразится сообщение `Finishing repair process for app package references`.
5. Если вы используете пользовательские сертификаты, добавьте файлы корневых и промежуточных пользовательских сертификатов центра сертификации для роли Deployer, сохраненные на этапе резервного копирования (см. раздел 19.2), в каталог `/opt/deployer/pki/trusted_ca/`.
6. 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.
7. 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>/' {} \;`.

8. Если ранее были добавлены файлы корневых и промежуточных пользовательских сертификатов, выполните команду для их обработки:

   ```
   deployer instance reconfigure -type Deployer
   ```

9. Создайте каталоги, в которых хранились файлы сертификатов.

   ```
   mkdir -p <Путь к каталогу сертификатов>
   ```

   Например:

   ```
   mkdir -p /var/lib/deployed-roles/mp10-application/core-1/certs
   ```

10. Скопируйте в эти каталоги файлы сертификатов, сохраненные при создании резервной копии:

    ```
    cp <Путь к каталогу резервной копии сертификатов>/* <Путь к каталогу сертификатов>
    ```

    Например:

    ```
    cp backup/certs/core/certs/* /var/lib/deployed-roles/mp10-application/core-1/certs
    ```

11. Установите роль SqlStorage.

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

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

12. Восстановите данные роли SqlStorage:

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

    Например:

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

13. Установите роль LogConnector:

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

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

14. Установите роль Observability:

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

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

15. Установите роли Management and Configuration и Knowledge Base.

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

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

16. 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>
    ```

17. Установите роли RMQ Message Bus и Core.

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

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

18. Восстановите данные роли Core:

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

19. Выполните одно из следующих действий:

    - Если в качестве хранилища событий используется Elasticsearch, установите роль SIEM Storage.

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

    - Если в качестве хранилища событий используется LogSpace, установите роль Event Storage.

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

20. Установите роли RMQ Message Bus и SIEM Server.

    ```
    pt_rmqmessagebus_<Номер версии>/install.sh
    pt_siemserver-linux_<Номер версии>/install.sh
    ```

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

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

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

    - Если резервная копия была создана на том же сервере, на котором выполняется восстановление, добавьте файлы пользовательских сертификатов, сохраненные на этапе резервного копирования (см. раздел 19.2), в каталоги `/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.
    - Если резервная копия была создана на одном сервере, а восстановление выполняется на другом, для доверенного сертификата в расширении Subject Alternative Name (SAN) должен быть указан IP-адрес или FQDN того сервера, на котором выполняется восстановление.

22. 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>
    ```

23. Выполните команду для восстановления экземпляров роли Collector:

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

24. Если ранее у вас были установлены роли Grafana, PT UCS, Retro Correlator и BAD, установите их.
25. Выполните реконфигурацию экземпляров ролей.
    ```
    deployer instance reconfigure -diff -silent
    ```
26. Если ключ инсталляции PT MC уже использовался для активации PT MC на другом устройстве, деактивируйте (см. раздел 37.42.5) PT MC.
27. Если вы деактивировали PT MC, повторно активируйте систему по инструкции «Активация PT MC» Руководства по внедрению.

    Внимание! Количество активаций ключа инсталляции PT MC ограничено. Если лимит активаций превышен, ваш экземпляр PT MC отключится через 30 дней с момента активации. Чтобы избежать этого, обратитесь в службу технической поддержки Positive Technologies.
28. Если вы деактивировали PT MC, повторно активируйте MaxPatrol SIEM по инструкции «Активация лицензии MaxPatrol SIEM» Руководства по внедрению.

См. также

Создание резервной копии данных (см. раздел 19.2)

20.2. Восстановление индексов Elasticsearch из резервной копии на Linux

При восстановлении 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.

Вы можете просмотреть список архивных индексов с помощью соответствующей команды (см. раздел 21.1).

В этом разделе

Восстановление всех индексов Elasticsearch из резервной копии на Linux (см. раздел 20.2.1)

Восстановление индексов Elasticsearch, созданных за определенный период, из резервной копии на Linux (см. раздел 20.2.2)

20.2.1. Восстановление всех индексов Elasticsearch из резервной копии на Linux

Внимание! Перед восстановлением индексов необходимо убедиться, что в системе отсутствуют индексы с датой создания, совпадающей с датой создания архивных индексов, — и при наличии таких индексов удалить (см. раздел 21.6) их.

- Чтобы восстановить индексы Elasticsearch из резервной копии на Linux:

1. На сервере с установленной ролью SIEM Server остановите службу SIEM Server storage:
   ```
   docker stop $(docker ps --format '{{.ID}} {{.Image}}' | awk '$2 ~ /\/storage:/ {print $1}')
   ```
2. На сервере с установленной ролью Event Storage остановите все службы Elasticsearch:
   ```
   systemctl stop -a elasticsearch*
   ```
   Внимание! При остановке служб SIEM Server storage и Elasticsearch компонент MP SIEM Events Storage прекратит получать события; некоторые данные при этом могут быть потеряны.
3. На сервере с установленной ролью Event Storage удалите каталог с индексами:
   ```
   rm -rf /<Путь к каталогу индексов>/*
   ```
   Примечание. Вы можете просмотреть путь к каталогу индексов в конфигурационном файле хранилища Elasticsearch `/etc/elasticsearch/*/elasticsearch.yml`.
4. Запустите все службы Elasticsearch:
   ```
   systemctl start -a elasticsearch*
   ```
5. На сервере с установленной ролью SIEM Server запустите службу SIEM Server storage для загрузки шаблона индекса:
   ```
   docker start $(docker ps -a --format '{{.ID}} {{.Image}}' | awk '$2 ~ /\/storage:/ {print $1}')
   ```
6. Остановите службу SIEM Server storage:
   ```
   docker stop $(docker ps --format '{{.ID}} {{.Image}}' | awk '$2 ~ /\/storage:/ {print $1}')
   ```
7. На сервере с установленной ролью Event Storage 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>"
   ```
8. 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>
   ```
9. На сервере с установленной ролью SIEM Server запустите службу SIEM Server storage:
   ```
   docker start $(docker ps -a --format '{{.ID}} {{.Image}}' | awk '$2 ~ /\/storage:/ {print $1}')
   ```

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

20.2.2. 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,

  выполните команду:

  ```
  /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.

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

20.3. Восстановление данных хранилища LogSpace из резервной копии

Для восстановления данных хранилища LogSpace из резервной копии используется утилита backup_tool. Она входит в состав пакета dbtools и устанавливается вместе с ролью Event Storage.

Полное восстановление данных из резервной копии

- Чтобы восстановить данные из резервной копии:

  1. На сервере MP SIEM Server остановите службу SIEM Server storage:

     ```
     docker stop $(docker ps --format '{{.ID}} {{.Image}}' | awk '$2 ~ /\/storage:/ {print $1}')
     ```

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

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

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

Внимание! При удалении таблиц будут также удалены все данные из них.

3. На сервере с ролью Event Storage выполните команду:

   ```
   /usr/local/bin/backup_tool --cmd full_restore --arc <Название резервной копии>
   ```

   Например:

   ```
   /usr/local/bin/backup_tool --cmd full_restore --arc siem.*.20220512.000001
   ```

   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.

4. Запустите службу SIEM Server storage:

   ```
   docker start $(docker ps -a --format '{{.ID}} {{.Image}}' | awk '$2 ~ /\/storage:/ {print $1}')
   ```

Восстановление данных за период

Вы также можете восстановить из резервной копии данные за период. Для этого восстановление необходимо выполнять в ту же БД, из которой была создана резервная копия. Если раздел уже существует в хранилище LogSpace, он не будет восстановлен.

- Чтобы восстановить данные за период из резервной копии,

  на сервере с ролью Event Storage выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd restore --from <Начальная дата в формате ГГГГММДД> --to <Конечная дата в формате ГГГГММДД>
  ```

  Например:

  ```
  /usr/local/bin/backup_tool --cmd restore --from 20240504 --to 20240505
  ```

20.4. Восстановление пользовательских определений роли RMQ Message Bus

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

- Чтобы восстановить данные из резервной копии,

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

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

20.5. 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, а по окончании восстановления открыть этот порт.

21. 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 высоконагруженной 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 `docker restart $(docker ps | awk '/storage.siemserver/ {print $NF}')`.

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

Вы можете изменить время хранения индексов в горячей стадии с помощью параметра `ElasticsearchManagedStorageWarmTime` роли SIEM Server по инструкции раздела «Изменение времени хранения индексов Elasticsearch в горячей стадии».

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

В этом разделе

Просмотр списка индексов (см. раздел 21.1)

Настройка ротации индексов (см. раздел 21.2)

Архивация индексов (см. раздел 21.3)

Восстановление индекса из архива (см. раздел 21.4)

Удаление архивных индексов (см. раздел 21.5)

Удаление индекса без архивации (см. раздел 21.6)

Перемещение индексов на Linux (см. раздел 21.7)

Настройка политик ILM при смене конфигурации MaxPatrol SIEM (см. раздел 21.8)

21.1. 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
  ```

21.2. 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`), в конфигурационных параметрах компонента MP SIEM Events Storage в соответствии с инструкцией по изменению конфигурации роли.

21.3. Архивация индексов

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

В этом разделе

Создание хранилища для архивных индексов (см. раздел 21.3.1)

Архивация индексов на Linux (см. раздел 21.3.2)

Архивация индексов по расписанию (см. раздел 21.3.3)

21.3.1. 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.
  ```

21.3.2. 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> -di false
  ```

  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> -di false
  ```

  Примечание. При выполнении команд архивации без ключа `-di false` сохраненные индексы будут удалены.

21.3.3. 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
```

21.4. Восстановление индекса из архива

Восстановление индекса из архива возможно только на том сервере, где была выполнена архивация этого индекса.

- 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.

21.5. Удаление архивных индексов

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

В этом разделе

Удаление архивных индексов на Linux (см. раздел 21.5.1)

Удаление архивных индексов по расписанию (см. раздел 21.5.2)

21.5.1. 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>
  ```

21.5.2. 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
```

21.6. 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.

21.7. Перемещение индексов на Linux

- Чтобы переместить индексы:

  1. Остановите все задачи на сканирование сети и на сбор данных.
  2. На сервере MP SIEM Server остановите службу SIEM Server storage:

     ```
     docker stop $(docker ps -aqf name=siem.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:

   ```
   mv <Путь к каталогу с индексами Elasticsearch>/* <Путь к каталогу нового хранилища>
   ```

   Например:

   ```
   mv /data/* /storage/
   ```

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

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

6. Запустите сценарий:

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

7. Нажмите **Yes**.
8. Выберите вариант с идентификатором приложения MaxPatrol 10.
9. Выберите вариант с названием экземпляра роли SIEM Storage.
10. Выберите **Basic configuration**.
11. Измените значение параметра `PathData`:

    ```
    PathData: <Путь к каталогу нового хранилища>
    ```

12. Нажмите **OK**.

    После изменения конфигурации появится сообщение `Deployment configuration successfully applied`.

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

    ```
    docker start $(docker ps -aqf name=siem.storage)
    ```

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

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

16. Запустите остановленные задачи.

21.8. Настройка политик ILM при смене конфигурации MaxPatrol SIEM

Настройка политик ILM при переходе с конфигурации для средненагруженных систем на конфигурацию для высоконагруженных систем с потоком событий выше 20 000 в секунду

- Чтобы настроить политики ILM:

  1. На сервере компонента MP SIEM Events Storage выполните команды:

     ```
     curl -H 'Content-Type: application/json' -X PUT -d '{"index.routing.allocation.require" : {"data" : "warm"}}' http://127.0.0.1:9200/*siem*/_settings
     curl -H 'Content-Type: application/json' -X PUT -d '{"index.routing.allocation.require" : {"data" : "warm"}}' http://127.0.0.1:9200/cp/_settings
     ```

  2. Выполните команду:

     ```
     systemctl stop --all elasticsearch*
     ```

  3. Перейдите в каталог с данными хранилища событий Elasticsearch (по умолчанию `/data`) и переименуйте каталоги с узлами данных:

     ```
     cd /<Каталог с данными хранилища событий Elasticsearch>
     mv data_1 data_3
     mv data_2 data_4
     ```

  4. Обновите роль SIEM Storage, указав в наборе параметров **Advanced configuration** значения следующих параметров:

     ```
     PathData: <Каталог для хранения индексов в теплой стадии и счетчиков всех индексов>
     PathDataHot: <Каталог для хранения индексов в горячей стадии>
     PathRepo: <Каталог для хранения резервных копий индексов>
     PathLog: <Каталог для хранения файлов журналов>
     [x] ManagedStorage
     ```

  5. Обновите роль SIEM Server, установив в наборе параметров **Advanced configuration** флажок **ManagedStorage**.

  Примечание. Вы можете проверить состояние хранилища Elasticsearch, выполнив команду `curl 127.0.0.1:9200/_cluster/health?pretty` и корректность размещения данных и индексов, выполнив команду `curl 127.0.0.1:9200/_cat/shards?v`.

Настройка политик ILM при переходе с конфигурации для высоконагруженных систем на конфигурацию для высоконагруженных систем с потоком событий выше 20 000 в секунду

- Чтобы настроить политики ILM:

1. На сервере компонента выполните команду:

   ```
   curl -H 'Content-Type: application/json' -X PUT -d '{"transient" :
   {"cluster.routing.allocation.exclude._name" : "data_1, data_2"}}' http://127.0.0.1:9200/
   _cluster/settings
   ```

   Начнется перемещение индексов с узлов данных data_1 и data_2 на узлы данных data_3 и data_4. Перемещение займет некоторое время, нужно дождаться окончания процесса.

   Примечание. Вы можете отслеживать перемещение индексов с помощью команды `curl 127.0.0.1:9200/_cat/shards?v`.

2. Выполните команды:

   ```
   curl -H 'Content-Type: application/json' -X PUT -d '{"index.routing.allocation.require" :
   {"data" : "warm"}}' http://127.0.0.1:9200/*siem*/_settings
   curl -H 'Content-Type: application/json' -X PUT -d '{"index.routing.allocation.require" :
   {"data" : "warm"}}' http://127.0.0.1:9200/cp/_settings
   ```

3. Обновите роль SIEM Storage, указав в наборе параметров **Advanced configuration** значения следующих параметров:

   ```
   PathData: <Каталог для хранения индексов>
   PathDataHot: <Каталог для хранения индексов в горячей стадии>
   PathRepo: <Каталог для хранения резервных копий индексов>
   PathLog: <Каталог для хранения файлов журналов>
   [x] ManagedStorage
   ```

4. Обновите роль SIEM Server, установив в наборе параметров **Advanced configuration** флажок **ManagedStorage**.

5. Отключите блокировку узлов данных data_1 и data_2:

   ```
   curl -H 'Content-Type: application/json' -X PUT -d '{"transient" :
   {"cluster.routing.allocation.exclude._name" : ""}}' http://127.0.0.1:9200/_cluster/
   settings
   ```

Примечание. Вы можете проверить статус Elasticsearch и корректность создания новых индексов с помощью команд `curl 127.0.0.1:9200/_cluster/health?pretty` и `curl 127.0.0.1:9200/_cat/shards?v` соответственно.

22. Разделы LogSpace: ротация, перемещение, резервное копирование и восстановление, переключение в режим гибридного хранилища

Внимание! Хранилище LogSpace (по умолчанию `/opt/logspaced/`) содержит каталоги `data`, `metadata` и `staging`. Эти каталоги должны располагаться в одной файловой системе, не перемонтируйте их и не используйте символические ссылки.

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, tailcutter и migrate.

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 Б) `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 Docker-контейнере dbtools, а сценарий ее запуска — в каталоге `/usr/local/bin/tailcutter`. Вы можете настроить параметры утилиты, изменяя конфигурацию роли Event Storage по инструкции или используя соответствующие ключи при запуске утилиты из командной строки.

Таблица 5. Ключи для запуска утилиты tailcutter

Ключ	Описание	Значение по умолчанию
`--help`	Вывод справочной информации о ключах, с которыми можно запускать утилиту tailcutter	—

Ключ	Описание	Значение по умолчанию
`--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%`
`--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`
`--loglevel <Уровень журналирования>`	Уровень журналирования событий утилиты tailcutter. Возможные значения — `DEBUG`, `INFO`, `WARNING`, `ERROR` или `CRITICAL`	`INFO`

Журналы утилиты tailcutter вы можете просмотреть с помощью команды `docker logs -f <Имя или идентификатор контейнера dbtools>`.

Резервное копирование и восстановление

Утилита backup_tool предназначена для резервного копирования (см. раздел 19.4) и восстановления данных хранилища LogSpace. Кроме того, утилита может удалять разделы и показывать списки существующих разделов и архивов хранилища.

После установки утилита хранится в Docker-контейнере dbtools, а сценарий ее запуска — в каталоге `/usr/local/bin/backup_tool`. Вы можете настроить параметры утилиты, используя соответствующие ключи при ее запуске из командной строки.

Таблица 6. 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`

Ключ	Описание	Значение по умолчанию
`--arc <Название резервной копии>`	Название файла резервной копии, из которого необходимо восстановить данные	—
`--delete-part <true или false>`	Удаление исходных разделов после создания их резервной копии	`false`
`--log <Имя файла>`	Путь к файлу журнала утилиты backup_tool	—
`--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 при использовании команды `deletepart` или сохранены при использовании команды `backup`	—
`--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 backup`	Создание резервной копии данных хранилища за определенный период. Период необходимо указать после команды с помощью ключа `--time` (`-t`) или пары ключей `--from` и `--to`	—
`--cmd restore`	Восстановление данных из резервной копии за определенный период. Период необходимо указать после команды с помощью пары ключей `--from` и `--to`	—

Ключ	Описание	Значение по умолчанию
`--cmd full_backup`	Создание резервной копии данных хранилища за все время	—
`---cmd full_restore`	Восстановление данных из резервной копии за все время	—
`--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`)	—

Перемещение

Перемещение разделов LogSpace 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.

Перенос данных из Elasticsearch

В состав набора утилит dbtools входит утилита migrate, которая позволяет перенести информацию о событиях из хранилища Elasticsearch в LogSpace.

После установки утилита хранится в Docker-контейнере dbtools, а сценарий ее запуска — в каталоге `/usr/local/bin/migrate`. Вы можете настроить параметры ее работы, используя соответствующие ключи при запуске утилиты из командной строки в соответствии с инструкцией. Описание ключей приведено в таблице ниже.

При запуске утилита проверяет доступность службы Elasticsearch, а также исходных базы данных и таблицы с информацией о событиях. После завершения проверки утилита поочередно обращается к каждому индексу Elasticsearch, выгружает из индекса информацию о событиях, преобразует полученные данные в формат для хранения в LogSpace и помещает на сервер, указанный при запуске. Утилита запрашивает данные из Elasticsearch в рамках

параллельных асинхронных процессов. Каждый процесс может включать в себя несколько подключений к хранилищу Elasticsearch. По умолчанию количество процессов и подключений соответствует количеству центральных процессоров на сервере с утилитой migrate.

При запуске утилиты в ее каталоге создается каталог `.complete`. В нем для каждого обработанного индекса Elasticsearch создается пустой файл с названием этого индекса. При следующем запуске утилита проверяет имена файлов из этого каталога и исключает из обработки все индексы Elasticsearch с такими же именами. Таким образом обеспечивается защита от сбоев при работе утилиты.

> **Внимание!** Количество файлов в каталоге `.complete`, созданных в результате запуска утилиты, соответствует количеству всех индексов исходной базы данных Elasticsearch — независимо от того, переносятся все данные или данные за период. Причина в том, что утилита берет дату создания события не из названия индекса, а из поля time самого события, а потому обрабатывает все индексы Elasticsearch. Поэтому после каждого успешного запуска утилиты необходимо удалять все файлы из каталога `.complete`.

Информация о каждой ошибке, вернувшейся в ответах на запросы к базе данных Elasticsearch, отображается в консоли. Помимо этого, каждый запрос с ошибкой в ответе утилита сохраняет в отдельный файл с именем вида `error_query_<Дата и время создания файла>`, например `error_query_2023-07-03 07:19:36.980885`.

Переключение LogSpace в режим гибридного хранилища

Для высоконагруженных систем вы можете настроить хранение данных в LogSpace с использованием разных типов хранилища для данных в горячей (SSD) и холодной (HDD) стадии.

В обычном режиме данные LogSpace находятся в корневом каталоге хранилища. В режиме гибридного хранилища в корневом каталоге будут храниться данные в горячей стадии, поэтому при переключении режима данные LogSpace необходимо перенести в каталог для хранения данных в холодной стадии.

В этом разделе

Просмотр списков разделов и архивов LogSpace (см. раздел 22.1)

Удаление разделов и архивов LogSpace (см. раздел 22.2)

Перемещение разделов LogSpace (см. раздел 22.3)

Резервное копирование разделов (см. раздел 22.4)

Архивация разделов (см. раздел 22.5)

Восстановление раздела из архива (см. раздел 22.6)

Перенос данных из Elasticsearch в LogSpace (см. раздел 22.7)

Переключение LogSpace в режим гибридного хранилища (см. раздел 22.8)

22.1. Просмотр списков разделов и архивов LogSpace

- Чтобы просмотреть список разделов хранилища LogSpace,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd listpart
  ```

- Чтобы просмотреть список архивов хранилища LogSpace,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd listarchive
  ```

22.2. Удаление разделов и архивов LogSpace

- Чтобы удалить раздел хранилища LogSpace,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd deletepart --part <Название раздела>
  ```

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

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd cleanarchive --time <Количество дней>
  ```

- Чтобы удалить архивы хранилища LogSpace за определенный период времени,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd cleanarchive --from <Начало периода в формате ГГГГММДД>
  --to <Окончание периода в формате ГГГГММДД>
  ```

22.3. Перемещение разделов LogSpace

- Чтобы переместить разделы:

  1. Остановите все задачи на сканирование сети и на сбор данных.
  2. На сервере MP SIEM Server остановите службу SIEM Server storage:

     ```
     docker stop $(docker ps -aqf name=siem.storage)
     ```

  3. На сервере MP SIEM Events Storage выполните команду:

     ```
     ps aux|grep logspaced
     ```

     Отобразится список параметров хранилища LogSpace. В качестве значения параметра `config-file` будет указан путь к конфигурационному файлу `config.xml`.

  4. Откройте конфигурационный файл `config.xml`:

     ```
     cat <Путь к конфигурационному файлу LogSpace>/config.xml
     ```

Например:

```
cat /etc/logspaced/config.xml
```

В качестве значения параметра `path` в конфигурационном файле будет указан путь к данным LogSpace, например `/opt/logspaced`.

5. На сервере MP SIEM Events Storage остановите службу LogSpace:
   ```
   systemctl stop logspaced
   ```
6. Переместите все файлы из каталога с разделами LogSpace в каталог нового хранилища:
   ```
   mv <Путь к каталогу с разделами LogSpace>/* <Путь к каталогу нового хранилища>
   ```
   Например:
   ```
   mv /opt/logspaced/* /storage/
   ```
7. На сервере с установленной ролью Deployer распакуйте архив `pt_eventstorage_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_eventstorage_<Номер версии>.tar.gz
   ```
8. Запустите сценарий:
   ```
   pt_eventstorage_<Номер версии>/install.sh
   ```
9. Нажмите **Yes**.
10. Выберите вариант с идентификатором приложения роли.
11. Выберите вариант с идентификатором экземпляра роли.
12. Выберите **Basic configuration**.
13. Измените значение параметра `PathData`:
    ```
    PathData: <Путь к каталогу нового хранилища>
    ```
14. Нажмите **OK**.

    После изменения конфигурации появится сообщение `Deployment configuration successfully applied`.
15. Нажмите **OK**.
16. На сервере MP SIEM Events Storage запустите службу LogSpace:
    ```
    systemctl start logspaced
    ```
17. На сервере MP SIEM Server запустите службу SIEM Server storage:
    ```
    docker start $(docker ps -aqf name=siem.storage)
    ```
18. Запустите остановленные задачи.

22.4. Резервное копирование разделов

- Чтобы выполнить резервное копирование разделов, созданных за определенный период,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd backup --from <Дата начала периода> --to <Дата окончания периода>
  ```

Примечание. Даты начала и окончания периода необходимо указывать в формате ГГГГММДД (например, 20241028).

22.5. Архивация разделов

- Чтобы архивировать разделы, созданные за определенный период,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd backup --from <Дата начала периода> --to <Дата окончания периода> --delete-part true
  ```

  Примечание. Даты начала и окончания периода необходимо указывать в формате ГГГГММДД (например, 20241028).

22.6. Восстановление раздела из архива

- Чтобы восстановить раздел из архива,

  в интерфейсе терминала Linux выполните команду:

  ```
  /usr/local/bin/backup_tool --cmd restore -a siem.events.<Дата архивации раздела>.<Порядковый номер архива>
  ```

Если раздел существует в хранилище LogSpace, он не будет восстановлен. Для просмотра разделов хранилища вы можете использовать команду `/usr/local/bin/backup_tool --cmd listpart`.

22.7. Перенос данных из Elasticsearch в LogSpace

Внимание! Для низконагруженных систем перенос данных из Elasticsearch в LogSpace не поддерживается.

Данные из каждого индекса Elasticsearch для передачи в утилиту migrate разбиваются на части, в каждой из которых около 10 000 событий. Максимальное количество таких частей в Elasticsearch по умолчанию ограничено до 1024. Для переноса индексов, которые содержат более 10 240 000 событий, необходимо предварительно изменить это ограничение. Поэтому перед запуском утилиты migrate необходимо запросить список индексов Elasticsearch с помощью команды `GET /_cat/indices` и определить индекс с наибольшим числом событий (N). Для такого индекса необходимо рассчитать количество частей, на которые его потребуется разделить для передачи в утилиту, по формуле `N/S`, где N — число событий в индексе Elasticsearch, а S — число событий в одном запросе утилиты migrate (определяется значением ключа `--size`).

Таким образом, при количестве событий в индексе, скажем, 59 217 754 и передаче за один запрос 10 000 событий необходимо будет разделить индекс на 59 217 754 : 10 000 ≈ 5922 части. Так как полученное значение превышает 1024, необходимо округлить его до тысяч в большую сторону и передать в Elasticsearch в качестве нового значения параметра `max_slices_per_scroll` с помощью запроса:

```
PUT /_all/_settings
{
"index" : {
"max_slices_per_scroll" : 6000
}
}
```

Внимание! Перед переносом данных из Elasticsearch в LogSpace необходимо переконфигурировать роль SIEM Server, указав в качестве значения параметра `StorageBackendType` — `logspace`, а в качестве значений параметров `LogSpaceHost` и `LogSpacePort` — IP-адрес или FQDN и порт сервера MP SIEM Events Storage соответственно.

- Чтобы перенести данные из Elasticsearch в LogSpace:

  1. В интерфейсе терминала Linux выполните команду:

     ```
     /usr/local/bin/migrate <Ключи для запуска утилиты> <Адрес сервера с хранилищем Elasticsearch>:<Порт> <Адрес сервера с хранилищем LogSpace>:<Порт>
     ```

     Например:

     ```
     ./migrate --size 10000 --workers 10 --connectors 10 --destination_database siem --destination_table events http://server1.example.com:9200 http://localhost:8123
     ```

     Запустится утилита migrate и начнется перенос информации о событиях из Elasticsearch в LogSpace.

  2. После завершения переноса данных на сервере с компонентом MP SIEM Events Storage остановите службу siemserver-storage.service:

     ```
     docker stop $(docker ps -qaf name="siem.storage")
     ```

  3. Удалите из базы данных LogSpace таблицу siem.cp:

     ```
     logspace-client -q "use siem; drop table cp"
     ```

  4. Запустите службу siemserver-storage.service:

     ```
     docker start $(docker ps -qaf name="siem.storage")
     ```

  5. Отключите службу Elasticsearch:

     ```
     systemctl stop -a elasticsearch_*
     systemctl disable -a elasticsearch_*
     ```

  Информация о событиях перенесена из Elasticsearch и отображается в интерфейсе MaxPatrol SIEM.

Таблица 7. Ключи для запуска утилиты migrate

Ключ	Описание	Значение по умолчанию
`--size`	Количество событий в одном запросе утилиты. Если ключ не указан, используется значение по умолчанию	`10000`
`--from`	Начало периода, события за который необходимо перенести из Elasticsearch в LogSpace, в формате ГГГГММДД. Соответствие событий указанному периоду проверяется по значению поля time в свойствах события	—
`--to`	Окончание периода, события за который необходимо перенести из Elasticsearch в LogSpace, в формате ГГГГММДД. Соответствие событий указанному периоду проверяется по значению поля time в свойствах события	—
`--destination_database`	Имя базы данных в LogSpace, в которую необходимо перенести данные из Elasticsearch. Если ключ не указан, используется значение по умолчанию	`siem`
`--destination_table`	Имя таблицы в LogSpace, в которую необходимо перенести данные из Elasticsearch. Если ключ не указан, используется значение по умолчанию	`events`
`--workers`	Количество процессов переноса данных из Elasticsearch, параллельно запускаемых утилитой	Равно количеству центральных процессоров на сервере с утилитой migrate
`--connectors`	Количество соединений с хранилищем Elasticsearch, которые может одновременно устанавливать утилита migrate	Равно количеству центральных процессоров на сервере с утилитой migrate
`--help`	Вывод на экран справочной информации о ключах, с которыми можно запускать утилиту migrate	—

22.8. Переключение LogSpace в режим гибридного хранилища

Примечание. Перед началом переключения LogSpace в режим гибридного хранилища рекомендуется уточнить и сохранить значения параметров `PathData` (путь к корневому каталогу хранилища по умолчанию `/opt/logspaced`) и `ColdPathData` (путь к каталогу для хранения данных в холодной стадии по умолчанию `/datacold`) роли Event Storage; сделать мгновенный снимок всех таблиц в БД с помощью команды `backup`. Также необходимо создать новый раздел диска с файловой системой для хранения данных в горячей стадии.

- Чтобы переключить LogSpace в режим гибридного хранилища:

  1. На сервере MP SIEM Events Storage остановите службу LogSpace:

     ```
     systemctl stop logspaced
     ```

  2. Отключите раздел диска с существующими данными LogSpace от корневого каталога хранилища:

     ```
     umount <Путь к корневому каталогу хранилища>
     ```

     Например:

     ```
     umount /opt/logspaced
     ```

  3. Подключите раздел диска с существующими данными LogSpace к каталогу для хранения данных в холодной стадии:

     ```
     mount /dev/<Раздел диска с существующими данными LogSpace> /<Путь к каталогу для хранения данных в холодной стадии>
     ```

     Например:

     ```
     mount /dev/sdb1 /datacold
     ```

  4. Подключите раздел диска для хранения данных в горячей стадии к корневому каталогу хранилища:

     ```
     mount /dev/<Раздел диска для хранения данных в горячей стадии> <Путь к корневому каталогу хранилища>
     ```

     Например:

     ```
     mount /dev/sdc1 /opt/logspaced
     ```

  5. Выведите на экран список идентификаторов (UUID) разделов дисков для хранения данных в холодной и горячей стадии:

     ```
     blkid
     ```

  6. В файле `/etc/fstab` в строке с идентификатором раздела диска для хранения данных в холодной стадии измените путь к корневому каталогу хранилища на путь к каталогу для хранения данных в холодной стадии:

     ```
     UUID=<Идентификатор раздела для хранения данных в холодной стадии> <Путь к каталогу для хранения данных в холодной стадии> ext4 defaults 0 0
     ```

     Например:

     ```
     UUID=f13746c4-c30b-4c0b-8002-1e04f1deff1a /datacold ext4 defaults 0 0
     ```

7. В файле `/etc/fstab` добавьте строку с идентификатором раздела для хранения данных в горячей стадии, указав в ней путь к корневому каталогу хранилища:

   ```
   UUID=<Идентификатор раздела для хранения данных в горячей стадии> <Путь к корневому каталогу хранилища> ext4 defaults 0 0
   ```

   Например:

   ```
   UUID=e3e5f4f3-5687-4ae4-a72c-7b959db2431e /opt/logspaced> ext4 defaults 0 0
   ```

8. Перенесите метаданные LogSpace:

   ```
   mv /<Путь к каталогу для хранения данных в холодной стадии>/{cores,flags,metadata,tmp} <Путь к корневому каталогу хранилища>
   ```

   Например:

   ```
   mv /datacold/{cores,flags,metadata,tmp} /opt/logspaced
   ```

9. Создайте структуру каталогов баз данных в корневом каталоге хранилища для размещения ссылок на существующие данные:

   ```
   mkdir -p /<Путь к корневому каталогу хранилища>/data/siem/{counters,events,cp}
   ```

   Например:

   ```
   mkdir -p /opt/logspaced/data/siem/{counters,events,cp}
   ```

10. Определите владельцем созданной структуры каталогов пользователя LogSpace:

    ```
    chown -R logspace:logspace /<Путь к корневому каталогу хранилища>/data
    ```

    Например:

    ```
    chown -R logspace:logspace /opt/logspaced/data
    ```

11. Создайте символические ссылки на существующие данные:

    ```
    ln -s /<Путь к каталогу для хранения данных в холодной стадии>/data/siem/events/* <Путь к корневому каталогу хранилища>/data/siem/events/
    ln -s /<Путь к каталогу для хранения данных в холодной стадии>/data/siem/counters/* <Путь к корневому каталогу хранилища>/data/siem/counters/
    ln -s /<Путь к каталогу для хранения данных в холодной стадии>/data/siem/cp/* <Путь к корневому каталогу хранилища>/data/siem/cp/
    ```

    Например:

    ```
    ln -s /datacold/data/siem/events/* /opt/logspaced/data/siem/events/
    ln -s /datacold/data/siem/counters/* /opt/logspaced/data/siem/counters/
    ln -s /datacold/data/siem/cp/* /opt/logspaced/data/siem/cp/
    ```

12. Измените конфигурацию роли Event Storage, установив в наборе параметров **Advanced configuration** флажок **ManagedStorage** и указав значения параметров:

    ```
    PathData: <Путь к корневому каталогу хранилища>
    ColdPathData: <Путь к каталогу для данных в холодной стадии>
    ```

Если переключение в режим гибридного хранилища произошло корректно, в веб-интерфейсе MaxPatrol SIEM будут доступны события.

23. Гибридное хранилище LogSpace: пути к хранилищам, политики переноса данных

Для высоконагруженных систем вы можете настроить хранение данных в LogSpace с использованием разных типов хранилища для данных в горячей (SSD) и холодной (HDD) стадии. Оба хранилища могут участвовать в обработке запросов, при этом использование хранилища для данных в холодной стадии зависит от глубины запроса и того, сколько данных может храниться на SSD.

Пути к хранилищам данных

Пути к хранилищам заданы в конфигурационном файле LogSpace `config.xml` в секции `logspace`:

— `path` — путь к хранилищу данных в горячей стадии (по умолчанию `/opt/logspaced/`);

— `cold_path` — путь к хранилищу данных в холодной стадии (по умолчанию `/opt/logspaced/cold/`).

Параметры политики переноса данных

Параметры политики переноса данных содержатся в конфигурационном файле `config.xml` в секции `logspace` → `merge_tree` → `multitier`:

— `policy` — действующая политика переноса данных. Возможные значения параметра:

- `noop` — перенос данных отключен, запись только в хранилище данных в горячей стадии (SSD), оба хранилища доступны для чтения;
- `hot_max` — запись в хранилище данных в горячей стадии (SSD) продолжается до тех пор, пока не будет достигнут лимит на использование памяти, установленный в параметре `hot_space`. При достижении лимита начинается перенос данных в хранилище холодной стадии (HDD);

  Примечание. Данные, перенесенные в хранилище холодной стадии, отображаются в хранилище горячей стадии с помощью символьных ссылок.

- `balance` — значение зарезервировано системой и недоступно для использования.

— `min_cold_part_gen` — репликация данных в зависимости от их поколения (по умолчанию `0`, все данные будут реплицированы вне зависимости от их поколения). Не рекомендуется к изменению;

— `min_cold_part_size` — репликация данных в зависимости от их размера (по умолчанию `0`, все данные будут реплицированы вне зависимости от их размера). Не рекомендуется к изменению;

— `hot_space` — объем свободного места в хранилище горячей стадии, по достижении которого начнется перенос данных в хранилище холодной стадии. Параметр может принимать значения от `0.1` до `0.9`. Например, если параметру `hot_space` присвоено значение `0.1`, перенос данных начнется, когда в хранилище горячей стадии останется 10% свободной памяти;

— `free_space` — параметр зарезервирован системой и недоступен для использования.

24. Настройка кэш-памяти для индексов LogSpace

Внимание! Изменение значений параметров, установленных по умолчанию, может ухудшить производительность LogSpace.

Для изменения доступны следующие параметры:

— `id_cache_size` — объем кэш-памяти, выделенный для словарей StringID;

— `mark_cache_size` — для разметки колонок на блоки;

— `index_cache_size` — для индексов;

— `fulltext_cache_size` — для полнотекстовых индексов.

Сумма значений всех четырех параметров не может превышать 25% общего объема оперативной памяти (ОЗУ) сервера LogSpace. Если вы присвоите этим параметрам значения, сумма которых превышает этот лимит, все четыре значения будут автоматически уменьшены с сохранением пропорции.

> **Примечание.** Перед изменением параметров вручную рекомендуется ознакомиться с тем, как кэш-память используется по умолчанию.

Просмотр использования кэш-памяти

► Чтобы узнать, как используется кэш-память,

выполните команду:

```
logspace-client -q"SELECT * FROM system.perf_counters WHERE name ILIKE '%cache%' FORMAT TabSeparated"
```

Настройка кэш-памяти

► Чтобы настроить кэш для индексов LogSpace:

1. Создайте файл `/etc/logspaced/profiles.d/cache-tune.xml`.
2. Добавьте в файл параметры `id_cache_size`, `mark_cache_size`, `index_cache_size` и `fulltext_cache_size` и их значения в гигабайтах.

   Например:

```
<logspace>
   <cache>
    <id_cache_size>6G</id_cache_size>
    <mark_cache_size>6G</mark_cache_size>
    <index_cache_size>25G</index_cache_size>
    <fulltext_cache_size>16G</fulltext_cache_size>
  </cache>
</logspace>
```

Примечание. Кэш-память `fulltext_cache_size` используется меньше всего, поэтому вы можете увеличить значения остальных параметров, уменьшив значение `fulltext_cache_size`.

3. Сохраните файл.

25. 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

Смена пароля служебной учетной записи в PostgreSQL (см. раздел 25.1)

Смена паролей служебных учетных записей в RabbitMQ (см. раздел 25.2)

Смена пароля служебной учетной записи в Grafana (см. раздел 25.3)

25.1. 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`.

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

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

  1. На сервере с установленной ролью Deployer выполните команду:
     ```
     deployer instance configure -type SqlStorage
     ```
  2. Измените конфигурацию (см. раздел 29.2) роли SqlStorage:
     ```
     PgPassword: <Новый пароль>
     ```
  3. Измените конфигурации (см. раздел 29.2) ролей LogConnector, Observability, Management and Configuration, Knowledge Base и Core.

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

25.2. 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 25.2.1)

RabbitMQ: смена паролей служебных учетных записей компонента MP SIEM Server на Linux (см. раздел 25.2.2)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Microsoft Windows (см. раздел 25.2.3)

RabbitMQ: смена пароля служебной учетной записи компонента MP 10 Collector на Linux (см. раздел 25.2.4)

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

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

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

- Чтобы сменить пароль служебной учетной записи MP 10 Core:

  1. На сервере MP 10 Core измените конфигурации (см. раздел 29.2) 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.

25.2.2. 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 25.2.2.1)

Смена паролей служебных учетных записей MP SIEM Server на Linux: компоненты MP SIEM Server и MP 10 Core установлены на разные серверы (см. раздел 25.2.2.2)

25.2.2.1. 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.

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

- 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 29.2)

25.2.2.2. 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.

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

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

  1. Измените конфигурацию 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 29.2)

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

По умолчанию при первой установке логин служебной учетной записи компонента MP 10 Collector на Microsoft Windows для доступа к RabbitMQ — `agent`, пароль — `P@ssw0rd`. При обновлении с версии 27.3 и ниже логин — `mpx_agent`.

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

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

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

     ```
     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 29.2)

25.2.4. 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`.

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

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

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

     ```
     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 29.2)

25.3. Смена пароля служебной учетной записи в Grafana

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

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

- Чтобы сменить пароль служебной учетной записи в Grafana,

  измените конфигурацию (см. раздел 29.2) роли Grafana, указав в качестве значения параметра `GrafanaAdminPassword` новый пароль учетной записи.

26. Смена пароля учетной записи администратора RabbitMQ

Учетная запись администратора используется для входа в веб-интерфейс (см. раздел 37.1.2) RabbitMQ. По умолчанию логин учетной записи — `Administrator`, пароль — `P@ssw0rd`.

> **Внимание!** Не рекомендуется использовать в пароле учетной записи администратора следующие символы: `\ / ' " $`.

Смена пароля УЗ администратора RabbitMQ, если MP 10 Core и MP SIEM Server установлены на один сервер

Если компоненты MP 10 Core и MP SIEM Server установлены на один сервер, они используют один брокер RabbitMQ и одну учетную запись администратора для доступа к нему.

- Чтобы изменить пароль учетной записи администратора RabbitMQ:

  1. Измените конфигурацию роли (см. раздел 29.2) RMQ Message Bus:
     ```
     RMQAdminPassword: <Новый пароль>
     ```
  2. Перезапустите Docker-контейнер роли RMQ Message Bus:
     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol SIEM>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
     docker-compose down
     docker-compose up -d
     ```

Смена пароля УЗ администратора RabbitMQ, если MP 10 Core и MP SIEM Server установлены на разные серверы

Если компоненты MP 10 Core и MP SIEM Server установлены на разные серверы, каждый компонент использует свой брокер RabbitMQ, поэтому пароль учетной записи администратора нужно изменить для обоих компонентов.

- Чтобы изменить пароль учетной записи администратора RabbitMQ MP 10 Core:

  1. Измените конфигурацию роли (см. раздел 29.2) RMQ Message Bus, установленной на сервере MP 10 Core:
     ```
     RMQAdminPassword: <Новый пароль>
     ```
  2. Перезапустите Docker-контейнер роли RMQ Message Bus:
     ```
     cd /var/lib/deployed-roles/<Идентификатор приложения MaxPatrol SIEM>/<Название экземпляра роли RMQ Message Bus>/images/messagebus-rabbitmq
     docker-compose down
     docker-compose up -d
     ```

- Чтобы изменить пароль учетной записи администратора RabbitMQ MP SIEM Server:

  1. Измените конфигурацию роли (см. раздел 29.2) RMQ Message Bus, установленной на сервере MP SIEM Server:

     ```
     RMQAdminPassword: <Новый пароль>
     ```

  2. Перезапустите Docker-контейнер роли RMQ Message Bus:

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

27. Настройка журналирования работы MaxPatrol SIEM

В разделе приведены инструкции по настройке журналирования работы компонентов системы.

В этом разделе

Настройка журналирования работы компонента MP 10 Core на Linux (см. раздел 27.1)

Настройка журналирования работы компонента MP SIEM Server (см. раздел 27.2)

Настройка журналирования работы компонента MP SIEM Events Storage (см. раздел 27.3)

Настройка журналирования работы компонента MP 10 Collector (см. раздел 27.4)

Настройка журналирования работы LogSpace (см. раздел 27.5)

27.1. 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.

27.2. 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:

     ```
     docker restart $(docker ps | awk '/<Название службы>.siemserver/ {print $NF}')
     ```

  Журналирование настроено.

27.3. 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.

27.4. Настройка журналирования работы компонента MP 10 Collector

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

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

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

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

- Чтобы настроить журналирование:

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

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

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

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

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

  3. Перезапустите службу Core Agent.

  Журналирование настроено.

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

27.5. Настройка журналирования работы LogSpace

- Чтобы настроить журналирование LogSpace:

  1. На сервере MP SIEM Events Storage в каталоге `/etc/logspaced/config.d` создайте файл `loglevel.xml`.
  2. Добавьте в файл строки:

     ```
     <logspace>
         <logger>
             <level><Уровень журналирования></level>
         </logger>
     ```

```
</logspace>
```

Примечание. Параметр `level` может принимать значения `fatal`, `critical`, `error`, `warning`, `notice`, `information`, `debug` или `trace`.

Например:

```
<logspace>
    <logger>
        <level>debug</level>
    </logger>
</logspace>
```

3. Выполните команды:

```
systemctl stop logspaced
systemctl start logspaced
```

28. Настройка обогащения событий данными геолокации

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

Примечание. База MaxMind GeoIP обновляется автоматически с глобального сервера обновлений Positive Technologies.

- Чтобы настроить обогащение событий данными геолокации из базы MaxMind GeoIP:

  1. Скопируйте файлы базы данных MaxMind GeoIP на сервер MP SIEM Server.
  2. В главном меню MaxPatrol SIEM в разделе **Система** выберите пункт **Управление системой**.

     Откроется страница **Управление системой**.
  3. В панели **Компоненты** выберите пункт **Конвейеры**.

     В рабочей области страницы отобразится таблица со списком конвейеров обработки событий.
  4. Выберите конвейер и в панели инструментов нажмите **Редактировать**.

     Откроется страница **Параметры конвейера**.
  5. Включите обогащение событий данными GeoIP.
  6. Если требуется, измените параметры обогащения событий данными геолокации.
  7. Нажмите **Сохранить**.

  Обогащение событий данными геолокации настроено.

Вы можете настроить обогащение событий данными геолокации из пользовательской базы данных.

Примечание. Для пользовательских баз данных обновление возможно только вручную.

- Чтобы сменить базу данных MaxMind GeoIP на пользовательскую:

  1. Добавьте файлы пользовательской базы данных в каталог на сервере MP SIEM Server, указанный в конфигурационном файле `/opt/siem/etc/siem.conf` в параметре `enricher` → `geo_ip` → `db_path`.

     Примечание. Файлы пользовательской базы данных должны иметь имена `GeoLite2-ASN.mmdb` и `GeoLite2-City.mmdb` и соответствовать формату MMDB.
  2. Для отключения автоматического обновления базы данных в конфигурационном файле `/opt/siem/etc/siem.conf` в секции `enricher` удалите параметр `geoip_db_cs`.

3. Сохраните изменения и закройте файл.
4. Выполните команду:

```
docker restart $(docker ps | awk '/processor.siemserver/ {print $NF}')
```

Таблица 8. Параметры обогащения событий данными геолокации

Параметр	Описание
dst.geo.asn	Номер автономной системы (ASN) узла назначения
dst.geo.city	Город узла назначения
dst.geo.country	Страна узла назначения
dst.geo.org	Организация, которой принадлежит узел назначения
src.geo.asn	Номер автономной системы (ASN) узла-источника
src.geo.city	Город узла-источника
src.geo.country	Страна узла-источника
src.geo.org	Организация, которой принадлежит узел-источник

29. 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.

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

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

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

В этом разделе

Просмотр конфигурации роли (см. раздел 29.1)

Изменение конфигурации роли (см. раздел 29.2)

Управление изменением конфигурации ролей с помощью манифеста (см. раздел 29.3)

Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch (см. раздел 29.4)

Изменение степени сжатия данных в Elasticsearch (см. раздел 29.5)

Регистрация событий при нарушении и восстановлении параметров источников (см. раздел 29.6)

Включение регистрозависимого поиска по схеме полей событий (см. раздел 29.7)

Настройка прокси-сервера для онлайн-активации PT MC (см. раздел 29.8)

Включение AI-поиска по запросам (см. раздел 29.9)

Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol SIEM (см. раздел 29.10)

Изменение времени устаревания активов (см. раздел 29.11)

Отключение правил Declarative Detect (см. раздел 29.12)

Изменение времени хранения индексов Elasticsearch в горячей стадии (см. раздел 29.13)

29.1. Просмотр конфигурации роли

- Чтобы просмотреть конфигурацию роли:

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

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

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

29.2. Изменение конфигурации роли

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

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

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

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

     Откроется страница со списком параметров (см. приложение Б).
  7. Измените значения параметров.

8. Нажмите кнопку **OK**.
9. Нажмите **Submit**.

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

Конфигурация роли изменена.

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

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

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

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

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

   Начнется изменение конфигурации роли. По его завершении появится сообщение `Deployment configuration successfully applied`.
7. Нажмите кнопку **OK**.
8. Выполните команду:
   ```
   deployer instance reconfigure -diff -silent
   ```

Конфигурация роли изменена.

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

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

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

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

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

См. также

Управление системой с помощью утилиты deployer (см. раздел 37.42.13)

29.3. Управление изменением конфигурации ролей с помощью манифеста

Для оптимизации работы вы можете выбрать необходимые роли и внести изменения в их конфигурацию одновременно. Для этого необходимо создать манифест (см. раздел 29.3.2) — файл формата YAML, который задает параметры изменения конфигурации.

В этом разделе

Изменение конфигурации ролей с помощью манифеста (см. раздел 29.3.1)

Создание манифеста для обновления компонентов или изменения конфигурации ролей (см. раздел 29.3.2)

29.3.1. Изменение конфигурации ролей с помощью манифеста

- Чтобы изменить конфигурацию ролей с помощью манифеста:

  1. Обновите роль Deployer.
  2. Создайте манифест (см. раздел 29.3.2).
  3. Если требуется, добавьте параметры в файл манифеста или измените значения существующих.

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

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

В консоли появится информация о результатах изменения конфигурации:

— Если конфигурация экземпляра роли была изменена успешно, рядом с его идентификатором будет добавлен комментарий `Instance installation is successful`.

— Если конфигурация экземпляра роли не была изменена, рядом с его идентификатором будет добавлен комментарий с причиной неудачи.

— Если конфигурация экземпляра роли не была изменена из-за отсутствия соединения с модулем Salt Minion, появится сообщение об ошибке `There are no SCM hosts available`.

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

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

29.3.2. Создание манифеста для обновления компонентов или изменения конфигурации ролей

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

► Чтобы создать манифест,

на сервере с установленной ролью Deployer запустите сценарий:

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

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

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

Таблица 9. Аргументы сценария

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

Аргумент	Описание	Пример использования
`Type`	Добавление в манифест информации о типе экземпляра роли. Для добавления информации обо всех ролях после аргумента необходимо добавить `"*"`	`deployer instance export -Type "*"`
`ExcludeType`	Исключение из манифеста информации о типе экземпляра роли. Чтобы исключить информацию о нескольких типах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -ExcludeType "rmqmessagebus,core,siemserver,agentlinux"`
`ExcludeId`	Исключение из манифеста информации об идентификаторе экземпляра роли. Чтобы исключить информацию о нескольких идентификаторах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -ExcludeId "rmq-1,kb-1"`
`IncludeType`	Добавление в манифест информации о типе экземпляра роли. Чтобы добавить информацию о нескольких типах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux"`
`IncludeId`	Добавление в манифест информации о идентификаторе экземпляра роли. Чтобы добавить информацию о нескольких идентификаторах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeId "rmq-1,kb-1"`
`IncludeParam`	Добавление в манифест информации о параметрах экземпляра роли. Чтобы добавить информацию о нескольких параметрах, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParam "RmqPassword"`
`IncludeParamValue`	Добавление в манифест определенных значений параметров экземпляра роли. Чтобы добавить несколько значений, необходимо указать их через запятую без пробелов	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -IncludeParamValue "P@ssw0rd"`

Аргумент	Описание	Пример использования
`NotExportParams`	Исключение из манифеста параметров экземпляров ролей. Параметры, к которым применены аргументы `IncludeParam` или `-IncludeParamValue`, не будут исключены из манифеста	`deployer instance export -AppId "*" -IncludeType "rmqmessagebus,core,siemserver,agentlinux" -NotExportParams "RmqPassword"`
`ExportVersion`	Сохранение текущих версий экземпляров ролей и компонентов. Аргумент применяется, если необходимо изменить конфигурацию ролей без обновления их версий	`deployer instance export -AppId "*" -ExportVersion`

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

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

Добавление в манифест роли Grafana

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

- Чтобы добавить в манифест роль Grafana:

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

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

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

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

Примечание. Список параметров роли вы можете посмотреть в разделе «Параметры конфигурации компонентов MaxPatrol SIEM на Linux (см. приложение Б)».

4. Сохраните изменения и закройте файл.

Примеры сценариев создания манифеста

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

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

  Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

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

— `deployer instance export -Type "agentlinux"`

  Манифест будет включать информацию обо всех экземплярах роли Collector.

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

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

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

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

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

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

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

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

29.4. Изменение объема оперативной памяти, выделяемого узлам кластера Elasticsearch

► Чтобы изменить объем оперативной памяти:

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

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

   Откроется страница со списком параметров (см. приложение Б).
7. Измените значение параметра **ClusterConfigurationProfile** на **Manual**.
8. В качестве значений параметров **MasterNodeHeapSize**, **ClientNodeHeapSize** и **DataNodeHeapSize** введите объем оперативной памяти, выделяемый для главного узла, клиентского узла и узла данных соответственно.
9. Нажмите кнопку **OK**.
10. Нажмите **Submit**.

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

Объем оперативной памяти изменен.

29.5. 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 распакуйте архив `pt_siemserver-linux_<Номер версии>.tar.gz`:
   ```
   tar -xf pt_siemserver-linux_<Номер версии>.tar.gz
   ```
2. Запустите сценарий:
   ```
   pt_siemserver-linux_<Номер версии>/install.sh
   ```
3. В открывшемся окне нажмите кнопку **Yes**.
4. Выберите вариант с идентификатором приложения роли.
5. Выберите вариант с идентификатором экземпляра роли.

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

   Откроется страница со списком параметров (см. приложение Б).
7. Измените 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**.
8. Нажмите кнопку **OK**.
9. Нажмите **Submit**.

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

Алгоритм сжатия данных выбран и будет применен к новым индексам.

29.6. 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 распакуйте архив `pt_core_<Номер версии>.tar.gz`:
     ```
     tar -xf pt_core_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_core_<Номер версии>/install.sh
     ```
  3. В открывшемся окне нажмите кнопку **Yes**.
  4. Выберите вариант с идентификатором приложения роли.
  5. Выберите вариант с идентификатором экземпляра роли.

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

     Откроется страница со списком параметров (см. приложение Б).
  7. Установите флажок **SendAlertsToSiem**.
  8. Нажмите кнопку **OK**.
  9. Нажмите **Submit**.

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

  Регистрация событий при нарушении и восстановлении параметров источников включена.

29.7. Включение регистрозависимого поиска по схеме полей событий

По умолчанию поиск по схеме полей событий — регистронезависимый. Например, если указать в PDQL-запросе для фильтрации событий значение `mgmt-VDOM`, в результат попадут и события со значением `mgmt-vdom`.

- Чтобы включить регистрозависимый поиск:

  1. Измените конфигурацию (см. раздел 29.2) роли Core, указав для параметра `EventsCaseSensitiveSearch` значение `True`.
  2. Измените конфигурацию (см. раздел 29.2) роли SIEM Server, указав для параметра `EventsCaseSensitiveSearch` значение `True`.

  Регистрозависимый поиск включен. Тип поиска применится только для тех событий, которые поступят после его изменения.

  Примечание. Если вы используете хранилище данных Elasticsearch, тип поиска изменится в течение суток после изменения параметров.

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

- Чтобы настроить прокси-сервер,

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

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

29.9. Включение AI-поиска по запросам

- Чтобы включить AI-поиск по PDQL-запросам,

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

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

29.10. Включение профиля безопасности в Docker-контейнерах ролей компонентов MaxPatrol SIEM

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

► Чтобы включить профиль безопасности в Docker-контейнерах ролей:

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

29.11. Изменение времени устаревания активов

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

Значение по умолчанию — 90 дней.

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

Таблица 10. Рекомендации по выбору значения параметра DefaultAssetTtl

Частота или условия сканирования	**Рекомендуемое время устаревания активов**	**Комментарий**
Раз в неделю или чаще	30–45 дней	Позволяет быстро удалять неактуальные активы и снижает объем устаревших данных
Раз в месяц	90 дней (по умолчанию)	Обеспечивает баланс между актуальностью данных и стабильностью учета активов
Раз в несколько месяцев	180–365 дней	Предотвращает преждевременное скрытие активов при редком получении данных
Повышенные требования к хранению (например, банки)	365 дней и более	Значение определяется внутренними регламентами и требованиями комплаенса

Практические замечания по настройке времени устаревания активов:

— Слишком большое значение (например, 90 дней и более при частом сканировании) может приводить к накоплению устаревших и дублирующихся активов, что усложняет работу с выборками и анализом данных.

— Уменьшение значения помогает снизить количество нерелевантных данных, особенно при интеграции с внешними источниками (например, антивирусами).

— Изменение параметра вступает в силу только после повторного обнаружения актива (например, при следующем сканировании).

— Удаление активов носит логический характер: они перестают отображаться в интерфейсе, но их данные сохраняются в базе и не освобождают физическое место хранения.

Примечание. Для освобождения дискового пространства необходимо настроить ротацию данных (см. раздел 13) сервиса Temporal Read Model.

► Чтобы изменить время устаревания активов,

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

29.12. Отключение правил Declarative Detect

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

Выборочное отключение правил Declarative Detect

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

► Чтобы изменить список отключенных правил Declarative Detect,

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

Отключение всех правил Declarative Detect

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

Внимание! Отключение Declarative Detect может привести к потере данных.

► Чтобы отключить все правила:

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

4. Удалите Docker-контейнер:
   ```
   docker rm -f $(docker ps -aqf name=<Имя Docker-контейнера>)
   ```
5. Перезапустите Docker-контейнер службы Assets.Processing:
   ```
   cd /var/lib/deployed-roles/<Название приложения>/<Название экземпляра роли>/images/
   core.assets.processing.extended/
   docker-compose up -d
   ```

29.13. Изменение времени хранения индексов Elasticsearch в горячей стадии

В сверхнагруженной конфигурации индексы Elasticsearch сначала хранятся в горячей стадии на твердотельных накопителях, а затем в теплой стадии на жестких дисках. Время хранения индексов определяется автоматически. Вы можете изменить время хранения индексов в горячей стадии с помощью параметра `ElasticsearchManagedStorageWarmTime` роли SIEM Server. Значение параметра задается в виде строки с указанием единицы времени. Значение параметра по умолчанию — `-1` (время хранения индексов в горячей стадии не зависит от параметра).

Вы можете проверить установленное значение параметра с помощью команды `deployer params get - <Идентификатор экземпляра роли SIEM Server>`. На экране отобразятся параметры роли с текущими значениями.

- Чтобы изменить время хранения индексов в горячей стадии:

  1. Выполните команду:
     ```
     deployer instance setparam -Id <Идентификатор экземпляра роли SIEM Server>
     ElasticsearchManagedStorageWarmTime=<Необходимое время хранения индексов в горячей стадии>
     ```
     Например:
     ```
     deployer instance setparam -Id siemserver-1 ElasticsearchManagedStorageWarmTime=5d
     ```
  2. Нажмите **Yes**.
  3. Выполните команду для изменения конфигурации роли SIEM Server:
     ```
     deployer instance reconfigure -type <Идентификатор типа роли SIEM Server>
     ```

  Внимание! Новое значение параметра будет применено только к индексам, созданным после его изменения. Для существующих индексов сохранится прежнее значение.

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

30. 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 `docker restart $(docker ps | awk '/normalizer.siemserver/ {print $NF}')`.

Отправка ненормализованных событий отключена.

31. Смена алгоритма контроля потока событий

Начиная с версии 27.3 в MaxPatrol SIEM реализован новый алгоритм работы механизма flowcontrol, контролирующего поток поступающих событий. Он используется по умолчанию, позволяет избежать резких перепадов нагрузки на систему и более гибко подстраивается под входящий поток событий. При этом сохраняется возможность использования старого алгоритма.

- Чтобы выбрать алгоритм контроля потока событий:

  1. На сервере MP SIEM Server откройте на редактирование конфигурационный файл `/opt/siem/etc/siem.conf`.
  2. Если требуется использовать старую версию алгоритма, в блоке параметров `monitoring` → `flowcontrol` в качестве значения параметра `version` укажите `1`.
  3. Если требуется использовать новую версию алгоритма, в блоке параметров `monitoring` → `flowcontrol` в качестве значения параметра `version` укажите `2`.
  4. Сохраните изменения в файле `siem.conf`.
  5. Перезапустите службу SIEM Server health monitor:

     ```
     docker restart $(docker ps | awk '/healthmon.siemserver/ {print $NF}')
     ```

32. Удаление экземпляра роли Collector

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

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

- Чтобы удалить экземпляр роли Collector:

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

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

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

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

33. Настройка очереди выпуска отчетов

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

- Чтобы настроить очередь выпуска отчетов:

  1. На сервере с установленной ролью Deployer распакуйте архив `pt_core_<Номер версии>.tar.gz` из комплекта поставки:
     ```
     tar xzf pt_core_<Номер версии>.tar.gz
     ```
  2. Запустите сценарий:
     ```
     pt_core_<Номер версии>/install.sh
     ```
  3. Выберите вариант с идентификатором приложения роли.
  4. Выберите вариант с идентификатором экземпляра роли.
  5. Выберите вариант **Advanced configuration**.
  6. В качестве значения параметра `PrintingQueueJobsLimit` укажите максимальное количество одновременно выпускаемых отчетов.

     Примечание. Чем больше это количество, тем выше будет нагрузка на аппаратные ресурсы сервера MaxPatrol SIEM.
  7. Нажмите **OK**.
  8. Нажмите **Submit**.

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

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

34. Пользовательские поля в модели актива

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

После добавления полей и ввода их значений пользователи системы смогут:

— просматривать значения добавленных полей в карточке и миникарточке актива;

— вводить поисковые запросы с учетом добавленных полей;

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

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

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

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

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

В этом разделе

Добавление пользовательских полей в модель актива (см. раздел 34.1)

Добавление описания пользовательских полей (см. раздел 34.2)

Изменение имен пользовательских полей (см. раздел 34.3)

Удаление пользовательских полей из модели актива (см. раздел 34.4)

34.1. Добавление пользовательских полей в модель актива

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

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

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

Первичное добавление пользовательских полей в модель актива

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

- Чтобы впервые добавить пользовательские поля в модель актива:

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

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

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

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

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

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

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

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

   Например:

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

6. Если требуется, добавьте описание пользовательских полей (см. раздел 34.2).

7. Перезапустите службы.

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

Повторное добавление пользовательских полей в модель актива

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

- Чтобы повторно добавить пользовательские поля в модель актива:

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

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

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

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

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

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

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

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

Например:

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

5. Если требуется, добавьте описание пользовательских полей (см. раздел 34.2).
6. Перезапустите службы.

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

Добавление пользовательских полей в модель актива после обновления системы

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

► Чтобы добавить поля в модель актива после обновления системы:

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

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

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

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

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

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

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

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

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

   Например:

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

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

5. Если требуется, добавьте описание пользовательских полей (см. раздел 34.2).
6. Перезапустите службы.

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

См. также

Добавление описания пользовательских полей (см. раздел 34.2)

34.2. Добавление описания пользовательских полей

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

► Чтобы добавить описание пользовательских полей:

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

Например, для активов на Windows необходимо указать:

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

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

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

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

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

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

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

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

   Например:

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

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

Описание пользовательских полей добавлено.

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

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

Имена пользовательских полей изменены.

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

Пользовательские поля удалены из модели актива.

35. 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

Создание инфраструктуры (см. раздел 35.1)

Изменение названия инфраструктуры (см. раздел 35.2)

Удаление инфраструктуры (см. раздел 35.3)

35.1. 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.

35.2. 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.

35.3. 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.

36. Изменение проверок по чек-листу

- Чтобы изменить параметры проверок:

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

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

См. также

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

37. Диагностика и решение проблем

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:

— синий — информирует о каком-либо событии, не связанном с ошибками в работе системы (например, об остановке служб);

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

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

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

В этом разделе

Обмен данными между компонентами системы (см. раздел 37.1)

Мониторинг состояния RabbitMQ и Elasticsearch (см. раздел 37.2)

Ошибка «Объем очередей SIEM Server Messaging Service на узле <FQDN сервера> достиг критического порога» (см. раздел 37.3)

Ошибка «Компонент SIEM Events Storage на узле <FQDN сервера> отвечает с задержками либо недоступен» (см. раздел 37.4)

Ошибка «Объем свободного места на диске, выделенном для Core Messaging Service, достиг критического порога» (см. раздел 37.5)

Ошибка «Объем свободного места на диске, выделенном для SIEM Messaging Service, достиг критического порога» (см. раздел 37.6)

Ошибка «Объем свободного места на диске, выделенном для SIEM Events Storage, достиг критического порога» (см. раздел 37.7)

Ошибка «Компонент Core Messaging Service недоступен. Health Monitoring Service не может получать сообщения от других систем» (см. раздел 37.8)

Предупреждение «Время выполнения запросов у SIEM Events Storage на узле <FQDN сервера> достигло критического порога» (см. раздел 37.9)

Система не получает данные от задачи (см. раздел 37.10)

Отсутствуют события от источников (см. раздел 37.11)

Задача аудита не собирает сведения об активах (см. раздел 37.12)

Не приходят уведомления, отправляемые по электронной почте (см. раздел 37.13)

Ошибка «Sdk пакет <Номер версии> поврежден. Необходимо восстановление» (см. раздел 37.14)

Не удается импортировать отчет из MaxPatrol 8 (см. раздел 37.15)

Настройка компонентов после изменения IP-адресов или FQDN их серверов (см. раздел 37.16)

Подсеть Docker-контейнера MaxPatrol SIEM совпадает с одной из подсетей предприятия (см. раздел 37.17)

Ошибка при установке, переконфигурации или обновлении компонентов в высоконагруженных системах (см. раздел 37.18)

Задача на сбор данных с коллектором на Windows завершается с ошибкой (см. раздел 37.19)

Ошибка «Глубина поиска по событиям сокращена до 7 дней» (см. раздел 37.20)

Ошибка «Запуск задач на сбор событий отключен» (см. раздел 37.21)

Ошибка «Корреляция событий отключена» (см. раздел 37.22)

Ошибка «Доля свободного дискового пространства, выделенного для табличных списков в <Название компонента> на узле <Название узла>, достигла 5%» (см. раздел 37.23)

Большое количество запросов к DNS-серверу от Docker-контейнеров сервера MP 10 Core (см. раздел 37.24)

Установка модуля Salt Minion завершается с ошибкой (см. раздел 37.25)

Не отображаются события в веб-интерфейсе после установки или обновления MaxPatrol SIEM (см. раздел 37.26)

Ошибка при загрузке шаблона для экспорта записей в формате XLSX (см. раздел 37.27)

Ошибка при проверке подключения (см. раздел 37.28)

Ошибка при обновлении роли Deployer (см. раздел 37.29)

Ошибка при создании резервной копии данных LogSpace после обновления Astra Linux (см. раздел 37.30)

Слишком много открытых файлов при создании резервной копии или восстановлении данных LogSpace (см. раздел 37.31)

Настройка LimitMEMLOCK для исправления ошибки ENOMEM при использовании LogSpace (см. раздел 37.32)

Ошибки, связанные с конфигурацией LogSpace (см. раздел 37.33)

Ошибки взаимодействия служб MaxPatrol SIEM с LogSpace (см. раздел 37.34)

Защита LogSpace от принудительной остановки службой OOM Killer (см. раздел 37.35)

На коллекторах накапливается и не разбирается очередь событий (см. раздел 37.36)

Ошибка при обновлении роли, связанная с именем Docker-контейнера (см. раздел 37.37)

Ошибка «There is no application package with following properties: WithHidden True Id <Идентификатор пакета приложения>» при обновлении MaxPatrol SIEM (см. раздел 37.38)

Ошибки, связанные с сертификатом MP 10 Collector на Microsoft Windows (см. раздел 37.39)

Ошибка «The repository <Ссылка на репозиторий> does not have a Release file» (см. раздел 37.40)

Диагностика и решение проблем при работе с Elasticsearch (см. раздел 37.41)

Справочная информация (см. раздел 37.42)

37.1. 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 служба-отправитель (producer) создает точку обмена сообщениями (exchange), служба-получатель (consumer) создает очередь сообщений (queue) и связывает очередь с точкой обмена с помощью правил (binding) с указанием ключа маршрутизации (routing key). Далее службы поддерживают постоянное соединение с брокером.
2. Получив сообщение, брокер уведомляет об этом службу-отправителя и направляет сообщение в точку обмена. Правила точки обмена определяют, в какую очередь направить сообщение, используя для этого ключ маршрутизации, содержащийся в сообщении.
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.

Для распределения нагрузки и повышения отказоустойчивости в RabbitMQ используется механизм Shovel. Он обеспечивает перенос сообщений из одной очереди в другую, в том числе — между различными узлами RabbitMQ в случае распределенной системы.

RabbitMQ обеспечивает только техническую доставку сообщений. Корректность формата и содержимого сообщений и логика маршрутизации зависят от служб компонентов MaxPatrol 10.

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 RabbitMQ. 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.

В этом разделе

Диагностика работы RabbitMQ (см. раздел 37.1.1)

Вход в веб-интерфейс RabbitMQ (см. раздел 37.1.2)

Мониторинг потока событий в RabbitMQ (см. раздел 37.1.3)

Очередь storageq не уменьшается (см. раздел 37.1.4)

Очередь siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq не уменьшается (см. раздел 37.1.5)

Очередь storageq растет и начинает уменьшаться только после появления ошибки (см. раздел 37.1.6)

Очередь siem.receiver.incoming, normalizeq, aggregatorq, event.resolve, enricherq, routerq, correlatorq или notifierq растет и начинает уменьшаться только после появления ошибки (см. раздел 37.1.7)

Не удается запустить контейнер RMQ (см. раздел 37.1.8)

Ошибка «Closing AMQP connection, missed heartbeats from client, timeout» (см. раздел 37.1.9)

Ошибка «Shovel <Имя> failed to connect (URI: <Адрес>): closed» (см. раздел 37.1.10)

Ошибка «Unknown CA, error handshake» (см. раздел 37.1.11)

Ошибка «No route to» (см. раздел 37.1.12)

37.1.1. Диагностика работы RabbitMQ

Проверка контейнеров

Вы можете проверить состояние контейнеров RabbitMQ с помощью команды `docker ps -af name=messagebus-rabbitmq --format "{{.State}} {{.Names}}"`. В результате выполнения команды отобразится статус для всех контейнеров, в названии которых содержится `messagebus-rabbitmq`.

Проверка портов

Вы можете проверить состояние стандартных для RabbitMQ портов с помощью команды `netstat -tlnp | grep -E "(25672|15672|5672|5671)"`. Успешный результат выполнения команды будет содержать список портов в статусе `LISTEN`.

Например:

```
tcp        0      0 0.0.0.0:25672           0.0.0.0:*               LISTEN 26131/
docker-proxy
tcp        0      0 0.0.0.0:15672           0.0.0.0:*               LISTEN      26166
/docker-proxy
tcp        0      0 0.0.0.0:5672            0.0.0.0:*               LISTEN      26188
/docker-proxy
tcp        0      0 0.0.0.0:5671            0.0.0.0:*               LISTEN      26227
/docker-proxy
```

Проверка сообщений журнала

Вы можете проверить последние 20 сообщений в журнале с помощью команды `docker logs $(docker ps -aqf name=messagebus-rabbitmq) -n20`. Успешный результат выполнения команды не должен содержать ошибок и сообщений о циклических перезапусках контейнера.

Например:

```
Adding vhost "mpx" ...
*** Vhost 'mpx' created and permited to users 'Administrator', 'core', 'siem',
'agent'
Adding vhost "siem" ...
*** Vhost 'siem' created and permited to users 'Administrator', 'core', 'siem',
'agent'
*** Manage users script finished with no errors
```

Утилита диагностики rabbitmq-diagnostics

Утилита rabbitmq-diagnostics является встроенным инструментом командной строки для мониторинга и диагностики брокера сообщений RabbitMQ. Она предоставляет детальную информацию о состоянии системы, потреблении ресурсов и работе кластера. Подробное описание утилиты см. на сайте rabbitmq.com/.

Для диагностики работы кластера используются следующие аргументы:

— `rabbitmq-diagnostics cluster_status` — используется для отображения состава и состояния кластера.

— `rabbitmq-diagnostics observer` — используется для отображения системных показателей потребления ресурсов.

Команды с использованием этих аргументов необходимо запускать в Docker-контейнере RabbitMQ:

— `docker exec -it $(docker ps -aqf name=messagebus-rabbitmq) rabbitmq-diagnostics cluster_status`

— `docker exec -it $(docker ps -aqf name=messagebus-rabbitmq) rabbitmq-diagnostics observer`

37.1.2. Вход в веб-интерфейс RabbitMQ

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

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

► Чтобы войти в веб-интерфейс RabbitMQ:

1. В адресной строке браузера введите:
   `<Протокол HTTP или HTTPS>://<IP-адрес или FQDN сервера RabbitMQ>:<Порт>`

   Например:
   `https://example.org:15671`

2. Введите логин и пароль.

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

3. Нажмите кнопку **Login**.

   Отобразится страница **Overview**.

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

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

37.1.3. 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 веб-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. В столбце **DiskSpace** отображается свободное место на диске в разделе, где находится база данных Mnesia и хранилище сообщений. В раскрывающемся блоке **Export definitions** по кнопке **Download broker definitions** вы можете скачать файл, содержащий все пользовательские определения роли.

Примечание. RabbitMQ прекращает прием новых сообщений при превышении лимитов, указанных в нижней части столбцов таблицы блока **Nodes**. В этом случае поле таблицы изменит цвет на красный.

Exchanges. На странице отображается таблица точек обмена. Таблица должна содержать точки обмена для приема сообщений, в том числе для приема сообщений от агентов — **pt.mpx.agent.v2**. 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.

— **Admin**. На сервере с установленной ролью SIEM Server должны быть настроены механизмы Shovels. Их статус и статистика работы отображаются на вкладке **Shovel status**. Для обеспечения бесперебойной работы системы необходимо, чтобы все записи в таблице имели статус **running**.

37.1.4. 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 37.42.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. раздел 37.41.2).
  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 37.42.7) службы SIEM Server storage.
  5. Перезапустите службу SIEM Server storage.

Если проблема не решилась, 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 37.42.7) службы SIEM Server storage;
- файлы журналов Elasticsearch, RabbitMQ и службы SIEM Server storage.

37.1.5. Очередь 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 37.42.3) MP SIEM Server. Если служба остановлена, запустите ее.

Если проблема не решилась, 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 37.42.3) MP SIEM Server;

— файлы журналов MP SIEM Server и RabbitMQ;

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

37.1.6. 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 37.42.1) на сервере MP SIEM Events Storage равен нулю.
3. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. раздел 37.42.6.3.3). Если таких индексов более 900, необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 21).
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 37.42.2). 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 проблема не решилась, 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 37.42.2) сервера MP SIEM Events Storage;

— результат запроса о состоянии индексов (см. раздел 37.42.6.3.3);

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

37.1.7. Очередь 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 37.42.2). Если такой процесс присутствует, сообщите о нем в службу технической поддержки Positive Technologies, приложив снимки экрана.

Если проблема не решилась, 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 37.42.2) на центральный процессор, ОЗУ и жесткие диски сервера MP SIEM Server.

37.1.8. Не удается запустить контейнер RMQ

Возможные причины

Возможными причинами проблемы является повреждение базы данных Mnesia, которая содержит информацию о конфигурации (например, в случае аварийного выключения питания контейнера или ручного удаления внутренних файлов базы данных).

Решение

Необходимо очистить данные RabbitMQ, предварительно создав их резервную копию.

> **Внимание!** В результате очистки будут удалены все пользовательские модификации определений (например, созданные вручную сущности queue, exchange или shovel), а также правила маршрутизации. Вы можете сохранить данные (см. раздел 19.5) в файл `rmq_definitions.json`, а затем восстановить их (см. раздел 20.4), или переустановить соответствующие роли.

► Чтобы решить проблему,

выполните следующие команды:

```
rmq_data_path=$(find /var/lib/deployed-roles/ -path "*/rmqmessagebus*/data" -print -quit)
echo "RMQ data path: ${rmq_data_path}"
[ ! -z "${rmq_data_path}" ] && docker stop $(docker ps -aqf name=messagebus-rabbitmq)
[ ! -z "${rmq_data_path}" ] && tar -czf ~/rmq_data_backup.tar.gz -C ${rmq_data_path} .
[ ! -z "${rmq_data_path}" ] && rm -rf ${rmq_data_path}/rabbitmq/*
[ ! -z "${rmq_data_path}" ] && docker start $(docker ps -aqf name=messagebus-rabbitmq)
```

В результате произойдет полная очистка и сброс состояния RabbitMQ.

37.1.9. Ошибка «Closing AMQP connection, missed heartbeats from client, timeout»

Проблема

RabbitMQ разрывает сетевое соединение, потому что в течение заданного таймаута (по умолчанию 10 секунд) не получил от клиента подтверждения активности.

Возможные причины

Возможными причинами проблемы могут быть перезагрузка сервера клиента или ошибки сетевого подключения.

Решение

Для решения проблемы рекомендуется проверить журнал на стороне клиента, доступность сетевого подключения, а также нагрузку на RabbitMQ и клиента.

37.1.10. Ошибка «Shovel <Имя> failed to connect (URI: <Адрес>): closed»

Проблема

Недоступно соединение между брокерами RabbitMQ для перемещения сообщений из одной очереди в другую.

Возможные причины

Возможными причинами проблемы могут быть перезагрузка удаленного сервиса, ошибки сетевого подключения или ошибки проверки SSL-сертификатов.

Решение

Для решения проблемы рекомендуется проверить состояние удаленного брокера RabbitMQ и сетевого подключения, а также валидность SSL-сертификатов.

37.1.11. Ошибка «Unknown CA, error handshake»

Возможные причины

Возможными причинами проблемы являются неправильная конфигурация SSL-сертификатов на стороне брокера RabbitMQ или отсутствие доверенных корневых сертификатов на стороне клиентских подключений.

Решение

Для решения проблемы рекомендуется добавить корневой сертификат в доверенное хранилище компонента, где возникает ошибка.

37.1.12. Ошибка «No route to»

Проблема

RabbitMQ не может доставить сообщение в очередь.

Возможные причины

Возможной причиной проблемы является отсутствие конечного пункта для указанного ключа маршрутизации.

Решение

Для решения проблемы рекомендуется переустановить соответствующую роль или обратиться в службу технической поддержки Positive Technologies.

37.2. 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 содержит модуль проверки и модуль 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.

37.3. 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 37.4).
  2. Войдите в RabbitMQ (см. раздел 37.1.2) и проверьте состояние очередей (см. раздел 37.1.3):

     - 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».

37.4. 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 37.42.4) для MP 10 Core.
3. На сервере MP SIEM Events Storage проверьте статус служб (см. раздел 37.42.3). Если служба Elasticsearch не запущена, перейдите к решению этой проблемы (см. раздел 37.41.2).
4. Проверьте состояние индексов Elasticsearch (см. раздел 37.42.6.3.3). Если в Elasticsearch есть индексы в состоянии red, перейдите к решению этой проблемы (см. раздел 37.41.1).

Если проблема не решилась, 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 37.42.2) серверов MP SIEM Server и MP SIEM Events Storage;

— результат запроса о состоянии индексов (см. раздел 37.42.6.3.3).

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

— файл журнала службы Core Health Monitoring;

— снимок экрана, отображающий свободное место на логическом диске.

37.6. 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 проблема не решилась, 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.

37.7. 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 21.3).
  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 проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— файл журнала службы Core Health Monitoring;

— снимок экрана, отображающий свободное место на логическом диске.

См. также

Удаление индекса без архивации (см. раздел 21.6)

37.8. 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 37.42.3). Если служба остановлена, запустите ее вручную.
  2. Проверьте доступность страницы входа в RabbitMQ (см. раздел 37.1.2). Если страница недоступна, сообщите об этом в службу технической поддержки Positive Technologies, приложив журналы службы RabbitMQ.

37.9. 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 37.42.1) на сервере MP SIEM Events Storage равен нулю.

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

- о нагрузке на файловую систему и запущенных процессах (см. раздел 37.42.2);
- файлы журналов (см. раздел 37.42.8) служб Core Health Monitoring и Elasticsearch;
- файлы журналов (см. раздел 37.42.8) службы SIEM Server storage, собранные в режиме расширенного журналирования, журналы контейнера events с сервера MP 10 Core;
- снимок экрана страницы **Система** → **Мониторинг обработки событий**;
- аппаратные характеристики сервера MP SIEM Events Storage, включая информацию об уровне RAID-массива и параметрах жестких дисков.

37.10. 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 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 37.1.2). 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 37.42.6.3.2). Если Elasticsearch имеет статус «red», перейдите к решению проблемы «Индексы Elasticsearch находятся в состоянии red» (см. раздел 37.41.1).
  9. Проверьте состояние служб (см. раздел 37.42.3) MP SIEM Server. Если служба остановлена, запустите ее вручную.

Если проблема не решилась, 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.

37.11. Отсутствуют события от источников

Возможные причины

Возможными причинами проблемы являются неправильная настройка источника событий или задачи на сбор 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 проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies, приложив следующую информацию:

— предупреждения и ошибки 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 37.42.3) 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**.

37.12. Задача аудита не собирает сведения об активах

Возможные причины

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

Решение

- Чтобы решить проблему:

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

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

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

— название и версию источника;

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

37.13. 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.

37.14. 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\pt_siemsdk-windows_<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 `pt_siemsdk-windows_<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**.

37.15. 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 проблема не решилась, 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.

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

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

> **Внимание!** После указания новых IP-адресов или FQDN серверов в параметрах компонентов необходимо деактивировать PT MC по инструкции (см. раздел 37.42.5).
>
> **Внимание!** Если компоненты MaxPatrol SIEM развернуты на нескольких площадках, перед сменой IP-адресов необходимо разорвать связи между площадками. После смены IP-адресов связи можно восстановить.

Настройка роли Deployer

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

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

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

2. Изменить конфигурацию роли Deployer, указав актуальное значение параметра `HostAddress`.

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

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

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

— `HostAddress`, `KBAddress` и `MCAddress` компонента MP 10 Core;

— `HostAddress`, `MCAddress` и `CoreAddress` компонента Knowledge Base;

— `HostAddress` компонента PT MC;

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

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

Настройка PT RC после изменения адреса MP SIEM Server

Если был изменен IP-адрес или FQDN сервера MP SIEM Server, необходимо указать актуальное значение параметра `SiemServerAddress` компонента PT RC (если установлен).

Настройка MP SIEM Events Storage

Если был изменен IP-адрес или FQDN сервера MP SIEM Events Storage, необходимо изменить конфигурацию роли SIEM Storage (если в качестве хранилища используется Elasticsearch) или конфигурацию роли Event Storage (если в качестве хранилища используется LogSpace), указав актуальные значения параметра `HostAddress`.

См. также

Изменение конфигурации роли (см. раздел 29.2)

37.17. Подсеть Docker-контейнера MaxPatrol SIEM совпадает с одной из подсетей предприятия

Решение

Необходимо изменить подсеть Docker-контейнера MaxPatrol SIEM.

Команды из инструкции необходимо выполнять в интерфейсе терминала Linux.

► Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol SIEM остановите Docker-контейнеры:
   `docker stop $(docker ps -qa)`
2. На всех серверах с установленным MaxPatrol SIEM удалите Docker-контейнеры:
   `docker rm $(docker ps -qa)`
3. На всех серверах с установленным MaxPatrol SIEM удалите действующие параметры сети Docker:
   `docker network prune`
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz`:
   `tar -xf pt_deployer_<Номер версии>.tar.gz`
5. На сервере с установленной ролью Deployer запустите сценарий:
   `pt_deployer_<Номер версии>/install.sh`
6. В открывшемся окне нажмите кнопку **Yes**.
7. Выберите вариант с идентификатором приложения роли.
8. Выберите вариант с идентификатором экземпляра роли.

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

   Откроется страница со списком параметров (см. приложение Б).
10. В качестве значения параметра `CustomDockerAddressPool` укажите подсеть для Docker-контейнеров MaxPatrol SIEM, отличную от подсетей, используемых в вашей организации.

    Внимание! Значение параметра должно содержать адрес подсети с маской /20 или шире (например, /19, /18 или /17) в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16. Например: 10.1.32.0/19 или 172.19.64.0/19.
11. В качестве значения параметра `CustomDockerNetworkSize` введите размер подсетей, которые будут выделяться из диапазона, указанного в параметре `CustomDockerAddressPool`.

    Примечание. Рекомендуется использовать значение, не превышающее 24 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра `CustomDockerAddressPool`, минимум на 4 бита.
12. Нажмите кнопку **OK**.
13. Нажмите **Submit**.

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

15. Если требуется подтвердить изменение конфигурации ролей, параметры которых связаны с изменяемой ролью, нажмите **Confirm**.
16. На сервере с установленной ролью Deployer запустите обновление конфигурации установленных компонентов MaxPatrol SIEM:
    ```
    deployer instance reconfigure '*' -Verbose
    ```

Подсеть Docker-контейнера изменена.

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

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

Изменение подсети Docker-контейнера коллектора

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

Изменение подсети Docker-контейнера при обновлении компонентов

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

- Чтобы изменить подсеть Docker-контейнера:

1. На всех серверах с установленным MaxPatrol SIEM остановите Docker-контейнеры:
   ```
   docker stop $(docker ps -qa)
   ```
2. На всех серверах с установленным MaxPatrol SIEM удалите Docker-контейнеры:
   ```
   docker rm $(docker ps -qa)
   ```
3. На всех серверах с установленным MaxPatrol SIEM удалите действующие параметры сети Docker:
   ```
   docker network prune
   ```
4. На сервере с установленной ролью Deployer распакуйте архив `pt_deployer_<Номер версии>.tar.gz` с новой версией роли:
   ```
   tar -xf pt_deployer_<Номер версии>.tar.gz
   ```
5. Запустите сценарий:
   ```
   pt_deployer_<Номер версии>/install.sh
   ```

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

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

7. Выберите вариант **Advanced configuration**.

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

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

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

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

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

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

11. Нажмите кнопку **OK**.

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

12. Нажмите кнопку **OK**.

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

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

Подсеть Docker-контейнера изменена.

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

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

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

Проблема

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

Возможные причины

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

Решение

Вы можете увеличить тайм-аут выполнения сервисных операций.

- Чтобы изменить тайм-аут:

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

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

Журнал выбранной подзадачи содержит следующую информацию об ошибке:

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

Возможные причины

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

Решение

- Чтобы решить проблему,

  восстановите файл из карантина.

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

37.20. Ошибка «Глубина поиска по событиям сокращена до 7 дней»

Перед возникновением ошибки система может отображать следующие сообщения:

— «В MaxPatrol SIEM показатель **EPS** за последние <Число> дней близок к лимиту (<Текущий EPS> из <Лимит EPS>). Сократите использование ресурсов приложения или увеличьте лицензируемый лимит»;

— «Не удалось получить данные от сервиса лицензионного контроля».

Возможные причины

Возможными причинами проблемы могут быть систематическое превышение лимита EPS, установленного лицензией MaxPatrol SIEM; ошибка в работе сервиса лицензионного контроля.

Решение

Для решения проблемы требуется учетная запись **Администратор** или любая другая учетная запись с привилегией «Управление лицензиями».

► Чтобы решить проблему:

1. В интерфейсе PT MC на странице **Управление лицензиями** проверьте соблюдение лимита EPS, установленного для лицензии. Если он превышен, выполните одно из следующих действий:
   - Если требуется уложиться в действующий лимит, остановите задачи сбора событий, поток событий от которых приводит к превышению лимита.
   - Если требуется увеличить лимит, обратитесь к вашему менеджеру Positive Technologies.
2. Если в MaxPatrol SIEM не поступают данные от сервиса лицензионного контроля, на сервере PT MC выполните команду:
   ```
   docker restart $(docker ps -aqf name=core.authorization.abac.decisionpoint)
   ```

После устранения причин ошибки функции MaxPatrol SIEM автоматически восстановятся в течение часа.

Если проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies.

37.21. Ошибка «Запуск задач на сбор событий отключен»

Перед возникновением ошибки система может отображать следующие сообщения:

— «В MaxPatrol SIEM показатель **EPS** за последние <Число> дней близок к лимиту (<Текущий EPS> из <Лимит EPS>). Сократите использование ресурсов приложения или увеличьте лицензируемый лимит»;

— «Не удалось получить данные от сервиса лицензионного контроля».

Возможные причины

Возможными причинами проблемы могут быть систематическое превышение лимита EPS, установленного лицензией MaxPatrol SIEM; ошибка в работе сервиса лицензионного контроля.

Решение

Для решения проблемы требуется учетная запись **Администратор** или любая другая учетная запись с привилегией «Управление лицензиями».

► Чтобы решить проблему:

1. В интерфейсе PT MC на странице **Управление лицензиями** проверьте соблюдение лимита EPS, установленного для лицензии. Если он превышен, выполните одно из следующих действий:
   - Если требуется уложиться в действующий лимит, остановите задачи сбора событий, поток событий от которых приводит к превышению лимита.
   - Если требуется увеличить лимит, обратитесь к вашему менеджеру Positive Technologies.
2. Если в MaxPatrol SIEM не поступают данные от сервиса лицензионного контроля, на сервере PT MC выполните команду:
   ```
   docker restart $(docker ps -aqf name=core.authorization.abac.decisionpoint)
   ```

После устранения причин ошибки функции MaxPatrol SIEM автоматически восстановятся в течение часа.

Если проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies.

37.22. Ошибка «Корреляция событий отключена»

Перед возникновением ошибки система может отображать следующие сообщения:

— «В MaxPatrol SIEM показатель **EPS** за последние <Число> дней близок к лимиту (<Текущий EPS> из <Лимит EPS>). Сократите использование ресурсов приложения или увеличьте лицензируемый лимит»;

— «Не удалось получить данные от сервиса лицензионного контроля».

Возможные причины

Возможными причинами проблемы могут быть систематическое превышение лимита EPS, установленного лицензией MaxPatrol SIEM; ошибка в работе сервиса лицензионного контроля.

Решение

Для решения проблемы требуется учетная запись **Администратор** или любая другая учетная запись с привилегией «Управление лицензиями».

- Чтобы решить проблему:

  1. В интерфейсе PT MC на странице **Управление лицензиями** проверьте соблюдение лимита EPS, установленного для лицензии. Если он превышен, выполните одно из следующих действий:

     - Если требуется уложиться в действующий лимит, остановите задачи сбора событий, поток событий от которых приводит к превышению лимита.
     - Если требуется увеличить лимит, обратитесь к вашему менеджеру Positive Technologies.

  2. Если в MaxPatrol SIEM не поступают данные от сервиса лицензионного контроля, на сервере PT MC выполните команду:

     ```
     docker restart $(docker ps -aqf name=core.authorization.abac.decisionpoint)
     ```

После устранения причин ошибки функции MaxPatrol SIEM автоматически восстановятся в течение часа.

Если проблема не решилась, необходимо сообщить об этом в службу технической поддержки Positive Technologies.

37.23. Ошибка «Доля свободного дискового пространства, выделенного для табличных списков в <Название компонента> на узле <Название узла>, достигла 5%»

Возможные причины

Осталось 5% свободного дискового пространства, выделенного для табличных списков в указанном компоненте.

Решение

- Чтобы решить проблему,

  измените конфигурацию (см. раздел 29.2) роли SIEM Server, увеличив значение параметра `EnriTableListsSize`.

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

Проблема

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

Решение

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

- Чтобы решить проблему:

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

     ```
     #    extra_hosts:
     #      - "fqdn:ip"
     ```

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

     Внимание! При редактировании файла необходимо соблюдать синтаксис языка YAML.

     Например:

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

  4. Запустите обновление конфигураций установленных компонентов MaxPatrol SIEM:

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

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

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

37.25. Установка модуля Salt Minion завершается с ошибкой

Решение

- Чтобы решить проблему:

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

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

37.26. Не отображаются события в веб-интерфейсе после установки или обновления MaxPatrol SIEM

Проблема

После установки или обновления MaxPatrol SIEM в веб-интерфейсе системы с установленным Kaspersky Endpoint Security на вкладке **События** появляется сообщение об ошибке, например «Внутренняя ошибка сервера» или «Не удалось получить список событий».

Возможные причины

Возможной причиной проблемы является работа Kaspersky Endpoint Security, в ходе которой создаются правила `iptables`, влияющие на обработку сетевого трафика.

Решение

Необходимо приостановить работу Kaspersky Endpoint Security.

Перед выполнением инструкции необходимо убедиться, что:

- результат выполнения команды `iptables_save | grep kesl_bypass` содержит записи с заголовками `kesl_bypass`;
- выполнение команды `docker exec -it $(docker ps -qf name=core.events) bash -c 'curl -k -vvv https://$HMSettings_Host_HostName/api/deployment_configuration/v1/application'` завершилось с ошибкой или не завершается в течение длительного времени.

► Чтобы решить проблему:

1. Выполните команду для приостановки Kaspersky Endpoint Security:
   ```
   systemctl stop kesl
   ```
2. Выполните команду:
   ```
   docker exec -it $(docker ps -qf name=core.events) bash -c 'curl -k -vvv https://$HMSettings_Host_HostName/api/deployment_configuration/v1/application'
   ```
   Выполнение команды завершится быстро и без ошибок, а события отобразятся в веб-интерфейсе MaxPatrol SIEM. Если события отсутствуют, необходимо обратиться в службу технической поддержки Positive Technologies.
3. Выполните команду для запуска Kaspersky Endpoint Security:
   ```
   systemctl start kesl.service
   ```

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

Проблема

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

Возможные причины

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

Решение

- Чтобы решить проблему,

  проверьте поля шаблона: если поле содержит ненужную формулу, удалите ее.

37.28. Ошибка при проверке подключения

Проблема

Задача на проверку подключения завершается ошибкой «Не удалось выполнить задачу на коллекторе <Название коллектора>. Выберите другой коллектор».

Решение

- Чтобы решить проблему:

  1. Обновите MaxPatrol SIEM и коллектор до версии 27.0 или выше.
  2. Запустите задачу на проверку подключения повторно. См. раздел «Запуск проверки подключения» Руководства оператора.

37.29. Ошибка при обновлении роли Deployer

Проблема

Ошибка при обновлении роли Deployer.

Возможные причины

Роль содержит пакеты с фиксированной версией, защищенные от обновления. Вы можете проверить наличие таких пакетов с помощью команды `apt-mark showhold`.

Решение

Вы можете отключить защиту версии пакетов от обновления.

Внимание! Защита версий от обновления будет отключена для всех пакетов, существующих в системе.

- Чтобы решить проблему,

  выполните команду:

  ```
  apt-mark showhold | xargs sudo apt-mark unhold
  ```

37.30. Ошибка при создании резервной копии данных LogSpace после обновления Astra Linux

Проблема

Если MaxPatrol SIEM установлен на Astra Linux и включен мандатный контроль целостности, после обновления операционной системы возникает ошибка при создании резервной копии данных хранилища событий LogSpace.

Возможные причины

Возможной причиной является несовпадение классификационных меток каталога, в котором сохраняются файлы с данными LogSpace, с метками самих файлов.

Решение

Необходимо зафиксировать атрибуты контроля целостности для каталога с данными хранилища.

- Чтобы решить проблему:

  1. Откройте конфигурационный файл `/etc/parsec/fs-ilev.conf`.
  2. Добавьте в файл строку:
     ```
     min /opt/logspaced
     ```
  3. Сохраните файл.
  4. Выполните команду:
     ```
     sudo set-fs-ilev enable
     ```

37.31. Слишком много открытых файлов при создании резервной копии или восстановлении данных LogSpace

В конфигурации ОС Linux существует лимит, ограничивающий количество файлов, которые можно одновременно открыть от имени учетной записи. Если хранилище данных LogSpace установлено на один сервер с другими компонентами MaxPatrol SIEM, этот лимит может исчерпываться быстрее.

Если лимит исчерпан, при создании резервной копии или восстановлении данных с помощью утилиты backup_tool отобразится сообщение об ошибке следующего вида: `Failed with exception: Error opening column or index file ..., errno: 24, strerror: Too many open files`.

Вы можете узнать, какой лимит установлен для учетной записи, с помощью команды `sudo -u logspace bash -c 'ulimit -{H,S}n'`.

Для изменения лимита для текущей сессии (без сохранения значения для следующих сессий) вы можете использовать команду `ulimit -n <Новый лимит>`.

Если нужно использовать новый лимит и в следующих сессиях, вы можете использовать один из способов:

— Указать новый лимит в конфигурационном файле `/etc/security/limits.conf`;

— Создать пользовательский конфигурационный файл `/etc/security/limits.d/limits.conf` и указать новый лимит в нем.

Примечание. Рекомендуемый лимит для работы с базами данных — не ниже 1 миллиона файлов.

37.32. Настройка LimitMEMLOCK для исправления ошибки ENOMEM при использовании LogSpace

Если при создании экземпляра uring возникает ошибка `ENOMEM` (недостаточно памяти), необходимо вручную увеличить объем оперативной памяти, защищенный от вытеснения на жесткий диск в раздел подкачки. Объем такой памяти в байтах задан в конфигурационном файле `/lib/systemd/system/logspaced.service` в параметре `LimitMEMLOCK`.

Вид сообщения об ошибке: `MemoryException: Cannot create io_uring instance 'BasicRing@0x7ffe904ae768'`.

Значение `LimitMEMLOCK` по умолчанию — `32M`. Максимальное рекомендуемое значение — `64M`.

Настройка LimitMEMLOCK в конфигурационном файле logspaced.service

► Чтобы настроить объем памяти, защищенный от вытеснения,

в файле `/lib/systemd/system/logspaced.service` измените значение параметра `Service` → `LimitMEMLOCK`.

Примечание. При обновлении LogSpace параметры в файле `logspaced.service` вернутся к значениям, установленным по умолчанию.

Настройка LimitMEMLOCK с созданием дополнительного конфигурационного файла

- Чтобы настроить объем памяти, защищенный от вытеснения:

  1. В каталоге `/etc/systemd/system/logspaced.service.d` создайте конфигурационный файл с расширением .conf.
  2. Добавьте в файл строки:

     ```
     [Service]
     LimitMEMLOCK = <Объем памяти, защищенный от вытеснения>
     ```

     Например:

     ```
     [Service]
     LimitMEMLOCK = 64M
     ```

Настройка LimitMEMLOCK с использованием systemd drop-in

- Чтобы настроить объем памяти, защищенный от вытеснения:

  1. Выполните команду:

     ```
     systemctl edit logspaced.service
     ```

  2. Добавьте в автоматически созданный файл строки:

     ```
     [Service]
     LimitMEMLOCK = <Объем памяти, защищенный от вытеснения>
     ```

     Например:

     ```
     [Service]
     LimitMEMLOCK = 64M
     ```

Вы можете проверить результат настройки `LimitMEMLOCK` с помощью команды `systemctl cat logspaced.service`.

37.33. Ошибки, связанные с конфигурацией LogSpace

Ошибка выделения памяти

Вид сообщения об ошибке: `<ERROR> Exec: Code: 41, e.displayText() = DB::MemoryException: Memory limit (for query) exceeded`.

Возможные причины

Ограничение объема памяти, выделенного для выполнения запроса. Чаще всего ошибка возникает при выполнении запросов с агрегацией или сортировкой, запросов с обращением к body.

Решение

- Чтобы решить проблему,

  в конфигурационном файле `/etc/logspaced/profiles.xml` увеличьте значения параметра `profiles` → `<Название используемого профиля>` → `max_memory_usage`.

  Примечание. Если на сервере LogSpace установлено примерно 150 ГБ ОЗУ, рекомендуемое значение параметра — 32 ГБ, если на сервере 200 ГБ ОЗУ и больше — 62 ГБ.

Ошибка чтения текста запроса

Вид сообщения об ошибке: `<ERROR> Exception: HTTPHandler: Code: 29, e.displayText() = DB::SyntaxError: syntax error, unexpected end of input, expecting '(' or '[': '00000006-4d4f []`

Возможные причины

Ограничение длины текста запроса. Чаще всего ошибка возникает при выполнении запросов `SELECT` с фильтром по множеству UUID.

Решение

- Чтобы решить проблему,

  в конфигурационном файле `/etc/logspaced/profiles.xml` установите для параметра `profiles` → `<Название используемого профиля>` → `max_query_size` значение `4M`.

Задержка или отмена вставки данных, синхронные слияния при INSERT

Вид сообщений об ошибках:

```
<Note> Part: Part count of table siem.events exceeded specified threshold 300. Starting synchronous merge 1
```

```
<Warn> Part: Part count of table siem.events exceeded specified threshold 300. Starting synchronous merge 10. Insert may be rejected in 1 next synchronous merges.
```

```
<ERROR> Exec: Code: 364, e.displayText() = DB::Exception: Rejecting insert: there are too many parts in the table siem.events
```

Возможные причины

Ограничение на количество активных разделов в таблице.

Решение

► Чтобы решить проблему:

1. Создайте файл `/etc/logspaced/config.d/config.xml`.
2. Добавьте в файл строки:

```
<?xml version="1.0"?>
<logspace>
    <merge_tree>
        <large_merges_max_threads><Значение></large_merges_max_threads>
        <parts_to_delay_insert><Значение></parts_to_delay_insert>
    </merge_tree>
</logspace>
```

3. Создайте файл `/etc/logspaced/profiles.d/profiles.xml`.
4. Добавьте в файл строки:

```
<?xml version="1.0"?>
<logspace>
    <profiles>
        <default>
        <background_pool_size><Значение></background_pool_size>
        </default>
    </profiles>
</logspace>
```

Примечание. Значения параметров рекомендуется выбирать в соответствии с таблицей «Рекомендуемые значения параметров хранилища LogSpace».

Таблица 11. Рекомендуемые значения параметров хранилища LogSpace

Параметр	Уровень нагрузки				
	До 5000 событий в секунду[3]	До 10 000 событий в секунду	До 20 000 событий в секунду	До 30 000 событий в секунду	До 100 000 событий в секунду
background_pool_size	3	4	5	6	10
large_merges_max_threads	1	1	2	2	3
parts_to_delay_insert	300	500	1000	2000	3000

3 Значения, используемые по умолчанию.

37.34. Ошибки взаимодействия служб MaxPatrol SIEM с LogSpace

Ошибка записи результата SELECT в сокет

Вид сообщения об ошибке: `<ERROR> Exec: Code: 15, e.displayText() = DB::NetException: Cannot write to ostream`.

Возможные причины

При выполнении запроса, который требует много времени на вычисление, соединение может быть прервано службой Core Events по тайм-ауту до того, как LogSpace закончит вычислять результат. Например, запрос `SELECT count() FROM core.events WHERE ...` потребует полной фильтрации данных, чтобы вернуть одно запрошенное значение.

Решение

- Чтобы решить проблему:

  1. На сервере MP 10 Core в файл `/var/lib/deployed-roles/<Идентификатор приложения>/<Идентификатор роли Core>/images/core.events.extended/config/custom.env` добавьте строку:

     `LogSpaceSettings_ResponseTimeout=<Время ожидания службы Core Events в формате чч:мм:сс>`

     Например:

     `LogSpaceSettings_ResponseTimeout=00:03:00`

  2. Выполните команду:

     `docker-compose -f /var/lib/deployed-roles/<Идентификатор приложения>/<Идентификатор роли Core>/images/core.events.extended/docker-compose.yaml up -d`

Ошибка чтения данных INSERT из сокета

Вид сообщения об ошибке: `<ERROR> Exec: Code: 14, e.displayText() = DB::Exception: Cannot read from istream`.

Возможные причины

Соединение может быть разорвано в момент чтения данных из-за нестабильной работы сети (например, обрывов соединения) или из-за сочетания сетевых задержек и слишком маленького значения тайм-аута для службы storage.

Решение

- Чтобы решить проблему,

  в конфигурационном файле `siem.conf` увеличьте значение параметра `storage` → `logspace` → `response_timeout`.

Ошибки парсинга данных INSERT

Вид сообщения об ошибках:

```
<ERROR> Exec: Code: 81, e.displayText() = DB::ParserException: Unexpected end
of escape sequence
```

```
<ERROR> Exec: Code: 513, e.displayText() = DB::Exception: Invalid UUID :|
198e94c0-3240-0001-0000-00000000004:
```

```
<ERROR> Exec: Code: 31, e.displayText() = DB::Exception: No enumerator for
label 'succes' found:
```

```
<ERROR> Exec: Code: 84, e.displayText() = DB::ParserException: Unable to parse
'2023-11-21' as DateTime:
```

```
<ERROR> Exec: Code: 80, e.displayText() = DB::ParserException: Error while
parsing: expected '\t' before '...\t\t\t\t\t\t10.3.90.50\\r\\n10.3.84'
```

Возможные причины

Парсер данных встречает конец потока в момент разбора значения. Появление таких ошибок может быть связано с увеличением времени обработки запросов `INSERT` из-за синхронных слияний: пока запрос `INSERT` находится в ожидании слияния, служба storage прерывает соединение по тайм-ауту. Такие ошибки могут быть результатом накопления ошибок чтения данных `INSERT` из сокета.

Решение

Избегать накопления ошибок чтения данных `INSERT` из сокета.

37.35. Защита LogSpace от принудительной остановки службой OOM Killer

Если компонент MP SIEM Events Storage с хранилищем событий LogSpace установлен на один сервер вместе с любым другим компонентом MaxPatrol SIEM, возникает риск принудительной остановки LogSpace службой OOM Killer.

- Чтобы защитить LogSpace от принудительной остановки:

  1. Создайте файл `/etc/systemd/system/logspaced.service.d/oom.conf`.
  2. Добавьте в файл строки:

     ```
     [Service]
     OOMScoreAdjust=<Значение>
     ```

     Например:

     ```
     [Service]
     OOMScoreAdjust=-1000
     ```

Примечание. Значение `OOMScoreAdjust=-1000` сделает LogSpace неуязвимым для OOM Killer, значение `OOMScoreAdjust=-500` значительно снизит вероятность принудительной остановки LogSpace.

37.36. На коллекторах накапливается и не разбирается очередь событий

Проблема

При большом количестве данных, собираемых модулями коллекторов, очередь событий быстро накапливается и не успевает разбираться.

Возможные причины

Причинами могут быть:

1. Отсутствие подключения к RabbitMQ (в журнале коллектора есть ошибки librmq).
2. Срабатывание механизма Flow Control (в журнале коллектора есть ошибки suspend).
3. Неоптимальная настройка передачи пакетов с событиями.
4. Недостаточное количество потоков записи событий в RabbitMQ.

Решение

Для увеличения количества потоков записи событий в RabbitMQ необходимо увеличить значение параметра `publisher_pool_size` в конфигурационном файле коллектора, на котором копится очередь.

- Чтобы изменить количество потоков записи событий:

  1. Если MP 10 Collector установлен на сервере под управлением ОС семейства Linux, откройте на редактирование конфигурационный файл `/opt/core-agent/config.json`.
  2. Если MP 10 Collector установлен на сервере под управлением Windows, откройте на редактирование конфигурационный файл `C:\ProgramData\Positive Technologies\MaxPatrol 10 Collector\config\agent.conf`.
  3. В блоке параметров `rmq` добавьте строку с параметром `publisher_pool_size` и укажите в качестве его значения необходимое количество потоков записи событий.

     Например:

     ```
     ...
     "vhost": "siem",
     "publisher_pool_size": "6",
     "auth":
     ...
     ```

Примечание. В зависимости от количества событий рекомендуется указать 6, 9 или 12 потоков.

4. Сохраните изменения и закройте файл.
5. Перезапустите службу коллектора.

Для настройки передачи пакетов с событиями в RabbitMQ необходимо поочередно увеличивать значения параметров модуля **Максимальное количество событий в пакете** и **Интервал отправки пакетов** и отслеживать состояние очереди на коллекторе. По умолчанию оба параметра имеют значение `1000`. Не рекомендуется увеличивать значения этих параметров больше `5000`.

- Чтобы изменить параметры передачи пакетов с событиями:

1. В главном меню MaxPatrol SIEM выберите **Сбор данных** → **Задачи**.
2. Выберите задачу на сбор данных, по которой на коллектор поступает наибольшее количество событий.
3. Нажмите **Изменить**.
4. В блоке параметров **Параметры сбора данных** включите отображение дополнительных параметров и выберите **Отправка данных в систему**.
5. Укажите новое значение параметра **Максимальное количество событий в пакете** или **Интервал отправки пакетов**.
6. Нажмите **Сохранить**.

37.37. Ошибка при обновлении роли, связанная с именем Docker-контейнера

Проблема

При обновлении роли возникает ошибка `The container name "<Имя Docker-контейнера>" is already in use by container "<Идентификатор Docker-контейнера>". You have to remove (or rename) that container to be able to reuse that name`.

Возможные причины

Docker-контейнер, с которым связана ошибка, ранее пересоздавался с помощью команды `docker-compose up -d`, например при изменении его конфигурации. Такой Docker-контейнер не может быть удален командой от Deployer, поэтому при обновлении роли в системе будут запущены два одинаковых Docker-контейнера, что приводит к появлению ошибки.

Решение

Если Docker-контейнер пересоздавался вручную, необходимо перед обновлением роли удалить его, например с помощью команды:

```
docker rm -f $(docker ps -aqf name=<Имя Docker-контейнера>)
```

Если после обновления требуется пересоздать Docker-контейнер, необходимо использовать команду `docker-compose up -d` с указанием полных путей к файлам, в том числе к файлам с переменными окружения:

```
/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/
packages/docker-compose --file /var/lib/deployed-roles/<Идентификатор приложения>/
<Название экземпляра роли>/images/<Имя микросервиса>/docker-compose.yaml --project-
name <Имя проекта> --env-file /var/lib/deployed-roles/<Идентификатор приложения>/
<Название экземпляра роли>/images/<Имя микросервиса>/.env --file /var/lib/deployed-
roles/<Идентификатор приложения>/<Название экземпляра роли>/images/<Имя
микросервиса>/docker-compose.override.yml up -d
```

Например:

```
/var/lib/deployed-roles/mp10-application/core-1/packages/docker-compose --file /var/
lib/deployed-roles/mp10-application/core-1/images/content-service/docker-compose.yaml
--project-name mp10-applicationcore-1 --env-file /var/lib/deployed-roles/mp10-
application/core-1/images/content-service/.env --file /var/lib/deployed-roles/mp10-
application/core-1/images/content-service/docker-compose.override.yml up -d
```

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

Ошибка может возникнуть во время обновления MaxPatrol SIEM.

Возможные причины

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

Решение

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

- Чтобы решить проблему:

  1. Запустите сценарий:

     ```
     deployer maintenance fix -AppPackage
     ```

Отобразятся сообщения:

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

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

2. Запустите обновление заново.

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

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

Ошибка доступа к сертификату и ключу

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

Возможные причины

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

Решение

- Чтобы решить проблему:

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

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

Указан неверный файл сертификата

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

Возможные причины

В качестве файла ключа RMQ_SSL_KEY указан неподходящий файл.

Решение

- Чтобы исправить проблему,

  Проверьте соответствие путей параметрам.

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

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

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

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

Возможные причины

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

Решение

- Чтобы решить проблему:

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

37.41. Диагностика и решение проблем при работе с Elasticsearch

В этом разделе приводятся инструкции по диагностике и решению проблем, возникающих при работе с хранилищем событий Elasticsearch.

В этом разделе

Индексы Elasticsearch находятся в состоянии red (см. раздел 37.41.1)

Служба Elasticsearch останавливается через некоторое время после запуска (см. раздел 37.41.2)

Индексы Elasticsearch не переходят из горячей стадии в теплую (см. раздел 37.41.3)

Ошибки Elasticsearch при замедлении его работы и потере отображения данных (см. раздел 37.41.4)

37.41.1. Индексы Elasticsearch находятся в состоянии red

Индексы Elasticsearch предназначены для хранения данных о событиях информационной безопасности и их последующего поиска. Если индекс находится в состоянии red, чтение данных из него невозможно.

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 37.42.3) 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 37.42.6.3.3) `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 21.6), которые находятся в состоянии `red`.

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

Вы можете проверить состояние индексов с помощью команды `curl 127.0.0.1:9200/_cat/indices?v`.

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

- данные о состоянии (см. раздел 37.42.6.3.3) индексов и шардов (фрагментов индексов);
- время запуска каждой команды `curl -XPOST localhost:9200/_cluster/reroute?retry_failed=true`;
- файлы журналов Elasticsearch, SIEM Health Monitor.

37.41.2. 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 37.42.6.3.3) 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 Б)), не превышает 58% от объема памяти ОЗУ сервера.
  4. Убедитесь, что объем раздела подкачки (см. раздел 37.42.1) на сервере MP SIEM Events Storage равен нулю.
  5. Проверьте, что Elasticsearch содержит не более 900 индексов со статусом open (см. раздел 37.42.6.3.3). Если таких индексов более 900, необходимо настроить архивацию и удаление индексов по расписанию (см. раздел 21).

Если проблема не решилась, 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.

37.41.3. Индексы Elasticsearch не переходят из горячей стадии в теплую

Возможные причины

Возможной причиной является выключенный режим многоуровневого хранилища: при установке роли SIEM Server не был включен параметр `ManagedStorage`.

Решение

- Чтобы решить проблему:

  1. Выполните команду для изменения значения параметра `ManagedStorage`:
     ```
     deployer instance setparam -Id <Идентификатор экземпляра роли SIEM Server> ManagedStorage =True
     ```
  2. Выполните команду для изменения конфигурации роли SIEM Server:
     ```
     deployer instance reconfigure -Id < Идентификатор экземпляра роли SIEM Server>
     ```

Вы можете отслеживать перемещение индексов с помощью команды `curl -X GET "http://localhost:9200/_cat/shards"`.

Также вы можете получить текущее состояние конкретного индекса в рамках политики ILM с помощью команды `curl localhost:9200/<Идентификатор индекса>/_ilm/explain`.

37.41.4. Ошибки Elasticsearch при замедлении его работы и потере отображения данных

Примечание. Elasticsearch взаимодействует с сервисами, отвечающими за настройку, запись и чтение данных. Поэтому сбои в отображении или поиске событий могут быть вызваны не только проблемами в самом хранилище.

В процессе эксплуатации в журналах Elasticsearch могут регистрироваться следующие ошибки. Их анализ позволяет выявить и устранить типовые неисправности.

Ошибка Data too large

Возможные причины

Возможной причиной является превышение пороговых значений потребления памяти. Защитный механизм Elasticsearch отслеживает потребление памяти и блокирует операции, способные привести к нестабильной работе сервера, паузам при сборке мусора или аварийной остановке сервиса.

Решение

Необходимо ограничить поток событий с проблемных агентов.

Если ограничение потока событий невозможно или не дает результата, вы можете применить один из следующих методов настройки Elasticsearch:

— если на сервере есть свободная оперативная память — увеличить объем оперативной памяти (см. раздел 29.4), выделяемого узлам кластера Elasticsearch.

— понизить порог срабатывания сборщика мусора. Для этого в конфигурационном файле `/etc/elasticsearch/*/jvm.options` необходимо установить значение параметра `10-:-XX:InitiatingHeapOccupancyPercent` равным `15`.

Ошибка превышения лимита ожидания

Возможные причины

В журнале Elasticsearch присутствуют сообщения вида:

```
<[Время события]>[WARN ][o.e.t.TransportService ] [siem] Received response for a
request that has timed out, sent [19660ms] ago, timed out [4612ms] ago, action
[cluster:monitor/nodes/stats[n]], node [{siem}{S3MtFlzMRTensQVviFjddQ}
{Lv06vDpvSTCv1wRNpotBkQ}{}{10.0.14.4:9300}{dimr}{xpack.installed=true,
transform.node=false}], id [1323092]
<[Время события]> [WARN ][o.e.m.f.FsHealthService ] [siem] health check took [5942ms]
which is above the warn threshold of [5s]
```

Возможной причиной является превышение установленного в Elasticsearch лимита ожидания при выполнении внутреннего запроса.

Решение

Необходимо провести диагностику аппаратных ресурсов сервера.

Также рекомендуется проверить состояние индексов с помощью команды `curl localhost:9200/_cat/indices?pretty`. При наличии индексов в статусе `red` вы можете устранить проблему по инструкции (см. раздел 37.41.1).

Ошибка max_bytes_length_exceeded_exception

Возможные причины

Возможной причиной является превышение ограничения размера поля в Elasticsearch при записи данных.

Решение

Необходимо выполнить следующие действия:

1. Установить, размер какого поля превысил ограничение.
2. Сравнить размер поля с данными схемы полей событий.
3. Внести коррективы в задачи на сбор данных.

См. также

Индексы Elasticsearch находятся в состоянии red (см. раздел 37.41.1)

37.42. Справочная информация

В разделе приведены рекомендации по выполнению шагов инструкций.

В этом разделе

Просмотр данных о распределении памяти ОЗУ и отключение раздела подкачки (см. раздел 37.42.1)

Сбор информации о нагрузке на файловую систему и запущенных процессах (см. раздел 37.42.2)

Просмотр статуса службы (см. раздел 37.42.3)

Проверка доступности сетевого порта сервера (см. раздел 37.42.4)

Деактивация PT MC (см. раздел 37.42.5)

Проверка работоспособности Elasticsearch (см. раздел 37.42.6)

Создание дампа памяти процесса (см. раздел 37.42.7)

Расположение файлов журналов (см. раздел 37.42.8)

Расположение временных файлов аудита (см. раздел 37.42.9)

Параметры мониторинга обработки активов (см. раздел 37.42.10)

Экспорт конфигурационных параметров ролей в файл (см. раздел 37.42.11)

Экспорт и импорт пользовательских профилей (см. раздел 37.42.12)

Управление системой с помощью утилиты deployer (см. раздел 37.42.13)

Настройка мандатного контроля целостности для Astra Linux (см. раздел 37.42.14)

Расположение пользовательских сертификатов (см. раздел 37.42.15)

Реорганизация данных в таблицах СУБД PostgreSQL (см. раздел 37.42.16)

Удаление неиспользуемых пакетов ролей (см. раздел 37.42.17)

Добавление исключений в Kaspersky Endpoint Security для БД PostgreSQL (см. раздел 37.42.18)

Особенности обновления Astra Linux при использовании хранилища LogSpace (см. раздел 37.42.19)

Просмотр версии LogSpace (см. раздел 37.42.20)

37.42.1. 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
  ```

37.42.2. 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`.

37.42.3. 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 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}}"
  ```

37.42.4. 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>`.

37.42.5. Деактивация PT MC

Вы можете деактивировать PT MC через веб-интерфейс.

Внимание! После деактивации PT MC лицензии будут автоматически отвязаны от приложений. После повторной активации лицензии необходимо привязать.

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

- Чтобы деактивировать PT MC через веб-интерфейс:

  1. В главном меню выберите **Лицензии**.
  2. Выберите лицензию.
  3. В панели инструментов нажмите ⋮ → **Деактивировать платформу**.
  4. Установите флажок **Я понимаю, что могу потерять доступ к приложениям и их данным**.
  5. Нажмите **Деактивировать**.

37.42.6. Проверка работоспособности Elasticsearch

В разделе приведены основные команды для мониторинга состояния хранилища событий Elasticsearch, диагностики проблем и оценки производительности узлов.

В этом разделе

Проверка прав доступа и портов (см. раздел 37.42.6.1)

Расположение индексов Elasticsearch (см. раздел 37.42.6.2)

Диагностика Elasticsearch на основании запросов к API (см. раздел 37.42.6.3)

37.42.6.1. Проверка прав доступа и портов

- Чтобы проверить права доступа к файлам и каталогам Elasticsearch,

  выполните команду:

  ```
  ls -ld /data /data/* /es_backup /etc/elasticsearch/* /run/elasticsearch/* | grep -Ev "^-|jvm.options"
  ```

Все указанные каталоги должны принадлежать владельцу с именем `elasticsearch:elasticsearch` с правами `drwxr-xr-x`.

- Чтобы проверить доступность портов Elasticsearch,

  выполните команду:

  ```
  netstat -tlnp | grep java
  ```

В выводе команды должны присутствовать строки с портами 9200 и 9300, которые прослушиваются как локально, так и для IP-адреса сервера.

37.42.6.2. Расположение индексов Elasticsearch

Расположение данных индексов Elasticsearch определяется значением параметра `path.data`, а путь к репозиторию архивных индексов — параметром `path.repo`. Оба параметра задаются в файле `/etc/elasticsearch/<Название узла>/elasticsearch_<Название узла>.yml`.

37.42.6.3. Диагностика Elasticsearch на основании запросов к API

Для диагностики состояния Elasticsearch вы можете отправлять запросы к REST API, который доступен через клиентский порт 9200. Отправлять запросы можно с использованием утилиты `curl` или другого HTTP-клиента. Ответ сервера возвращается в формате JSON.

В этом разделе

Проверка работоспособности кластера (см. раздел 37.42.6.3.1)

Просмотр состояния Elasticsearch (см. раздел 37.42.6.3.2)

Просмотр состояния индексов Elasticsearch (см. раздел 37.42.6.3.3)

Просмотр данных о политиках ILM (см. раздел 37.42.6.3.4)

Выгрузка событий за интервал времени (см. раздел 37.42.6.3.5)

37.42.6.3.1. Проверка работоспособности кластера

- Чтобы проверить подключение к клиентскому серверу,

  выполните команду:

  ```
  curl localhost:9200
  ```

Ответ будет содержать поля `name`, `cluster_name`, `version`.

- Чтобы проверить состояние кластера,

  выполните команду:

  ```
  curl localhost:9200/_cat/health
  ```

Кластер должен находится в статусе `green`.

- Чтобы получить информацию о состоянии узлов кластера,

  выполните команду:

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

Ответ будет содержать информацию об узлах кластера: IP-адресах, загрузке процессора и использованию оперативной памяти. Поле `node.role` будет содержать информацию о назначенной узлу роли. Например, значение `dimr` указывает на то, что узлу назначены следующие роли:

— `data` — узел данных;

— `ingest` — узел-обработчик;

— `master` — узел, имеющий право быть избранным мастером кластера;

— `remote_cluster_client` — узел, который может выступать в роли клиента для подключения к удаленному кластеру.

- Чтобы получить расширенную информацию с детальной статистикой по выбранному узлу,

  выполните команду:

  ```
  curl localhost:9200/_nodes/<Имя узла кластера>/stats?pretty
  ```

Ответ будет содержать информацию об узле кластера: его роли, загрузке процессора, использованию оперативной памяти, а также информацию о состоянии дисков и индексов.

37.42.6.3.2. Просмотр состояния Elasticsearch

- Чтобы просмотреть состояние Elasticsearch,

  выполните команду:

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

37.42.6.3.3. 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 всех 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`.

- Чтобы просмотреть состояние шардов для конкретного индекса

  выполните команду:

  ```
  curl localhost:9200/_cat/shards/<Идентификатор индекса>?v
  ```

Поле state отражает текущее состояние шарда. Возможны следующие состояния:

— STARTED — штатный режим. Шард активен, доступен для чтения и записи, все операции с ним выполняются в обычном порядке.

— INITIALIZING — подготовка шарда после запуска сервиса. Временное состояние.

— UNASSIGNED — шард не назначен ни на один узел кластера. Нормальное состояние при запуске сервиса во время первоначальной инициализации индекса, когда шарды еще не распределены. В рабочем кластере сигнализирует о нарушениях в данных шарда.

— RELOCATING — шард перемещается между узлами кластера в ходе перераспределения нагрузки. Временное состояние.

37.42.6.3.4. 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/<Идентификатор индекса>/_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 одну из следующих команд:

  - если используется общее хранилище данных:

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

  - если используется многоуровневое хранилище данных:

    ```
    curl 127.0.0.1:9200/_ilm/policy/siem_highload_events_policy?pretty
    ```

37.42.6.3.5. Выгрузка событий за интервал времени

Вы можете выгрузить все события за определенный период времени с помощью команды `curl 'localhost:9200/<Идентификатор индекса>/_search?pretty&size=<Количество событий>' -H 'Content-Type: application/json' -d \'{"query":{"range":{"time":{"gte":"<Начало периода>","lte":"<Окончание периода>"}}}}' \-o <Название файла для выгрузки событий>`

Пример выгрузки первых двух событий в интервале с `2024-11-30T00:10:00Z` по `2024-11-30T23:20:00Z` из индекса `ds-siem_events-2024.11.30-000001` в файл `~/events.jsoncurl`:

```
curl 'localhost:9200/.ds-siem_events-2024.11.30-000001/_search?pretty&size=2' -H
'Content-Type: application/json' -d \ '{"query":{"range":{"time":
{"gte":"2024-11-30T00:10:00Z","lte":"2024-11-30T23:20:00Z"}}}}' \ -o ~/events.json
```

Пример выгрузки первых двух событий с полем `recv_ipv4` со значением `10.0.52.218` из индекса `ds-siem_events-2024.11.30-000001` в файл `~/events.jsoncurl`:

```
curl 'localhost:9200/.ds-siem_events-2024.11.30-000001/_search?pretty&size=2' -H
'Content-Type: application/json' -d \ '{"query":{"match":{"recv_ipv4" :
"10.0.52.218"}}}' \ -o ~/events.json
```

37.42.7. 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.

37.42.8. Расположение файлов журналов

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

Таблица 12. 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`
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`
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`

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`.

37.42.9. Расположение временных файлов аудита

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

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

37.42.10. 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 файлах `/var/lib/deployed-roles/mp10-application/core-*/images/<Название службы>/config/custom.env` и приведены в таблице. Для реконфигурации всех ролей необходимо выполнить команду `deployer instance reconfigure -type Core`.

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

Таблица 13. Параметры мониторинга обработки активов

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

Стадия обработки	Служба	Длина очереди		Время ожидания		Период вычисления средней скорости обработки
		Допустимое значение	Критическое значение	Допустимое значение	Критическое значение	
Слияние данных об активах	Assets Processing	Statistics_AssetsMergingQueueLengthAllowedThreshold	Statistics_AssetsMergingQueueLengthCriticalThreshold	Statistics_AssetsMergingWaitingTimeAllowedThreshold	Statistics_AssetsMergingWaitingTimeCriticalThreshold	Statistics_AssetsMergingProcessingSpeedCalculationPeriod
Расчет содержимого динамических групп	Assets Groups	Statistics_DynamicGroupsCalculationQueueLengthAllowedThreshold	Statistics_DynamicGroupsCalculationQueueLengthCriticalThreshold	Statistics_DynamicGroupsCalculationWaitingTimeAllowedThreshold	Statistics_DynamicGroupsCalculationWaitingTimeCriticalThreshold	Statistics_DynamicGroupsCalculationProcessingSpeedCalculationPeriod
Обновление отображаемых данных об активе	Assets Temporal Read Model	Statistics_QueueLengthAllowedThreshold	Statistics_QueueLengthCriticalThreshold	Statistics_WaitingTimeAllowedThreshold	Statistics_WaitingTimeCriticalThreshold	Statistics_ProcessingSpeedCalculationPeriod
Обновление табличных списков	Tables	Statistics_QueueLengthAllowedThreshold	Statistics_QueueLengthCriticalThreshold	Statistics_WaitingTimeAllowedThreshold	Statistics_WaitingTimeCriticalThreshold	Statistics_ProcessingSpeedCalculationPeriod

37.42.11. Экспорт конфигурационных параметров ролей в файл

Вы можете экспортировать конфигурационные параметры ролей MaxPatrol SIEM в файл манифеста с помощью утилиты Export-Configuration, поставляемой с ролью Deployer. Полученный в результате экспорта манифест вы можете использовать при развертывании MaxPatrol SIEM на другом сервере.

- Чтобы экспортировать конфигурационные параметры ролей в файл:

  1. Запустите утилиту Export-Configuration:
     `/opt/deployer/bin/Export-Configuration.ps1`
  2. В открывшемся окне выберите варианты с идентификаторами приложений.
  3. В открывшемся окне выберите экземпляры ролей, для которых необходимо экспортировать конфигурационные параметры.

     Начнется экспорт параметров выбранных экземпляров ролей. В каталоге с утилитой появится файл `export_manifest.yaml`.

     Примечание. Если в каталоге уже существует файл с именем `export_manifest.yaml`, в конец его имени будут добавлены дата и время создания нового файла: `export_manifest.yaml.<yyyyMMddHHmmss>`. Новый файл будет сохранен с именем `export_manifest.yaml`.

  Параметры роли экспортированы.

При запуске утилиты вы можете также использовать специальные ключи:

- для указания приложения — ключ `AppInstanceId <Идентификатор приложения>`. Например: `/opt/deployer/bin/Export-Configuration.ps1 -AppInstanceId mc-application`

  Примечание. После запуска утилиты с этим ключом в файл манифеста будут экспортированы конфигурационные параметры всех ролей приложения, указанного в ключе.

- для указания роли — ключ `RoleInstanceId <Идентификатор экземпляра роли>`. Например: `/opt/deployer/bin/Export-Configuration.ps1 -RoleInstanceId managementandconfiguration`

Для каждого ключа можно указать только один идентификатор.

37.42.12. Экспорт и импорт пользовательских профилей

Вы можете экспортировать и импортировать пользовательские профили, а также справочники и учетные записи, относящиеся к этим профилям, с помощью скрипта unitmigrator.

Для запуска скрипта необходимы следующие конфигурационные файлы:

— `enabled_profiles.yaml` — содержит список профилей, которые необходимо экспортировать (импортировать);

— `hosts` — содержит параметры подключения к узлу, с которого необходимо экспортировать (или на который импортировать) профили.

Перед первым запуском скрипта необходимо создать файлы `enabled_profiles.yaml` и `hosts` в каталоге `/var/lib/deployed-roles/mp10-application/core/data/unitmigrator/config/` на сервере с MP 10 Core.

Приведенные ниже инструкции необходимо выполнять на сервере компонента MP 10 Core.

Экспорт профилей

► Чтобы экспортировать пользовательские профили:

1. В конфигурационный файл `enabled_profiles.yaml` добавьте строки с названиями профилей, которые необходимо экспортировать:

   ```
   - "<Название профиля 1>"
   - "<Название профиля 2>"
   ...
   - "<Название профиля N>"
   ```

   Примечание. Для экспорта всех профилей конфигурационный файл `enabled_profiles.yaml` необходимо оставить пустым.

2. В конфигурационный файл `hosts` добавьте строки с параметрами подключения к узлу, с которого необходимо экспортировать профили:

   ```
   [export]
   <IP-адрес или FQDN сервера MP 10 Core> ansible_user=<Логин> ansible_password=<Пароль>
   ```

3. Перейдите в каталог `core.unitmigrator`:

   ```
   cd /var/lib/deployed-roles/mp10-application/core/images/core.unitmigrator
   ```

4. Запустите скрипт с помощью команды:

   ```
   docker-compose run --rm core.unitmigrator export
   ```

   Начнется процесс экспорта профилей, по завершению которого в каталоге `/var/lib/deployed-roles/mp10-application/core/data/unitmigrator/export/` появится JSON-файл с названием вида `Профили_<Дата начала экспорта>.json`.

JSON-файл с результатами экспорта содержит следующие объекты:

— `hash` — хеш-сумма файла без учета пробелов;

— `microservice_version` — версия микросервиса, из которого экспортировались профили;

— `scanning_api_version` — версия API (ресурса), из которого экспортировались профили;

— `dictionaries_api_version` — версия API (ресурса), из которого экспортировались справочники;

— `credentials_api_version` — версия API (ресурса), из которого экспортировались учетные записи;

— `profiles` — список экспортируемых профилей;

— `dictionaries` — список пользовательских справочников, которые относятся к экспортируемым профилям;

— `credentials` — список учетных записей, которые относятся к экспортируемым профилям.

Импорт профилей

► Чтобы импортировать пользовательские профили:

1. В конфигурационный файл `enabled_profiles.yaml` добавьте строки с названиями профилей, которые необходимо импортировать:

   ```
   - "<Название профиля 1>"
   - "<Название профиля 2>"
   ...
   - "<Название профиля N>"
   ```

   Примечание. Для импорта всех профилей конфигурационный файл `enabled_profiles.yaml` необходимо оставить пустым.

2. В конфигурационный файл `hosts` добавьте строки с параметрами подключения к узлу, на который необходимо импортировать профили:

   ```
   [import]
   < IP-адрес или FQDN сервера MP 10 Core> ansible_user=<Логин> ansible_password=<Пароль>
   ```

3. Скопируйте в каталог `/var/lib/deployed-roles/mp10-application/core/data/unitmigrator/import/` JSON-файл, полученный при экспорте профилей.

4. Перейдите в каталог `core.unitmigrator`:

   ```
   cd /var/lib/deployed-roles/mp10-application/core/images/core.unitmigrator
   ```

5. Запустите скрипт с помощью команды с параметрами импорта:

   ```
   docker-compose run --rm core.unitmigrator import "profiles_strategy=<Значение>
   dictionaries_strategy=<Значение> credentials_strategy=<Значение> importable_file_name=<Имя
   файла с профилями>"
   ```

   Например:

   ```
   docker-compose run --rm core.unitmigrator import "profiles_strategy=Update
   dictionaries_strategy= Update credentials_strategy=CreateNew
   importable_file_name=Профили_2023-12-18-18-39-57Z.json"
   ```

   Примечание. Описание и допустимые значения параметров `profiles_strategy`, `dictionaries_strategy`, `credentials_strategy` и `importable_file_name` приведены в таблице ниже.

Профили импортированы.

Журналы скрипта хранятся в каталоге `/var/lib/deployed-roles/mp10-application/core/log/unitmigrator/`.

Таблица 14. Параметры запуска скрипта при импорте профилей

Параметр	Описание	Значение по умолчанию
`profiles_strategy`	Действие скрипта при совпадении импортируемого профиля с существующим в системе. Допустимые значения: `CreateNew` — импортировать профиль как копию с уникальным именем; `Update` — заменить существующий профиль импортируемым; `Abort` — не импортировать профиль и сохранить существующий. Необязательный параметр. Если параметр не указан, скрипт использует значение по умолчанию	`CreateNew`
`dictionaries_strategy`	Действие скрипта при совпадении импортируемого справочника с существующим в системе. Допустимые значения: `CreateNew` — импортировать справочник как копию с уникальным именем; `Update` — заменить существующий справочник импортируемым; `Abort` — не импортировать справочник и сохранить существующий. Необязательный параметр. Если параметр не указан, скрипт использует значение по умолчанию	`CreateNew`
`credentials_strategy`	Действие скрипта при совпадении импортируемой учетной записи с существующей в системе. Допустимые значения: `CreateNew` — импортировать учетную запись как копию с уникальным именем; `Abort` — не импортировать учетную запись и сохранить существующую. Необязательный параметр. Если параметр не указан, скрипт использует значение по умолчанию	`Abort`

Параметр	Описание	Значение по умолчанию
`importable_file_name`	Название JSON-файла с импортируемыми профилями. Обязательный параметр	—

37.42.13. Управление системой с помощью утилиты deployer

С ролью Deployer поставляется утилита `deployer`, предназначенная для управления системой. Утилита вызывает сценарии PowerShell, которые разворачиваются в каталог `/opt/deployer/bin` при установке Deployer. Рекомендуется запускать сценарии PowerShell с помощью утилиты `deployer`.

- Чтобы запустить сценарий роли Deployer с помощью утилиты,

  выполните команду:

  ```
  deployer <Код сценария> <Аргумент 1> <Аргумент 2>…
  ```

  Например:

  ```
  deployer instance list
  ```

Вы можете просмотреть справку об аргументах для каждого сценария и их синтаксисе, выполнив команду `deployer <Код сценария> --help`. А также — получить список кодов сценариев и узнать, в каком каталоге находится утилита `deployer`, с помощью команды `deployer --help`.

Таблица 15. Коды сценариев

Код сценария	Сценарий	Назначение
`application deploy`	Deploy-Application.ps1	Установка приложения
`instance configure`	Start-Configuration.ps1	Изменение конфигурации экземпляра роли или создание нового экземпляра роли
`instance list` `instance ls`	Get-RoleInstances.ps1	Получение списка экземпляров роли
`instance reconfigure`	Restart-Configuration.ps1	Изменение конфигурации экземпляров ролей без выбора экземпляра
`minion deploy`	Deploy-Minion.ps1	Установка модуля Salt Minion

Код сценария	Сценарий	Назначение

`package get`
`package list`
`package ls`
	Get-Packages.ps1	Получение списка пакетов роли

`package install`	Install-RolePackage.ps1	Установка пакета роли
`params get`	Get-Params.ps1	Получение параметров экземпляров роли
`instance setparam`	Set-Param.ps1	Установка и сброс параметров экземпляров роли
`instance clearparam`	Clear-Param.ps1	Сброс параметров экземпляров роли до значений по умолчанию
`instance availableparam`	Get-AvaliableParam.ps1	Получение списка доступных параметров экземпляров роли, их описания и типов
`package clean`	Clean-Packages.ps1	Удаление неиспользуемых пакетов для ролей

В командах вы можете указать идентификатор экземпляра роли с помощью аргумента `-id` и тип роли с помощью аргумента `-type`.

Таблица 16. Примеры использования аргументов в командах

Команда	Назначение	Примечание
`deployer instance configure -type <Тип роли>`	Изменение конфигурации экземпляра роли или создание нового экземпляра роли указанного типа	—
`deployer instance reconfigure -type <Тип роли>`	Изменение конфигурации экземпляров ролей указанного типа без выбора экземпляра	—
`deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр>=<Значение>`	Установка значения указанного параметра для указанного идентификатора экземпляра роли	После изменения параметров роли необходимо изменить конфигурацию роли с помощью команды `deployer instance reconfigure -type <Тип роли>`

Команда	Назначение	Примечание
`deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр>=`	Сброс значения указанного параметра для указанного идентификатора экземпляра роли до значения по умолчанию	После символа = значение указывать не нужно. После изменения параметров роли необходимо изменить конфигурацию роли с помощью команды `deployer instance reconfigure -type <Тип роли>`
`deployer instance setparam -Id <Идентификатор экземпляра роли> <Параметр 1>=<Значение> <Параметр 2>=`	Установка значения одного указанного параметра и сброс значения другого указанного параметра до значения по умолчанию для указанного идентификатора экземпляра роли	После выполнения команды необходимо изменить конфигурацию роли с помощью команды `deployer instance reconfigure -type <Тип роли>`
`deployer instance clearparam -Id <Идентификатор экземпляра роли>`	Сброс всех параметров до значений по умолчанию для указанного экземпляра роли	После изменения параметров роли необходимо изменить конфигурацию роли с помощью команды `deployer instance reconfigure -type <Тип роли>`

37.42.14. Настройка мандатного контроля целостности для Astra Linux

Если MaxPatrol SIEM устанавливается на Astra Linux и включен мандатный контроль целостности (МКЦ), для учетной записи, которая используется при установке компонентов системы, необходим максимальный уровень целостности (63). Вы можете проверить, включен ли МКЦ, с помощью команды `astra-mic-control status`. Также вы можете просмотреть уровень МКЦ пользователя с помощью команды `sudo pdpl-user <Имя пользователя>`.

- Чтобы изменить уровень целостности,

  выполните команды:

  ```
  sudo gpasswd -a <Имя пользователя> astra-admin
  sudo pdpl-user <Имя пользователя> -i <Уровень целостности>
  ```

После установки MaxPatrol SIEM рекомендуется установить прежнее значение уровня целостности.

37.42.15. Расположение пользовательских сертификатов

При резервном копировании и восстановлении данных вам могут потребоваться файлы пользовательских сертификатов. Вы можете найти их в списке параметров всех установленных ролей.

- Чтобы отобразить параметры ролей,

  на сервере с установленной ролью Deployer выполните команду:

  ```
  deployer params get
  ```

В полученном списке параметров требуется найти разделы с заголовком `UserDefined` для каждой роли. Файлы с расширениями `.key`, `.pem` или `.crt` в этих разделах — это файлы пользовательских сертификатов.

> **Примечание.** Список параметров роли может не содержать файлов пользовательских сертификатов, если пользовательские сертификаты для нее не создавались.

Сервер, на котором сохранен сертификат, указан в начале каждого списка параметров в строке вида: `<Название роли> (<Название роли> <Версия системы>) on <Название сервера> params`.

Путь к найденным файлам сертификатов указан в подразделе `InstanceDefined` в значении параметра `CertificatesDir` каждой роли, для которой был добавлен сертификат: `CertificatesDir=/var/lib/deployed-roles/<Идентификатор приложения>/<Название экземпляра роли>/certs`.

37.42.16. Реорганизация данных в таблицах СУБД PostgreSQL

При работе с СУБД PostgreSQL данные таблиц БД могут фрагментироваться, что приводит к ухудшению производительности работы системы и нерациональному использованию дискового пространства. Чтобы безопасно реорганизовать фрагментированные данные таблиц, восстановить индексы и вернуть дисковое пространство без влияния на производительность БД, можно использовать утилиту pgcompacttable, которая поставляется с ролью SqlStorage.

Утилита pgcompacttable является альтернативой команды `VACUUM FULL`, но, в отличие от `VACUUM FULL`, не требует большого количества свободного места на диске и не блокирует таблицы на время своей работы. В ходе работы утилиты таблицы обрабатываются с адаптивными задержками для предотвращения перегрузки ввода и вывода данных и задержек репликации.

> **Внимание!** Не запускайте утилиту pgcompacttable и команду `VACUUM FULL` одновременно.

Для работы утилиты pgcompacttable необходимо свободное место, равное размеру самого большого индекса в БД. Перед запуском утилиты для каждой БД, где планируется использовать утилиту, необходимо создать расширение `pgstattuple` с помощью команды `docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}') psql -U pt_system -d <Имя БД PostgreSQL> -c "CREATE EXTENSION IF NOT EXISTS pgstattuple;"`.

Узнать размер БД для сравнения результатов до и после работы утилиты вы можете с помощью команды `docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}') psql -c "SELECT datname AS Database_Name, pg_size_pretty(pg_database_size(datname)) AS Size FROM pg_database ORDER BY pg_database_size(datname) DESC LIMIT 15;" -d postgres -U pt_system`.

Продолжительность работы утилиты зависит от размера БД PostgreSQL, объема фрагментированных данных, а также от аппаратного обеспечения сервера и нагрузки на него, и в некоторых случаях может занимать до нескольких часов. Чтобы работа утилиты не прервалась из-за разрыва соединения, рекомендуется выполнять запуск в одном из терминальных мультиплексоров, например в screen.

- Чтобы запустить утилиту,

  на сервере с установленной ролью SqlStorage выполните команду:

  ```
  docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}')
  pgcompacttable --verbose -U pt_system -d <Имя БД PostgreSQL> >> /var/tmp/
  pgcompacttable.log
  ```

Журнал работы утилиты будет сохранен в файл `/var/tmp/pgcompacttable.log`.

При запуске утилиты вы можете использовать специальные ключи:

— `-a` и `--all`

  Запуск утилиты на всех БД кластера.

— `-t TABLE` и `--table TABLE`

  Запуск утилиты для конкретной таблицы.

— `-T TABLE` и `--exclude-table TABLE`

  Исключение таблицы из обработки.

— `-n SCHEMA` и `--schema SCHEMA`

  Обработка таблиц и индексов в конкретной схеме.

— `- N SCHEMA` и `--exclude-schema SCHEMA`

  Исключение схемы из обработки.

— `-f` и `--force`

  Принудительный запуск обработки.

Примечание. Без использования этого ключа таблицы и индексы с избыточностью данных менее 20% по умолчанию не обрабатываются.

— `--man`

Просмотр списка всех доступных ключей и информации о них.

Пример запуска утилиты на всех БД кластера:

```
docker exec -it $(docker ps | awk '/storage-postgres/ && !/EDR/ {print $NF}')
pgcompacttable --all --verbose -U pt_system >> /var/tmp/pgcompacttable.log
```

37.42.17. Удаление неиспользуемых пакетов ролей

Вы можете удалить неиспользуемые пакеты ролей компонентов MaxPatrol SIEM с помощью утилиты deployer, которая поставляется с ролью Deployer. Запускать утилиту в интерфейсе терминала необходимо с правами суперпользователя (root) на сервере с установленной ролью Deployer.

Примечание. Утилита запускается автоматически после установки или обновления роли, а в низконагруженных системах — после автоматического развертывания конфигурации. Если в хранилище есть неиспользуемые пакеты, вам будет предложено подтвердить их удаление.

Вы можете удалить неиспользуемые пакеты всех ролей сразу или пакеты одной роли.

- Чтобы удалить неиспользуемые пакеты всех ролей:

  1. Выполните команду:
     ```
     deployer package clean
     ```
  2. Выберите пакеты для удаления и нажмите **Confirm**.

- Чтобы удалить неиспользуемые пакеты одной роли:

  1. Выполните команду:
     ```
     deployer package clean -type <Тип роли>
     ```
     Например:
     ```
     deployer package clean -type SqlStorage
     ```
  2. Выберите пакеты для удаления и нажмите **Confirm**.

37.42.18. Добавление исключений в Kaspersky Endpoint Security для БД PostgreSQL

В процессе проверки на вирусы Kaspersky Endpoint Security может ошибочно помещать в карантин нужные файлы БД PostgreSQL. Вы можете исключить такие файлы из проверки. Для этого необходимо определить путь расположения файлов и добавить его в список исключений Kaspersky Endpoint Security.

► Чтобы определить путь расположения файлов,

выполните одно из следующих действий:

- если PostgreSQL установлена в Docker-контейнере, выполните команду:

  ```
  docker inspect -f 'Name: {{println .Name}}{{range .Mounts }}Mount: {{println .Source}}
  {{end}}' $(docker ps -aqf name=postgres)
  ```

  На экране появится имя контейнера и пути расположения файлов и журналов.

  Например:

  ```
  Name: /storage-postgres.mc-application.sqlstorage-1
  Mount: /var/lib/deployed-roles/mc-application/sqlstorage-1/data
  Mount: /var/lib/deployed-roles/mc-application/sqlstorage-1/log
  ```

  Примечание. По умолчанию файлы БД PostgreSQL расположены в каталоге `/data`.

- если PostgreSQL установлена как служба, выполните команду:

  ```
  ps -auxw | grep -Eo "postgres\s+?-D\s+[^\s]+\s"
  ```

  На экране появится путь расположения файлов:

  ```
  postgres -D <Путь расположения файлов>
  ```

  Примечание. Если служба работает под управлением Patroni, по умолчанию файлы расположены в каталоге `/data/patroni`.

После определения пути расположения файлов PostgreSQL его необходимо добавить в списки исключений (подробнее см. на сайте support.kaspersky.ru).

37.42.19. Особенности обновления Astra Linux при использовании хранилища LogSpace

Если MaxPatrol SIEM установлен на Astra Linux и включен мандатный контроль целостности, после обновления операционной системы может возникнуть ошибка (см. раздел 37.30) при создании резервной копии данных хранилища событий LogSpace. Причиной может быть несовпадение классификационных меток каталога, в котором сохраняются файлы с данными, с метками самих файлов.

Чтобы избежать этого, перед обновлением операционной системы необходимо зафиксировать атрибуты контроля целостности для каталога с данными хранилища.

► Чтобы зафиксировать атрибуты контроля целостности:

1. Откройте конфигурационный файл `/etc/parsec/fs-ilev.conf`.
2. Добавьте в файл строку:

   ```
   min /opt/logspaced
   ```

3. Сохраните файл.

37.42.20. Просмотр версии LogSpace

Чтобы узнать, какая версия хранилища данных LogSpace установлена на сервере,

выполните одно из действий:

- Если требуется использовать командную строку, на сервере MP SIEM Events Storage выполните команду:

  ```
  /usr/bin/logspaced --version
  ```

- Если требуется использовать утилиту curl, выполните команду:

  ```
  curl -sS --data "SELECT * FROM system.version FORMAT jsoneachrow" 'http://<FQDN или IP-адрес сервера LogSpace>:8123/'
  ```

- Если требуется использовать клиент LogSpace, выполните команду:

  ```
  logspace-client -q'select * from system.version format pretty'
  ```

38. О технической поддержке

Гарантийная поддержка доступна для всех владельцев действующих лицензий на MaxPatrol SIEM в течение периода предоставления обновлений и включает в себя следующий набор услуг.

Предоставление доступа к обновленным версиям продукта

Обновления продукта выпускаются в порядке и в сроки, определяемые Positive Technologies. Positive Technologies поставляет обновленные версии продукта в течение оплаченного периода получения обновлений, указанного в бланке лицензии приобретенного продукта Positive Technologies.

Positive Technologies не производит установку обновлений продукта в рамках гарантийной поддержки и не несет ответственности за инциденты, возникшие в связи с некорректной или несвоевременной установкой обновлений продукта.

Восстановление работоспособности продукта

Специалист Positive Technologies проводит диагностику заявленного сбоя и предоставляет рекомендации для восстановления работоспособности продукта. Восстановление работоспособности может заключаться в выдаче рекомендаций по установке продукта заново с потенциальной потерей накопленных данных либо в восстановлении версии продукта из доступной резервной копии (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственности за потерю данных в случае неверно настроенного резервного копирования.

> **Примечание.** Помощь оказывается при условии, что конечным пользователем продукта соблюдены все аппаратные, программные и иные требования и ограничения, описанные в документации к продукту.

Устранение ошибок и дефектов в работе продукта в рамках выпуска обновленных версий

Если в результате диагностики обнаружен дефект или ошибка в работе продукта, Positive Technologies обязуется включить исправление в ближайшие возможные обновления продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Рассмотрение предложений по доработке продукта

При обращении с предложением по доработке продукта необходимо подробно описать цель такой доработки. Вы можете поделиться рекомендациями по улучшению продукта и оптимизации его функциональности. Positive Technologies обязуется рассмотреть все предложения, однако не принимает на себя обязательств по реализации каких-либо

доработок. Если Positive Technologies принимает решение о доработке продукта, то способы и сроки ее реализации остаются на усмотрение Positive Technologies. Заявки принимаются на портале технической поддержки.

Портал технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять заявки и читать новости продуктов.

Для получения доступа к порталу технической поддержки нужно создать учетную запись, используя адрес электронной почты в официальном домене вашей организации. Вы можете указать другие адреса электронной почты в качестве дополнительных. Добавьте в профиль название вашей организации и контактный телефон — так нам будет проще с вами связаться.

Поддержка на портале предоставляется на русском и английском языках.

Условия предоставления гарантийной поддержки

Для получения гарантийной поддержки необходимо оставить заявку на портале технической поддержки и предоставить следующие данные:

— номер лицензии на использование продукта;

— файлы журналов и наборы диагностических данных, которые требуются для анализа;

— снимки экрана.

Positive Technologies не берет на себя обязательств по оказанию услуг гарантийной поддержки в случае вашего отказа предоставить запрашиваемую информацию или отказа от внедрения предоставленных рекомендаций.

Если заказчик не предоставляет необходимую информацию по прошествии 20 календарных дней с момента ее запроса, специалист технической поддержки имеет право закрыть заявку. Оказание услуг может быть возобновлено по вашей инициативе при условии предоставления запрошенной ранее информации.

Услуги по гарантийной поддержке продукта не включают в себя услуги по переустановке продукта, решение проблем с операционной системой, инфраструктурой заказчика или сторонним программным обеспечением.

Заявки могут направлять уполномоченные сотрудники заказчика, владеющего продуктом на законном основании (включая наличие действующей лицензии). Специалисты заказчика должны иметь достаточно знаний и навыков для сбора и предоставления диагностической информации, необходимой для решения заявленной проблемы.

Услуги по гарантийной поддержке оказываются в отношении поддерживаемых версий продукта. Информация о поддерживаемых версиях содержится в «Политике поддержки версий программного обеспечения» и (или) иных информационных материалах, размещенных на официальном веб-сайте Positive Technologies.

Время реакции и приоритизация заявок

При получении заявки ей присваивается регистрационный номер, специалист службы технической поддержки классифицирует ее (присваивает тип и уровень значимости) и выполняет дальнейшие шаги по ее обработке.

Время реакции рассчитывается с момента получения заявки до первичного ответа специалиста технической поддержки с уведомлением о взятии заявки в работу. Время реакции зависит от уровня значимости заявки. Специалист службы технической поддержки оставляет за собой право переопределить уровень значимости в соответствии с приведенными ниже критериями. Указанные сроки являются целевыми, но возможны отклонения от них по объективным причинам.

Таблица 17. Время реакции на заявку

Уровень значимости заявки	**Критерии значимости заявки**	**Время реакции на заявку**
Критический	Аварийные сбои, приводящие к невозможности штатной работы продукта (исключая первоначальную установку) либо оказывающие критически значимое влияние на бизнес заказчика	До 4 часов
Высокий	Сбои, проявляющиеся в любых условиях эксплуатации продукта и оказывающие значительное влияние на бизнес заказчика	До 8 часов
Средний	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес заказчика	До 8 часов
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 8 часов

Указанные часы относятся к рабочему времени (рабочие дни с 9:00 до 18:00 UTC+3) специалистов технической поддержки. Под рабочим днем понимается любой день за исключением субботы, воскресенья и дней, являющихся официальными нерабочими днями в Российской Федерации.

Обработка и закрытие заявок

По мере рассмотрения заявки и выполнения необходимых действий специалист службы поддержки сообщает вам:

— о ходе диагностики по заявленной проблеме и ее результатах;

— планах выпуска обновленной версии продукта (если требуется для устранения проблемы).

Если по итогам обработки заявки необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (с учетом релизного цикла продукта, приоритета дефекта или ошибки, сложности требуемых изменений, а также экономической целесообразности исправления). Сроки выпуска обновлений продукта остаются на усмотрение Positive Technologies.

Специалист закрывает заявку, если:

- предоставлены решение или возможность обойти проблему, не влияющие на критически важную функциональность продукта (по усмотрению Positive Technologies);
- диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения, исправление дефекта запланировано к выходу в рамках планового обновления продукта;
- заявленная проблема вызвана программным обеспечением или оборудованием сторонних производителей, на которые не распространяются обязательства Positive Technologies;
- заявленная проблема классифицирована специалистами Positive Technologies как неподдерживаемая.

  Примечание. Если продукт приобретался вместе с аппаратной платформой в виде программно-аппаратного комплекса (ПАК), решение заявок, связанных с ограничением или отсутствием работоспособности аппаратных компонентов, происходит согласно условиям и срокам, указанным в гарантийных обязательствах (гарантийных талонах) на такие аппаратные компоненты.

Приложение А. Привилегии и роли MaxPatrol SIEM

При изменении роли коды добавленных и удаленных привилегий отображаются на странице **Журнал действий пользователя** в приложении Management and Configuration.

Таблица 18. Привилегии и роли MaxPatrol SIEM

Код привилегии	Привилегия	Администратор	Оператор	Наблюдатель
Assets	**Активы**			
Assets	Создание, просмотр, изменение, удаление	+	+	-
AssetsRead	Просмотр	-	-	+
Common	**Общее**			
AccessAdmin	Расширенные полномочия	+	-	-
DataCollect	**Сбор данных**			
EventsMonitoring	Мониторинг источников			
EventsMonitoring	Создание, просмотр, изменение, удаление	+	+	-
EventsMonitoringRead	Просмотр	+	+	+
DataCollectTasks	**Задачи**			
DataCollectTasks	Создание, просмотр, изменение, удаление	+	+	-
DataCollectTasksRead	Просмотр	-	-	+
DataCollectProfiles	**Профили**			
DataCollectProfiles	Создание, просмотр, изменение, удаление	+	+	-
DataCollectProfilesRead	Просмотр	-	-	+
DataCollectIdentity	**Учетные записи**			
DataCollectIdentity	Создание, просмотр, изменение, удаление	+	+	-
DataCollectIdentityRead	Просмотр	-	-	+
DataCollectReferences	**Справочники**			

Код привилегии	Привилегия	Администратор	Оператор	Наблюдатель
DataCollectReferences	Создание, просмотр, изменение, удаление	+	+	-
DataCollectReferencesRead	Просмотр	-	-	+
DataCollectExclusions	**Исключения**			
DataCollectExclusionsViewing	Просмотр	-	-	+
DataCollectExclusionsEditing	Создание, просмотр, изменение, удаление	+	+	-
Infrastructure	**Инфраструктура**	+	-	-
RulesAndTableLists	**Правила и табличные списки**			
SiemCorrelationRules	Правила корреляции			
SiemCorrelationRules	Создание, просмотр, изменение, удаление	+	+	-
SiemCorrelationRulesRead	Просмотр	+	+	+
SiemEnrichmentRules	Правила обогащения			
SiemEnrichmentRules	Создание, просмотр, изменение, удаление	+	+	-
SiemEnrichmentRulesRead	Просмотр	+	+	+
SiemTableLists	Табличные списки			
SiemTableLists	Создание, просмотр, изменение, удаление	+	—	—
SiemTableListsRead	Просмотр	+	+	+
System	**Система**			
AccessRights	Права доступа	+	-	-
Triggers	Уведомления	+	+	-
SystemManagement	Управление системой	+	+	-
ChecksManagement	Управление контролями	+	+	-
Reports	Отчеты	+	+	-
SiemEventTemplates	Шаблоны для карточек событий			
SiemEventTemplates	Создание, просмотр, изменение, удаление	+	-	-
SiemEventTemplatesRead	Просмотр	+	-	+

Код привилегии	Привилегия	Администратор	Оператор	Наблюдатель
AI.Assistant	**AI-помощник**			
AI.Assistant	Использование AI-помощника	+	+	-
Events	**События**			
Events	Создание, просмотр, изменение, удаление	+	+	-
EventsRead	Просмотр	+	-	+
EventsOtherSites	Распределенный поиск событий	+	-	-
Incidents	**Инциденты**			
Incidents	Инциденты	+	+	-
IncidentsAccessToUnlinkedIncidents	Доступ к непривязанным инцидентам	+	-	-
Topology	**Топология**			
TopologyAnalyzer	Расчет достижимости	+	+	-
Topology	Топология	+	+	-

Приложение Б. Параметры конфигурации компонентов MaxPatrol SIEM на Linux

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

Таблица 19. Параметры конфигурации роли Deployer

Параметр	Описание	Значение по умолчанию
`CertificateVendorEmail`	Адрес электронной почты вендора. **Примечание.** Этот параметр может быть изменен только при первой установке продукта	`pt@ptsecurity.com`
`CertificateVendorLocality`	Город, где располагается главный офис вендора. **Примечание.** Этот параметр может быть изменен только при первой установке продукта	`Moscow`
`CertificateVendorName`	Название вендора. **Примечание.** Этот параметр может быть изменен только при первой установке продукта	`Positive Technologies`
`CustomDockerAddressPool`	Подсеть Docker, которую необходимо использовать для Docker-контейнеров вместо подсети по умолчанию. Рекомендуется использовать подсеть с маской /20 или шире в одной из следующих сетей: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	—

Параметр	Описание	Значение по умолчанию
CustomDockerNetworkSize	Размер подсетей, которые будут выделяться из диапазона, указанного в параметре CustomDockerAddressPool. Рекомендуется использовать значение, не превышающее 24 бит. Значение параметра также должно быть больше маски подсети, указанной в значении параметра CustomDockerAddressPool, как минимум на 4 бит	—
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	—
Network	Сетевое имя реестра Docker-образов	registry-network
NetworkDriver	Драйвер Docker-образов	bridge
RegistryPort	Номер порта для доступа к локальному реестру Docker-образов	5000

Таблица 20. Параметры конфигурации роли SqlStorage

Параметр	Описание	Значение по умолчанию
CACertificateFileName	Имя файла корневого сертификата	rootCA.crt
CollectorAgentHttpPort	Порт доступа к коллектору OpenTelemetry для роли SqlStorage по протоколу HTTP	4319
CollectorAgentSyslogUdpPort	Порт для прослушивания журналов syslog по протоколу UDP	54528
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
DockerRegistry	Адрес и порт для доступа к реестру Docker-образов	Адрес и порт сервера MP 10 Core
EnableFilesLogCollection	Запись журналов в файл вместо их централизованного сбора включена (True) или выключена (False)	False

Параметр	Описание	Значение по умолчанию
HostAddress	IP-адрес или FQDN сервера с установленной ролью SqlStorage	—
Network	Сетевое имя реестра Docker-образов	storage-network.sqlstorage
NetworkDriver	Драйвер Docker-образов	bridge
PgAdminPort	Порт для доступа к pgAdmin	9001
PgAnalyzeScaleFactor	Доля от числа кортежей в таблице, которая прибавляется к значению параметра PgAnalyzeThreshold при расчете порога срабатывания команды ANALYZE. Например, если значение PgAnalyzeThreshold равно 200 000, а значение параметра PgAnalyzeScaleFactor равно 0,1, то для таблицы в 1 000 000 кортежей порог срабатывания команды будет 200 000 + 100 000 = 300 000 кортежей	0.0
PgAnalyzeThreshold	Минимальное число добавленных, измененных или удаленных кортежей, при котором будет выполняться команда ANALYZE для отдельно взятой таблицы	200000
PgChecksums	Включение контрольных сумм на страницах данных СУБД PostgreSQL. Возможные значения: auto, on, off. Если выбрано значение auto, контрольные суммы при первичной установке роли SqlStorage включаются, а при обновлении или переустановке роли — остаются без изменений. **Примечание.** При обновлении или изменении конфигурации роли SqlStorage подсчет контрольных сумм может занять длительное время. До завершения процесса база данных не будет запущена и продолжение работы будет невозможно	auto
PgEffectiveCacheSize	Эффективный размер дискового кэша, доступный для одного запроса	6GB

Параметр	Описание	Значение по умолчанию
PgEmail	Электронный адрес служебной учетной записи для доступа к СУБД PostgreSQL	email@email.com
PgHardDiskType	Тип используемого оборудования для хранилища (возможные значения — HDD или SSD)	HDD
PgInitArgs	Параметры инициализации кластера PostgreSQL	--locale='en_US.UTF8'
PgLogLevel	Уровень журналирования работы СУБД PostgreSQL (возможные значения — panic, fatal, log, error, warning, notice, info, debug1, debug2, debug3, debug4 или debug5)	warning
PgMasterPasswordRequired	Запрос мастер-пароля для СУБД PostgreSQL включен (флажок установлен) или выключен (флажок снят)	Флажок снят
PgPassword	Пароль служебной учетной записи для доступа к СУБД PostgreSQL. **Внимание!** Не рекомендуется использовать в паролях служебных учетных записей в PostgreSQL следующие символы: # \ / ' " ; $	P@ssw0rdP@ssw0rd
PgPort	Порт для доступа к СУБД PostgreSQL	5432
PgServerMode	Режим сервера для экземпляра СУБД PostgreSQL	Флажок снят
PgSharedBufferSize	Объем памяти, который будет использовать сервер баз данных для буферов в разделяемой памяти	4GB
PgTimeZone	Часовой пояс для экземпляра СУБД PostgreSQL	Europe/Moscow
PgUpgradeJobs	Количество одновременных процессов или потоков, используемых для pg_upgrade	4

Параметр	Описание	Значение по умолчанию
PgUpgradeVerbose	Детализированное ведение журнала для pg_upgrade включено (флажок установлен) или выключено (флажок снят)	Флажок снят
PgUser	Логин служебной учетной записи для доступа к СУБД PostgreSQL	pt_system
PgVacuumNapTime	Минимальная задержка между двумя запусками автоочистки для отдельной базы данных	20min
PgWorkMem	Объем памяти, который будет использоваться для внутренних операций сортировки и хеш-таблиц, прежде чем будут задействованы временные файлы на диске	200MB
SSLCertificatePemFileName	Имя файла сертификата SSL в формате PEM	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа SSL-сертификата	Portal.key

Таблица 21. Параметры конфигурации роли LogConnector

Параметр	Описание	Значение по умолчанию
DockerBindHost	IP-адрес или FQDN сервера с локальным реестром Docker-образов	0.0.0.0
HostAddress	IP-адрес или FQDN сервера с установленной ролью Deployer	—
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для доступа к серверу СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от PT MC	5432
PostgreUserName	Логин служебной учетной записи для доступа к серверу СУБД PostgreSQL	pt_system

Параметр	Описание	Значение по умолчанию
TelemetryCollectCron	Время начала ежедневного сбора телеметрии. По умолчанию — 04:00 в текущей временной зоне	0 0 4 * * ? *
TelemetryConnectAuthority	FQDN сервера MaxPatrol SIEM с указанием порта	—
TelemetryCronScheduleEnabled	Данные телеметрии отправляются (True) или не отправляются (False) на сервер приема телеметрии	True
TelemetryExportDataPath	Путь к каталогу для экспорта данных телеметрии	/tmp/telemetry/files
TelemetryTrackerDataPath	Путь к каталогу для отправки данных телеметрии	./observability/telemetry/files
TelemetryType	Типы собираемых данных телеметрии	CFG, API, STATE, UAL

Таблица 22. Параметры конфигурации роли Management and Configuration

Параметр	Описание	Значение по умолчанию
ActionLogBatchSize	Количество записей о действиях пользователей, которые служба MC Identity and Access Management Service единовременно отправляет службе MC User Action Logging Service	100
ActionLogMillisecondsDelay	Тайм-аут между попытками отправки записей о действиях пользователей (в миллисекундах)	1000
PackageManagementPort	Номер порта сервиса управления пакетами Package Management	8585
PackagesSourceUri	Адрес сервера обновлений	—
Policy_RecalculationInterval	Тип значения: интервал времени в формате hh:mm:ss.	00:07:30

Параметр	Описание	Значение по умолчанию
	Определяет интервал между пересчетами политик и применением их действия. Влияет на все политики MaxPatrol SIEM. При слишком большом интервале (например, раз в сутки) возможна значительная задержка реакции политик: новая критичная или трендовая уязвимость будет обработана только при следующем пересчете. Слишком маленький интервал может увеличивать нагрузку систему при обработке большого количества активов и уязвимостей. Рекомендации: — Для обработки уязвимостей в соответствии с регламентами используйте значения в диапазоне нескольких минут, например, 15. — Не рекомендуется использовать длительные интервалы, например, сутки. — При необходимости быстрой реакции на критические уязвимости допускается сокращение интервала пересчета. Предварительно нужно оценить объем данных для обработки и текущую производительность экземпляра приложения MaxPatrol SIEM	
`UseProxy`	Использовать ли прокси-сервер для онлайн-активации	`false`

Таблица 23. Параметры конфигурации роли Knowledge Base

Параметр	Описание	Значение по умолчанию
`ClientId`	Идентификатор для регистрации приложения Knowledge Base в PT MC	`ptkb`

Параметр	Описание	Значение по умолчанию
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
MCAddress	IP-адрес или FQDN сервера PT MC	—
OriginNameENG	Полное название поставщика для объектов Knowledge Base на английском языке	Local system
OriginNameRUS	Полное название поставщика для объектов Knowledge Base на русском языке	Локальная система
OriginNickName	Псевдоним поставщика для объектов Knowledge Base	LOC
OriginSystemName	Поставщик объектов Knowledge Base	Local
PostgreHost	IP-адрес или FQDN сервера БД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения Knowledge Base к СУБД PostgreSQL	P@ssw0rdP@ssw0rd

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

Параметр	Описание	Значение по умолчанию
SmtpUser	Логин служебной учетной записи для подключения Knowledge Base к SMTP-серверу	—
StartPage	Стартовая страница при входе в веб-интерфейс Knowledge Base	statistics

Таблица 24. Параметры конфигурации роли Core

Параметр	Описание	Значение по умолчанию
AssetGridValidTimePeriodIndexFormat	Режим оптимизации выполнения PDQL-запросов: IdAndPeriod (по умолчанию) —максимальное повышение производительности; PeriodOnly — среднее повышение производительности	IdAndPeriod
AssetGridVersionRangeModeEnabled	Режим оптимизации выполнения PDQL-запросов включен (флажок установлен) или выключен (флажок снят)	Флажок установлен
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 Feeds	localhost
CybsiEnabled	MP 10 Core получает (флажок установлен) или не получает (флажок снят) данные от PT Feeds	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
`ElasticsearchAggregationSize`	Максимальное количество групп, отображаемое в результате группировки или агрегации событий	`1000`
`EmailNotificationRetryCount`	Максимальное количество попыток отправки сообщения на SMTP-сервер	`10`
`EmailNotificationRetryPeriodSeconds`	Период между попытками отправки сообщения на SMTP-сервер (в секундах)	`60`
`EventsCaseSensitiveSearch`	Тип поиска по схеме полей событий: регистрозависимый (`True`) или регистронезависимый (`False`). **Примечание.** Тип поиска применится только для тех событий, которые поступят после его изменения. Если вы используете хранилище данных Elasticsearch, тип поиска изменится в течение суток после изменения параметра	`False`
`HistoryRotationCronSchedule`	Периодичность запуска ротации с помощью планировщика заданий cron	`0 0 2 1 *`
`HistoryRotationDepth`	Период истории изменения активов, данные за который необходимо удалять, в формате <Дни>.<Часы>:<Минуты>:<Секунды>. Минимально допустимое значение — 14 дней (`14.00:00:00`)	`365.00:00:00`
`HistoryRotationEnabled`	Автоматическая ротация истории изменения активов включена (флажок установлен) или выключена (флажок снят)	Флажок снят
`HostAddress`	IP-адрес или FQDN сервера MP 10 Core	`localhost`
`IncidentAggregationTimeout`	Период, в течение которого срабатывания одного и того же правила корреляции агрегируются в один автоинцидент (<Часы>:<Минуты>:<Секунды>)	`00:01:00`

Параметр	Описание	Значение по умолчанию
IncidentIdenticalNotificationLimit	Максимальное количество срабатываний правила корреляции, которые могут агрегироваться в один инцидент	100
KBAddress	IP-адрес или FQDN сервера Knowledge Base	—
MaxScanSizeKb	Максимальный размер собранных данных по активам в килобайтах	716800
MCAddress	IP-адрес или FQDN сервера PT MC	—
PostgreHost	IP-адрес или FQDN сервера СУБД PostgreSQL	localhost
PostgrePassword	Пароль служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	P@ssw0rdP@ssw0rd
PostgrePort	Порт сервера СУБД PostgreSQL для входящих подключений от MP 10 Core	—
PostgreUserName	Логин служебной учетной записи для подключения MP 10 Core к СУБД PostgreSQL	pt_system
PrintingQueueJobsLimit	Максимальное количество одновременно выпускаемых отчетов	5
ProcessingWorkerCount	Количество потоков обработки событий идентификации активов в сервисе Assets.Processing	2
PtkbDbName	Имя базы знаний, из которой импортируются данные об уязвимостях	—
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
RMQSslCertificateFileName	Имя файла сертификата SSL	RMQ_Core_Client.crt
RMQSslKeyFileName	Имя файла закрытого ключа сертификата SSL	RMQ_Core_Client.key
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для подключения MP 10 Core к RabbitMQ	mpx_core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
ScansRotationBatchDelay	Задержка между началом обработки пакетов в одной процедуре ротации результатов сканирования	00:00:30
ScansRotationBatchSize	Количество результатов сканирования в пакете в процедуре ротации результатов сканирования Допустимые значения — от 1 до 10 000	1000
ScansRotationDepth	Глубина хранения результатов сканирования	90.00:00:00
ScansRotationEnabled	Ротация результатов сканирования включена (True) или выключена (False)	True
ScansRotationRotationDelay	Задержка между процедурами ротации	01:00:00
SendAlertsToSiem	При нарушении и восстановлении контролируемых параметров источников регистрируются соответствующие события (флажок установлен). Если флажок не установлен, события не регистрируются	Флажок не установлен
SmtpHost	IP-адрес или FQDN SMTP-сервера	localhost
SmtpIgnoreCertificateValidation	MP 10 Core проверяет (False) или не проверяет (True) валидность сертификата при подключении к SMTP-серверу	True

Параметр	Описание	Значение по умолчанию
SmtpPassword	Пароль служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—
SmtpPort	Порт SMTP-сервера для входящих подключений от MP 10 Core	25
SmtpSecureSocketOptions	Варианты шифрования при подключении к SMTP-серверу: — None — шифрование не используется; — Auto — почтовый сервер определяет, использовать ли протокол SSL или протокол TLS. Если сервер не поддерживает протоколы SSL и TLS, то шифрование не используется; — SslOnConnect — протоколы SSL или TLS используются при соединении; — StartTls — протокол TLS используется после приветствия сервера. Если сервер не поддерживает расширение STARTTLS, соединение прерывается; — StartTlsWhenAvailable — протокол TLS используется после приветствия сервера, если сервер поддерживает расширение STARTTLS	Auto
SmtpSender	Значение поля «Отправитель» в уведомлении, отправляемом по электронной почте	Notification System <NoReply@SiemNotifications.com>
SmtpUser	Логин служебной учетной записи для подключения MP 10 Core к SMTP-серверу	—

Параметр	Описание	Значение по умолчанию
TableListsWorkersCount	Количество потоков, которые используются для одновременного перерасчета табличных списков	1
Text2PdqlEnabled	Доступен AI-поиск по PDQL-запросам для поиска активов и уязвимостей (флажок установлен)	Флажок не установлен
TtlCheckPeriod	Период проверки (<Дни>.<Часы>:<Минуты>:<Секунды>) состояния актива (устарел актив или нет)	01.00:00:00
UsageMonitoringCheckingPeriod	Период запуска проверок по чек-листу (<Часы>:<Минуты>:<Секунды>)	00:15:00
UserIdleLogoutEnabled	Завершать ли сессию пользователя при его бездействии в системе	False

Таблица 25. 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	—

Параметр	Описание	Значение по умолчанию
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	—
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.	localhost

Параметр	Описание	Значение по умолчанию
	Примечание. Брокер RabbitMQ обеспечивает обмен сообщениями между компонентами MaxPatrol SIEM. Брокер устанавливается на сервер MP 10 Core в конфигурации для низконагруженных систем и на серверы MP 10 Core и MP SIEM Server в конфигурации для средне- и высоконагруженных систем	
`AgentRMQPassword`	Пароль служебной учетной записи для подключения MP 10 Collector к RabbitMQ	`P@ssw0rd`
`AgentRMQPort`	Порт сервера RabbitMQ для входящих подключений от MP 10 Collector	`5671`
`AgentRMQUser`	Логин служебной учетной записи для подключения MP 10 Collector к RabbitMQ	`agent`
`AgentRMQVirtualHost`	Имя виртуального узла RabbitMQ. Выбирается при установке роли из возможных значений: `SIEM` или `Core`	`SIEM`
`Agent_RMQ_SSL_CA_Certificate`	Путь к файлу корневого SSL-сертификата	`RMQ_Server.crt`
`Agent_RMQ_SSL_Certificate`	Путь к файлу публичного SSL-сертификата	`RMQ_Agent_Client.crt`
`Agent_RMQ_SSL_Enabled`	MP 10 Collector подключается к RabbitMQ через защищенное (флажок установлен) или незащищенное (флажок снят) соединение	Флажок установлен
`Agent_RMQ_SSL_Key`	Путь к файлу закрытого ключа SSL-сертификата	`RMQ_Agent_Client.key`

Таблица 26. 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)	`12g`
`ClusterConfigurationProfile`	Объем оперативной памяти, выделяемый каждому типу узлов кластера Elasticsearch. Для выбора доступны следующие варианты: — `AIO` — значения соответствуют требованиям конфигурации MaxPatrol SIEM для низконагруженных систем. В этой конфигурации будет создан один узел данных; — `Standard` — значения соответствуют требованиям конфигурации MaxPatrol SIEM для средненагруженных систем. В этой конфигурации будет создано два узла данных; — `HighLoad` — значения соответствуют требованиям конфигурации MaxPatrol SIEM для высоконагруженных систем. В этой конфигурации будет создано четыре узла данных	`Standard`
`ColdPathData`	Путь к индексам, находящимся в холодной стадии	`/datacold`
`DataNodeHeapSize`	Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах).	`25g`

Параметр	Описание	Значение по умолчанию
	Примечание. Перед изменением параметра необходимо выбрать `Standard` или `HighLoad` в качестве значения параметра `ClusterConfigurationProfile`	
`ElasticSearchGlobalAccess`	Доступ к Elasticsearch с глобальных IP-адресов (флажок установлен) или только с локальных (флажок снят)	Флажок снят
`ElasticNetworkHost`	Режим использования сетевых интерфейсов для Elasticsearch: — `auto` — все IP-адреса, привязанные к сетевому интерфейсу основного маршрута IPv4; — `_site_` — любой локальный IP-адрес в системе; — `_global_` — любой публичный IP-адрес в системе; — `custom` — IP-адрес или имя сетевого интерфейса из значения параметра `ElasticNetworkHostCustom`	`auto`
`ElasticNetworkHostCustom`	IP-адрес или имя сетевого интерфейса Elasticsearch. Недопустимые значения: `0.0.0.0`, `127.0.0.1`	—
`HostAddress`	IP-адрес или FQDN сервера MP SIEM Events Storage	—
`ManagedStorage`	Многоуровневое хранилище включено (флажок установлен) или выключено (флажок снят)	Флажок снят
`MasterNodeHeapSize`	Объем оперативной памяти, выделяемый для главного узла (в гигабайтах)	`12g`
`PathData`	Путь к индексам Elasticsearch. Если включено многоуровневое хранилище — путь к индексам, находящимся в теплой стадии	`/data`

Параметр	Описание	Значение по умолчанию
PathDataHot	Путь к индексам, находящимся в горячей стадии	/datahot
PathLog	Путь к файлам журналов	/es_logs
PathRepo	Путь к резервным копиям индексов	/es_backup
SingleNodeHeapSize	Объем оперативной памяти, выделяемый для одного узла данных (в гигабайтах). Рассчитывается как ⅓ от объема памяти сервера, но не более 30 ГБ. **Примечание.** Перед изменением параметра необходимо выбрать AIO в качестве значения параметра ClusterConfigurationProfile	30g
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 27. 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`
`ColdPathData`	Путь к каталогу для хранения данных в холодной стадии	`/datacold`
`Database`	Название базы данных хранилища LogSpace	`siem`
`HotSpaceRatio`	Минимальный объем свободного дискового пространства, при котором данные из каталога для данных в горячей стадии перемещаются в каталог для данных в холодной стадии, в процентах	`20%`
`ManagedStorage`	Гибридное хранилище включено (флажок установлен) или выключено (флажок снят)	Флажок снят
`PathData`	Корневой каталог хранилища LogSpace	`/opt/logspaced`
`RotateCount`	Максимальное количество сохраняемых файлов журналов	`10`
`RotateSize`	Максимальный размер сохраняемых файлов журналов (`G` для гигабайтов, `M` для мегабайтов, `k` для килобайтов)	`200M`
`TailcutterDbspace`	Максимальный объем дискового пространства, выделяемый для разделов хранилища, в гигабайтах (например, `1000`) или процентах от общего объема жесткого диска (например, `65%`)	`92%`
`TailcutterLogLevel`	Уровень журналирования работы утилиты tailcutter (возможные значения — `CRITICAL`, `ERROR`, `WARNING`, `INFO`, `DEBUG` и `NOTSET`)	`WARNING`

Параметр	Описание	Значение по умолчанию
TailcutterTtl	Срок хранения разделов для событий (в днях)	365
TailcutterTtlc	Срок хранения разделов для счетчиков событий (в днях)	7

Таблица 28. Параметры конфигурации роли SIEM Server

Параметр	Описание	Значение по умолчанию
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	—
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).	ssl

Параметр	Описание	Значение по умолчанию
	Примечание. Этот брокер устанавливается на сервер MP 10 Core и обеспечивает обмен сообщениями между компонентами MaxPatrol SIEM	
`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`
`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`
`ElasticsearchAPIVersion`	Версия API, используемая для взаимодействия с Elasticsearch	`7.4`
`ElasticsearchCompression`	Алгоритм сжатия данных, используемый в Elasticsearch	`default`

Параметр	Описание	Значение по умолчанию
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
EventsCaseSensitiveSearch	Тип поиска по схеме полей событий: регистрозависимый (True) или регистронезависимый (False). **Примечание.** Тип поиска применится только для тех событий, которые поступят после его изменения. Если вы используете хранилище данных Elasticsearch, тип поиска изменится в течение суток после изменения параметра	False
EventsRefreshInterval	Период обновления данных о событиях (в секундах)	60
FrontendHost	IP-адрес компонента ReverseProxy	localhost
GlobalRabbitHost	IP-адрес или FQDN сервера RabbitMQ.	127.0.0.1

Параметр	Описание	Значение по умолчанию
	Примечание. Этот брокер RabbitMQ устанавливается на сервер MP SIEM Server и обеспечивает обмен сообщениями между службами MP SIEM Server	
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
HostAddress	IP-адрес или FQDN MP SIEM Server	—
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
LogSpacePort	Порт сервера MP SIEM Events Storage	8123
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
MonitoringOomMemoryLimit	Объем оперативной памяти, выделенный для работы правил корреляции (в гигабайтах)	60

Параметр	Описание	Значение по умолчанию
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
RMQ_SSL_CERTIFICATE	Путь к файлу публичного SSL-сертификата	/opt/mpxsiem/etc/RMQ_SIEM_Client.crt

Параметр	Описание	Значение по умолчанию
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
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
RowBatchSize	Количество строк табличного списка, экспортируемых службой SIEM Server commander	5000
SiemOnAgent	Установлена облегченная (флажок установлен) или стандарная (флажок снят) версия MP SIEM Server	Флажок снят

Параметр	Описание	Значение по умолчанию
`StatsPublishPeriod`	Период обновления данных, отображаемых в рабочей области главной страницы MaxPatrol SIEM (в секундах)	`30`
`StorageBackendType`	В качестве хранилища 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 29. 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. Выбирается при установке роли из возможных значений: SIEM или Core	SIEM
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

Параметр	Описание	Значение по умолчанию
Agent_RMQ_SSL_Key	Путь к файлу закрытого ключа SSL-сертификата	RMQ_Agent_Client.key
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 30. Параметры конфигурации роли RMQ Message Bus

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

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
RMQLogRotateSize	Максимальный размер сохраняемых файлов журналов (G для гига-байтов, M для мегабайтов, k для килобайтов)	50M
RMQPassword	Пароль служебной учетной записи для доступа MP 10 Core к RabbitMQ	P@ssw0rd
RMQQueueVersion	Версия формата хранения метаданных очередей RabbitMQ	2
RMQSiemPassword	Пароль служебной учетной записи для доступа MP SIEM Server к RabbitMQ	P@ssw0rd
RMQSiemUser	Логин служебной учетной записи для доступа MP SIEM Server к RabbitMQ	siem
RMQSslServerName	IP-адрес или FQDN SSL-сервера RabbitMQ	localhost
RMQUser	Логин служебной учетной записи для доступа MP 10 Core к RabbitMQ	core
RMQVirtualHost	Имя виртуального узла RabbitMQ	mpx
RMQ_DISK_FREE_LIMIT	Пороговое значение для объема свободного места на логическом диске с RabbitMQ (в гигабайтах).	20

Параметр	Описание	Значение по умолчанию
	Примечание. Если объем свободного места становится меньше порогового значения, RabbitMQ останавливает прием входящих сообщений	
SSLCertificatePemFileName	Имя файла публичного сертификата для веб-интерфейса RabbitMQ	Portal.crt
SSLKeyFileName	Имя файла закрытого ключа сертификата для веб-интерфейса RabbitMQ	Portal.key
WATERMARK_PAGING_RATIO	Пороговое значение для объема оперативной памяти, потребляемой RabbitMQ (в доле от значения, указанного в MEMORY_HIGH_WATERMARK). **Примечание.** Если объем оперативной памяти становится больше порогового значения, RabbitMQ начинает сохранять входящие сообщения на диск	0.5

Таблица 31. 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;	Установлены флажки KB SIEM DATA, KB BINARY, KB SDK и CYBSI FEED

Параметр	Описание	Значение по умолчанию
	— `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 Feeds	
`DeleteObsoleteProductVersions`	PT UCS загружает обновления только начиная с определенных версий объектов и удаляет из репозитория более старые версии (флажок установлен) или загружает все версии объектов (флажок снят)	Флажок установлен
`LogLevel`	Уровень журналирования для служб PT UCS	`info`
`ProxyAddress`	IP-адрес или FQDN прокси-сервера	`proxy.server.fqdn.or.ip`
`ProxyEnabled`	PT UCS использует (флажок установлен) или не использует (флажок снят) прокси-сервер для подключения к глобальному серверу обновлений Positive Technologies	Флажок снят
`ProxyPassword`	Пароль служебной учетной записи для подключения PT UCS к прокси-серверу	—
`ProxyPort`	Порт прокси-сервера для входящего подключения от PT UCS	`8080`
`ProxyUser`	Логин служебной учетной записи для подключения PT UCS к прокси-серверу	—
`SaltMasterHost`	IP-адрес или FQDN сервера с модулем Salt Master	—
`SaltMinionLogLevel`	Уровень журналирования для модуля Salt Minion (возможные значения — `fatal`, `error`, `warn`, `info`, `debug` или `trace`)	`info`

Приложение В. Параметры проверок по чек-листу

В разделе приведены описания параметров и их значения по умолчанию.

Инструкция по изменению проверок приведена в разделе «Изменение проверок по чек-листу» (см. раздел 36).

Таблица 32. 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 Г. О проверке серверов перед установкой ролей

При установке и обновлении ролей серверы компонентов автоматически проверяются на наличие факторов, которые могут помешать корректной установке или обновлению MaxPatrol SIEM. Также серверы проверяются на соответствие программным и аппаратным требованиям (подробнее см. в разделе «Программные и аппаратные требования» Руководства по внедрению). Проверка выполняется для всех ролей как на локальных, так и на удаленных серверах. Описание параметров, по которым проводится проверка, а также возможные ошибки приведены в таблице ниже.

В результате проверки появится одно из сообщений:

— `OK` — проверка пройдена успешно;

— `Warning` — рекомендуется устранить несоответствия, но установка может быть продолжена;

— `Error` — проверка не пройдена, установка будет прервана.

Таблица 33. Параметры соответствия сервера программным и аппаратным требованиям

Параметр	Ошибка	Описание ошибки и рекомендации по ее устранению
`check_os_version`	`Error`	Версия ОС не соответствует требуемой. Используйте ОС той версии, которая указана в разделе «Программные и аппаратные требования» Руководства по внедрению
`check_kernel_version`	`Warning`	Версия ядра ОС для Debian и Astra Linux не соответствует требуемой. Рекомендуется использовать версию ядра, указанную в разделе «Программные и аппаратные требования» Руководства по внедрению
`check_os_arch`	`Error`	Архитектура процессора отличается от x86-64. Для корректной установки MaxPatrol 10 необходимо использовать процессор x86-64
`check_apt_sources`	`Error`	Обнаружен некорректный репозиторий системного менеджера пакетов APT.

Параметр	Ошибка	Описание ошибки и рекомендации по ее устранению
		Необходимо удалить некорректный репозиторий или закомментировать содержащую его строку и перезапустить установку. Путь к репозиторию указан в тексте ошибки
`check_disk_space`	`Error` или `Warning`	Недостаточно свободного места на жестком диске (HDD) или твердотельном накопителе (SSD). Меньше 20 ГБ — `Error`, от 20 до 40 ГБ — `Warning`. Необходимо освободить место на диске или накопителе
`check_breaking_packages`	`Error`	Обнаружен пакет, несовместимый с ролью Deployer, например `golang-docker-credential-helpers`. Необходимо удалить пакет из системы. Название пакета указано в тексте ошибки

Приложение Д. Возможности привилегии «Расширенные полномочия»

Раздел содержит описание возможностей привилегии «Расширенные полномочия».

Таблица 34. Возможности привилегии «Расширенные полномочия»

Ресурс или сервис	**Действия**
База уязвимостей	Обновление
Все объекты в системе	Просмотр
Инфраструктура	Создание, изменение, удаление
Инциденты	Удаление
Коллектор	Обновление, удаление
Конвейер	Изменение, удаление
Мониторинг источников	Настройка, включение и отключение предупреждения, удаление источника
Отчеты	Создание, редактирование и удаление шаблонов отчетов (в том числе удаление шаблонов, созданных другими пользователями)
Политики	Создание, изменение, удаление, применение, просмотр правил политик
Правила корреляции	Запуск, остановка (разделы «Правила корреляции», «Табличные списки»)
Правила обогащения	Запуск, остановка (разделы «Правила обогащения», «Табличные списки»)
Табличные списки	Редактирование, очищение, импорт

Предметный указатель

А

архивы LogSpace
- просмотр 126
- удаление 126

В

восстановление данных из копии 103

Д

доступ
- к активам 25
- к инцидентам 25
- к источникам 25
- к событиям 24

И

индексы Elasticsearch
- архивация 114
- восстановление из архива 116
- перемещение 117
- просмотр 114
- резервное копирование 100
- удаление 116, 117

инфраструктуры 182

источники событий
- мониторинг 39
- просмотр 39

К

компоненты системы
- алгоритм взаимодействия 16
- описание 12

корреляция событий 46

М

мониторинг источников
- экспорт 39

О

обогащение событий 46

П

пользовательские поля 171
- добавление 177
- изменение 179
- удаление 180

правило
- обогащения 46

Р

разделы LogSpace
- восстановление из архива 128
- перемещение 126
- просмотр 126
- удаление 126

распределенный поиск
удаление связи 29
резервное копирование 97
репликация событий
добавление правила 30
изменение правила 30
удаление правила 31

Т

табличный список 42

У

уведомления
о состоянии системы 185
учетная запись служебная
смена пароля 137



positive technologies

Positive Technologies — один из лидеров в области результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI). Количество акционеров превышает 220 тысяч.